NSFOCUS Firewall Series

NF Command Reference

NSFOCUS Technologies, Inc.

Document version: 6W600-20230221

About the NSFOCUS firewall series command references

The NSFOCUS firewall series command references describe the commands and command syntax options available for the NSFOCUS firewall series.

Applicable hardware and software versions

To obtain software version information for a device, use the **`display version`** command in any view on the device. The command references use the R8560P28 versions as examples to illustrate feature commands. For information about feature changes in other software versions, see the release notes for your device.

Contents

Table 1 lists features included in each command reference. Support for the features depends on the device model.

Table 1 Command reference content

Command reference	Content
Fundamentals Command Reference	Covers the commands for using the CLI and logging in to and setting up a firewall. This command reference includes: • CLI (command privilege settings and CLI management commands) • RBAC • Login management (including login methods and login user access control) • License management • Device management • FTP and TFTP • File system management • Configuration file management • Software upgrade • ISSU • Automatic configuration • Tcl • Python
Virtual Technologies Command Reference	Covers the commands for configuring virtual technologies features. .This command reference includes: • IRF • Context • Reth interface and redundancy group
Security Command Reference	Covers security feature commands. Available security features include identity authentication (AAA and PKI), access security (portal), secure management (SSH), and attack protection (ARP attack protection, uRPF, and attack detection and prevention). This command reference includes: • Security zone • Security policy • ASPF

Command reference	Content
	• Session management • Object group • IP source guard • AAA • 802.1X • User identification • Password control • Portal • MAC authentication • IPoE • Public key management • PKI • SSH • SSL • Connection limit • Attack detection and prevention • Server connection detection • ARP attack protection • ND attack defense • uRPF • IP-MAC binding • APR • Keychain • Crypto engine • MAC learning through a Layer 3 device • SMS
DPI Command Reference	Covers the commands for configuring deep packet inspection (DPI). This command reference includes: • DPI engine • IPS • URL filtering • Data filtering • File filtering • Anti-virus • Data analysis center • Proxy policy
NAT Command Reference	Covers the commands for configuring NAT features. This command reference includes: • NAT • NAT66 • AFT
VPN Command Reference	Covers the commands of multiple VPN technologies. This command reference includes: • SSL VPN • IPsec, • ADVPN • Tunneling • GRE • L2TP
Internet Access Behavior	Covers the Internet access behavior management commands. This

Command reference	Content
Management Command Reference	command reference includes: • Bandwidth management • Application audit and management • NetShare control
Load Balancing Command Reference	Covers the commands for configuring load balancing.
High Availability Command Reference	Covers high availability commands for managing failure detection and failover.
Interface Command Reference	Covers the interface management commands. This command reference includes: • Bulk interface • Ethernet interface • Loopback, null, and inloopback interfaces
Layer 2—LAN Switching Command Reference	Covers the commands for configuring Layer 2 technologies and features in a LAN switched network. This command reference includes: • MAC address table • Ethernet link aggregation • VLAN • VLAN termination • Spanning tree • LLDP • Layer 2 forwarding
Layer 2—WAN Access Command Reference	Covers the Layer 2 WAN access commands. This command reference includes: • PPP • Mobile communication modem
Layer 3—IP Services Command Reference	Covers the commands for configuring and managing IP addressing (including static and dynamic IPv4 and IPv6 address assignment), network performance optimization, ARP, and interoperation between IPv4 and IPv6. This command reference includes: • IP addressing • IP forwarding basics • Fast forwarding • ARP (including proxy ARP) • IPv6 basics • IPv6 fast forwarding • DHCP • DHCPv6 • DNS • IP performance optimization • Multi-CPU packet distribution • Adjacency table • Web caching
Layer 3—IP Routing Command Reference	Covers the commands for configuring routes for IPv4 and IPv6 networks of different sizes, route filtering, route control, and policy based routing. This command reference includes: • Basic IP routing • Static routing • IPv6 static routing • RIP

Command reference	Content
	• RIPng • OSPF • OSPFv3 • IS-IS • BGP • Policy-based routing • IPv6 policy-based routing • Routing policy • Guard route • RIR
ACL and QoS Command Reference	Covers the commands for classifying traffic with ACLs, and allocating network resources and managing congestions with QoS technologies to improve network performance and network use efficiency. This command reference includes: • ACL • QoS (including QoS policy and traffic policing) • Time range
IP Multicast Command Reference	Covers the commands for Layer 3 multicast protocols. This command reference includes: • Multicast routing and forwarding • IGMP • PIM • IPv6 multicast routing and forwarding • MLD
Network Management and Monitoring Command Reference	Covers the commands that help you manage and monitor your network, for example, manage system events, collect traffic statistics, sample packets, assess network performance, and test network connectivity. This command reference includes: • Information center • Flow log • Fast log output • NetStream • Cloud connection • Mirroring • Packet capture • NQA • Track • BFD • Monitor Link • Smart Link • Interface backup • Interface collaboration • System maintenance and debugging • NTP • EAA • Process monitoring and maintenance • NETCONF • SNMP • RMON • Event MIB • CWMP

Command reference	Content
	• Process placement
VPN Instance Command Reference	Covers the commands for configuring VPN instances.
VXLAN Command Reference	Covers the commands for configuring VXLANs.
Service Chain Command Reference	Covers the commands for configuring *Service Chain*.

NSFOCUS Firewall Series

NF Fundamentals Command Reference

NSFOCUS Technologies, Inc.

Document version: 6W600-20230221

Preface

This command reference describes commands that help you get started with the device. It includes the commands for the following features and tasks:

This preface includes the following topics about the documentation:

- Audience.
- Conventions.

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators.

Conventions

The following information describes the conventions used in the documentation.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select a minimum of one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
CAUTION:	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Contents

Basic CLI commands

alias

Use **alias** to configure a command alias.

Use **undo alias** to delete a command alias.

Syntax

alias *alias command*

undo alias *alias*

Default

The device has a set of system-defined command aliases, as listed in Table 1.

Table 1 System-defined command aliases

Command alias	Command or command keyword
access-list	**acl**
end	**return**
erase	**delete**
exit	**quit**
hostname	**sysname**
logging	**info-center**
no	**undo**
show	**display**
write	**save**

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

alias: Specifies an alias, a case-sensitive string of 1 to 20 characters. An alias cannot be **alias** or contain spaces.

command: Specifies a command string. Make sure the command string meets the syntax requirements.

Usage guidelines

System-defined command aliases cannot be deleted.

You can configure one or more aliases for a command or the starting keywords of commands. Then, you can use the aliases to execute the command or commands. If the command or commands have **undo** forms, you can also use the aliases to execute the **undo** command or commands.

For example, if you configure the alias **shiprt** for **display ip routing-table**, you can enter **shiprt** to execute the **display ip routing-table** command. If you configure the alias **ship** for **display ip**, you can use **ship** to execute all commands that start with **display ip**:

- Enter **ship routing-table** to execute the **display ip routing-table** command.
- Enter **ship interface** to execute the **display ip interface** command.

The command string can include up to nine parameters. Each parameter starts with the dollar sign ($) and a sequence number in the range of 1 to 9. For example, you can configure the alias **shinc** for the **display ip $1 | include $2** command. Then, to execute the **display ip routing-table | include Static** command, you only need to enter **shinc routing-table Static**. To execute the **display ip interface | include GigabitEthernet1/0/1** command, you only need to enter **shinc interface GigabitEthernet1/0/1**.

Examples

Configure **shiprt** as the alias for the **display ip routing-table** command and verify the configuration.

```
<Sysname> system-view
[Sysname] alias shiprt display ip routing-table
[Sysname] shiprt
Destinations : 13        Routes : 13
Destination/Mask   Proto   Pre Cost        NextHop         Interface
0.0.0.0/32         Direct  0   0           127.0.0.1       InLoop0
3.3.3.3/32         Static  60  0           192.168.1.62    GE1/0/1
127.0.0.0/8        Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/32       Direct  0   0           127.0.0.1       InLoop0
127.0.0.1/32       Direct  0   0           127.0.0.1       InLoop0
127.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
169.254.0.0/24     Direct  0   0           169.254.0.188   GE1/0/1
169.254.0.0/32     Direct  0   0           169.254.0.188   GE1/0/1
169.254.0.188/32   Direct  0   0           127.0.0.1       InLoop0
169.254.0.255/32   Direct  0   0           169.254.0.188   GE1/0/1
224.0.0.0/4        Direct  0   0           0.0.0.0         NULL0
224.0.0.0/24       Direct  0   0           0.0.0.0         NULL0
255.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
```

Configure **shinc** as the alias for **display ip $1 | include $2**.

```
[Sysname] alias shinc display ip $1 | include $2
```

Use alias **shinc** to display all static routes.

```
[Sysname] shinc routing-table Static
3.3.3.3/32         Static  60  0           192.168.1.62     GE1/0/1
```

Related commands

display alias

display | { begin | exclude | include }

Use **display |** { **begin** | **exclude** | **include** } to filter the output from a **display** command with a regular expression.

Syntax

display *command* **|** { **begin** | **exclude** | **include** } *regular-expression*

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

command: Specifies the keywords and arguments of a **display** command. To display available keywords and arguments, enter **display ?**.

begin: Displays the first line matching the specified regular expression and all subsequent lines.

exclude: Displays all lines not matching the specified regular expression.

include: Displays all lines matching the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Usage guidelines

Use the **|** { **begin** | **exclude** | **include** } *regular-expression* option with a **display** command to filter the command output. For more information about regular expressions, see *Fundamentals Configuration Guide*.

Examples

Display the lines that contain **vlan** in the running configuration.

```
<Sysname> display current-configuration | include vlan
vlan 1
vlan 999
 port access vlan 999
```

display | by-linenum

Use **display | by-linenum** to number each output line for a **display** command.

Syntax

display *command* **| by-linenum**

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

command: Specifies the keywords and arguments of a **display** command. To display available keywords and arguments, enter **display ?**.

Usage guidelines

By numbering each output line from a **display** command, you can easily identify the lines of interest.

Each line number is displayed as a 5-character string and might be followed by a colon (:) or hyphen (-). If you specify both **| by-linenum** and **| begin** *regular-expression* for a **display** command, a hyphen is displayed for all lines that do not match the regular expression.

Examples

Display VLAN 999 settings, with each output line identified by a number.

```
<Sysname> display vlan 999 | by-linenum
    1:  VLAN ID: 999
    2:  VLAN type: Static
    3:  Route interface: Configured
    4:  IPv4 address: 192.168.2.1
    5:  IPv4 subnet mask: 255.255.255.0
    6:  Description: For LAN Access
    7:  Name: VLAN 0999
    8:  Tagged ports:   None
    9:  Untagged ports:
   10:     GigabitEthernet1/0/1
   11:
```

Display the first line that begins with **user-group** in the running configuration and all of the following lines.

```
<Sysname> display current-configuration | by-linenum begin user-group
  114:  user-group system
  115-  #
  116-  return
```

display >

Use **display >** to save the output from a **display** command to a separate file.

Syntax

display *command* **>** *filename*

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

command: Specifies the keywords and arguments of a **display** command. To display available keywords and arguments, enter **display ?**.

filename: Specifies the name of the file that is used to save the output, a string of 1 to 63 characters.

Usage guidelines

The **display** commands show the configuration, statistics, and states of the device. You can use the **display >** command to save the output to a file.

If the specified file does not exist, the system creates the file and saves the output to the file. If the file already exists, the system overwrites the file.

Examples

Save VLAN 1 settings to a separate file named **vlan.txt**.

```
<Sysname> display vlan 1 > vlan.txt
```

Check the content of the **vlan.txt** file.

```
<Sysname> more vlan.txt
VLAN ID: 1
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0001
 Name: VLAN 0001
 Tagged ports:   None
 Untagged ports:
    GigabitEthernet1/0/2
```

display >>

Use **display >>** to append the output from a **display** command to the end of a file.

Syntax

display *command* **>>** *filename*

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

command: Specifies the keywords and arguments of a **display** command. To display available keywords and arguments, enter **display ?**.

filename: Specifies the name of the file that is used to save the output, a string of 1 to 63 characters.

Usage guidelines

The **display** commands show the configuration, statistics, and states of the device. You can use **display >>** to save the output to a file.

If the specified file does not exist, the system creates the file and saves the output to the file. If the file already exists, the system appends the output to the end of the file.

Examples

Append the VLAN 999 settings to the end of the **vlan.txt** file.

```
<Sysname> display vlan 999 >> vlan.txt
<Sysname>
```

Check the content of the **vlan.txt** file.

```
<Sysname> more vlan.txt
VLAN ID: 1
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0001
 Name: VLAN 0001
 Tagged ports:   None
 Untagged ports:
    GigabitEthernet1/0/2

 VLAN ID: 999
 VLAN type: Static
 Route interface: Configured
 IPv4 address: 192.168.2.1
 IPv4 subnet mask: 255.255.255.0
 Description: For LAN Access
 Name: VLAN 0999
 Tagged ports:   None
 Untagged ports:
    GigabitEthernet1/0/2
```

display alias

Use **display alias** to display command aliases.

Syntax

display alias [*alias*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

alias: Specifies a command alias. If you do not specify this argument, the command displays all command aliases.

Examples

Display all command aliases.

```
<Sysname> display alias
Index     Alias               Command key
1         access-list         acl
2         end                 return
3         erase               delete
4         exit                quit
5         hostname            sysname
6         logging             info-center
7         no                  undo
8         shinc               display $1 | include $2
9         show                display
10        sirt                display ip routing-table
11        write               save
```

Display the command alias **shinc**.

```
<Sysname> display alias shinc
Alias               Command key
shinc               display ip $1 | include $2
```

Related commands

alias

display history-command

Use **display history-command** to display all commands that are saved in the command history buffer for the current CLI session.

Syntax

display history-command

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Usage guidelines

The system automatically saves commands you have successfully executed to the command history buffer for the current CLI session. You can view them and execute them again.

By default, the system can save up to 10 commands in the buffer. You can use the **history-command max-size** command to change the buffer size. To buffer a new command when the buffer is full, the system deletes the oldest command entry in the buffer.

All commands in the command history buffer for the current CLI session will be cleared when you log out.

Examples

Display all commands saved in the command history buffer for the current CLI session.

```
<Sysname> display history-command
  system-view
  vlan 2
  quit
```

Related commands

history-command max-size

display history-command all

Use **display history-command all** to display all commands that are saved in the command history buffer for all CLI sessions.

Syntax

display history-command all

Views

Any view

Predefined user roles

network-admin

context-admin

Usage guidelines

The system automatically saves commands successfully executed by users to the command history buffer for all CLI sessions. Users can view them but cannot recall them from the buffer.

Up to 1024 commands can be saved in the command history buffer. To buffer a new command when the buffer is full, the system deletes the oldest command entry in the buffer.

A user logout does not cause the system to delete commands from the history buffer for all CLI sessions.

Examples

Display all commands saved in the command history buffer for all CLI sessions.

```
<Sysname> display history-command all
  Date       Time     Terminal   Ip              User
  03/16/2017 20:03:33 vty0       192.168.1.26    **
  Cmd:dis his all

  03/16/2017 20:03:29 vty0       192.168.1.26    **
  Cmd:sys
```

Table 2 Command output

Field	Description
Date	Date when the command was executed.
Time	Time when the command was executed.
Terminal	User line used by the user.

Field	Description
Ip	IP address of the terminal used by the user.
User	Username used by the user if the user login authentication mode is **scheme**. If the login authentication mode is **none** or **password**, this field displays ******.
Cmd	Command string entered by the user.

Related commands

`display history-command`

display hotkey

Use **`display hotkey`** to display hotkey information.

Syntax

`display hotkey`

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display hotkey information.

```
<Sysname> display hotkey
----------------- Hotkeys -----------------
           -Defined command hotkeys-
CTRL_G display current-configuration
CTRL_L display ip routing-table
CTRL_O undo debugging all
           -Undefined command hotkeys-
CTRL_T NULL
CTRL_U NULL
           -System-reserved hotkeys-
CTRL_A  Move the cursor to the beginning of the line.
CTRL_B  Move the cursor one character to the left.
CTRL_C  Stop the current command.
CTRL_D  Erase the character at the cursor.
CTRL_E  Move the cursor to the end of the line.
CTRL_F  Move the cursor one character to the right.
CTRL_H  Erase the character to the left of the cursor.
CTRL_K  Abort the connection request.
CTRL_N  Display the next command in the history buffer.
CTRL_P  Display the previous command in the history buffer.
CTRL_R  Redisplay the current line.
```

```
CTRL_V  Paste text from the clipboard.
CTRL_W  Delete the word to the left of the cursor.
CTRL_X  Delete all characters from the beginning of the line to the cursor.
CTRL_Y  Delete all characters from the cursor to the end of the line.
CTRL_Z  Return to the User View.
CTRL_]  Kill incoming connection or redirect connection.
ESC_B   Move the cursor back one word.
ESC_D   Delete all characters from the cursor to the end of the word.
ESC_F   Move the cursor forward one word.
ESC_N   Move the cursor down a line.
ESC_P   Move the cursor up a line.
ESC_<   Move the cursor to the beginning of the clipboard.
ESC_>   Move the cursor to the end of the clipboard.
```

Table 3 Command output

Field	Description
CTRL_]	Terminates the current connection.
ESC_D	Deletes all characters from the cursor to the end of the word.
ESC_N	Moves the cursor down a line.
ESC_P	Moves the cursor up a line.
ESC_<	Moves the cursor to the beginning of the clipboard.
ESC_>	Moves the cursor to the end of the clipboard.

Related commands

hotkey

hotkey

Use **hotkey** to assign a command to a configurable command hotkey.

Use **undo hotkey** to restore the default.

Syntax

hotkey { **ctrl_g** | **ctrl_l** | **ctrl_o** | **ctrl_t** | **ctrl_u** } *command*

undo hotkey { **ctrl_g** | **ctrl_l** | **ctrl_o** | **ctrl_t** | **ctrl_u** }

Default

- **Ctrl+G**: **display current-configuration** (display the running configuration).
- **Ctrl+L**: **display ip routing-table** (display the IPv4 routing table information).
- **Ctrl+O**: **undo debugging all** (disable all debugging functions).
- **Ctrl+T**: No command is assigned to this hotkey.
- **Ctrl+U**: No command is assigned to this hotkey.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ctrl_g: Assigns a command to **Ctrl+G**.

ctrl_l: Assigns a command to **Ctrl+L**.

ctrl_o: Assigns a command to **Ctrl+O**.

ctrl_t: Assigns a command to **Ctrl+T**.

ctrl_u: Assigns a command to **Ctrl+U**.

command: Specifies the command to be assigned to the hotkey.

Usage guidelines

The system defines some hotkeys and provides five configurable command hotkeys. Pressing a command hotkey executes the command assigned to the hotkey.

To display system-defined and configurable hotkeys, use the **display hotkey** command.

Examples

Assign the **display tcp statistics** command to hotkey **Ctrl+T**.

```
<Sysname> system-view
[Sysname] hotkey ctrl_t display tcp statistics
```

Related commands

display hotkey

quit

Use **quit** to return to the upper-level view.

Syntax

quit

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Usage guidelines

Executing this command in user view disconnects you from the device.

Examples

Return from GigabitEthernet 1/0/1 interface view to system view and then to user view.

```
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] quit
<Sysname>
```

repeat

Use **repeat** to repeat commands in the command history buffer for the current CLI session.

Syntax

repeat [*number*] [**count** *times*] [**delay** *seconds*]

Views

Any view

Predefined user roles

network-admin

context-admin

Parameters

number: Specifies the number of the most recently executed commands in the command history buffer for the current CLI session that you want to execute. The value range is 1 to 10. The default is 1.

count *times*: Specifies the number of times that you want to execute the commands. The value range is 0 to 4294967295. The default is 0. If you do not specify this option, the system keeps executing the commands until you press the escape key to terminate the execution.

delay *seconds*: Specifies the time (in seconds) for the system to wait before executing the commands again. The value range is 0 to 4294967295. The default is 1.

Usage guidelines

To repeat a command, first enter the view for the command. To repeat multiple commands, first enter the view for the first command.

The **repeat** command executes commands in the order they were executed.

The system waits for your interaction when it repeats an interactive command.

Examples

Configure the system to execute the two most recently executed commands (**display cpu-usage** and **display clock**) three times at an interval of 10 seconds.

```
<Sysname> repeat 2 count 3 delay 10
<Sysname> display cpu
Unit CPU usage:
      33% in last 5 seconds
      32% in last 1 minute
      33% in last 5 minutes

<Sysname> display clock
07:02:18 UTC Thu 06/19/2017
<Sysname> display cpu-usage
Unit CPU usage:
      33% in last 5 seconds
      32% in last 1 minute
      33% in last 5 minutes

<Sysname> display clock
07:02:28 UTC Thu 06/19/2017
```

```
<Sysname> display cpu-usage
Unit CPU usage:
      33% in last 5 seconds
      32% in last 1 minute
      33% in last 5 minutes

<Sysname> display clock
07:02:38 UTC Thu 06/19/2017
```

Related commands

`display history-command`

`escape-key`

`history-command max-size`

return

Use **`return`** to return to user view from any other view except Tcl configuration view and Python shell view.

Syntax

`return`

Views

Any view except user view, Tcl configuration view, and Python shell view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Usage guidelines

In any view except user view, Tcl configuration view, and Python shell view, pressing **Ctrl+Z** has the same effect as the **`return`** command.

To return to user view from Tcl configuration view, use the **`tclquit`** command.

To return to user view from Python shell view, use the **`exit()`** command.

Examples

Return to user view from GigabitEthernet 1/0/1 interface view.

```
[Sysname-GigabitEthernet1/0/1] return
<Sysname>
```

screen-length disable

Use **`screen-length disable`** to disable pausing between screens of output for the current CLI session.

Use **`undo screen-length disable`** to enable pausing between screens of output for the current CLI session.

Syntax

screen-length disable

undo screen-length disable

Default

The default depends on the configuration of the **screen-length** command in user line view.

The following are the default settings for the **screen-length** command:

- Pausing between screens of output.
- Displaying up to 24 lines on a screen.

Views

User view

Predefined user roles

network-admin

context-admin

Usage guidelines

If you disable pausing between screens of output, all output is displayed. The screen is refreshed continuously until the final screen is displayed.

This command takes effect only for the current CLI session. When you are logged out, the default is restored.

Examples

Disable pausing between screens of output for the current CLI session.

```
<Sysname> screen-length disable
```

Related commands

screen-length

system-view

Use **system-view** to enter system view from user view.

Syntax

system-view

Views

User view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Enter system view from user view.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname]
```

Contents

RBAC commands

description

Use **description** to configure a description for a user role for easy identification.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

A user role does not have a description.

Views

User role view

Predefined user roles

network-admin

context-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 128 characters.

Examples

Configure the description as **labVIP** for user role **role1**.

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] description labVIP
```

Related commands

display role

role

display role

Use **display role** to display user role information.

Syntax

display role [**name** *role-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

name *role-name*: Specifies a user role name, a case-sensitive string of 1 to 63 characters. If you do not specify a user role name, the command displays information about all user roles, including the predefined user roles.

Examples

Display information about user role **123**.

```
<Sysname> display role name 123
Description: 123
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)
```

Display information about all user roles.

```
<Sysname> display role
Role: network-admin
  Description: Predefined network admin role has access to all commands on the device
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  sys-1   permit       command       *
  sys-2   permit RWX   web-menu      -
  sys-3   permit RWX   xml-element   -
  sys-4   deny         command       display security-logfile summary
  sys-5   deny         command       system-view ; info-center securi
                                     ty-logfile directory *
  sys-6   deny         command       security-logfile save
  sys-7   permit RW-   oid           1
  R:Read W:Write X:Execute

Role: network-operator
  Description: Predefined network operator role has access to all read commands on the
device
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  sys-1   permit       command       display *
  sys-2   permit       command       xml
  sys-3   deny         command       display history-command all
  sys-4   deny         command       display exception *
  sys-5   deny         command       display cpu-usage configuration
```

```
                                    *
  sys-6   deny         command       display kernel exception *
  sys-7   deny         command       display kernel deadloop *
  sys-8   deny         command       display kernel starvation *
  sys-9   deny         command       display kernel reboot *
  sys-12  permit       command       system-view ; local-user *
  sys-13  permit       command       system-view ; switchto *
  sys-14  permit R--   web-menu      -
  sys-15  permit RW-   web-menu      m_device/m_maintenance/m_changep
                                    assword
  sys-16  permit R--   xml-element   -
  sys-17  deny         command       display security-logfile summary
  sys-18  deny         command       system-view ; info-center securi
                                    ty-logfile directory *
  sys-19  deny         command       security-logfile save
  sys-20  deny         command       system-view ; local-user-import
                                    *
  sys-21  deny         command       system-view ; local-user-export
                                    *
  sys-22  permit R--   oid           1
  R:Read W:Write X:Execute

Role: context-admin
  Description: Predefined context admin role has access to all commands within a context
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  sys-1   permit       command       *
  sys-2   permit RWX   web-menu      -
  sys-3   permit RWX   xml-element   -
  sys-4   deny   RWX   feature       context
  sys-5   permit       command       display context *
  sys-6   deny         command       display security-logfile summary
  sys-7   deny         command       system-view ; info-center securi
                                    ty-logfile directory *
  sys-8   deny         command       security-logfile save
  sys-9   permit RW-   oid           1
  R:Read W:Write X:Execute

Role: context-operator
  Description: Predefined context operator role has access to all read commands within
a context
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
```

```
  Security zone policy: Permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  sys-1   permit       command       display *
  sys-2   permit       command       xml
  sys-3   deny         command       display history-command all
  sys-4   deny         command       display exception *
  sys-5   deny         command       display cpu-usage configuration
                                     *
  sys-6   deny         command       display kernel exception *
  sys-7   deny         command       display kernel deadloop *
  sys-8   deny         command       display kernel starvation *
  sys-9   deny         command       display kernel reboot *
  sys-12  permit       command       system-view ; local-user *
  sys-13  permit R--   web-menu      -
  sys-14  permit RW-   web-menu      m_device/m_maintenance/m_changep
                                     assword
  sys-15  permit R--   xml-element   -
  sys-16  deny         command       display security-logfile summary
  sys-17  deny         command       system-view ; info-center securi
                                     ty-logfile directory *
  sys-18  deny         command       security-logfile save
  sys-19  permit R--   oid           1
  R:Read W:Write X:Execute

Role: level-0
  Description: Predefined level-0 role
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  sys-1   permit       command       tracert *
  sys-2   permit       command       telnet *
  sys-3   permit       command       ping *
  sys-4   permit       command       ssh2 *
  sys-5   permit       command       super *
  R:Read W:Write X:Execute

Role: level-1
  Description: Predefined level-1 role
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)
```

```
  ------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ------------------------------------------------------------------
  sys-1   permit       command       tracert *
  sys-2   permit       command       telnet *
  sys-3   permit       command       ping *
  sys-4   permit       command       ssh2 *
  sys-5   permit       command       display *
  sys-6   permit       command       super *
  sys-7   deny         command       display history-command all
  R:Read W:Write X:Execute

Role: level-2
  Description: Predefined level-2 role
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)

Role: level-3
  Description: Predefined level-3 role
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)

Role: level-4
  Description: Predefined level-4 role
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)

Role: level-5
  Description: Predefined level-5 role
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)

Role: level-6
  Description: Predefined level-6 role
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)

Role: level-7
```

```
  Description: Predefined level-7 role
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)

Role: level-8
  Description: Predefined level-8 role
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)

Role: level-9
  Description: Predefined level-9 role
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)
  ---------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ---------------------------------------------------------------------
  sys-1   permit RWX   feature       -
  sys-2   deny   RWX   feature       device
  sys-3   deny   RWX   feature       filesystem
  sys-4   permit       command       display *
  sys-5   deny         command       display history-command all
  R:Read W:Write X:Execute

Role: level-10
  Description: Predefined level-10 role
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)

Role: level-11
  Description: Predefined level-11 role
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)

Role: level-12
  Description: Predefined level-12 role
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
```

```
  Security zone policy: Permit (default)

Role: level-13
  Description: Predefined level-13 role
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)

Role: level-14
  Description: Predefined level-14 role
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)

Role: level-15
  Description: Predefined level-15 role
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  sys-1   permit       command       *
  sys-2   permit RWX   web-menu      -
  sys-3   permit RWX   xml-element   -
  sys-4   deny         command       display security-logfile summary
  sys-5   deny         command       system-view ; info-center securi
                                     ty-logfile directory *
  sys-6   deny         command       security-logfile save
  sys-7   permit RW-   oid           1
  R:Read W:Write X:Execute

Role: security-audit
  Description: Predefined security audit role only has access to commands for the security
log administrator
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  sys-1   deny         command       *
  sys-2   permit       command       display security-logfile summary
  sys-3   permit       command       system-view ; info-center securi
                                     ty-logfile directory *
```

```
  sys-4   permit       command       security-logfile save
  sys-5   permit       command       cd *
  sys-6   permit       command       copy *
  sys-7   permit       command       delete *
  sys-8   permit       command       dir *
  sys-9   permit       command       mkdir *
  sys-10  permit       command       more *
  sys-11  permit       command       move *
  sys-12  permit       command       rmdir *
  sys-13  permit       command       pwd
  sys-14  permit       command       rename *
  sys-15  permit       command       undelete *
  sys-16  permit       command       ftp *
  sys-17  permit       command       sftp *
  R:Read W:Write X:Execute

Role: guest-manager
  Description: Predefined guest manager role can't access to commands
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  sys-1   permit RWX   xml-element   useraccounts/approveguest/
  sys-2   permit RWX   xml-element   useraccounts/exportguestaccount/
  sys-3   permit RWX   xml-element   useraccounts/generateguestaccoun
                                     t/
  sys-4   permit RWX   xml-element   useraccounts/guest/
  sys-5   permit RWX   xml-element   useraccounts/guestconfigure/
  sys-6   permit RWX   xml-element   useraccounts/importguestaccount/
  sys-7   permit RWX   xml-element   useraccounts/exportguesttemplet/
  sys-8   permit RWX   xml-element   rpc/
  sys-9   permit RWX   web-menu      m_global/m_networksecurity/m_gue
                                     stmanage/m_guestlist/
  sys-10  permit RWX   web-menu      m_global/m_networksecurity/m_gue
                                     stmanage/m_importguest/
  sys-11  permit RWX   web-menu      m_global/m_networksecurity/m_gue
                                     stmanage/m_generateguest/
  sys-12  permit RWX   web-menu      m_global/m_networksecurity/m_gue
                                     stmanage/m_approveguest/
  sys-13  deny         command       *
  R:Read W:Write X:Execute

Role: system-admin
  Description: Predefined system admin role only has access to commands for the system
administrator
  VLAN policy: Permit (default)
```

```
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)
  ------------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ------------------------------------------------------------------------
sys-1   permit RWX   web-menu      dashboard/
  sys-2   permit RWX   web-menu      m_monitor/m_monitorlog/m_syslog
  sys-3   permit RWX   web-menu      m_network/m_ipservice/m_http
  sys-4   permit RWX   web-menu      m_device/m_virtualdevice/m_clust
                                     er
  sys-5   permit RWX   web-menu      m_device/m_virtualdevice/m_conte
                                     xt/
  sys-6   permit RWX   web-menu      m_device/m_highavailability/m_ho
                                     tbackup
  sys-7   permit RWX   web-menu      m_device/m_highavailability/m_vr
                                     rp
  sys-8   permit RWX   web-menu      m_device/m_highavailability/m_tr
                                     ack
  sys-9   permit RWX   web-menu      m_device/m_highavailability/m_nq
                                     a
  sys-10  permit RWX   web-menu      m_device/m_highavailability/m_bf
                                     d
  sys-11  permit RWX   web-menu      m_device/m_highavailability/m_vr
                                     rpinterface
  sys-12  permit RWX   web-menu      m_device/m_logconf/m_basiclog
  sys-13  permit RWX   web-menu      m_device/m_logconf/m_lblog
  sys-14  permit RWX   web-menu      m_device/m_logconf/m_emailserver
  sys-15  permit RWX   web-menu      m_device/m_reportconf/m_lb_expor
                                     tform
  sys-16  permit RWX   web-menu      m_device/m_logconf/m_emailserver
  sys-17  permit RWX   web-menu      m_device/m_logconf/m_natlog
  sys-18  permit RWX   web-menu      m_device/m_diagnosis/m_ipsecdiag
  sys-19  permit RWX   web-menu      m_device/m_logconf/m_sessionlog
  sys-20  permit RWX   web-menu      m_device/m_logconf/m_atkadvancel
                                     og
  sys-21  permit RWX   web-menu      m_device/m_logconf/m_ipreputatio
                                     nlog
  sys-22  permit RWX   web-menu      m_device/m_logconf/m_bandwidthal
                                     arm
  sys-23  permit RWX   web-menu      m_device/m_logconf/m_threatenlog
  sys-24  permit RWX   web-menu      m_device/m_logconf/m_urlfilterlo
                                     g
  sys-25  permit RWX   web-menu      m_device/m_logconf/m_waflog
  sys-26  permit RWX   web-menu      m_device/m_logconf/m_avclog
  sys-27  permit RWX   web-menu      m_device/m_logconf/m_auditlog
  sys-28  permit RWX   web-menu      m_device/m_logconf/m_netsharelog
  sys-29  permit RWX   web-menu      m_device/m_logconf/m_securitypol
```

```
                                    icylog
sys-30  permit RWX   web-menu       m_device/m_logconf/m_heartbeatlo
                                    g
sys-31  permit RWX   web-menu       m_device/m_logconf/m_aftlog
sys-32  permit RWX   web-menu       m_device/m_logconf/m_terminalala
                                    rmlog
sys-33  permit RWX   web-menu       m_device/m_logconf/m_iplog
sys-34  permit RWX   web-menu       m_device/m_logconf/m_maclog
sys-35  permit RWX   web-menu       m_device/m_logconf/m_sandboxlog
sys-36  permit RWX   web-menu       m_device/m_logconf/m_cfgadvancel
                                    og
sys-37  permit RWX   web-menu       m_device/m_reportconf/m_reportsu
                                    bscription
sys-38  permit RWX   web-menu       m_device/m_reportconf/m_mailserv
                                    erconfig
sys-39  permit RWX   web-menu       m_device/m_sessionagingtimeset/m
                                    _protocolstatesessionagingtime
sys-40  permit RWX   web-menu       m_device/m_sessionagingtimeset/m
                                    _appagingtime
sys-41  permit RWX   web-menu       m_device/m_sessionagingtimeset/m
                                    _sessionsettings
sys-42  permit RWX   web-menu       m_device/m_signatureupgrade/m_up
                                    gradecenter
sys-43  permit RWX   web-menu       m_device/m_signatureupgrade/m_up
                                    grade
sys-44  permit RWX   web-menu       m_device/m_license
sys-45  permit RWX   web-menu       m_device/m_maintenance/m_devices
                                    ettings/
sys-46  permit RWX   web-menu       m_device/m_maintenance/m_macreco
                                    gnition/
sys-47  permit RWX   web-menu       m_device/m_maintenance/m_snmp
sys-48  permit RWX   web-menu       m_device/m_maintenance/m_config
sys-49  permit RWX   web-menu       m_device/m_maintenance/m_reboot
sys-50  permit RWX   web-menu       m_device/m_maintenance/m_about/
sys-51  permit RWX   web-menu       m_device/m_diagnosis/m_pcapware
sys-52  permit RWX   web-menu       m_device/m_diagnosis/m_webdiag
sys-53  permit RWX   web-menu       m_device/m_diagnosis/m_diagnosti
                                    c
sys-54  permit RWX   web-menu       m_device/m_diagnosis/m_troublesh
                                    oot
sys-55  permit RWX   web-menu       m_device/m_diagnosis/m_lbschedul
                                    etest
sys-56  permit RWX   web-menu       m_device/m_configguide/m_interne
                                    tguide
sys-57  permit RWX   web-menu       m_device/m_maintenance/m_changep
                                    assword
sys-58  permit RWX   web-menu       m_device/m_adminuser/m_admin
sys-59  permit RWX   web-menu       m_device/m_adminuser/m_rbacrole
```

```
  sys-60  permit       command       tracert *
  sys-61  permit       command       ping *
  R:Read W:Write X:Execute

Role: security-admin
  Description: Predefined security admin role only has access to commands for the security
administrator
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)
  ---------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ---------------------------------------------------------------------
sys-1   permit RWX   web-menu      m_monitor/m_atklog/m_blacklistlo
                                     g
  sys-2   permit RWX   web-menu      m_monitor/m_atklog/m_terminallog
  sys-3   permit RWX   web-menu      m_monitor/m_videosafe/m_videohot
  sys-4   permit RWX   web-menu      m_monitor/m_atklog/m_singleatk
  sys-5   permit RWX   web-menu      m_monitor/m_atklog/m_scanatk
  sys-6   permit RWX   web-menu      m_monitor/m_atklog/m_floodatk
  sys-7   permit RWX   web-menu      m_monitor/m_atklog/m_threatlog
  sys-8   permit RWX   web-menu      m_monitor/m_atklog/m_reputationl
                                     og
  sys-9   permit RWX   web-menu      m_monitor/m_riskassets
  sys-10  permit RWX   web-menu      m_monitor/m_botnetlog
  sys-11  permit RWX   web-menu      m_monitor/m_atklog/m_urllog
  sys-12  permit RWX   web-menu      m_monitor/m_atklog/m_filefilterl
                                     og
  sys-13  permit RWX   web-menu      m_monitor/m_atklog/m_zonepairlog
  sys-14  permit RWX   web-menu      m_monitor/m_atklog/m_aptlog
  sys-15  permit RWX   web-menu      m_monitor/m_atklog/m_natflowlog
  sys-16  permit RWX   web-menu      m_monitor/m_atklog/m_sslvpnuserl
                                     og
  sys-17  permit RWX   web-menu      m_monitor/m_atklog/m_sslvpnresou
                                     rcelog
  sys-18  permit RWX   web-menu      m_monitor/m_auditlogs/m_auditimc
                                     hatlog
  sys-19  permit RWX   web-menu      m_monitor/m_auditlogs/m_auditcom
                                     munitylog
  sys-20  permit RWX   web-menu      m_monitor/m_auditlogs/m_auditsea
                                     rchenginelog
  sys-21  permit RWX   web-menu      m_monitor/m_auditlogs/m_auditmai
                                     llog
  sys-22  permit RWX   web-menu      m_monitor/m_auditlogs/m_auditfil
                                     etransferlog
  sys-23  permit RWX   web-menu      m_monitor/m_auditlogs/m_auditrel
                                     axstocklog
  sys-24  permit RWX   web-menu      m_monitor/m_auditlogs/m_auditoth
```

```
                                    erapplog
sys-25  permit RWX   web-menu       m_monitor/m_monitorlog/m_traffic
                                    log
sys-26  permit RWX   web-menu       m_monitor/m_online/m_ipv4user
sys-27  permit RWX   web-menu       m_monitor/m_online/m_ipv6user
sys-28  permit RWX   web-menu       m_monitor/m_online/m_macuser
sys-29  permit RWX   web-menu       m_monitor/m_rank/m_trafficrank/
sys-30  permit RWX   web-menu       m_monitor/m_rank/m_threadrank/
sys-31  permit RWX   web-menu       m_monitor/m_rank/m_urlfilterrank
                                    /
sys-32  permit RWX   web-menu       m_monitor/m_rank/m_ffilterrank/
sys-33  permit RWX   web-menu       m_monitor/m_rank/m_secpolicytarg
                                    etrank
sys-34  permit RWX   web-menu       m_monitor/m_rank/m_securityaudit
                                    /
sys-35  permit RWX   web-menu       m_monitor/m_rank/m_lb_serverrepo
                                    rt/
sys-36  permit RWX   web-menu       m_monitor/m_rank/m_lb_linkreport
                                    /
sys-37  permit RWX   web-menu       m_monitor/m_rank/m_lb_dnsproxyre
                                    port/
sys-38  permit RWX   web-menu       m_monitor/m_rank/m_dropstats
sys-39  permit RWX   web-menu       m_monitor/m_trend/m_traffictrend
                                    /
sys-40  permit RWX   web-menu       m_monitor/m_trend/m_threadtrend/
sys-41  permit RWX   web-menu       m_monitor/m_trend/m_urlfiltertre
                                    nd/
sys-42  permit RWX   web-menu       m_monitor/m_trend/m_ffiltertrend
                                    /
sys-43  permit RWX   web-menu       m_monitor/m_trend/m_secpolicytar
                                    gettrend
sys-44  permit RWX   web-menu       m_monitor/m_trend/m_linkloadtren
                                    d/
sys-45  permit RWX   web-menu       m_monitor/m_trend/m_virtualserve
                                    rtrend/
sys-46  permit RWX   web-menu       m_monitor/m_trend/m_serverfarmtr
                                    end/
sys-47  permit RWX   web-menu       m_monitor/m_trend/m_realservertr
                                    end/
sys-48  permit RWX   web-menu       m_monitor/m_trend/m_dnsdomaintre
                                    nd
sys-49  permit RWX   web-menu       m_monitor/m_trend/m_lb_linktrend
                                    /
sys-50  permit RWX   web-menu       m_monitor/m_trend/m_lb_linkpolic
                                    y/
sys-51  permit RWX   web-menu       m_monitor/m_trend/m_lb_vstrend/
sys-52  permit RWX   web-menu       m_monitor/m_trend/m_lb_serfarmtr
                                    end/
```

```
sys-53  permit RWX   web-menu      m_monitor/m_trend/m_lb_realsertr
                                   end/
sys-54  permit RWX   web-menu      m_monitor/m_trend/m_dnsdomaintre
                                   nd
sys-55  permit RWX   web-menu      m_monitor/m_trend/m_lb_urltrend
sys-56  permit RWX   web-menu      m_monitor/m_trend/m_sslvpn_usert
                                   rend
sys-57  permit RWX   web-menu      m_monitor/m_threatanalysis
sys-58  permit RWX   web-menu      m_monitor/m_cdas
sys-59  permit RWX   web-menu      m_monitor/m_report
sys-60  permit RWX   web-menu      m_monitor/m_lb_dnscaches
sys-61  permit RWX   web-menu      m_monitor/m_session
sys-62  permit RWX   web-menu      m_monitor/m_lbsessioninfo
sys-63  permit RWX   web-menu      m_monitor/m_userinfocenter
sys-64  permit RWX   web-menu      m_policy/m_firewall/m_secpolicy
sys-65  permit RWX   web-menu      m_policy/m_firewall/m_targetpoli
                                   cy
sys-66  permit RWX   web-menu      m_policy/m_firewall/m_redundancy
                                   rules
sys-67  permit RWX   web-menu      m_policy/m_firewall/m_appoptimit
                                   ed
sys-68  permit RWX   web-menu      m_policy/m_interfacenat/m_nat66
sys-69  permit RWX   web-menu      m_policy/m_attackdefense/m_atkpo
                                   licy
sys-70  permit RWX   web-menu      m_policy/m_attackdefense/m_riska
                                   nalysis
sys-71  permit RWX   web-menu      m_policy/m_attackdefense/m_clien
                                   tverifyprotectip
sys-72  permit RWX   web-menu      m_policy/m_attackdefense/m_black
                                   listmanual
sys-73  permit RWX   web-menu      m_policy/m_attackdefense/m_white
                                   listmanual
sys-74  permit RWX   web-menu      m_policy/m_attackdefense/m_clien
                                   tverifyzone
sys-75  permit RWX   web-menu      m_policy/m_attackdefense/m_connl
                                   imitpolicies
sys-76  permit RWX   web-menu      m_policy/m_attackdefense/m_iplim
                                   it
sys-77  permit RWX   web-menu      m_monitor/m_rank/m_topn
sys-78  permit RWX   web-menu      m_policy/m_attackdefense/m_urpf/
sys-79  permit RWX   web-menu      m_policy/m_threatintelligence/m_
                                   ipreputation
sys-80  permit RWX   web-menu      m_policy/m_threatintelligence/m_
                                   dnsreputation
sys-81  permit RWX   web-menu      m_policy/m_threatintelligence/m_
                                   urlreputation
sys-82  permit RWX   web-menu      m_policy/m_nat/m_natbasicchange
sys-83  permit RWX   web-menu      m_policy/m_natglobalpolicy
```

```
sys-84  permit RWX   web-menu      m_policy/m_interfacenat/m_nat
sys-85  permit RWX   web-menu      m_policy/m_interfacenat/m_aft
sys-86  permit RWX   web-menu      m_policy/m_interfacenat/m_nat/m_
                                   natoutboundconfig/
sys-87  permit RWX   web-menu      m_policy/m_interfacenat/m_nat/m_
                                   natserverconfig/
sys-88  permit RWX   web-menu      m_policy/m_interfacenat/m_nat/m_
                                   natstaticchange/
sys-89  permit RWX   web-menu      m_policy/m_interfacenat/m_nat/m_
                                   natoutbound444config/
sys-90  permit RWX   web-menu      m_policy/m_interfacenat/m_nat/m_
                                   natoutboundstatic444config/
sys-91  permit RWX   web-menu      m_policy/m_interfacenat/m_nat/m_
                                   natsettings/
sys-92  permit RWX   web-menu      m_policy/m_interfacenat/m_aft/m_
                                   aftaddrgrp
sys-93  permit RWX   web-menu      m_policy/m_interfacenat/m_aft/m_
                                   aftnat64
sys-94  permit RWX   web-menu      m_policy/m_interfacenat/m_aft/m_
                                   aftoutbound
sys-95  permit RWX   web-menu      m_policy/m_interfacenat/m_aft/m_
                                   aftset
sys-96  permit RWX   web-menu      m_policy/m_appaudit/m_auditpolic
                                   y
sys-97  permit RWX   web-menu      m_policy/m_appaudit/m_keywordgro
                                   ups
sys-98  permit RWX   web-menu      m_policy/m_bandwidthmanagement/m
                                   _bandwidthpolicy
sys-99  permit RWX   web-menu      m_policy/m_bandwidthmanagement/m
                                   _bandwidthchannel
sys-100 permit RWX   web-menu      m_policy/m_bandwidthmanagement/m
                                   _interfacebandwidth
sys-101 permit RWX   web-menu      m_policy/m_loadbalance/m_lb_glob
                                   alconfig/
sys-102 permit RWX   web-menu      m_policy/m_loadbalance/m_lb_serv
                                   er/
sys-103 permit RWX   web-menu      m_policy/m_loadbalance/m_lb_link
                                   /
sys-104 permit RWX   web-menu      m_policy/m_scd
sys-105 permit RWX   web-menu      m_policy/m_proxymanagement/m_pro
                                   xypolicy
sys-106 permit RWX   web-menu      m_policy/m_proxymanagement/m_whi
                                   telisthostname
sys-107 permit RWX   web-menu      m_policy/m_proxymanagement/m_ssl
                                   certificate
sys-108 permit RWX   web-menu      m_resource/m_healthmonitor
sys-109 permit RWX   web-menu      m_policy/m_netshare/m_netsharepo
                                   licy
```

```
sys-110 permit RWX   web-menu      m_policy/m_netshare/m_netsharest
                                   atus
sys-111 permit RWX   web-menu      m_resource/m_user/m_usercontrol/
sys-112 permit RWX   web-menu      m_resource/m_user/m_authenticati
                                   on/
sys-113 permit RWX   web-menu      m_resource/m_user/m_access/
sys-114 permit RWX   web-menu      m_resource/m_dpi/m_ipscfg/
sys-115 permit RWX   web-menu      m_resource/m_dpi/m_wafcfg/
sys-116 permit RWX   web-menu      m_resource/m_dpi/m_antiviruscfg/
sys-117 permit RWX   web-menu      m_resource/m_dpi/m_dfltcfg/
sys-118 permit RWX   web-menu      m_resource/m_dpi/m_ufltcfg/
sys-119 permit RWX   web-menu      m_resource/m_dpi/m_ffltcfg/
sys-120 permit RWX   web-menu      m_resource/m_dpi/m_aptcfg/
sys-121 permit RWX   web-menu      m_resource/m_dpi/m_apprecognitio
                                   n/
sys-122 permit RWX   web-menu      m_resource/m_dpi/m_terminal/
sys-123 permit RWX   web-menu      m_resource/m_dpi/m_securityactio
                                   n/
sys-124 permit RWX   web-menu      m_resource/m_dpi/m_dpicfg
sys-125 permit RWX   web-menu      m_resource/m_objectgroup/m_ipv4o
                                   bjectgroup
sys-126 permit RWX   web-menu      m_resource/m_objectgroup/m_ipv6o
                                   bjectgroup
sys-127 permit RWX   web-menu      m_resource/m_objectgroup/m_macob
                                   jectgroup
sys-128 permit RWX   web-menu      m_resource/m_objectgroup/m_natad
                                   drgrp
sys-129 permit RWX   web-menu      m_resource/m_objectgroup/m_aftad
                                   drgrp
sys-130 permit RWX   web-menu      m_resource/m_objectgroup/m_servi
                                   ceobjectgroup
sys-131 permit RWX   web-menu      m_resource/m_objectgroup/m_timer
                                   ange
sys-132 permit RWX   web-menu      m_resource/m_acl/m_ipv4acl
sys-133 permit RWX   web-menu      m_resource/m_acl/m_ipv6acl
sys-134 permit RWX   web-menu      m_resource/m_acl/m_macacl
sys-135 permit RWX   web-menu      m_resource/m_ssl/m_sslserver
sys-136 permit RWX   web-menu      m_resource/m_ssl/m_sslclient
sys-137 permit RWX   web-menu      m_resource/m_ssl/m_ssladvanceset
                                   tiing
sys-138 permit RWX   web-menu      m_resource/m_publickey/m_publick
                                   eylocal
sys-139 permit RWX   web-menu      m_resource/m_publickey/m_publick
                                   eypeer
sys-140 permit RWX   web-menu      m_resource/m_pki_cert/m_pki
sys-141 permit RWX   web-menu      m_resource/m_pki_cert/m_certific
                                   atepolicy
sys-142 permit RWX   web-menu      m_resource/m_pki_cert/m_certific
```

```
                                atesubject
sys-143 permit RWX   web-menu      m_network/m_eps
sys-144 permit RWX   web-menu      m_network/m_vrf
sys-145 permit RWX   web-menu      m_network/m_if/m_interface
sys-146 permit RWX   web-menu      m_network/m_if/m_inlineall
sys-147 permit RWX   web-menu      m_network/m_if/m_collaborations
sys-148 permit RWX   web-menu      m_network/m_if/m_lagg
sys-149 permit RWX   web-menu      m_network/m_seczone
sys-150 permit RWX   web-menu      m_network/m_link/m_vlan
sys-151 permit RWX   web-menu      m_network/m_link/m_mac_sum/
sys-152 permit RWX   web-menu      m_network/m_dns_sum/m_dnshosts
sys-153 permit RWX   web-menu      m_network/m_dns_sum/m_dns
sys-154 permit RWX   web-menu      m_network/m_dns_sum/m_ddns
sys-155 permit RWX   web-menu      m_network/m_dns_sum/m_dnsadvance
sys-156 permit RWX   web-menu      m_network/m_arp
sys-157 permit RWX   web-menu      m_network/m_nd
sys-158 permit RWX   web-menu      m_network/m_alg
sys-159 permit RWX   web-menu      m_network/m_ipfw
sys-160 permit RWX   web-menu      m_network/m_vpn/m_gre
sys-161 permit RWX   web-menu      m_network/m_vpn/m_ipsec/
sys-162 permit RWX   web-menu      m_network/m_vpn/m_advpn/
sys-163 permit RWX   web-menu      m_network/m_vpn/m_l2tp/
sys-164 permit RWX   web-menu      m_network/m_secaccess/m_macauth/
sys-165 permit RWX   web-menu      m_network/m_secaccess/m_ipauth/
sys-166 permit RWX   web-menu      m_network/m_sslvpn/m_sslvpn_cont
                                ext
sys-167 permit RWX   web-menu      m_network/m_sslvpn/m_sslvpn_gate
                                way
sys-168 permit RWX   web-menu      m_network/m_sslvpn/m_sslvpn_ipv4
                                addrpool
sys-169 permit RWX   web-menu      m_network/m_sslvpn/m_sslvpn_acif
sys-170 permit RWX   web-menu      m_network/m_sslvpn/m_sslvpn_glob
                                alconfig
sys-171 permit RWX   web-menu      m_network/m_sslvpn/m_sslvpn_stat
                                istics
sys-172 permit RWX   web-menu      m_network/m_sslvpn/m_sslvpn_temp
                                management
sys-173 permit RWX   web-menu      m_network/m_routing/m_routingtab
                                le
sys-174 permit RWX   web-menu      m_network/m_routing/m_staticrout
                                ing
sys-175 permit RWX   web-menu      m_network/m_routing/m_policyrout
                                ing/
sys-176 permit RWX   web-menu      m_network/m_routing/m_ospf
sys-177 permit RWX   web-menu      m_network/m_routing/m_bgp
sys-178 permit RWX   web-menu      m_network/m_routing/m_rip
sys-179 permit RWX   web-menu      m_network/m_multicast/m_multicas
                                trouting
```

```
  sys-180 permit RWX   web-menu      m_network/m_multicast/m_pim
  sys-181 permit RWX   web-menu      m_network/m_multicast/m_igmp
  sys-182 permit RWX   web-menu      m_network/m_multicast/m_ipv6mult
                                     icastrouting
  sys-183 permit RWX   web-menu      m_network/m_multicast/m_mld
  sys-184 permit RWX   web-menu      m_network/m_dhcp/m_dhcpservice
  sys-185 permit RWX   web-menu      m_network/m_dhcp/m_dhcppool
  sys-186 permit RWX   web-menu      m_network/m_ipservice/m_ssh
  sys-187 permit RWX   web-menu      m_network/m_ipservice/m_ntp
  sys-188 permit RWX   web-menu      m_network/m_ipservice/m_ftp
  sys-189 permit RWX   web-menu      m_network/m_ipservice/m_telnet
  sys-190 permit RWX   web-menu      m_device/m_diagnosis/m_ping
  sys-191 permit RWX   web-menu      m_device/m_diagnosis/m_tracert
  sys-192 permit RWX   web-menu      m_device/m_maintenance/m_changep
                                     assword
  sys-193 permit       command       tracert *
  sys-194 permit       command       ping *
  R:Read W:Write X:Execute

Role: audit-admin
  Description: Predefined audit admin role only has access to commands for the audit
administrator
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)
  ------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ------------------------------------------------------------------
  sys-1   permit RWX   web-menu      m_monitor/m_monitorlog/m_operati
                                     onlog
  sys-2   permit RWX   web-menu      m_device/m_maintenance/m_changep
                                     assword
  sys-3   permit       command       tracert *
  sys-4   permit       command       ping *
  R:Read W:Write X:Execute
```

Table 1 Command output

Field	Description
Role	User role name. Predefined user role names: • network-admin. • network-operator. • context-admin. • context-operator. • level-*n* (where *n* represents an integer in the range of 0 to 15). • security-audit. • guest-manager. • system-admin. • security-admin. • audit-admin.
Description	User role description.
VLAN policy	VLAN policy of the user role: • **Deny**—Denies access to any VLANs except for permitted VLANs. • **Permit (default)**—Default VLAN policy, which enables the user role to access all VLANs.
Permitted VLANs	VLANs accessible to the user role.
Interface policy	Interface policy of the user role: • **Deny**—Denies access to any interfaces except for permitted interfaces. • **Permit (default)**—Default interface policy, which enables the user role to access all interfaces.
Permitted interfaces	Interfaces accessible to the user role.
VPN instance policy	VPN instance policy of the user role: • **Deny**—Denies access to any VPN instances except for permitted VPN instances. • **Permit (default)**—Default VPN instance policy, which enables the user role to access all VPN instances.
Permitted VPN instances	VPN instances accessible to the user role.
Security zone policy	Security zone policy of the user role: • **Deny**—Denies access to any security zones except for permitted security zones. • **Permit (default)**—Default security zone policy, which enables the user role to access all security zones.
Permitted security zones	Security zones accessible to the user role.
Rule	User role rule number. Predefined user role rules are identified by sys-*n*, where *n* represents an integer.
Perm	Access control type: • **Permit**—User role has access to the items in the **Entity** field. • **Deny**—User role does not have access to the items in the **Entity** field.

Field	Description
Type	Controlled type: • **R**—Read-only. • **W**—Write. • **X**—Execute.
Scope	Rule control scope: • **command**—Controls access to the command or commands, as specified in the **Entity** field. • **feature**—Controls access to the commands of the feature, as specified in the **Entity** field. • **feature-group**—Controls access to the commands of the features in the feature group, as specified in the **Entity** field. • **web-menu**—Controls access to Web menus. • **xml-element**—Controls access to XML elements. • **oid**—Controls access to MIB nodes.
Entity	Command string, feature name, feature group, Web menu, XML element, or OID specified in the user role rule: • An en dash (–) represents any feature. • An asterisk (*) represents zero or more characters.

Related commands

role

display role feature

Use **display role feature** to display features available in the system.

Syntax

display role feature [**name** *feature-name* | **verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

name *feature-name*: Specifies a feature by feature name. The *feature-name* argument represents the feature name, and all letters must be in lower case.

verbose: Displays the commands of each feature.

Usage guidelines

If you do not specify any parameters, the command displays only the list of features available in the system.

Examples

Display the list of feature names.

```
<Sysname> display role feature
```

```
Feature: device          (Device configuration related commands)
Feature: interface       (Interface related commands)
Feature: lconn           (Lconn related commands)
Feature: syslog          (Syslog related commands)
...
```

Display the commands of each feature.

```
<Sysname> display role feature verbose
Feature: stress          (Stress related commands)
  process *    (W)
  memory memset *    (W)
  memory policy *    (W)
  memory trace *    (W)
  display memory trace *    (R)
  kernel memory trace *    (W)
  display kernel memory trace *    (R)
  system-view ; probe ; system handshake *    (W)
  system-view ; probe ; lipc *    (W)
  system-view ; probe ; display system internal file *    (R)
  system-view ; probe ; monitor thread-switch *    (W)
  system-view ; probe ; display system internal monitor thread-switch *    (R)
  system-view ; probe ; hook *    (W)
  system-view ; probe ; display system internal hook *    (R)
  system-view ; probe ; debugging transceiver etag-test interface *    (W)
  system-view ; probe ; debugging transceiver flowid *    (W)
  system-view ; probe ; cavium slot *    (W)
  system-view ; probe ; tupdate cpld *    (W)
  system-view ; probe ; set perf *    (W)
  system-view ; probe ; clean hardware internal *    (W)
  system-view ; probe ; switch *    (W)
  system-view ; probe ; testmode-get interface *    (W)
  system-view ; probe ; watchdog slot *    (W)
  system-view ; diagnose *    (W)
  system-view ; diagnose ; twrite *    (W)
  system-view ; diagnose ; twrite interface *    (W)
  system-view ; diagnose ; testmode-set interface *    (W)
  debugging opt-mod info *    (W)
  debugging i2c *    (W)
  debugging sae *    (W)
  display hardware internal debugging sae *    (R)
  display packet-capture *    (R)
Feature: lconn           (Lconn related commands)
  connectto *    (X)
Feature: device          (Device configuration related commands)
  display clock    (R)
  debugging dev    (W)
  display debugging dev    (R)
  display device *    (R)
  display diagnostic-information *    (R)
```

```
  display environment *    (R)
  display fan *    (R)
  display alarm *    (R)
  display power *    (R)
  display current-configuration *    (R)
  display saved-configuration *    (R)
  display default-configuration *    (R)
  display startup    (R)
  display this *    (R)
  display archive configuration    (R)
  display configuration replace server    (R)
  display system stable state *    (R)
  clock datetime *    (W)
  reboot *    (W)
  save *    (W)
  repeat *    (W)
...
```

Display the commands of feature **aaa**.

```
<Sysname> display role feature name aaa
Feature: aaa             (AAA related commands)
  system-view ; domain *    (W)
  system-view ; header *    (W)
  system-view ; aaa *    (W)
  display domain *    (R)
  system-view ; user-group *    (W)
  system-view ; local-user *    (W)
  display local-user *    (R)
  display user-group *    (R)
  display debugging local-server    (R)
  debugging local-server *    (W)
  super *    (X)
  display password-control *    (R)
  reset password-control *    (W)
  system-view ; password-control *    (W)
...
```

Table 2 Command output (display role feature name aaa)

Field	Description
Feature	Displays the name and brief function description of the feature.
system-view ; domain *	All commands that start with the **domain** keyword in system view, and all commands in ISP domain view.
system-view ; header *	All commands that start with the **header** keyword in system view.
system-view ; aaa *	All commands that start with the **aaa** keyword in system view.
display domain *	All commands that start with the **display domain** keywords in user view.
system-view ; user-group *	All commands that start with the **user-group** keyword in system view, and all commands in user group view.

Field	Description
system-view ; local-user *	All commands that start with the **local-user** keyword in system view, and all commands in local user view.
display local-user *	All commands that start with the **display local-user** keywords in user view.
display user-group *	All commands that start with the **display user-group** keywords in user view.
display debugging local-server	All commands that start with the **display debugging local-server** keywords in user view.
debugging local-server *	All commands that start with the **debugging local-server** keywords in user view.
super *	All commands that start with the **super** keyword in user view.
display password-control *	All commands that start with the **display password-control** keywords in user view.
reset password-control *	All commands that start with the **reset password-control** keywords in user view.
system-view ; password-control *	All commands that start with the **password-control** keyword in system view.
(W)	Command type is Write. A write command configures the system.
(R)	Command type is Read. A read command displays configuration or maintenance information.
(X)	Command type is Execute. An execute command executes a specific function.

Related commands

feature

display role feature-group

Use **display role feature-group** to display feature group information.

Syntax

display role feature-group [**name** *feature-group-name*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

name *feature-group-name*: Specifies a feature group. The *feature-group-name* argument represents the feature group name, a case-sensitive string of 1 to 31 characters. If you do not specify a feature group, the command displays information about all feature groups.

verbose: Displays the commands of each feature in feature groups. If you do not specify this keyword, the command displays only the feature lists of feature groups.

Usage guidelines

Feature groups **L2** and **L3** are predefined feature groups.

Examples

Display the feature lists of feature groups.

```
<Sysname> display role feature-group
Feature group: L2
Feature: igmp-snooping   (IGMP-Snooping related commands)
Feature: mld-snooping    (MLD-Snooping related commands)
Feature: lacp            (LACP related commands)
Feature: stp             (STP related commands)
Feature: lldp            (LLDP related commands)
Feature: dldp            (DLDP related commands)
Feature: smart-link      (Smart-link related commands)
Feature: monitor-link    (Monitor-link related commands)
Feature: loopbk-detect   (Loopback-detection related commands)
Feature: vlan            (Virtual LAN related commands)
Feature: evb             (EVB related commands)
Feature: ptp             (PTP related commands)
Feature: ofp             (OFP related commands)
Feature: port-security   (Port-security related commands)

Feature group: L3
Feature: route           (Route management related commands)
Feature: usr             (Unicast static route related commands)
Feature: ospf            (Open Shortest Path First protocol related commands)
Feature: rip             (Routing Information Protocol related commands)
Feature: isis            (ISIS protocol related commands)
Feature: bgp             (Border Gateway Protocol related commands)
Feature: l3vpn           (Layer 3 Virtual Private Network related commands)
Feature: route-policy    (Routing Policy related commands)
Feature: multicast       (Multicast related commands)
Feature: pim             (Protocol Independent Multicast related commands)
Feature: igmp            (Internet Group Management Protocol related commands)
Feature: mld             (Multicast Listener Discovery related commands)
Feature: rir             (RIR related commands)

Feature group: security-features
```

Display the commands in each feature group. For more information about the wildcards and marks used in the command list, see Table 2.

```
<Sysname> display role feature-group verbose
Feature group: L2
Feature: igmp-snooping   (IGMP-Snooping related commands)
  display l2-multicast *    (R)
  system-view ; probe ; display system internal l2-multicast *    (R)
  reset l2-multicast *    (W)
```

```
Feature: mld-snooping    (MLD-Snooping related commands)
  display ipv6 l2-multicast *    (R)
  system-view ; probe ; display system internal ipv6 l2-multicast *    (R)
  reset ipv6 l2-multicast *    (W)
Feature: lacp            (LACP related commands)
  display link-aggregation *    (R)
  display lacp *    (R)
  system-view ; interface Bridge-Aggregation *    (W)
  system-view ; interface Route-Aggregation *    (W)
  system-view ; link-aggregation *    (W)
  system-view ; lacp *    (W)
  system-view ; interface * ; link-aggregation *    (W)
  system-view ; interface * ; port link-aggregation *    (W)
  system-view ; interface * ; lacp *    (W)
  system-view ; probe ; display system internal link-aggregation *    (R)
  system-view ; probe ; debugging system internal link-aggregation *    (W)
  system-view ; probe ; reset system internal link-aggregation *    (W)
  reset lacp *    (W)
  debugging link-aggregation *    (W)
  display debugging link-aggregation *    (R)
  display irf-port load-sharing mode *    (R)
  system-view ; interface * ; mad enable    (W)
  system-view ; irf-port * ; irf-port load-sharing mode *    (W)
Feature: stp             (STP related commands)
  display stp *    (R)
  system-view ; stp *    (W)
  system-view ; interface * ; stp *    (W)
  system-view ; snmp-agent trap enable stp *    (W)
  reset stp *    (W)
  debugging stp *    (W)
  display debugging stp *    (R)
  system-view ; probe ; display system internal stp *    (R)
  system-view ; probe ; debugging system internal stp *    (W)
  system-view ; probe ; debugging system internal stg *    (W)
  system-view ; probe ; reset system internal stp *    (W)
...
```

Display the feature list of the **L3** feature group.

```
<Sysname> display role feature-group name L3
Feature group: L3
Feature: route           (Route management related commands)
Feature: usr             (Unicast static route related commands)
Feature: ospf            (Open Shortest Path First protocol related commands)
Feature: rip             (Routing Information Protocol related commands)
Feature: isis            (ISIS protocol related commands)
Feature: bgp             (Border Gateway Protocol related commands)
Feature: l3vpn           (Layer 3 Virtual Private Network related commands)
Feature: route-policy    (Routing Policy related commands)
Feature: multicast       (Multicast related commands)
```

```
Feature: pim             (Protocol Independent Multicast related commands)
Feature: igmp            (Internet Group Management Protocol related commands)
Feature: mld             (Multicast Listener Discovery related commands)
Feature: rir             (RIR related commands)
```

Related commands

feature

role feature-group

feature

Use **feature** to add a feature to a feature group.

Use **undo feature** to remove a feature from a feature group.

Syntax

feature *feature-name*

undo feature *feature-name*

Default

A user-defined feature group does not have any features.

Views

Feature group view

Predefined user roles

network-admin

context-admin

Parameters

feature-name: Specifies a feature name. You must enter the feature name in lower case.

Usage guidelines

Repeat the **feature** command to add multiple features to a feature group.

Examples

Add the AAA and ACL features to feature group **security-features**.

```
<Sysname> system-view
[Sysname] role feature-group name security-features
[Sysname-featuregrp-security-features] feature aaa
[Sysname-featuregrp-security-features] feature acl
```

Related commands

display role feature

display role feature-group

role feature-group

interface policy deny

Use **interface policy deny** to enter user role interface policy view.

Use **undo interface policy deny** to restore the default.

Syntax

interface policy deny

undo interface policy deny

Default

A user role has access to all interfaces.

Views

User role view

Predefined user roles

network-admin

context-admin

Usage guidelines

CAUTION:

This command denies a user role access to any interfaces if you do not specify accessible interfaces by using the **permit interface** command. To configure an interface, make sure the interface is permitted by the user role interface policy in use.

To limit the scope of interfaces accessible to a user role, perform the following tasks:

1. Use **interface policy deny** to enter user role interface policy view and deny the user role access to any interfaces.
2. Use **permit interface** to specify accessible interfaces.

You can perform the following tasks on an accessible interface:

- Create, remove, or configure the interface.
- Enter interface view.
- Specify the interface in feature commands.

The create and remove operations are available only for logical interfaces.

Any change to a user role interface policy takes effect only on users who log in with the user role after the change.

Examples

Enter user role interface policy view of **role1**, and deny **role1** to access any interfaces.

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] interface policy deny
[Sysname-role-role1-ifpolicy] quit
```

Enter user role interface policy view of **role1**, and permit **role1** to access only interfaces GigabitEthernet 1/0/1 to GigabitEthernet 1/0/2.

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] interface policy deny
[Sysname-role-role1-ifpolicy] permit interface gigabitethernet 1/0/1 to gigabitethernet
1/0/2
```

Related commands

display role

permit interface

role

permit interface

Use **permit interface** to configure a list of interfaces accessible to a user role.

Use **undo permit interface** to disable the access of a user role to specific interfaces.

Syntax

permit interface *interface-list*

undo permit interface [*interface-list*]

Default

No permitted interfaces are configured in user role interface policy view.

Views

User role interface policy view

Predefined user roles

network-admin

context-admin

Parameters

interface-list: Specifies a space-separated list of up to 10 interface items. Each interface item specifies one interface in the *interface-type interface-number* form or a range of interfaces in the *interface-type interface-number* **to** *interface-type interface-number* form. If you specify an interface range, the end interface must meet the following requirements:

- Be the same type as the start interface.
- Have a higher interface number than the start interface.

Usage guidelines

To permit a user role to access an interface after you use the **interface policy deny** command, you must add the interface to the permitted interface list of the policy. With the user role, you can perform the following tasks to the interfaces in the permitted interface list:

- Create, remove, or configure the interfaces.
- Enter the interface views.
- Specify the interfaces in feature commands.

The create and remove operations are available only for logical interfaces.

You can repeat the **permit interface** command to add multiple permitted interfaces to a user role interface policy.

The **undo permit interface** command removes the entire list of permitted interfaces if you do not specify an interface.

Any change to a user role interface policy takes effect only on users who log in with the user role after the change.

Examples

1. Configure user role **role1**:

Permit user role **role1** to execute all commands available in interface view.

```
<Sysname> system-view
[Sysname] role name role1
```

```
[Sysname-role-role1] rule 1 permit command system-view ; interface *
```

Permit the user role to execute all commands available in VLAN view.

```
[Sysname-role-role1] rule 2 permit command system-view ; vlan *
```

Permit the user role to access only GigabitEthernet 1/0/1.

```
[Sysname-role-role1] interface policy deny
[Sysname-role-role1-ifpolicy] permit interface gigabitethernet 1/0/1
[Sysname-role-role1-ifpolicy] quit
[Sysname-role-role1] quit
```

2. Verify that you cannot use user role **role1** to work on any interfaces except for GigabitEthernet 1/0/1:

Verify that you can enter GigabitEthernet 1/0/1 interface view.

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] quit
```

Verify that you can assign GigabitEthernet 1/0/1 to VLAN 10. In this example, the user role can access all VLANs because the default VLAN policy of the user role is used.

```
[Sysname] vlan 10
[Sysname-vlan10] port gigabitethernet 1/0/1
[Sysname-vlan10] quit
```

Verify that you cannot enter interface view of GigabitEthernet 1/0/2.

```
[Sysname] interface gigabitethernet 1/0/2
Permission denied.
```

Related commands

display role

interface policy deny

role

permit security-zone

Use **permit security-zone** to configure a list of security zones accessible to a user role.

Use **undo permit security-zone** to remove the permission for a user role to access specific security zones.

Syntax

permit security-zone *security-zone-name*&<1-10>

undo permit security-zone [*security-zone-name*&<1-10>]

Default

No permitted security zones are configured in user role security zone policy view.

Views

User role security zone policy view

Predefined user roles

network-admin

context-admin

Parameters

security-zone-name&<1-10>: Specifies a space-separated list of up to 10 security zone names. Each name is a case-sensitive string of 1 to 31 characters.

Usage guidelines

To permit a user role to access a security zone after you use the **security-zone policy deny** command, you must add the security zone to the permitted security zone list of the policy. With the user role, you can perform the following tasks on the security zones in the permitted security zone list:

- Create, remove, or configure the security zones.
- Enter the security zone views.
- Specify the security zones in feature commands.

You can repeat the **permit security-zone** command to add multiple permitted security zones to a user role security zone policy.

The **undo permit security-zone** command removes the entire list of permitted security zones if you do not specify a security zone.

Any change to a user role security zone policy takes effect only on users who log in with the user role after the change.

Examples

1. Configure user role **role1**:

Permit user role **role1** to execute all commands available in system view.

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] rule 1 permit command system-view ; *
```

Permit the user role to access security zones **trust** and **abc**.

```
[Sysname-role-role1] security-zone policy deny
[Sysname-role-role1-zonepolicy] permit security-zone trust abc
[Sysname-role-role1-zonepolicy] quit
[Sysname-role-role1] quit
```

2. Verify that you cannot use user role **role1** to work on any security zones except for security zones **trust** and **abc**:

Verify that you can create security zone **abc** and enter security zone view.

```
[Sysname] security-zone name abc
[Sysname-security-zone-abc] quit
```

Verify that you can create a zone pair with source security zone **trust** and destination zone **abc**.

```
[Sysname] zone-pair security source trust destination abc
[Sysname-zone-pair-security-Trust-abc] quit
```

Verify that you cannot create security zone **local** or enter security zone view.

```
[Sysname] security-zone name local
Permission denied.
```

Related commands

display role

role

security-zone policy deny

permit vlan

Use **permit vlan** to configure a list of VLANs accessible to a user role.

Use **undo permit vlan** to remove the permission for a user role to access specific VLANs.

Syntax

permit vlan *vlan-id-list*

undo permit vlan [*vlan-id-list*]

Default

No permitted VLANs are configured in user role VLAN policy view.

Views

User role VLAN policy view

Predefined user roles

network-admin

context-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 10 VLAN items. Each VLAN item specifies a VLAN by VLAN ID or specifies a range of VLANs in the form of *vlan-id1* **to** *vlan-id2*. The value range for the VLAN IDs is 1 to 4094. If you specify a VLAN range, the value for the *vlan-id2* argument must be greater than the value for the *vlan-id1* argument.

Usage guidelines

To permit a user role to access a VLAN after you use the **vlan policy deny** command, you must add the VLAN to the permitted VLAN list of the policy. With the user role, you can perform the following tasks on the VLANs in the permitted VLAN list:

- Create, remove, or configure the VLANs.
- Enter the VLAN views.
- Specify the VLANs in feature commands.

You can repeat the **permit vlan** command to add multiple permitted VLANs to a user role VLAN policy.

The **undo permit vlan** command removes the entire list of permitted VLANs if you do not specify a VLAN.

Any change to a user role VLAN policy takes effect only on users who log in with the user role after the change.

By default, all access ports belong to VLAN 1. To assign an access port to any other VLAN by using the **port access vlan** command, make sure you have a user role that can access both VLAN 1 and the new VLAN.

Examples

1. Configure user role **role1**:

Permit user role **role1** to execute all commands available in interface view and VLAN view.

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] rule 1 permit command system-view ; interface *
[Sysname-role-role1] rule 2 permit command system-view ; vlan *
```

Permit user role **role1** to access VLANs 1, 2, 4, and 50 to 100.

```
[Sysname-role-role1] vlan policy deny
[Sysname-role-role1-vlanpolicy] permit vlan 1 2 4 50 to 100
[Sysname-role-role1-vlanpolicy] quit
[Sysname-role-role1] quit
```

2. Verify that you cannot use user role **role1** to work on any VLANs except for VLANs 1, 2, 4, and 50 to 100:

   # Verify that you can create VLAN 100 and enter VLAN view.

   ```
   [Sysname] vlan 100
   [Sysname-vlan100] quit
   ```

   # Verify that you can add GigabitEthernet 1/0/1 to VLAN 100 as an access port.

   ```
   [Sysname] interface gigabitethernet 1/0/1
   [Sysname-GigabitEthernet1/0/1] port access vlan 100
   [Sysname-GigabitEthernet1/0/1] quit
   ```

   # Verify that you cannot create VLAN 101 or enter VLAN view.

   ```
   [Sysname] vlan 101
   Permission denied.
   ```

Related commands

display role

role

vlan policy deny

permit vpn-instance

Use **permit vpn-instance** to configure a list of MPLS L3VPN instances accessible to a user role.

Use **undo permit vpn-instance** to disable the access of a user role to specific MPLS L3VPN instances.

Syntax

permit vpn-instance *vpn-instance-name*&<1-10>

undo permit vpn-instance [*vpn-instance-name*&<1-10>]

Default

No permitted VPN instances are configured in user role VPN instance policy.

Views

User role VPN instance policy view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance-name&<1-10>: Specifies a space-separated list of up to 10 MPLS L3VPN instance names. Each name is a case-sensitive string of 1 to 31 characters.

Usage guidelines

To permit a user role to access a VPN instance after you use the **vpn-instance policy deny** command, you must add the VPN instance to the permitted VPN instance list of the policy. With the user role, you can perform the following tasks on the VPN instances in the permitted VPN instance list:

- Create, remove, or configure the VPN instances.
- Enter the VPN instance views.

- Specify the VPN instances in feature commands.

You can repeat the **permit vpn-instance** command to add multiple permitted VPN instances to a user role VPN instance policy.

The **undo permit vpn-instance** command removes the entire list of permitted VPN instances if you do not specify a VPN instance.

Any change to a user role VPN instance policy takes effect only on users who log in with the user role after the change.

Examples

1. Configure user role **role1**:

Permit the user role to execute all commands available in system view and in the child views of system view.

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] rule 1 permit command system-view ; *
```

Permit the user role to access VPN instance **vpn1**.

```
[Sysname-role-role1] vpn policy deny
[Sysname-role-role1-vpnpolicy] permit vpn-instance vpn1
[Sysname-role-role1-vpnpolicy] quit
[Sysname-role-role1] quit
```

2. Verify that you cannot use user role **role1** to work on any VPN instances except for **vpn1**:

Verify that you can enter the view of **vpn1**.

```
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] quit
```

Verify that you can specify the primary accounting server at 10.110.1.2 in VPN instance **vpn1** for RADIUS scheme **radius1**.

```
[Sysname] radius scheme radius1
[Sysname-radius-radius1] primary accounting 10.110.1.2 vpn-instance vpn1
[Sysname-radius-radius1] quit
```

Verify that you cannot create VPN instance **vpn2** or enter VPN instance view.

```
[Sysname] ip vpn-instance vpn2
Permission denied.
```

Related commands

display role

role

vpn-instance policy deny

role

Use **role** to create a user role and enter its view, or enter the view of an existing user role.

Use **undo role** to delete a user role.

Syntax

role name *role-name*

undo role name *role-name*

Default

The system has the following predefined user roles: network-admin, network-operator, context-admin, context-operator, level-*n* (where *n* represents an integer in the range of 0 to 15), guest-manager, security-audit, system-admin, security-admin, and audit-admin.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

name *role-name*: Specifies a username. The *role-name* argument is a case-sensitive string of 1 to 63 characters.

Usage guidelines

You can create a maximum of 64 user roles in addition to the predefined user roles.

You cannot delete the predefined user roles or change the permissions assigned to network-admin, network-operator, context-admin, context-operator, level-15, guest-manager, security-audit, system-admin, security-admin, or audit-admin.

The access permissions of the level-0 to level-14 user roles can be modified through user role rules and resource access policies. However, you cannot make changes on the predefined access permissions of these user roles. For example, you cannot change the access permission of these user roles to the **display history-command all** command.

Examples

Create user role **role1** and enter its view.

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1]
```

Related commands

display role

interface policy deny

rule

vlan policy deny

vpn-instance policy deny

role default-role enable

Use **role default-role enable** to enable the default user role feature for remote AAA users.

Use **undo role default-role enable** to restore the default.

Syntax

role default-role enable [*role-name*]

undo role default-role enable

Default

The default user role feature is disabled. AAA users who do not have a user role cannot log in to the device.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

role-name: Specifies a user role by its name for the default user role. The user role must already exist. The argument is a case-sensitive string of 1 to 63 characters.

Usage guidelines

The default user role feature assigns the default user role to AAA-authenticated users if the authentication server (local or remote) does not assign any user roles to the users. These users are allowed to access the system with the default user role.

For local authorization, this command is required if you do not use the **authorization-attribute user role** command to assign user roles to local users.

If AAA users have been assigned user roles, they log in with the user roles.

If you do not specify the *role-name* argument, the following default user role settings apply:

- For login to the default context, the default user role is network-operator.
- For login to a non-default context, the default user role is context-operator.

Examples

Enable the default user role feature.

```
<Sysname> system-view
[Sysname] role default-role enable
```

Related commands

role

role feature-group

Use **role feature-group** to create a user role feature group and enter its view, or enter the view of an existing user role feature group.

Use **undo role feature-group** to delete a user role feature group.

Syntax

role feature-group name *feature-group-name*

undo role feature-group name *feature-group-name*

Default

Two user role feature groups **L2** and **L3** exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

name *feature-group-name*: Specifies a feature group name. The *feature-group-name* argument is a case-sensitive string of 1 to 31 characters.

Usage guidelines

The **L2** feature group includes all Layer 2 feature commands, and the **L3** feature group includes all Layer 3 feature commands. These predefined feature groups are not user configurable.

In addition to the predefined feature groups **L2** and **L3**, you can create a maximum of 64 user role feature groups.

Examples

Create feature group **security-features** and enter its view.

```
<Sysname> system-view
[Sysname] role feature-group name security-features
[Sysname-featuregrp-security-features]
```

Related commands

display role feature

display role feature-group

feature

rule

Use **rule** to create or change a user role rule.

Use **undo rule** to delete user role rules.

Syntax

rule *number* { **deny** | **permit** } { **command** *command-string* | { **execute** | **read** | **write** } * { **feature** [*feature-name*] | **feature-group** *feature-group-name* | **oid** *oid-string* | **web-menu** [*web-string*] | **xml-element** [*xml-string*] } }

undo rule { *number* | **all** }

Default

A user-defined user role does not have any rules and cannot access any resources.

Views

User role view

Predefined user roles

network-admin

context-admin

Parameters

number: Specifies a rule number in the range of 1 to 256.

deny: Denies access to the specified commands, Web menus, XML elements, or MIB nodes.

permit: Permits access to the specified commands, Web menus, XML elements, or MIB nodes.

command *command-string*: Specifies a command string. The command string can represent a command or a group of commands. The *command-string* argument is a case-sensitive string of 1 to 128 characters, including the wildcard asterisk (*), the delimiters space and tab, and all printable characters. If the command string includes a left bracket ([) or right bracket (]), you must add a back

slash (\) as the escape character before the left or right bracket. For example, to specify the **statistics[ifindex="*"]** command, you must enter **statistics\[ifindex="*"\]** for the *command-string* argument.

execute: Specifies the execute commands, Web menus, XML elements, or MIB nodes to execute a specific function or program. The **ping** command is an example of execute commands.

read: Specifies the read commands, Web menus, XML elements, or MIB nodes to display configuration or maintenance information. The **display**, **dir**, **more**, and **pwd** commands are examples of read commands.

write: Specifies the write commands, Web menus, XML elements, or MIB nodes to configure the system. The **ssh server enable** command is an example of write commands.

feature [*feature-name*]: Specifies one or all features. The *feature-name* argument is a case-sensitive character string. If you do not specify a feature name, you specify all the features in the system.

feature-group *feature-group-name*: Specifies a user-defined or predefined feature group. The *feature-group-name* argument represents the feature group name, a case-sensitive string of 1 to 31 characters. If the feature group has not been created, the rule takes effect after the group is created. To display the feature groups that have been created, use the **display role feature-group** command.

oid *oid-string*: Specifies an OID of a MIB node. The *oid-string* argument represents the OID, a case-insensitive string of 1 to 255 characters. The OID is a dotted numeric string that uniquely identifies the path from the root node to this node. For example, 1.3.6.1.4.1.25506.8.35.14.19.1.1.

web-menu [*web-string*]: Specifies a Web menu. The *web-string* argument represents the ID path of the Web menu, a case-insensitive string of 1 to 255 characters. Use the forward slash (/) to separate ID items, for example, M_DEVICE/I_BASIC_INFO/I_reboot. If you do not specify a Web menu, the rule applies to all Web items. To verify the ID path of a Web menu, use the **display web menu** command.

xml-element [*xml-string*]: Specifies an XML element. The *xml-string* argument represents the XPath of the XML element, a case-insensitive string of 1 to 255 characters. Use the forward slash (/) to separate Xpath items, for example, Interfaces/Index/Name. If you do not specify an XML element, the rule applies to all XML elements.

all: Specifies all the user role rules.

Usage guidelines

You can define the following types of rules for different access control granularities:

- **Command rule**—Controls access to a command or a set of commands that match a regular expression.
- **Feature rule**—Controls access to the commands of a feature by command type.
- **Feature group rule**—Controls access to the commands of a group of features by command type.
- **Web menu rule**—Controls access to Web menus by menu type.
- **XML element rule**—Controls access to XML elements by element type.
- **OID rule**—Controls access to the specified MIB node and its child nodes by node type.

A user role can access the set of permitted resources specified in the user role rules. User role rules include predefined (identified by sys-n) and user-defined user role rules.

You can configure a maximum of 256 user-defined rules for a user role. The total number of user-defined user role rules cannot exceed 1024.

Any rule modification, addition, or removal for a user role takes effect only on the users who log in with the user role after the change.

Access to the file system commands is controlled by both the file system command rules and the file system feature rule.

A command with output redirection to the file system is permitted only when the command type write is assigned to the file system feature.

The following guidelines apply to non-OID rules:

- If two user-defined rules of the same type conflict, the rule with the higher ID takes effect. For example, a user role can use the **tracert** command but not the **ping** command if the user role contains rules configured by using the following commands:
  - **rule** *1* **permit command** *ping*
  - **rule** *2* **permit command** *tracert*
  - **rule** *3* **deny command** *ping*
- If a predefined user role rule and a user-defined user role rule conflict, the user-defined user role rule takes effect.

The following guidelines apply to OID rules:

- The system compares an OID with the OIDs specified in rules, and it uses the longest match principle to select a rule for the OID. For example, a user role cannot access the MIB node with OID 1.3.6.1.4.1.25506.141.3.0.1 if the user role contains rules configured by using the following commands:
  - **rule** *1* **permit read write oid** *1.3.6*
  - **rule** *2* **deny read write oid** *1.3.6.1.4.1*
  - **rule** *3* **permit read write oid** *1.3.6.1.4*
- If the same OID is specified in multiple rules, the rule with the higher ID takes effect. For example, a user role can access the MIB node with OID 1.3.6.1.4.1.25506.141.3.0.1 if the user role contains rules configured by using the following commands:
  - **rule** *1* **permit read write oid** *1.3.6*
  - **rule** *2* **deny read write oid** *1.3.6.1.4.1*
  - **rule** *3* **permit read write oid** *1.3.6.1.4.1*

When you specify a command string, follow the guidelines in Table 3.

Table 3 Command string configuration rules

Rule	Guidelines
Semicolon (;) is the delimiter.	Use a semicolon to separate the command of each view that you must enter before you access a command or a set of commands. However, do not use a semicolon to separate commands available in user view or any view, for example, **display** and **dir**. Each semicolon-separated segment must have a minimum of one printable character. To specify the commands in a view but not the commands in the view's subviews, use a semicolon as the last printable character in the last segment. To specify the commands in a view and the view's subviews, the last printable character in the last segment must not be a semicolon. For example, you must enter system view before you enter interface view. To specify all commands starting with the **ip** keyword in any interface view, you must use the "system ; interface * ; ip * ;" command string. For another example, the "system ; radius scheme * ;" command string represents all commands that start with the **radius scheme** keywords in system view. The "system ; radius scheme *" command string represents all commands that start with the **radius scheme** keywords in system view and all commands in RADIUS scheme view.

Rule	Guidelines
Asterisk (*) is the wildcard.	An asterisk represents zero or multiple characters. In a non-last segment, you can use an asterisk only at the end of the segment. In the last segment, you can use an asterisk in any position of the segment. If the asterisk appears at the beginning, you cannot specify a printable character behind the asterisk. For example, the "system ; *" command string represents all commands available in system view and all subviews of the system view. The "debugging * event" command string represents all event debugging commands available in user view.
Keyword abbreviation is allowed.	You can specify a keyword by entering the first few characters of the keyword. Any command that starts with this character string matches the rule. For example, "**rule 1 deny command display arp source** *" denies access to the **display arp source-mac interface** and **display arp source-suppression** commands.
To control the access to a command, you must specify the command immediately after the view that has the command.	To control access to a command, you must specify the command immediately behind the view to which the command is assigned. The rules that control command access for any subview do not apply to the command. For example, the "rule 1 deny command system ; interface * ; *" command string disables access to any command that is assigned to interface view. However, you can still execute the **acl advanced** command in interface view, because this command is assigned to system view rather than interface view. To disable access to this command, use "rule 1 deny command system ; acl *;".
Do not include the vertical bar (|), greater-than sign (>), or double greater-than sign (>>) when you specify **display** commands in a user role command rule.	The system does not treat the redirect signs and the parameters that follow the signs as part of command lines. However, in user role command rules, these redirect signs and parameters are handled as part of command lines. As a result, no rule that includes any of these signs can find a match. For example, "rule 1 permit command display debugging > log" can never find a match. This is because the system has a **display debugging** command but not a **display debugging > log** command.

Examples

Permit user role **role1** to execute the **display acl** command.

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] rule 1 permit command display acl
```

Permit user role **role1** to execute all commands that start with the **display** keyword.

```
[Sysname-role-role1] rule 2 permit command display *
```

Permit user role **role1** to execute the **radius scheme aaa** command in system view and use all commands assigned to RADIUS scheme view.

```
[Sysname-role-role1] rule 3 permit command system ; radius scheme aaa
```

Deny the access of **role1** to the read or write commands of any features.

```
[Sysname-role-role1] rule 4 deny read write feature
```

Deny the access of **role1** to the read commands of the **aaa** feature.

```
[Sysname-role-role1] rule 5 deny read feature aaa
```

Permit **role1** to access all read, write, and execute commands of feature group **security-features**.

```
[Sysname-role-role1] rule 6 permit read write execute feature-group security-features
```

Permit **role1** to access all read and write MIB nodes starting from the node with OID 1.1.2.

```
[Sysname-role-role1] rule 7 permit read write oid 1.1.2
```

Related commands

display role

display role feature

display role feature-group

display web menu

role

security-zone policy deny

Use **security-zone policy deny** to enter user role security zone policy view.

Use **undo security-zone policy deny** to restore the default.

Syntax

security-zone policy deny

undo security-zone policy deny

Default

A user role has access to all security zones.

Views

User role view

Predefined user roles

network-admin

context-admin

Usage guidelines

CAUTION:

This command denies a user role access to any security zones if you do not specify accessible security zones by using the **permit security-zone** command. To configure a security zone, make sure the security zone is permitted by the user role security zone policy in use.

To limit the scope of security zones accessible to a user role, perform the following tasks:

1. Use **security-zone policy deny** to enter user role security zone policy view and deny the user role access to any security zones.
2. Use **permit security-zone** to specify accessible security zones.

You can perform the following tasks on an accessible security zone:

- Create, remove, or configure the security zone.
- Enter security zone view.
- Specify the security zone in feature commands.

Any change to a user role security zone policy takes effect only on users who log in with the user role after the change.

Examples

Enter user role security zone policy view of **role1**, and deny the access of **role1** to any security zones.

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] security-zone policy deny
[Sysname-role-role1-zonepolicy] quit
```

Enter user role security zone policy view of **role1**, and deny the access of **role1** to any security zones except for security zones **trust** and **abc**.

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] security-zone policy deny
[Sysname-role-role1-zonepolicy] permit security-zone trust abc
```

Related commands

display role

permit security-zone

role

super

Use **super** to obtain another user role without reconnecting to the device.

Syntax

super [*role-name*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

role-name: Specifies a user role, a case-sensitive string of 1 to 63 characters. The user role must exist in the system and cannot be security-audit or guest-manager. If you do not specify a user role, you obtain the default target user role which is set by using the **super default role** command.

Usage guidelines

The obtained user role is a temporary user role, because this command is effective only on the current login. The next time you are logged in with the user account, the original user role settings take effect.

To enable a user to obtain another user role without reconnecting to the device, you must configure user role authentication.

Enter the username (if any) and password within 60 seconds after you enter the **super** command. If you fail to do so, the command will time out. To obtain the role, you will need to re-execute the command.

- If no local password is configured in the local password authentication (**local**), a console user can obtain the user role by either entering a string or not entering anything.
- If no local password is configured in the local-then-remote authentication (**local scheme**), a console or VTY user performs remote authentication.

Examples

Obtain the user role network-operator.

```
<Sysname> super network-operator
Password:
User privilege role is network-operator, and only those commands that authorized to the role can be used.
```

Related commands

authentication super (*Security Command Reference*)

super authentication-mode

super password

super authentication-mode

Use **super authentication-mode** to set an authentication mode for temporary user role authorization.

Use **undo super authentication-mode** to restore the default.

Syntax

super authentication-mode { **local** | **scheme** } *

undo super authentication-mode

Default

Local password authentication applies.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

local: Enables local password authentication.

scheme: Enables remote AAA authentication.

Usage guidelines

For local password authentication, use the **super password** command to set a password.

For remote AAA authentication, set the username and password on the RADIUS or HWTACACS server.

If you specify both **local** and **scheme** keywords, the keyword first entered in the command takes precedence.

- **scheme local**—Enables remote-then-local authentication mode. The device first performs AAA authentication to obtain a temporary user role. Local password authentication is performed if the remote HWTACACS or RADIUS server does not respond, or if the AAA configuration on the device is invalid.
- **local scheme**—Enables local-then-remote authentication mode. The device first performs local password authentication. If no password is configured for the user role, the device performs remote authentication for VTY users.A console user can obtain another user role by either entering a string or not entering anything.

For more information about AAA, see *Security Configuration Guide*.

Examples

Enable local-only authentication for temporary user role authorization.

```
<Sysname> system-view
[Sysname] super authentication-mode local
```

Enable remote-then-local authentication for temporary user role authorization.

```
<Sysname> system-view
[Sysname] super authentication-mode scheme local
```

Related commands

authentication super (*Security Command Reference*)

super password

super default role

Use **super default role** to specify the default target user role for temporary user role authorization.

Use **undo super default role** to restore the default.

Syntax

super default role *role-name*

undo super default role

Default

If you log in to the default context, the default target user role is network-admin.

If you log in to a non-default context, the default target user role is context-admin.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

role-name: Specifies the name of the default target user role, a case-sensitive string of 1 to 63 characters. The user role must exist in the system and cannot be security-audit or guest-manager.

Usage guidelines

The default target user role is applied to the **super** or **super password** command when you do not specify a user role for the command.

Examples

Specify **network-operator** as the default target user role for temporary user role authorization.

```
<Sysname> system-view
[Sysname] super default role network-operator
```

Related commands

super

super password

super password

Use **super password** to set a password for a user role.

Use **undo super password** to delete the password for a user role.

Syntax

super password [**role** *role-name*] [{ **hash** | **simple** } *string*]

undo super password [**role** *role-name*]

Default

No password is set for a user role.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

role *role-name*: Specifies a user role, a case-sensitive string of 1 to 63 characters. The user role must exist in the system and cannot be security-audit or guest-manager. If you do not specify a user role, the command sets a password for the default target user role which is set by using the **super default role** command.

hash: Specifies a password in hashed form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in hashed form.

string: Specifies the password. The plaintext form of the password is a case-sensitive string of 1 to 63 characters. The hashed form of the password is a case-sensitive string of 1 to 110 characters.

Usage guidelines

If you do not specify any parameters, you specify a plaintext password in the interactive mode.

Set a password if you configure local password authentication for temporary user role authorization.

It is a good practice to specify different passwords for different user roles.

When the global password control feature is enabled, the device maintains a history of super passwords, which are stored in hashed form.

Use the following guidelines when you change the authentication password for a user role when the global password control feature is enabled:

- If you set the new password in plaintext form, you must make sure the password is different from the current one and those stored in the history super password records.
- If you set the new password in hashed form, the system does not compare the new super password with the current one or the history super password records. The password can be the same as the current one or a history password retained by the device.

Examples

Set the password to **123456TESTplat&!** in plaintext form for user role network-operator.

```
<Sysname> system-view
[Sysname] super password role network-operator simple 123456TESTplat&!
```

Set the password to **123456TESTplat&!** in the interactive mode for user role network-operator.

```
<Sysname> system-view
[Sysname] super password role network-operator
Password:
Confirm :
Updating user information. Please wait......
```

Related commands

super authentication-mode

super default role

super use-login-username

Use **super use-login-username** to enable the device to automatically obtain the login username when a login user requests temporary user role authorization from a remote authentication server.

Use **undo super use-login-username** to restore the default.

Syntax

super use-login-username

undo super use-login-username

Default

The device prompts for a username when a login user requests temporary user role authorization from a remote authentication server.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command is applicable only to the login from a user line that uses scheme authentication, which requires a username for login.

If the user was logged in from a user line that uses password authentication or no authentication, the device cannot obtain the login username. The request for temporary user role authorization from a remote authentication server will fail.

This command does not take effect on local password authentication for temporary user role authorization.

Examples

Enable the device to automatically obtain the login username when a login user requests temporary user role authorization from a remote authentication server.

```
<Sysname> system-view
[Sysname] super use-login-username
```

Related commands

authentication super (*Security Command Reference*)

super authentication-mode

super password

vlan policy deny

Use **vlan policy deny** to enter user role VLAN policy view.

Use **undo vlan policy deny** to restore the default.

Syntax

vlan policy deny

undo vlan policy deny

Default

A user role has access to all VLANs.

Views

User role view

Predefined user roles

network-admin

context-admin

Usage guidelines

CAUTION:

This command denies a user role access to any VLANs if you do not specify accessible VLANs by using the **permit vlan** command. To configure a VLAN, make sure the VLAN is permitted by the user role VLAN policy in use.

To limit the scope of VLANs accessible to a user role, perform the following tasks:

1. Use **vlan policy deny** to enter user role VLAN policy view and deny the user role access to any VLANs.
2. Use **permit vlan** to specify accessible VLANs.

You can perform the following tasks on an accessible VLAN:

- Create, remove, or configure the VLAN.
- Enter VLAN view.
- Specify the VLAN in feature commands.

Any change to a user role VLAN policy takes effect only on users who log in with the user role after the change.

Examples

Enter user role VLAN policy view of **role1**, and deny the access of **role1** to any VLANs.

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] vlan policy deny
[Sysname-role-role1-vlanpolicy] quit
```

Enter user role VLAN policy view of **role1**, and deny the access of **role1** to any VLANs except for VLANs 50 to 100.

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] vlan policy deny
[Sysname-role-role1-vlanpolicy] permit vlan 50 to 100
```

Related commands

display role

permit vlan

role

vpn-instance policy deny

Use **vpn-instance policy deny** to enter user role VPN instance policy view.

Use **undo vpn-instance policy deny** to restore the default.

Syntax

vpn-instance policy deny

undo vpn-instance policy deny

Default

A user role has access to all VPN instances.

Views

User role view

Predefined user roles

network-admin

context-admin

Usage guidelines

CAUTION:

This command denies a user role access to any VPN instances if you do not specify accessible VPN instances by using the **permit vpn-instance** command. To configure a VPN instance, make sure the VPN instance is permitted by the user role VPN instance policy in use.

To limit the scope of VPN instances accessible to a user role, perform the following tasks:

1. Use **vpn-instance policy deny** to enter user role VPN instance policy view and deny the user role access to any VPN instances.
2. Use **permit vpn-instance** to specify accessible VPN instances.

You can perform the following tasks on an accessible VPN instance:

- Create, remove, or configure the VPN instance.
- Enter VPN instance view.
- Specify the VPN instance in feature commands.

Any change to a user role VPN instance policy takes effect only on users who log in with the user role after the change.

Examples

Enter user role VPN instance policy view of **role1**, and deny the access of **role1** to any VPN instances.

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] vpn-instance policy deny
[Sysname-role-role1-vpnpolicy] quit
```

Enter user role VPN instance policy view of **role1**, and deny the access of **role1** to any VPN instances except for **vpn2**.

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] vpn-instance policy deny
[Sysname-role-role1-vpnpolicy] permit vpn-instance vpn2
```

Related commands

display role

permit vpn-instance

role

Contents

Login management commands

Some login management commands are available in both user line view and user line class view. For these commands, the device uses the following rules to determine the settings to be activated:

- A setting in user line view applies only to the user line. A setting in user line class view applies to all user lines of the class.
- A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view.
- A setting in user line class view takes effect on login sessions that are established after the setting is configured.

activation-key

Use **activation-key** to set the terminal session activation key. Pressing this shortcut key starts a terminal session.

Use **undo activation-key** to restore the default.

Syntax

activation-key *key-string*

undo activation-key

Default

The terminal session activation key is **Enter**.

Views

User line view

User line class view

Predefined user roles

network-admin

context-admin

Parameters

key-string: Specifies a shortcut key. It can be a character (case sensitive), or an ASCII code value in the range of 0 to 127. For example, if you use **activation-key 1**, the shortcut key is **Ctrl+A**. If you use **activation-key a**, the shortcut key is **a**. For information about ASCII code values of individual characters, see the standard ASCII code chart. For information about ASCII code values of combined keys that use the **Ctrl** key, see Table 1.

Usage guidelines

This command is not supported in VTY line view or VTY line class view.

This command takes effect immediately.

This command is available in both user line view and user line class view. A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view.

You can use only the specified terminal session activation key to start a terminal session. To display the current terminal session activation key, use the **display current-configuration | include activation-key** command.

Table 1 ASCII code values for combined keys that use the Ctrl key

Combined key	ASCII code value
Ctrl+A	1
Ctrl+B	2
Ctrl+C	3
Ctrl+D	4
Ctrl+E	5
Ctrl+F	6
Ctrl+G	7
Ctrl+H	8
Ctrl+I	9
Ctrl+J	10
Ctrl+K	11
Ctrl+L	12
Ctrl+M	13
Ctrl+N	14
Ctrl+O	15
Ctrl+P	16
Ctrl+Q	17
Ctrl+R	18
Ctrl+S	19
Ctrl+T	20
Ctrl+U	21
Ctrl+V	22
Ctrl+W	23
Ctrl+X	24
Ctrl+Y	25
Ctrl+Z	26

Examples

Configure character **s** as the terminal session activation key for console line 0.

```
<Sysname> system-view
[Sysname] line console 0
[Sysname-line-console0] activation-key s
```

To verify the configuration:

1. Exit the console session.

   ```
   [Sysname-line-console0] return
   <Sysname> quit
   ```

2. Log in again through the console line.

The following message appears:

```
Press ENTER to get started.
```

3. Press **Enter**.

   Pressing **Enter** does not start a session.

4. Press **s**.

   A terminal session is started.

```
<Sysname>
```

authentication-mode

Use **authentication-mode** to set the authentication mode for a user line.

Use **undo authentication-mode** to restore the default.

Syntax

authentication-mode { **none** | **password** | **scheme** }

undo authentication-mode

Default

The authentication mode is **scheme** for the VTY and console lines.

Views

User line view

User line class view

Predefined user roles

network-admin

context-admin

Parameters

none: Disables authentication.

password: Performs local password authentication.

scheme: Performs AAA authentication. For more information about AAA, see *Security Configuration Guide*.

Usage guidelines

CAUTION:

- When authentication is disabled, users can login without authentication. For security purpose, disable authentication with caution.
- When you enable password authentication, you must also configure an authentication password for the line or line class. If no authentication password is configured, you cannot log in to the device through the line or line class at the next time.
- When you enable scheme authentication, make sure an authentication user account is available. If no authentication user account is available, you cannot log in to the device through the line or line class at the next time.

Only users assigned the network-admin, context-admin, or level-15 user role can execute this command. Other users cannot execute this command, even if they are granted the right to execute this command.

In VTY line view, this command is associated with the **protocol inbound** command.

- If the settings of the two commands in VTY line view are both the default settings, the settings for the commands in VTY line class view take effect.
- If the settings of the two commands in VTY line view are both non-default settings, the non-default settings in VTY line view take effect.
- If only one command has a non-default setting in VTY line view, the other command uses the default setting, regardless of the setting in VTY line class view.

An authentication mode change does not take effect on the current session. It takes effect on subsequent login sessions.

Examples

Enable the **none** authentication mode for VTY line 0.

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] authentication-mode none
```

Enable password authentication for VTY line 0 and set the password to **hello12345**.

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] authentication-mode password
[Sysname-line-vty0] set authentication password simple hello12345
```

Enable scheme authentication for VTY line 0. Configure local user **test** and set the password to **hello12345**. Assign the Telnet service and the user role network-admin to the user.

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] authentication-mode scheme
[Sysname-line-vty0] quit
[Sysname] local-user test
[Sysname-luser-manage-test] password simple hello12345
[Sysname-luser-manage-test] service-type telnet
[Sysname-luser-manage-test] authorization-attribute user-role network-admin
```

Related commands

set authentication password

auto-execute command

Use **auto-execute command** to specify the command to be automatically executed for a login user.

Use **undo auto-execute command** to restore the default.

Syntax

auto-execute command *command*

undo auto-execute command

Default

No command is specified to be automatically executed for a login user.

Views

User line view

User line class view

Predefined user roles

network-admin

context-admin

Parameters

command: Specifies the command to be automatically executed.

Usage guidelines

CAUTION:

After using this command for a user line, you might be unable to access the CLI through the user line. Make sure you can access the CLI through a different user line before you use this command and save the configuration.

The device will automatically execute the specified command when a user logs in through the user line, and close the user connection after the command is executed.

This command is not supported in console line view or console line class view.

This command is available in both user line view and user line class view. A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view.

A configuration change made by this command does not take effect on the current session. It takes effect on subsequent login sessions.

Examples

Configure the device to automatically execute the **`telnet 192.168.1.41`** command when a user logs in through VTY line 0.

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] auto-execute command telnet 192.168.1.41
This action will lead to configuration failure through line-vty0. Are you sure?
[Y/N]:y
[Sysname-line-vty0]
```

To verify the configuration, Telnet to the device (192.168.1.40).

The device automatically Telnets to 192.168.1.41. The following output is displayed on the configuration terminal:

```
C:\> telnet 192.168.1.40
******************************************************************************
* Copyright (c) 2004-2017 NSFOCUS. All rights reserved.                      *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

<Sysname>
Trying 192.168.1.41 ...
Press CTRL+K to abort
Connected to 192.168.1.41 ...
******************************************************************************
* Copyright (c) 2004-2017 NSFOCUS. All rights reserved.                      *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
```

```
**************************************************************************
<Sysname.41>
```

This operation is the same as directly logging in to the device at 192.168.1.41 through Telnet. When you close the Telnet connection to 192.168.1.41, the Telnet connection to 192.168.1.40 is closed at the same time.

command accounting

Use **command accounting** to enable command accounting.

Use **undo command accounting** to disable command accounting.

Syntax

command accounting

undo command accounting

Default

Command accounting is disabled. The accounting server does not record executed commands.

Views

User line view

User line class view

Predefined user roles

network-admin

context-admin

Usage guidelines

When command accounting is enabled but command authorization is not, every executed command is recorded on the HWTACACS server. When both command accounting and command authorization are enabled, only authorized commands that are executed are recorded on the HWTACACS server.

Invalid commands are not recorded.

A configuration change made by this command does not take effect on the current session. It takes effect on subsequent login sessions.

After you use the **command accounting** command in user line class view, you cannot use the **undo command accounting** command in any user line views in the class.

Examples

Enable command accounting for VTY line 0.

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] command accounting
```

Related commands

accounting command (*Security Command Reference*)

command authorization

command authorization

Use **command authorization** to enable command authorization.

Use **undo command authorization** to disable command authorization.

Syntax

command authorization

undo command authorization

Default

Command authorization is disabled. Logged-in users can execute commands without authorization.

Views

User line view

User line class view

Predefined user roles

network-admin

context-admin

Usage guidelines

When command authorization is enabled, commands available for a user vary by the user's login authentication mode.

- If authentication is disabled or password authentication is enabled, command authorization does not take effect, and the user cannot use any commands.
- If scheme authentication is enabled, commands available for a user vary by the user's access authentication method.
  - If local authentication is used, the device uses the user roles assigned to the user to perform command authorization.
  - If remote authentication is used, the remote authorization server performs command authorization to determine whether a command entered by a login user is permitted. If remote authorization fails, the device uses the user roles of a local user with the same name as the login user to determine whether the command can be used. If the authorization also fails, the login user cannot use the command.

Command authorization configuration changes in user line class view do not take effect on the current session. The changes take effect only on subsequent login sessions. Command authorization configuration changes in user line view take effect immediately on all users that access the user line.

If you use the **command authorization** command in user line class view, command authorization is enabled for all user lines in the class. You cannot use the **undo command authorization** command in the view of a user line in the class.

Examples

Enable command authorization for VTY line 0.

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] command authorization
```

Related commands

authorization command (*Security Command Reference*)

command accounting

databits

Use **databits** to specify the number of data bits for a character.

Use **undo databits** to restore the default.

Syntax

databits { | **7** | **8** }

undo databits

Default

Eight data bits are used for a character.

Views

User line view

Predefined user roles

network-admin

context-admin

Parameters

7: Uses seven data bits for a character.

8: Uses eight data bits for a character.

Usage guidelines

This command is not supported in VTY line class view.

This setting must be the same as the setting on the configuration terminal.

Examples

Set the number of data bits for a character to 7.

```
<Sysname> system-view
[Sysname] line console 0
[Sysname-line-console0] databits 7
```

display ip http

Use **display ip http** to display HTTP service configuration and status information.

Syntax

display ip http

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display HTTP service configuration and status information. In this example, a Layer 2 ACL is applied to the HTTP service.

```
<Sysname> display ip http
HTTP port: 80
ACL: 4444 (Layer 2)
Operation status: Enabled
```

Display HTTP service configuration and status information. In this example, an IPv4 basic ACL and an IPv6 basic ACL are applied to the HTTP service.

```
<Sysname> display ip http
HTTP port: 80
IPv4 ACL: 2222 (basic)
IPv6 ACL: 2333 (basic)
Operation status: Enabled
```

Table 2 Command output

Field	Description
HTTP port	HTTP service port number.
ACL/IPv4 ACL/IPv6 ACL	Number or name of the Layer 2, IPv4, or IPv6 ACL used to control HTTP access. If no ACL is used, this field displays **0**. The ACL type is enclosed into a pair of parentheses. Available ACL types: • **basic**—Basic ACL. • **advanced**—Advanced ACL. • **Layer 2—**Layer 2 ACL.
Operation status	Whether the HTTP service is enabled.

Related commands

ip http acl

ip http enable

ip http port

display ip https

Use **display ip https** to display HTTPS service configuration and status information.

Syntax

display ip https

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display HTTPS service configuration and status information. In this example, a Layer 2 ACL is applied to the HTTPS service.

```
<Sysname> display ip https
HTTPS port: 443
SSL server policy: test
Certificate access-control-policy: Not configured
ACL: 4444 (layer 2)
Operation status: Enabled
```

Display HTTPS service configuration and status information. In this example, an IPv4 basic ACL and an IPv6 basic ACL are applied to the HTTPS service.

```
<Sysname> display ip https
HTTPS port: 443
SSL server policy: test
Certificate access-control-policy: Not configured
IPv4 ACL: 2222 (basic)
IPv6 ACL: 2333 (basic)
Operation status: Enabled
```

Table 3 Command output

Field	Description
HTTPS port	HTTPS service port number.
SSL server policy	SSL server policy applied to the HTTPS service. If no SSL server policy is applied, this field displays **Not configured**.
Certificate access-control-policy	Certificate-based access control policy used to control client access rights. If no certificate-based access control policy is used, this field displays **Not configured**.
ACL/IPv4 ACL/IPv6 ACL	Number or name of the Layer 2, IPv4, or IPv6 ACL used to control HTTPS access. If no ACL is used, this field displays **0**. The ACL type is enclosed into a pair of parentheses. Available ACL types: • **basic**—Basic ACL. • **advanced**—Advanced ACL. • **Layer 2**—Layer 2 ACL.
Operation status	Whether the HTTPS service is enabled.

Related commands

ip https acl

ip https enable

ip https port

ip https ssl-server-policy

ip https certificate access-control-policy

display line

Use **display line** to display user line information.

Syntax

display line [*number1* | { **console** | **vty** } *number2*] [**summary**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

number1: Specifies the absolute number of a user line. To view the value range for this argument, enter a question mark (?) in the place of this argument.

console: Specifies the console line.

vty: Specifies the VTY line.

number2: Specifies the relative number of a user line. To view the value range for this argument, enter a question mark (?) in the place of this argument.

summary: Displays summary information about user lines. If you do not specify this keyword, the command displays detailed information.

Examples

Display information about user line 0.

```
<Sysname> display line 0
  Idx  Type     Tx/Rx      Modem Auth  Int        Location
+ 0    CON 0    9600       -     N     -           1/0

  +    : Line is active.
  F    : Line is active and in async mode.
  Idx  : Absolute index of line.
  Type : Type and relative index of line.
  Auth : Login authentication mode.
  Int  : Physical port of the line.
  A    : Authentication use AAA.
  N    : No authentication is required.
  P    : Password authentication.
```

Table 4 Command output

Field	Description
Modem	Whether the modem allows calling in or out. By default, this attribute is not configured and this field displays a hyphen (-). This field is not supported in the current software version.
Int	Physical port for the line. If there is no physical port for the line or the port is a console port, this field displays a hyphen (-).
Location	Physical position of the line, in the form of *slot number*/*CPU number*.

Display summary information about all user lines.

```
<Sysname> display line summary
  Line type : [CON]
            0:XX
  Line type : [VTY]
            2:UUUX XXXX XXXX XXXX
           18:XXXX XXXX XXXX XXXX
           34:XXXX XXXX XXXX XXXX
           50:XXXX XXXX XXXX XXXX

   3 lines used.      (U)
  63 lines not used.  (X)
```

Table 5 Command output

Fields	Description
Line type	Type of the user line: • **CON**—Console line. • **VTY**—VTY line.
number:*status*	*number*: Absolute number of the first user line in the user line class. *status*: User line status. **X** is for unused and **U** is for used.

display telnet client

Use **display telnet client** to display the packet source setting for the Telnet client.

Syntax

display telnet client

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Usage guidelines

This command displays the source IPv4 address or source interface specified for the Telnet client to use in outgoing Telnet packets, depending on the **telnet client source** command.

Examples

Display the packet source setting for the Telnet client.

```
<Sysname> display telnet client
 The source IP address is 1.1.1.1.
```

Related commands

telnet client source

display user-interface

Use **display user-interface** to display user line information.

Syntax

display user-interface [*number1* | { **console** | **vty** } *number2*] [**summary**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

number1: Specifies the absolute number of a user line. To view the value range for this argument, enter a question mark (?) in the place of this argument.

console: Specifies the console line.

vty: Specifies the VTY line.

number2: Specifies the relative number of a user line. To view the value range for this argument, enter a question mark (?) in the place of this argument.

summary: Displays summary information about user lines. If you do not specify this keyword, the detailed information is displayed.

Usage guidelines

This command is an older version reserved for backward compatibility purposes. It has the same functionality and output as the **display line** command. As a best practice, use the **display line** command.

Examples

Display information about user line 0.

```
<Sysname> display user-interface 0
  Idx  Type     Tx/Rx      Modem Auth  Int        Location
+ 0    CON 0    9600       -     N     -          1/0

  +    : Line is active.
  F    : Line is active and in async mode.
  Idx  : Absolute index of line.
  Type : Type and relative index of line.
  Auth : Login authentication mode.
  Int  : Physical port of the line.
  A    : Authentication use AAA.
  N    : No authentication is required.
  P    : Password authentication.
```

Table 6 Command output

Field	Description
Modem	Whether the modem allows calling in or out. By default, this attribute is not configured and this field displays a hyphen (-). This field is not supported in the current software version.
Int	Physical port for the line. If there is no physical port for the line or the port is a console port, this field displays a hyphen (-).
Location	Physical position of the line, in the form of *slot number*/*CPU number*.

Display summary information about all user lines.

```
<Sysname> display user-interface summary
  Line type : [CON]
            0:XX
  Line type : [VTY]
            2:UUUX XXXX XXXX XXXX
           18:XXXX XXXX XXXX XXXX
           34:XXXX XXXX XXXX XXXX
           50:XXXX XXXX XXXX XXXX
```

Table 7 Command output

Fields	Description
Line type	Type of the user line: • **CON**—Console line. • **VTY**—VTY line.
number:*status*	*number*: Absolute number of the first user line in the user line class. *status*: User line status. **X** is for unused and **U** is for used.

display users

Use **display users** to display online CLI users.

Syntax

display users [**all**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

all: Displays all user lines supported by the device.

Examples

Display online user information.

```
<Sysname> display users
  Idx  Line     Idle       Time              Pid     Type
+ 10   VTY 0    00:00:00   Jan 01 00:33:10   484     TEL
  12   VTY 2    00:06:22   Jan 01 00:33:22   495     TEL

Following are more details.
VTY 0   :
        Location: 192.168.1.107
VTY 2   :
        Location: 192.168.1.134
 +    : Current operation user.
 F    : Current operation user works in async mode.
```

Table 8 Command output

Field	Description
Idx	Absolute number of the user line.
Line	Type and relative number of the user line.
Idle	Time elapsed after the user's most recent input, in the *hh*:*mm*:*ss* format.
Time	Login time of the user.
Pid	Process ID of the user session.
Type	User type: • **TEL**—Telnet user. • **SSH**—SSH user. • **Switchto User**—User who logged in by using the **`switchto context`** command. • For a user who logged in through the console port, this field does not display anything.
+	User line you are using.
User name	Username used by the user. This field is displayed only if the user provided a username and password for authentication at login.
Location	IP address of the user.

display web menu

Use **`display web menu`** to display Web interface navigation tree information.

Syntax

`display web menu` [**`chinese`**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

chinese: Displays information about the Chinese Web interface navigation tree. If you do not specify this keyword, the command displays information about the English Web interface navigation tree.

Usage guidelines

This command displays all options on the Web interface navigation tree.

Examples

Display Web interface navigation tree information.

```
<Sysname> display web menu
  .
  |--Dashboard: ID = dashboard
  |    |--Operation Monitor: ID = m_dashboard
  |    |--Traffic Monitor: ID = m_flowdetection
  |    |--Threat Monitor: ID = m_threatdetection
  |    |--Filtering Monitor: ID = m_urldetection
  |    |--LoadBalance Monitor: ID = m_loadbalancedash
  |    |--User-Defined Monitor: ID = m_definedboard
  |    `--Interface Information: ID = m_ifinfopanel
  |--Monitor: ID = m_monitor
  |    |--Application Analysis Center: ID = m_cdas
  |    |--Security Logs: ID = m_atklog
  |    |    |--Blacklist Logs: ID = m_blacklistlog
  |    |    |--Single-Packet Attack Logs: ID = m_singleatk
  |    |    |--Scanning Attack Logs: ID = m_scanatk
  |    |    |--Flood Attack Logs: ID = m_floodatk
  |    |    |--Threat Logs: ID = m_threatlog
  |    |    |--URL Filtering Logs: ID = m_urllog
  |    |    |--File Filtering Logs: ID = m_filefilterlog
  |    |    |--Security Policy Logs: ID = m_zonepairlog
  |    |    |--Sandbox Logs: ID = m_aptlog
  |    |    |--NAT Logs: ID = m_natflowlog
  |    |    |--SSL VPN User Access Logs: ID = m_sslvpnuserlog
---- More ----
```

display web users

Use **display web users** to display online Web users.

Syntax

display web users

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display online Web users.

```
<Sysname> display web users
UserID          Name            Type   Language JobCount LoginTime LastOperation
AB2039483271293 Administrator   HTTP   Chinese     3     12:00:23  14:10:05
F09382BA2014AC8 user            HTTPS  English     1     13:05:00  14:11:00
```

Table 9 Command output

Field	Description
UserID	ID used to uniquely identify the online Web user.
JobCount	Number of connections established by the user.

escape-key

Use **escape-key** to set the escape key.

Use **undo escape-key** to disable the escape key.

Syntax

escape-key { *key-string* | **default** }

undo escape-key

Default

The escape key is **Ctrl+C**.

Views

User line view

User line class view

Predefined user roles

network-admin

context-admin

Parameters

key-string: Specifies a shortcut key. It can be a character (case sensitive, except for **d** and **D**), or an ASCII code value in the range of 0 to 127. For example, if you use **escape-key 1**, the shortcut key is **Ctrl+A**. If you use **escape-key a**, the shortcut key is **a**. If you specify the character **d** or **D** for this argument, the actual shortcut key is **Ctrl+C**. To use **d** or **D** as the shortcut key, you must specify the ASCII code value of the character for this argument. For information about ASCII code values of individual characters, see the standard ASCII code chart. For information about ASCII code values of combined keys that use the **Ctrl** key, see Table 1.

default: Restores the default escape key **Ctrl+C**.

Usage guidelines

You can press the escape key to abort a command that is being executed, for example, a **ping** or **tracert** command. Whether a command can be aborted by **Ctrl+C** by default depends on the

software implementation of the command. For more information, see the usage guidelines for the command.

As a best practice, use a key sequence as the escape key. If you define a single character as the escape key, pressing the key while a command is being executed stops the command. If no command is being executed, pressing the key enters the character as a common character. If you Telnet from the device to a remote device, pressing the key enters the character as a common character on the remote device. The key acts as the escape key on the remote device only when the following conditions are met:

- You define the same character as the escape key on the remote device.
- You press the key while a command is being executed on the remote device.

The **undo escape-key** command disables the current escape key. After you execute this **undo** command, no escape key is available.

This command is available in both user line view and user line class view. A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view.

The setting in user line view takes effect immediately on the current session. The setting in user line class view takes effect on login sessions that are established after the setting is configured.

To display the current escape key, use the **display current-configuration | include escape-key** command.

Examples

Configure character **a** as the escape key for VTY line 0.

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] escape-key a
```

To verify the configuration:

1. Ping IP address 192.168.1.49, specifying the **-c** keyword to set the number of ICMP echo request packets to 20.

   ```
   Ping 192.168.1.49 (192.168.1.49): 56 data bytes, press 'a' to break
   56 bytes from 192.168.1.49: icmp_seq=0 ttl=255 time=1.000 ms
   56 bytes from 192.168.1.49: icmp_seq=1 ttl=255 time=0.000 ms
   ```

2. Press **a**.

   The system aborts the command and returns to user view.

   ```
   --- Ping statistics for 192.168.1.49 ---
   20 packet(s) transmitted, 20 packet(s) received, 0.0% packet loss
   round-trip min/avg/max/std-dev = 0.000/0.200/1.000/0.400 ms
   <Sysname>
   ```

flow-control

Use **flow-control** to configure the flow control mode.

Use **undo flow-control** to restore the default.

Syntax

flow-control { **hardware** | **none** | **software** }

undo flow-control

Default

Flow control is disabled.

Views

User line view

Predefined user roles

network-admin

context-admin

Parameters

hardware: Performs hardware flow control.

none: Disables flow control.

software: Performs software flow control.

Usage guidelines

This command is not supported in VTY line view.

The device supports flow control in both the inbound and outbound directions.

- For flow control in the inbound direction, the local device listens to flow control information from the remote device.
- For flow control in the outbound direction, the local device sends flow control information to the remote device.

The flow control setting takes effect in both directions.

To communicate, two devices must operate in the same flow control mode.

Examples

Configure software flow control in the inbound and outbound directions for console line 0.

```
<Sysname> system-view
[Sysname] line console 0
[Sysname-line-console0] flow-control software
```

free line

Use **free line** to release a user line.

Syntax

free line { *number1* | { **console** | **vty** } *number2* }

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

number1: Specifies the absolute number of a user line. To view the value range for this argument, enter a question mark (?) in the place of this argument.

console: Specifies the console line.

vty: Specifies the VTY line.

number2: Specifies the relative number of a user line. To view the value range for this argument, enter a question mark (?) in the place of this argument.

Usage guidelines

This command does not release the line you are using.

Examples

Release VTY line 1.

```
<Sysname> free line vty 1
Are you sure to free line vty1? [Y/N]:y
 [OK]
```

free user-interface

Use **free user-interface** to release a user line.

Syntax

free user-interface { *number1* | { **console** | **vty** } *number2* }

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

number1: Specifies the absolute number of a user line. To view the value range for this argument, enter a question mark (?) in the place of this argument.

console: Specifies the console line.

vty: Specifies the VTY line.

number2: Specifies the relative number of a user line. To view the value range for this argument, enter a question mark (?) in the place of this argument.

Usage guidelines

This command does not release the line you are using.

This command is an older version reserved for backward compatibility purposes. It has the same functionality and output as the **free line** command. As a best practice, use the **free line** command.

Examples

Release VTY line 1.

```
<Sysname> free user-interface vty 1
Are you sure to free line vty1? [Y/N]:y
 [OK]
```

free web users

Use **free web users** to log off online Web users.

Syntax

free web users { **all** | **user-id** *user-id* | **user-name** *user-name* }

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

all: Specifies all Web users.

user-id *user-id*: Specifies a Web user by the ID, a hexadecimal number of 15 digits. The system assigns each Web user a unique ID at login to identify the user.

user-name: Specifies a Web user by the username, a case-sensitive string of 1 to 255 characters.

Examples

Log off all online Web users.

```
<Sysname> free web users all
```

Related commands

display web users

history-command max-size

Use **history-command max-size** to set the size of the command history buffer for a user line.

Use **undo history-command max-size** to restore the default.

Syntax

history-command max-size *size-value*

undo history-command max-size

Default

The command history buffer for a user line stores up to 10 history commands.

Views

User line view

User line class view

Predefined user roles

network-admin

context-admin

Parameters

size-value: Specifies the maximum number of history commands the buffer can store, in the range of 0 to 256.

Usage guidelines

Each user line uses a separate command history buffer to store commands successfully executed by its user. The buffer size determines how many history commands the buffer can store.

To display history commands in the buffer for your session, press the up or down arrow key, or execute the **display history-command** command. For more information about the command history buffer, see *Fundamentals Configuration Guide*.

Terminating a CLI session clears the commands in the command history buffer.

The setting in user line view takes effect immediately on the current session. The setting in user line class view takes effect on login sessions that are established after the setting is configured.

Examples

Set the command history buffer size to 20 for VTY line 0.

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] history-command max-size 20
```

http method

Use **http method** to specify the HTTP methods to be added to the reply to an OPTIONS request.

Use **undo http method** to remove the HTTP methods to be added to the reply to an OPTIONS request.

Syntax

http method { **delete** | **get** | **head** | **options** | **post** | **put** } *

undo http method { **delete** | **get** | **head** | **options** | **post** | **put** } *

Default

No HTTP methods are specified.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

delete: Specifies the DELETE method.

get: Specifies the GET method.

head: Specifies the HEAD method.

options: Specifies the OPTIONS method.

post: Specifies the POST method.

put: Specifies the PUT method.

Usage guidelines

An HTTP client sends an OPTIONS request to the device to obtain the HTTP methods supported by the device. The device identifies whether the requested URL resources have a service that has registered for the OPTIONS method.

- If yes, the service responds to the OPTIONS request.
- If not, the device identifies whether the **options** keyword is specified for this command.
  - If yes, the device uses the settings for this command to generate and return a reply to the OPTIONS request.
  - If not, the device returns the **405 Method Not Allowed** message.

This command does not affect HTTP requests except for OPTIONS requests.

Examples

Specify GET, HEAD, POST, and OPTIONS methods as the HTTP methods to be added to the reply to an OPTIONS request.

```
<Sysname> system-view
[Sysname] http method get head post options
```

idle-timeout

Use **idle-timeout** to set the CLI connection idle-timeout timer.

Use **undo idle-timeout** to restore the default.

Syntax

idle-timeout *minutes* [*seconds*]

undo idle-timeout

Default

The CLI connection idle-timeout timer is 10 minutes.

Views

User line view

User line class view

Predefined user roles

network-admin

context-admin

Parameters

minutes: Specifies the number of minutes, in the range of 0 to 35791.

seconds: Specifies the number of seconds, in the range of 0 to 59. The default is 0 seconds.

Usage guidelines

The system automatically terminates a user connection if no information interaction occurs on the connection within the idle-timeout interval.

To disable the idle-timeout feature, execute the **idle-timeout 0** command.

This command is available in both user line view and user line class view. A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view.

The setting in user line view takes effect immediately on the current session. The setting in user line class view takes effect on login sessions that are established after the setting is configured.

Examples

Set the CLI connection idle-timeout timer to 1 minute and 30 seconds for VTY line 0.

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] idle-timeout 1 30
```

ip http acl

Use **ip http acl** to apply an ACL to the HTTP service.

Use **undo ip http acl** to restore the default.

Syntax

ip http acl [**ipv6**] [**advanced**] { *acl-number* | **name** *acl-name* }

ip http acl mac { *acl-number* | **name** *acl-name* }

undo ip http acl [**ipv6**]

undo ip http acl mac

Default

No ACL is applied to the HTTP service.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ipv6: Specifies an IPv6 ACL. If you do not specify this keyword, the command applies an IPv4 ACL to the HTTP service.

advanced: Specifies an advanced ACL. If you do not specify this keyword, the command applies a basic ACL to the HTTP service.

mac: Specifies a Layer 2 ACL.

acl-number: Specifies an ACL number in the range of 2000 to 4999.

- 2000 to 2999 for a basic ACL.
- 3000 to 3999 for an advanced ACL.
- 4000 to 4999 for a Layer 2 ACL.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters. It must start with an English letter and to avoid confusion, it cannot be **all**. The specified ACL takes effect only when the ACL exists.

Usage guidelines

To specify an IPv4 basic ACL, do not specify the **advanced** or **ipv6** keyword. To specify an IPv6 basic ACL, specify the **ipv6** keyword without the **advanced** keyword.

In an advanced ACL applied to the HTTP service, only the following match criteria take effect:

- Source and destination IP addresses.
- Source and destination ports.
- Transport layer protocol.

In a Layer 2 ACL applied to the HTTP service, only the source MAC address match criterion takes effect.

When no ACL is applied to the HTTP service or the applied ACL does not exist or does not have rules, all clients can access the device through HTTP. To control HTTP access, specify an ACL that exists and has rules so only clients permitted by the ACL can access the device through HTTP.

You can apply one IPv4 basic ACL and one IPv6 basic ACL to the HTTP service, or apply one IPv4 advanced ACL and one IPv6 advanced ACL to the HTTP service. If you execute this command multiple times for the same type of ACLs, the most recent configuration takes effect.

If a VPN instance is specified in an ACL rule, the rule applies only to the packets of the VPN instance. If no VPN instance is specified in an ACL rule, the rule applies only to the packets on the public network.

For more information about ACLs, see *ACL and QoS Configuration Guide.*

Examples

Use IPv4 basic ACL 2001 to allow only users from 10.10.0.0/16 to access the device through HTTP.

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 10.10.0.0 0.0.255.255
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] ip http acl 2001
```

Related commands

`acl` (*ACL and QoS Command Reference*)

ip http enable

Use **`ip http enable`** to enable the HTTP service.

Use **`undo ip http enable`** to disable the HTTP service.

Syntax

`ip http enable`

`undo ip http enable`

Default

The HTTP service is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

To allow users to access the device through HTTP, you must enable the HTTP service.

To improve device security, the system automatically enables the HTTPS service when you enable the HTTP service. When the HTTP service is enabled, you cannot disable the HTTPS service.

Examples

Enable the HTTP service.

```
<Sysname> system-view
[Sysname] ip http enable
```

Related commands

`ip https enable`

ip http port

Use **`ip http port`** to specify the HTTP service port number.

Use **undo ip http port** to restore the default.

Syntax

ip http port *port-number*

undo ip http port

Default

The HTTP service port number is 80.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

port-number: Specifies a port number in the range of 1 to 65535.

Usage guidelines

When the HTTP service is enabled, changing the HTTP service port number re-enables the HTTP service and closes all HTTP connections. To log in again, users must enter the new URL in the Web browser's address bar.

Examples

Set the HTTP service port number to 80.

```
<Sysname> system-view
[Sysname] ip http port 80
```

ip https acl

Use **ip https acl** to apply an ACL to the HTTPS service.

Use **undo ip https acl** to restore the default.

Syntax

ip https acl [**ipv6**] [**advanced**] { *acl-number* | **name** *acl-name* }

ip https acl mac { *acl-number* | **name** *acl-name* }

undo ip https acl [**ipv6**]

undo ip https acl mac

Default

No ACL is applied to the HTTPS service.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ipv6: Specifies an IPv6 ACL. If you do not specify this keyword, the command applies an IPv4 ACL to the HTTPS service.

advanced: Specifies an advanced ACL. If you do not specify this keyword, the command applies a basic ACL to the HTTPS service.

mac: Specifies a Layer 2 ACL.

acl-number: Specifies an ACL number in the range of 2000 to 4999.

- 2000 to 2999 for a basic ACL.
- 3000 to 3999 for an advanced ACL.
- 4000 to 4999 for a Layer 2 ACL.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters. It must start with an English letter and to avoid confusion, it cannot be **all**. The specified ACL takes effect only when the ACL exists.

Usage guidelines

To specify an IPv4 basic ACL, do not specify the **advanced** or **ipv6** keyword. To specify an IPv6 basic ACL, specify the **ipv6** keyword without the **advanced** keyword.

In an advanced ACL applied to the HTTPS service, only the following match criteria take effect:

- Source and destination IP addresses.
- Source and destination ports.
- Transport layer protocol.

In a Layer 2 ACL applied to the HTTPS service, only the source MAC address match criterion takes effect.

When no ACL is applied to the HTTPS service or the applied ACL does not exist or does not have rules, all clients can access the device through HTTPS. To control HTTPS access, specify an ACL that exists and has rules so only clients permitted by the ACL can access the device through HTTPS.

Because the device always uses HTTPS to transfer Web login requests, the ACL applied to the HTTPS service controls both HTTPS and HTTP logins. To access the device, HTTP clients must be permitted by the following ACLs:

- ACL applied to the HTTP service.
- ACL applied to the HTTPS service.

You can apply one IPv4 basic ACL and one IPv6 basic ACL to the HTTPS service, or apply one IPv4 advanced ACL and one IPv6 advanced ACL to the HTTPS service. If you execute this command multiple times for the same type of ACLs, the most recent configuration takes effect.

If a VPN instance is specified in an ACL rule, the rule applies only to the packets of the VPN instance. If no VPN instance is specified in an ACL rule, the rule applies only to the packets on the public network.

For more information about ACLs, see *ACL and QoS Configuration Guide.*

Examples

Use IPv4 basic ACL 2001 to allow only users from 10.10.0.0/16 to access the device through HTTPS or HTTP.

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 10.10.0.0 0.0.255.255
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] ip https acl 2001
```

Related commands

acl (*ACL and QoS Command Reference*)

ip https certificate access-control-policy

Use **ip https certificate access-control-policy** to apply a certificate-based access control policy to control HTTPS access.

Use **undo ip https certificate access-control-policy** to restore the default.

Syntax

ip https certificate access-control-policy *policy-name*

undo ip https certificate access-control-policy

Default

No certificate-based access control policy is applied for HTTPS access control.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies a certificate-based access control policy by its name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

For more information about the certificate-based access control policy, see PKI configuration in *Security Configuration Guide*.

Examples

Use certificate-based access control policy **myacl** to control HTTPS access.

```
<Sysname> system-view
[Sysname] ip https certificate access-control-policy myacl
```

Related commands

pki certificate access-control-policy (*Security Command Reference*)

ip https enable

Use **ip https enable** to enable the HTTPS service.

Use **undo ip https enable** to disable the HTTPS service.

Syntax

ip https enable

undo ip https enable

Default

The HTTPS service is enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

To allow users to access the device through HTTPS, you must enable the HTTPS service.

Enabling the HTTPS service triggers the SSL handshake negotiation process.

- If the device has a local certificate, the SSL handshake negotiation succeeds and the HTTPS service starts up.
- If the device does not have a local certificate, the certificate application process starts. Because the certificate application process takes a long time, the SSL handshake negotiation might fail and the HTTPS service might not be started. To solve the problem, execute this command again until the HTTPS service is enabled.

Examples

Enable the HTTPS service.

```
<Sysname> system-view
[Sysname] ip https enable
```

Related commands

ip https certificate access-control-policy

ip https ssl-server-policy

ip https port

Use **ip https port** to specify the HTTPS service port number.

Use **undo ip https port** to restore the default.

Syntax

ip https port *port-number*

undo ip https port

Default

The HTTPS service port number is 443.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

port-number: Specifies a port number in the range of 1 to 65535.

Usage guidelines

When the HTTPS service is enabled, changing the HTTPS service port number re-enables the HTTPS service and closes all HTTPS and HTTP connections. To log in again, users must enter the new URL in the Web browser's address bar.

Examples

Set the HTTPS service port number to 8080.

```
<Sysname> system-view
[Sysname] ip https port 8080
```

ip https ssl-server-policy

Use **ip https ssl-server-policy** to apply an SSL server policy to control HTTPS access.

Use **undo ip https ssl-server-policy** to restore the default.

Syntax

ip https ssl-server-policy *policy-name*

undo ip https ssl-server-policy

Default

No SSL server policy is applied. The HTTPS service uses a self-signed certificate.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies an SSL server policy name, a string of 1 to 31 characters.

Usage guidelines

If the HTTP service and HTTPS service are enabled, changes to the applied SSL server policy do not take effect. For the changes to take effect, you must disable HTTP and HTTPS, and then apply the policy and enable HTTP and HTTPS again.

To restore the default, you must disable HTTP and HTTPS, execute the **undo ip https ssl-server-policy** command, and then enable HTTP and HTTPS again.

Examples

Apply SSL server policy **myssl** to the HTTPS service.

```
<Sysname> system-view
[Sysname] ip https ssl-server-policy myssl
```

Related commands

ssl server-policy (*Security Command Reference*)

line

Use **line** to enter one or multiple user line views.

Syntax

line { *first-number1* [*last-number1*] | { **console** | **vty** } *first-number2* [*last-number2*] }

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

first-number1: Specifies the absolute number of the first user line. To view the value range for this argument, enter a question mark (?) in the place of this argument.

last-number1: Specifies the absolute number of the last user line. To view the value range for this argument, enter a question mark (?) in the place of this argument. This number must be greater than *first-number1*.

console: Specifies the console line.

vty: Specifies the VTY line.

first-number2: Specifies the relative number of the first user line. To view the value range for this argument, enter a question mark (?) in the place of this argument.

last-number2: Specifies the relative number of the last user line. To view the value range for this argument, enter a question mark (?) in the place of this argument. This number must be greater than *first-number2*.

Examples

Enter the view of VTY line 0.

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0]
```

Enter the views of VTY lines 0 to 63.

```
<Sysname> system-view
[Sysname] line vty 0 63
[Sysname-line-vty0-63]
```

Related commands

line class

line class

Use **line class** to enter user line class view.

Syntax

line class { **console** | **vty** }

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

console: Specifies the console line class view.

vty: Specifies the VTY line class view.

Usage guidelines

To configure the same settings for all user lines of a line class, use this command to enter the user line class view.

In user line class view, you can execute the following commands:

- **activation-key**
- **auto-execute command**
- **authentication-mode**
- **command accounting**
- **command authorization**
- **escape-key**
- **history-command max-size**
- **idle-timeout**
- **protocol inbound**
- **screen-length**
- **set authentication password**
- **shell**
- **terminal type**
- **user-role**

For commands that are available in both user line view and user line class view, the device uses the following rules to determine the settings to use:

- A setting in user line view applies only to the user line. A setting in user line class view applies to all user lines of the class.
- A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view.
- A setting in user line class view does not take effect on current online users. It takes effect only on new login users.

Examples

Set the CLI connection idle-timeout timer to 15 minutes in VTY line class view.

```
<Sysname> system-view
[Sysname] line class vty
[Sysname-line-class-vty] idle-timeout 15
```

In console line class view, configure the character **s** as the terminal session activation key.

```
<Sysname> system-view
[Sysname] line class console
[Sysname-line-class-console] activation-key s
[Sysname-line-class-console] quit
```

In the view of console line 0, restore the default terminal session activation key.

```
[Sysname] line console 0
[Sysname-line-console0] undo activation-key
```

Alternatively, you can use the following command:

```
[Sysname-line-console0] activation-key 13
```

To verify the configuration:

1. Exit the session on console line 0.
   ```
   [Sysname-line-console0] return
   <Sysname> quit
   ```
2. Log in again through the user line.
   The following message appears:
   ```
   Press ENTER to get started.
   ```
3. Press **Enter**.
   Pressing **Enter** does not start a session.
4. Enter **s**.
   A terminal session is started.
   ```
   <Sysname>
   ```

Related commands

line

lock

Use **lock** to lock the current user line and set the password for unlocking the line.

Syntax

lock

Default

The system does not lock any user lines.

Views

User view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command locks the current user line to prevent unauthorized users from using the line. You must set the password for unlocking the line as prompted. The user line is locked after you enter the password and confirm the password.

To unlock the user line, press **Enter** and enter the password you set.

Examples

Lock the current user line and set the password for unlocking the line.

```
<Sysname> lock
Please input password<1 to 16> to lock current line:
Password:
Again:

                    locked !
```

// The user line is locked. To unlock it, press **Enter** and enter the password:

```
Password:
<Sysname>
```

lock reauthentication

Use **lock reauthentication** to lock the current user line and enable unlocking authentication.

Syntax

lock reauthentication

Default

The system does not lock any user lines or initiate reauthentication.

Views

Any view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command locks the current user line. To unlock the user line, you must press **Enter** and provide the login password to pass reauthentication. If you have changed the login password after login, you must provide the new password. If no login password is set, the system unlocks the user line after you press **Enter**.

Examples

Lock the current user line and enable unlocking authentication.

```
<Sysname> lock reauthentication

Please press Enter to unlock the screen.
```

// The user line is locked. To unlock it, press **Enter** and enter the login password:

```
Password:

<Sysname>
```

Related commands

lock-key

lock-key

Use **lock-key** to set the user line locking key. Pressing this shortcut key locks the current user line and enables unlocking authentication.

Use **undo lock-key** to restore the default.

Syntax

lock-key *key-string*

undo lock-key

Default

No user line locking key is set.

Views

User line view

User line class view

Predefined user roles

network-admin

context-admin

Parameters

key-string: Specifies a shortcut key. It can be a character (case sensitive), or an ASCII code value in the range of 0 to 127. For example, if you use **lock-key 1**, the shortcut key is **Ctrl+A**. If you use **lock-key a**, the shortcut key is **a**. For information about ASCII code values of individual characters, see the standard ASCII code chart. For information about ASCII code values of combined keys that use the **Ctrl** key, see Table 1.

Usage guidelines

As a best practice, specify a combined key as the user line locking key. If you specify a single character as the key, the character acts only as the user line locking key. You cannot type the character for any commands, keywords, or arguments.

Pressing the user line locking key is equivalent to executing the **lock reauthentication** command.

This command takes effect immediately.

To display the current user line locking key, use the **display current-configuration | include lock-key** command.

Examples

Set the user line locking key to **Ctrl+A** for VTY line 0.

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] lock-key 1
[Sysname-line-vty0] quit
```

To verify the configuration:

1. Press **Ctrl+A**.

```
[Sysname]

Please press Enter to unlock the screen.
```

2. Press **Enter** and enter the login password.

```
Password:

[Sysname]
```

Related commands

lock reauthentication

parity

Use **parity** to specify the parity.

Use **undo parity** to restore the default.

Syntax

parity { **even** | **mark** | **none** | **odd** | **space** }

undo parity

Default

The setting is **none**. No parity is used.

Views

User line view

Predefined user roles

network-admin

context-admin

Parameters

even: Uses even parity.

mark: Uses mark parity.

none: Uses no parity.

odd: Uses odd parity.

space: Uses space parity.

Usage guidelines

This command is not supported in VTY line view.

The configuration terminal and the device must use the same parity.

Examples

Configure console line 0 to use odd parity.

```
<Sysname> system-view
[Sysname] line console 0
[Sysname-line-console0] parity odd
```

protocol inbound

Use **protocol inbound** to specify the supported protocols.

Use **undo protocol inbound** to restore the default.

Syntax

protocol inbound { **all** | **ssh** | **telnet** }

undo protocol inbound

Default

All of the protocols are supported.

Views

VTY line view

VTY line class view

Predefined user roles

network-admin

context-admin

Parameters

all: Supports both Telnet and SSH.

ssh: Supports SSH only.

telnet: Supports Telnet only.

Usage guidelines

Only users assigned the network-admin, context-admin, or level-15 user role can execute this command. Other users cannot execute this command, even if they are granted the right to execute this command.

A configuration change in user line view does not take effect on the current session. It takes effect on subsequent login sessions.

Before configuring a user line to support SSH, set the authentication mode to **scheme** for the user line.

In VTY line view, this command is associated with the **authentication-mode** command. If you specify a non-default value for one of the two commands, the other command uses the default setting, regardless of the setting in VTY line class view.

- If the settings of the two commands in VTY line view are both the default settings, the settings for the commands in VTY line class view take effect.
- If the settings of the two commands in VTY line view are both non-default settings, the non-default settings in VTY line view take effect.
- If only one command has a non-default setting in VTY line view, the other command uses the default setting, regardless of the setting in VTY line class view.

Examples

Enable user lines VTY 0 through VTY 4 to support only SSH.

```
<Sysname> system-view
[Sysname] line vty 0 4
[Sysname-line-vty0-4] authentication-mode scheme
[Sysname-line-vty0-4] protocol inbound ssh
```

Enable SSH support and set the authentication mode to scheme in VTY line class view. Enable user lines VTY 0 through VTY 4 to support all protocols and disable authentication for the user lines.

```
<Sysname> system-view
[Sysname] line class vty
[Sysname-line-class-vty] authentication-mode scheme
[Sysname-line-class-vty] protocol inbound ssh
[Sysname-line-class-vty] line vty 0 4
[Sysname-line-vty0-4] authentication-mode none
```

To verify the configuration:

1. Telnet to the device.

```
<Client> telnet 192.168.1.241
Trying 192.168.1.241 ...
Press CTRL+K to abort
Connected to 192.168.1.241 ...

******************************************************************************
* Copyright (c) 2004-2017 NSFOCUS. All rights reserved.                      *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

<Server>
```

You are logged in without authentication.

2. Display online CLI user information.

```
<Server> display users
  Idx  Line     Idle       Time              Pid     Type
+ 50   VTY 0    00:00:00   Jan 17 15:29:27   189     TEL

Following are more details.
VTY 0   :
        Location: 192.168.1.186
 +    : Current operation user.
 F    : Current operation user works in async mode.
```

The output shows that you are using VTY 0. The configuration in user line view is effective.

Related commands

authentication-mode

restful http enable

Use **restful http enable** to enable RESTful access over HTTP.

Use **undo restful http enable** to disable RESTful access over HTTP.

Syntax

restful http enable

undo restful http enable

Default

RESTful access over HTTP is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

For users to access the device through the HTTP-based RESTful API, you must enable RESTful access over HTTP.

Examples

Enable RESTful access over HTTP.

```
<Sysname> system-view
[Sysname] restful http enable
```

restful http port

Use **restful http port** to specify the service port number for RESTful access over HTTP.

Use **undo restful http port** to restore the default.

Syntax

restful http port *port-number*

undo restful http port

Default

The service port number for RESTful access over HTTP is 80.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

port-number: Specifies a port number in the range of 1 to 65535.

Usage guidelines

When RESTful access over HTTP is enabled, changing the service port number re-enables the service and closes all RESTful access over HTTP connections. To log in again, users must use the new port number.

Examples

Set the service port number to 1000 for RESTful access over HTTP.

```
<Sysname> system-view
[Sysname] restful http port 1000
```

restful https enable

Use **restful https enable** to enable RESTful access over HTTPS.

Use **undo restful https enable** to disable RESTful access over HTTPS.

Syntax

restful https enable

undo restful https enable

Default

RESTful access over HTTPS is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

For users to access the device through the HTTPS-based RESTful API, you must enable RESTful access over HTTPS.

Examples

Enable RESTful access over HTTPS.

```
<Sysname> system-view
[Sysname] restful https enable
```

restful https port

Use **restful https port** to specify the service port number for RESTful access over HTTPS.

Use **undo restful https port** to restore the default.

Syntax

restful https port *port-number*

undo restful https port

Default

The service port number for RESTful access over HTTPS is 443.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

port-number: Specifies a port number in the range of 1 to 65535.

Usage guidelines

When RESTful access over HTTPS is enabled, changing the service port number re-enables the service and closes all RESTful access over HTTPS connections. To log in again, users must use the new port number.

Examples

Set the service port number to 1000 for RESTful access over HTTPS.

```
<Sysname> system-view
[Sysname] restful https port 1000
```

restful https ssl-server-policy

Use **restful https ssl-server-policy** to apply an SSL server policy to the RESTful access over HTTPS service.

Use **undo restful https ssl-server-policy** to restore the default.

Syntax

restful https ssl-server-policy *policy-name*

undo restful https ssl-server-policy

Default

No SSL server policy is applied to the RESTful access over HTTPS service.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies an SSL server policy name, a string of 1 to 31 characters.

Usage guidelines

The RESTful access over HTTPS service will use the SSL server policy to enhance service security. For more information about SSL server policies, see SSL configuration in *Security Configuration Guide*.

You can use this command only when RESTful access over HTTPS is disabled.

This command takes effect after you enable RESTful access over HTTPS.

If you execute this command multiple times, the most recent configuration takes effect.

After the RESTful access over HTTPS service is enabled, changes to the applied SSL server policy take effect only on HTTPS connections established after the changes. These changes do not take effect on existing HTTPS connections.

Examples

Apply SSL server policy **myssl** to the RESTful access over HTTPS service.

```
<Sysname> system-view
[Sysname] restful https ssl-server-policy myssl
```

Related commands

restful https enable

ssl server-policy (*Security Command Reference*)

screen-length

Use **screen-length** to set the maximum number of lines of command output to send to the terminal at a time when the screen pausing feature is enabled.

Use **undo screen-length** to restore the default.

Syntax

screen-length *screen-length*

undo screen-length

Default

A maximum of 24 lines are sent.

Views

User line view

User line class view

Predefined user roles

network-admin

context-admin

Parameters

screen-length: Specifies the maximum number of lines to send, in the range of 0 to 512. To send command output without pausing, set the number to 0 or execute the **screen-length disable** command.

Usage guidelines

The number of lines that can be displayed on the terminal screen is restricted by both this setting and the display specification of the terminal. For example, if this setting is 40, the device sends 40 lines to the terminal at a time. If the terminal display specification is 24 lines, only the last 24 lines are displayed on the terminal screen. To view the previous 16 lines, you must press **PgUp**.

To continue to display command output after a pause, press the space bar.

By default, pausing between screens of output is enabled.

This command is available in both user line view and user line class view. A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view.

The setting in user line view takes effect immediately on the current session. The setting in user line class view takes effect on login sessions that are established after the setting is configured.

Examples

Set the maximum number of lines to send at a time to 30 for VTY line 0.

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] screen-length 30
```

Related commands

screen-length disable

send

Use **send** to send messages to online login users.

Syntax

send { **all** | *number1* | { **console** | **vty** } *number2* }

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

all: Specifies all user lines.

number1: Specifies the absolute number of a user line. To view the value range for this argument, enter a question mark (?) in the place of this argument.

console: Specifies the console line.

vty: Specifies the VTY line.

number2: Specifies the relative number of a user line. To view the value range for this argument, enter a question mark (?) in the place of this argument.

Usage guidelines

You can use this command to send notifications to online users before performing an operation that might affect other online users, for example, before rebooting the device.

To end a message, press **Enter**. To abort the send operation, press **Ctrl+C**.

Examples

Send a notification to the user on VTY 1.

```
<Sysname> send vty 1
Input message, end with Enter; abort with CTRL+C:
Your attention, please. I will reboot the system in 3 minutes.
Send message? [Y/N]:y
```

The message should appear on the user's terminal screen as follows:

```
[Sysname]

***
***
***Message from vty0 to vty1
***
Your attention, please. I will reboot the system in 3 minutes.
```

set authentication password

Use **set authentication password** to set the password for local password authentication.

Use **undo set authentication password** to restore the default.

Syntax

set authentication password { **hash** | **simple** } *string*

undo set authentication password

Default

No password is set for local password authentication.

Views

User line view

User line class view

Predefined user roles

network-admin

context-admin

Parameters

hash: Specifies a password in hashed form.

simple: Sets a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in hashed form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 4 to 16 characters and must contain a minimum of two character types. Its hashed form is a case-sensitive string of 1 to 110 characters.

Usage guidelines

Only users assigned the network-admin, context-admin, or level-15 user role can execute this command. Other users cannot execute this command, even if they are granted the right to execute this command.

This command is available in both user line view and user line class view. A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view.

A password change does not take effect on the current session. It takes effect on subsequent login sessions.

Examples

Set the password to **hello12345** for local password authentication on VTY line 0.

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] authentication-mode password
[Sysname-line-vty0] set authentication password simple hello12345
```

Related commands

authentication-mode

shell

Use **shell** to enable the terminal service for user lines.

Use **undo shell** to disable the terminal service for user lines.

Syntax

shell

undo shell

Default

The terminal service is enabled on all user lines.

Views

User line view

User line class view

Predefined user roles

network-admin

context-admin

Usage guidelines

The **undo shell** command is not supported in console line view or console line class view.

You cannot disable the terminal service on the user line you are using.

When the device acts as a Telnet or SSH server, you cannot use the **undo shell** command.

If the **undo shell** command is used in user line class view, you cannot use the **shell** command in the view of a user line in the class.

Examples

Disable the terminal service for VTY lines VTY 0 through 4 so no user can log in to the device through the user lines.

```
<Sysname> system-view
[Sysname] line vty 0 4
[Sysname-line-vty0-4] undo shell
Disable ui-vty0-4 , are you sure? [Y/N]:y
[Sysname-line-vty0-4]
```

speed

Use **speed** to set the transmission rate (also called the baud rate) on a user line.

Use **undo speed** to restore the default.

Syntax

speed *speed-value*

undo speed

Default

The transmission rate is 9600 bps on a user line.

Views

User line view

Predefined user roles

network-admin

context-admin

Parameters

speed-value: Specifies the transmission rate in bps. Supported transmission rates depend on the network environment. The transmission rates for asynchronous serial interfaces might include:

- 300 bps.
- 600 bps.
- 1200 bps.
- 2400 bps.
- 4800 bps.
- 9600 bps.
- 19200 bps.
- 38400 bps.
- 57600 bps.
- 115200 bps.

Usage guidelines

This command is not supported in VTY line view.

The configuration terminal and the device must be configured with the same transmission rate to communicate.

Examples

Set the transmission rate to 19200 bps for console line 0.

```
<Sysname> system-view
[Sysname] line console 0
[Sysname-line-console0] speed 19200
```

stopbits

Use **stopbits** to specify the number of stop bits for a character.

Use **undo stopbits** to restore the default.

Syntax

stopbits { **1** | **1.5** | **2** }

undo stopbits

Default

One stop bit is used.

Views

User line view

Predefined user roles

network-admin

context-admin

Parameters

1: Uses one stop bit.

1.5: Uses one and a half stop bits. The device does not support using one and a half stop bits. If you specify this keyword, two stop bits are used.

2: Uses two stop bits.

Usage guidelines

This command is not supported in VTY line view.

The configuration terminal and the device must use the same number of stop bits to communicate.

Examples

Set the number of stop bits to 1 for console line 0.

```
<Sysname> system-view
[Sysname] line console 0
[Sysname-line-console0] stopbits 1
```

telnet

Use **telnet** to Telnet to a host in an IPv4 network.

Syntax

telnet *remote-host* [*service-port*] [**vpn-instance** *vpn-instance-name*] [**source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] [**dscp** *dscp-value*] [**escape** *character*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

remote-host: Specifies the IPv4 address or host name of a remote host. A host name can be a case-insensitive string of 1 to 253 characters. Valid characters include letters, digits, hyphens (-), underscores (_), and dots (.).

service-port: Specifies the TCP port number for the Telnet service on the remote host. The value range is 0 to 65535 and the default is 23.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the remote host belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the remote host belongs to the public network, do not specify this option.

source: Specifies a source IPv4 address or source interface for outgoing Telnet packets. If you do not specify this option, the device uses the primary IPv4 address of the output interface for the route to the server as the source address.

interface *interface-type interface-number*: Specifies the source interface. The primary IPv4 address of the interface will be used as the source IPv4 address for outgoing Telnet packets.

ip *ip-address*: Specifies the source IPv4 address for outgoing Telnet packets.

dscp *dscp-value*: Specifies a DSCP value for outgoing Telnet packets. The value range is 0 to 63. The default is 48.

escape *character*: Specifies an escape character. You can use the escape character together with a dot (.) as the escape key to terminate the current Telnet connection and return to the upper level connection. The value for the *character* argument is case sensitive and must be different from the login username. As a best practice, specify a tilde (~) for the *character* argument.

Usage guidelines

Methods for terminating Telnet connections include:

- Pressing **Ctrl+K**—Terminates all Telnet connections. You can use this method in any scenarios unless you configure an escape character. After you configure an escape character, pressing **Ctrl+K** does not terminate Telnet connections.
- Executing the **quit** command—Terminates the current Telnet connection and returns to the upper level connection. This method is not available when the Telnet server reboots or fails.
- Using the escape key—Terminates the current Telnet connection and returns to the upper level connection. You can use this method in any scenarios.

To use the escape key to terminate the current Telnet connection, enter the escape character and a dot in a new line. If you enter any other characters or perform any other operations (for example, pressing the backspace key) before entering the escape character, the escape character does not take effect.

The source address or interface specified by this command is applied only to the Telnet connection that is being established.

Examples

Telnet to host 1.1.1.2, using 1.1.1.1 as the source IP address for outgoing Telnet packets.

```
<Sysname> telnet 1.1.1.2 source ip 1.1.1.1
```

Related commands

telnet client source

telnet client source

Use **telnet client source** to specify a source IPv4 address or source interface for the Telnet client to use for outgoing Telnet packets.

Use **undo telnet client source** to restore the default.

Syntax

telnet client source { **interface** *interface-type interface-number* | **ip** *ip-address* }

undo telnet client source

Default

No source IPv4 address or source interface is specified. The Telnet client uses the primary IPv4 address of the output interface for the route to the server as the source IPv4 address.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interface *interface-type interface-number*: Specifies a source interface. The primary IPv4 address of the interface will be used as the source IPv4 address for outgoing Telnet packets.

ip *ip-address*: Specifies a source IPv4 address.

Usage guidelines

The setting configured by this command applies to all Telnet connections but has a lower precedence than the source setting specified for the **telnet** command.

Examples

Set the source IPv4 address to 1.1.1.1 for outgoing Telnet packets.

```
<Sysname> system-view
[Sysname] telnet client source ip 1.1.1.1
```

Related commands

display telnet client

telnet ipv6

Use **telnet ipv6** to Telnet to a host in an IPv6 network.

Syntax

telnet ipv6 *remote-host* [**-i** *interface-type interface-number*] [*port-number*] [**vpn-instance** *vpn-instance-name*] [**source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] [**dscp** *dscp-value*] [**escape** *character*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

remote-host: Specifies the IPv6 address or host name of a remote host. A host name can be a case-insensitive string of 1 to 253 characters. Valid characters include letters, digits, hyphens (-), underscores (_), and dots (.).

-i *interface-type interface-number*: Specifies the interface for sending Telnet packets. This option is required when the remote host address is a link-local address. When the server address is a global unicast address, you cannot specify this option.

port-number: Specifies the TCP port number for the Telnet service on the remote host. The value range is 0 to 65535 and the default is 23.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the remote host belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the remote host belongs to the public network, do not specify this option.

source: Specifies a source IPv6 address or source interface for outgoing Telnet packets. If you do not specify this option, the device uses the primary IPv6 address of the output interface for the route to the server as the source address.

interface *interface-type interface-number*: Specifies the source interface. The primary IPv6 address of the interface will be used as the source IPv6 address for outgoing Telnet packets.

ipv6 *ipv6-address*: Specifies the source IPv6 address for outgoing Telnet packets.

dscp *dscp-value*: Specifies a DSCP value for outgoing Telnet packets. The value range is 0 to 63. The default is 48.

escape *character*: Specifies an escape character. You can use the escape character together with a dot (.) as the escape key to terminate the current Telnet connection and return to the upper level connection. The value for the *character* argument is case sensitive and must be different from the login username. As a best practice, specify a tilde (~) for the *character* argument.

Usage guidelines

Methods for terminating Telnet connections include:

- Pressing **Ctrl+K**—Terminates all Telnet connections. You can use this method in any scenarios unless you configure an escape character. After you configure an escape character, pressing **Ctrl+K** does not terminate Telnet connections.
- Executing the **quit** command—Terminates the current Telnet connection and returns to the upper level connection. This method is not available when the Telnet server reboots or fails.
- Using the escape key—Terminates the current Telnet connection and returns to the upper level connection. You can use this method in any scenarios.

To use the escape key to terminate the current Telnet connection, enter the escape character and a dot in a new line. If you enter any other characters or perform any other operations (for example, pressing the backspace key) before entering the escape character, the escape character does not take effect.

Examples

Telnet to the host at 5000::1.

```
<Sysname> telnet ipv6 5000::1
```

Telnet to the host at 2000::1. Use 1000::1 as the source address for outgoing Telnet packets.

```
<Sysname> telnet ipv6 2000::1 source ipv6 1000::1
```

telnet server acl

Use **telnet server acl** to apply an ACL to filter Telnet logins.

Use **undo telnet server acl** to restore the default.

Syntax

telnet server acl [**mac**] *acl-number*

undo telnet server acl

Default

No ACL is used to filter Telnet logins.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

mac: Specifies a Layer 2 ACL. To specify an ACL of a different type, do not specify this keyword.

acl-number: Specifies an ACL by its number. If you specify the **mac** keyword, the value range of this argument is 4000 to 4999. If you do not specify the **mac** keyword, the value range of this argument is 2000 to 3999.

Usage guidelines

When no ACL is applied to the Telnet service, all users can Telnet to the device. To control Telnet logins, specify an ACL that exists and has rules so only users permitted by the ACL can Telnet to the device. If you specify an ACL that does not exist or does not have rules, no users can Telnet to the device.

If a VPN instance is specified in an ACL rule, the rule applies only to the packets of the VPN instance. If no VPN instance is specified in an ACL rule, the rule applies only to the packets on the public network.

For more information about ACLs, see *ACL and QoS Configuration Guide*.

If you execute this command multiple times, the most recent configuration takes effect.

This command does not take effect on existing Telnet connections.

Examples

Permit only the user at 1.1.1.1 to Telnet to the device.

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] telnet server acl 2001
```

telnet server acl-deny-log enable

Use **telnet server acl-deny-log enable** to enable logging for Telnet login attempts that are denied by the Telnet login control ACL.

Use **undo telnet server acl-deny-log enable** to disable logging for Telnet login attempts that are denied by the Telnet login control ACL.

Syntax

telnet server acl-deny-log enable

undo telnet server acl-deny-log enable

Default

Logging is disabled for Telnet login attempts that are denied by the Telnet login control ACL.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

Only clients permitted by the Telnet login control ACL can Telnet to the device. This logging feature generates log messages for Telnet login attempts that are denied by the Telnet login control ACL.

For information about log message output, see the information center in *Network Management and Monitoring Configuration Guide*. For information about configuring a Telnet login control ACL, see the **telnet server acl** or **telnet server ipv6 acl** command.

Examples

Enable logging for Telnet login attempts that are denied by the Telnet login control ACL.

```
<Sysname> system-view
[Sysname] telnet server acl-deny-log enable
```

Related commands

telnet server acl

telnet server ipv6 acl

telnet server dscp

Use **telnet server dscp** to specify the DSCP value for IPv4 to use for Telnet packets sent to a Telnet client.

Use **undo telnet server dscp** to restore the default.

Syntax

telnet server dscp *dscp-value*

undo telnet server dscp

Default

IPv4 uses the DSCP value 48 for Telnet packets sent to a Telnet client.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

dscp-value: Specifies a DSCP value in the range of 0 to 63.

Usage guidelines

The DSCP value is carried in the ToS field of an IPv4 packet to indicate the packet transmission priority.

Examples

Set the DSCP value for IPv4 to use for outgoing Telnet packets to 30 on a Telnet server.

```
<Sysname> system-view
[Sysname] telnet server dscp 30
```

telnet server enable

Use **telnet server enable** to enable the Telnet server.

Use **undo telnet server enable** to disable the Telnet server.

Syntax

telnet server enable

undo telnet server enable

Default

The Telnet server is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

Users can Telnet to the device only when the Telnet server is enabled.

Examples

Enable the Telnet server.

```
<Sysname> system-view
[Sysname] telnet server enable
```

telnet server ipv6 acl

Use **telnet server ipv6 acl** to apply an IPv6 ACL to filter IPv6 Telnet logins.

Use **undo telnet server ipv6 acl** to restore the default.

Syntax

telnet server ipv6 acl { **ipv6** | **mac** } *acl-number*

undo telnet server ipv6 acl

Default

No IPv6 ACL is used to filter IPv6 Telnet logins.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ipv6: Specifies an IPv6 ACL.

mac: Specifies a Layer 2 ACL. To specify an ACL of a different type, do not specify this keyword.

acl-number: Specifies an ACL by its number. If you specify the **ipv6** keyword, the value range of this argument is 2000 to 3999. If you specify the **mac** keyword, the value range of this argument is 4000 to 4999.

Usage guidelines

When no ACL is applied to the Telnet service, all users can Telnet to the device. To control Telnet logins, specify an ACL that exists and has rules so only users permitted by the ACL can Telnet to the device. If you specify an ACL that does not exist or does not have rules, no users can Telnet to the device.

If a VPN instance is specified in an ACL rule, the rule applies only to the packets of the VPN instance. If no VPN instance is specified in an ACL rule, the rule applies only to the packets on the public network.

For more information about ACLs, see *ACL and QoS Configuration Guide*.

If you execute this command multiple times, the most recent configuration takes effect.

This command does not take effect on existing Telnet connections.

Examples

Permit only the user at 2000::1 to Telnet to the device.

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2001
[Sysname-acl6-ipv6-basic-2001] rule permit source 2000::1 128
[Sysname-acl6-ipv6-basic-2001] quit
[Sysname] telnet server ipv6 acl ipv6 2001
```

telnet server ipv6 dscp

Use **telnet server ipv6 dscp** to specify the DSCP value for IPv6 to use for Telnet packets sent to a Telnet client.

Use **undo telnet server ipv6 dscp** to restore the default.

Syntax

telnet server ipv6 dscp *dscp-value*

undo telnet server ipv6 dscp

Default

IPv6 uses the DSCP value 48 for Telnet packets sent to a Telnet client.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

dscp-value: Specifies a DSCP value in the range of 0 to 63.

Usage guidelines

The DSCP value is carried in the Traffic class field of an IPv6 packet to indicate the packet transmission priority.

Examples

Set the DSCP value for IPv6 to use for outgoing Telnet packets to 30 on a Telnet server.

```
<Sysname> system-view
[Sysname] telnet server ipv6 dscp 30
```

telnet server ipv6 port

Use **telnet server ipv6 port** to specify the IPv6 Telnet service port number.

Use **undo telnet server ipv6 port** to restore the default.

Syntax

telnet server ipv6 port *port-number*

undo telnet server ipv6 port

Default

The IPv6 Telnet service port number is 23.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

port-number: Specifies a port number. The value can be 23 or in the range of 1025 to 65535.

Usage guidelines

This command terminates all existing Telnet connections to the IPv6 Telnet server. To use the Telnet service, users must reestablish Telnet connections.

Examples

Set the IPv6 Telnet service port number to 1026.

```
<Sysname> system-view
[Sysname] telnet server ipv6 port 1026
```

telnet server port

Use **telnet server port** to specify the IPv4 Telnet service port number.

Use **undo telnet server port** to restore the default.

Syntax

telnet server port *port-number*

undo telnet server port

Default

The IPv4 Telnet service port number is 23.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

port-number: Specifies a port number. The value can be 23 or in the range of 1025 to 65535.

Usage guidelines

This command terminates all existing Telnet connections to the IPv4 Telnet server. To use the Telnet service, users must reestablish Telnet connections.

Examples

Set the IPv4 Telnet service port number to 1025.

```
<Sysname> system-view
[Sysname] telnet server port 1025
```

terminal type

Use **terminal type** to specify the terminal display type.

Use **undo terminal type** to restore the default.

Syntax

terminal type { **ansi** | **vt100** }

undo terminal type

Default

The terminal display type is ANSI.

Views

User line view

User line class view

Predefined user roles

network-admin

context-admin

Parameters

ansi: Specifies the ANSI type.

vt100: Specifies the VT100 type.

Usage guidelines

The device supports two terminal display types: ANSI and VT100. As a best practice, specify the VT100 type on both the device and the configuration terminal. If either side uses the ANSI type, a display problem might occur when a command line has more than 80 characters. For example, a cursor positioning error might occur.

This command is available in both user line view and user line class view. A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view.

A terminal display type change does not take effect on the current session. It takes effect on subsequent login sessions.

Examples

Set the terminal display type to VT100.

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] terminal type vt100
```

user-interface

Use **user-interface** to enter one or multiple user line views.

Syntax

user-interface { *first-number1* [*last-number1*] | { **console** | **vty** } *first-number2* [*last-number2*] }

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

first-number1: Specifies the absolute number of the first user line. To view the value range for this argument, enter a question mark (?) in the place of this argument.

last-number1: Specifies the absolute number of the last user line. To view the value range for this argument, enter a question mark (?) in the place of this argument. This number must be greater than *first-number1*.

console: Specifies the console line.

vty: Specifies the VTY line.

first-number2: Specifies the relative number of the first user line. To view the value range for this argument, enter a question mark (?) in the place of this argument.

last-number2: Specifies the relative number of the last user line. To view the value range for this argument, enter a question mark (?) in the place of this argument. This number must be greater than *first-number2*.

Usage guidelines

This command is an older version reserved for backward compatibility purposes. It has the same functionality and output as the **line** command. As a best practice, use the **line** command.

To configure settings for a single user line, use this command to enter the user line view.

To configure the same settings for multiple user lines, use this command to enter multiple user line views.

Examples

Enter the view of console line 0.

```
<Sysname> system-view
[Sysname] user-interface console 0
[Sysname-line-console0]
```

Enter the views of VTY lines 0 to 4.

```
<Sysname> system-view
[Sysname] user-interface vty 0 4
```

```
[Sysname-line-vty0-4]
```

Related commands

user-interface class

user-interface class

Use **user-interface class** to enter user line class view.

Syntax

user-interface class { **console** | **vty** }

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

console: Specifies the console line class view.

vty: Specifies the VTY line class view.

Usage guidelines

This command is an older version reserved for backward compatibility purposes. It has the same functionality and output as the **line class** command. As a best practice, use the **line class** command.

To configure the same settings for all user lines of a line class, you can use this command to enter the user line class view.

The following commands are available in user line class view:

- **activation-key**
- **auto-execute command**
- **authentication-mode**
- **command accounting**
- **command authorization**
- **escape-key**
- **history-command max-size**
- **idle-timeout**
- **protocol inbound**
- **screen-length**
- **set authentication password**
- **shell**
- **terminal type**
- **user-role**

For commands that are available in both user line view and user line class view, the device uses the following rules to determine the settings to use:

- A setting in user line view applies only to the user line. A setting in user line class view applies to all user lines of the class.
- A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view.
- A setting in user line class view does not take effect on current online users. It takes effect only on new login users.

Examples

Set the CLI connection idle-timeout timer to 15 minutes in VTY line class view.

```
<Sysname> system-view
[Sysname] user-interface class vty
[Sysname-line-class-vty] idle-timeout 15
```

In console line class view, configure character **s** as the terminal session activation key.

```
<Sysname> system-view
[Sysname] user-interface class console
[Sysname-line-class-console] activation-key s
[Sysname-line-class-console] quit
```

In the view of console line 0, restore the default terminal session activation key.

```
[Sysname] user-interface console 0
[Sysname-line-console0] undo activation-key
```

Alternatively, you can use the following command:

```
[Sysname-line-console0] activation-key 13
```

To verify the configuration:

1. Exit the session on console line 0.

   ```
   [Sysname-line-console0] return
   <Sysname> quit
   ```

2. Log in again through the console line.

   The following message appears:

   ```
   Press ENTER to get started.
   ```

3. Press **Enter**.

   Pressing **Enter** does not start a session.

4. Enter **s**.

   A terminal session is started.

   ```
   <Sysname>
   ```

Related commands

user-interface

user-role

Use **user-role** to assign a user role to a user line. The device assigns the user role to a user of the line when the user logs in.

Use **undo user-role** to remove a user role or restore the default.

Syntax

user-role *role-name*

undo user-role [*role-name*]

Default

A console user of the default context is assigned the **network-admin** user role. Other users on the default context are assigned the **network-operator** user role. A user on a non-default context is assigned the **context-operator** user role.

Views

User line view

User line class view

Predefined user roles

network-admin

context-admin

Parameters

role-name: Specifies a user role name, a case-sensitive string of 1 to 63 characters. The user role can be user-defined or predefined. Available predefined user roles include network-admin, network-operator, context-admin, context-operator,and level-0 to level-15. The predefined security-audit and guest-manager user roles are not supported in user line view or user line class view. If you do not specify this argument, the **undo user-role** command restores the default user roles.

Usage guidelines

Only users assigned the network-admin, context-admin, or level-15 user role can execute this command. Other users cannot execute this command, even if they are granted the right to execute this command.

This command is available in both user line view and user line class view. A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view.

A user role change does not take effect on the current session. It takes effect on subsequent login sessions.

You can assign up to 64 user roles to a user line.

For more information about user roles, see RBAC configuration in *Fundamentals Configuration Guide*.

Examples

Assign user role network-admin to VTY line 0 to 63.

```
<Sysname> system-view
[Sysname] line vty 0 63
[Sysname-line-vty0-63] user-role network-admin
```

web captcha

Use **web captcha** to specify a fixed verification code for Web login.

Use **undo web captcha** to restore the default.

Syntax

web captcha *verification-code*

undo web captcha

Default

No fixed verification code is specified for Web login. A Web user must enter the verification code displayed on the login page.

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

verification-code: Specifies the fixed verification code, a case-sensitive 4-character string.

Usage guidelines

In test environments where a script is used for Web function tests, you can configure a fixed verification code to improve test efficiency.

For Web access security purposes, do not use this feature in production environments.

If you execute the **web captcha** command multiple times, the most recent configuration takes effect.

This command is not saved to the configuration file and will not take effect after a reboot.

Examples

Set the fixed verification code to **test** for Web login.

```
<Sysname> web captcha test
```

web https-authorization mode

Use **web https-authorization mode** to set the authentication and authorization mode for HTTPS login.

Use **undo web https-authorization mode** to restore the default.

Syntax

web https-authorization mode { **auto** | **certificate** | **certificate-manual** | **manual** }

undo web https-authorization mode

Default

Manual mode is used for HTTPS login authentication and authorization.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

auto: Requires the user to provide a username and password or a certificate for authentication and authorization

certificate: Requires the user to provide a certificate for authentication and authorization.

certificate-manual: Requires the user to provide a username and password as well as a certificate for authentication and authorization.

manual: Requires the user to provide a username and password for authentication and authorization.

Usage guidelines

For a user to use a certificate for HTTPS login authentication and authorization, perform the following tasks:

- Apply an SSL server policy to the HTTPS service and enable client authentication in the policy so the SSL server performs certificate-based authentication.
- Specify the certificate field to be used as the username for certificate-based authentication, and create a local user that uses the same username.

During HTTPS connection establishment, a user must select the correct certificate.

Examples

Set the HTTPS login authentication and authorization mode to **certificate**.

```
<Sysname> system-view
[Sysname] web https-authorization mode certificate
```

Related commands

web https-authorization username

web https-authorization username

Use **web https-authorization username** to specify the certificate field to be used as the username for certificate-based authentication.

Use **undo web https-authorization username** to restore the default.

Syntax

web https-authorization username { **cn** | **email-prefix** | **oid** *oid-value* }

undo web https-authorization username

Default

The CN field in the certificate is used as the username for certificate-based authentication.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

cn: Uses the CN field in the certificate as the username.

email-prefix: Uses the string before the @ sign in the emailAddress field of the certificate as the username.

oid *oid-value*: Uses the field corresponding to an OID as the username. The *oid-value* argument is a dotted decimal string of 1 to 255 characters.

Usage guidelines

This command is required when the authentication and authorization mode for HTTPS login is certificate or auto.

Examples

Specify the field corresponding to an OID as the username for certificate-based authentication.

```
<Sysname> system-view
[Sysname] web https-authorization username oid 1.2.840.113549.1.9.1
```

Related commands

web https-authorization mode

web idle-timeout

Use **web idle-timeout** to set the Web connection idle-timeout timer.

Use **undo web idle-timeout** to restore the default.

Syntax

web idle-timeout *idle-time*

undo web idle-timeout

Default

The Web connection idle-timeout timer is 10 minutes.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

idle-time: Specifies the Web connection idle-timeout timer in minutes. The value range is 1 to 999.

Usage guidelines

The system automatically terminates a Web user connection if no mouse or keyboard operation occurs within the idle-timeout interval.

This command takes effect immediately on current Web connections.

Examples

Set the Web connection idle-timeout timer to 100 minutes.

```
<Sysname> system-view
[Sysname] web idle-timeout 100
```

Contents

License management commands

All commands in this chapter are supported only on the default context. Features licensed to the default context are also licensed to non-default contexts. For information about contexts, see *Virtual Technologies Configuration Guide*.

display license

Use **display license** to display detailed license information.

Syntax

display license [**activation-file**] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

activation-file: Displays license information about activation files.

slot *slot-number*: Specifies the member ID of an IRF member device. If no member device is specified, this command displays license information for all IRF member devices.

Usage guidelines

If you do not specify any parameters, this command displays detailed information about all licenses.

Examples

Display detailed information about all licenses.

```
<Sysname> display license
Slot 1:
flash:/license/NGFirewall20171114195245137 53.ak
Feature: IPS
Product Description: Trial IPS License, 30 Days
Registered at: 2017-11-14 20:07:06
License Type: Trial (date restricted)
Trial Validity Period: 2017-11-14 to 2017-12-14
Current State: Expired
```

Table 1 Command output

Field	Description
Feature	Feature name.
Product Description	License description.
Registered at	Time when the license was installed.
License Type	License type by validity period:

Field	Description
	• **NA**—The system cannot obtain the license type. • **Permanent**—Purchased license that never expires and is always valid. • **Days restricted**—Purchased license that is valid for a period of days, for example, 30 days. • **Trial (days restricted)**—Free trial license that is valid for a period of days.
Time Left (days)	Remaining days of the license. This field is available for a purchased license.
Trial Time Left (days)	Remaining days of the trial period. This field is available for a trial license.

Current State	State of the license:
	• **In use**—The license is being used.
	• **Usable**—The license is available for use.
	  ○ If multiple days-restricted licenses for one feature are installed, only one license is in **In use** state and the rest licenses are in **Usable** state.
	  ○ A date restricted license is in this state if its start date is not reached.
	• **Expired**—The license has expired.
	• **Uninstalled**—The license has been uninstalled.
	• **Unusable**—The license cannot be used.
	• **Invalid**—The license is invalid and cannot be used.

Uninstall Key	This field is available for licenses that have been uninstalled.
Uninstall Date	Date when the activation file was uninstalled.

display license device-id

Use **`display license device-id`** to display SN and DID information.

Syntax

`display license device-id slot` *`slot-number`*

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

`slot` *`slot-number`*: Specifies the member ID of an IRF member device.

Usage guidelines

When you register a license for a device, you must provide its unique SN and DID.

The DID changes each time you use the **`license compress`** command to compress the license storage. Use the **`display license device-id`** command to identify the up-to-date DID each time you register licenses.

Examples

Display the SN and DID for the specified slot.

```
<Sysname> display license device-id slot 1
```

```
SN: 210235A1FXH164000026
Device ID: flash:/license/210235A1FXH164000026.did
```

display license feature

Use **display license feature** to display brief license information for features.

Syntax

display license feature

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display brief feature license information.

```
<Sysname> display license feature
Slot 1:
Total: 32  Usage: 0
Feature                        Licensed        State
ACG                            N               -
AV                             N               -
IPRPT                          N               -
IPS                            N               -
SSLVPN                         N               -
UFLT                           N               -
```

Table 2 Command output

Field	Description
Total	Total number of licenses that can be installed.
Usage	Number of licenses stored in the license storage.
Feature	Feature that must be licensed before being used.
Licensed	Licensing state of the feature: • **N**—Not licensed. • **Y**—Licensed.
State	License type by purchasing state: • **Formal**—Purchased license. • **Trial**—Trial license. • **Pre-licensed**—Preinstalled license. If the feature is not licensed, this field displays a hyphen (-). To use the feature, you must install a valid license file.

license activation-file install

Use **license activation-file install** to install an activation file.

Syntax

license activation-file install *license-file* **slot** *slot-number*

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

license-file: Specifies the path of an activation file, a case-sensitive string of 1 to 127 characters. The activation file must be valid and stored on the device.

slot *slot-number*: Specifies the member ID of an IRF member device.

Usage guidelines

To install a license activation file successfully, make sure the SN and DID used for registering the feature license matches the current SN and DID of the device.

Activation files are device locked. A licensed feature can run on the IRF member device where its activation file is installed even after the member device is moved from one IRF fabric to another IRF fabric.

Examples

Install activation file package 20170101.tar.

```
<Sysname> system-view
[Sysname] license activation-file install flash:/license/20170101.tar
This operation might take some time. Do not perform any other operations until the operation
is completed or a failure message is displayed. Please wait...
Decompress......Done.
Begain to install test01.ak …Done.
Begain to install test02.ak …Done.
Begain to install test03.ak …Done.

Total Num:3
Success Num:3
Failed Num:0
```

Install activation file 20170811.ak to the specified slot.

```
<Sysname> system-view
[Sysname] license activation-file install flash:/license/20170811.ak slot 1
This operation might take some time. Do not perform any other operations until the operation
is completed or a failure message is displayed. Please wait...Done.
```

Related commands

display license

display license device-id

license activation-file uninstall

license compress

Use **license compress** to compress the license storage.

Syntax

license compress slot *slot-number*

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

slot *slot-number*: Specifies the member ID of an IRF member device.

Usage guidelines

The license storage is limited. You can execute this command to clear expired licenses and uninstalled licenses from the license storage.

If uninstalled licenses or expired licenses exist on the device, the compression operation will make the DID or DID file change. Before performing a compression, make sure all licenses registered with the old DID or DID file have been installed. You will be unable to install such licenses after the compression.

Examples

Compress the license storage on the specified slot.

```
<Sysname> system-view
[Sysname] license compress slot 1
This command will delete all data relevant to uninstalled and expired keys/licenses,
including Uninstall keys, and create a new device ID for activation keys/files. Make sure
you have saved the Uninstall keys so you can apply for a new activation key/file for the
unexpired licenses that were covered by the uninstalled activation keys/files.
Are you sure you want to continue? [Y/N]: Y
This operation might take some time. Do not perform any other operations until the operation
is completed or a failure message is displayed. Please wait...Done.
```

Contents

Device management commands

clock datetime

Use **clock datetime** to set the system time.

Syntax

clock datetime *time date*

Default

The system time is Coordinated Universal Time (UTC) 00:00:00 01/01/2011.

Views

User view

Predefined user roles

network-admin

Parameters

time: Specifies a time in the *hh:mm:ss* format. The value range for *hh* is 0 to 23. The value range for *mm* is 0 to 59. The value range for *ss* is 0 to 59. The leading zero in a segment can be omitted. If the seconds segment is 0 (*hh*:*mm*:00), you can omit it. If both the minutes and seconds segments are 0 (*hh*:00:00), you can omit both of the segments. For example, to specify 08:00:00, you can enter 8.

date: Specifies a date in the *MM/DD/YYYY* or *YYYY/MM/DD* format. The value range for *YYYY* is 2000 to 2035. The value range for *MM* is 1 to 12. The value range for *DD* varies by month.

Usage guidelines

CAUTION:

This command changes the system time, which affects the execution of system time-related features (for example, scheduled tasks) and collaborative operations of the device with other devices (for example, log reporting and statistics collection). Before executing this command, make sure you fully understand its impact on your live network.

This command is supported only on the default context.

Correct system time is essential to network management and communication. You must configure the system time correctly before you run the device on the network.

For the device to use the local system time, execute the **clock protocol none** command and this command in turn. The specified system time takes effect immediately. Then, the device uses the clock signals generated by its built-in crystal oscillator to maintain the system time.

Examples

Set the system time to 08:08:08 01/01/2015.

```
<Sysname> clock datetime 8:8:8 1/1/2015
```

Set the system time to 08:10:00 01/01/2015.

```
<Sysname> clock datetime 8:10 2015/1/1
```

Related commands

clock protocol

clock summer-time

clock timezone

display clock

clock protocol

Use **clock protocol** to specify the method for obtaining the system time.

Use **undo clock protocol** to restore the default.

Syntax

clock protocol { **none** | **ntp context** *context-id* }

undo clock protocol

Default

The device uses the system time set by using the **clock datetime** command.

Views

System view

Predefined user roles

network-admin

Parameters

none: Uses the system time set by using the **clock datetime** command.

ntp: Uses NTP to obtain the UTC time periodically. You must configure NTP correctly. For more information about NTP and NTP configuration, see *Network Management and Monitoring Configuration Guide*.

context *context-id*: Specifies a context. For more information about context and the value range for the context ID, see *Virtual Technologies Command Reference*.

The following compatibility matrixes show the support of hardware platforms for the **context** *context-id* option:

Models	Parameter compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080	Yes
NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	No

Usage guidelines

This command is supported only on the default context.

Correct system time is essential to network management and communication. You must configure the system time correctly before you run the device on the network.

- If you execute the **clock protocol none** command, you can use the **clock datetime** command to configure the system time. The device then uses the clock signals generated by its built-in crystal oscillator to maintain the system time.
- If you execute the **clock protocol ntp** command, the device obtains the UTC time through GNSS or NTP periodically. After obtaining the UTC time, the device uses the UTC time, time zone, and daylight saving time to calculate the system time. If the GNSS or NTP signals are lost, the device uses the clock signals generated by its built-in crystal oscillator to maintain the system time. After the GNSS or NTP signals recover, the device obtains the UTC time again from the signals.

If you execute this command multiple times, the most recent configuration takes effect.

All contexts on the device use the same system time. After obtaining the system time from a context, the device automatically synchronizes the system time to the other contexts.

Examples

Configure the device to use the local UTC time.

```
<Sysname> system-view
[Sysname] clock protocol none
```

clock summer-time

Use **clock summer-time** to set the daylight saving time.

Use **undo clock summer-time** to restore the default.

Syntax

clock summer-time *name* *start-time* *start-date* *end-time* *end-date* *add-time*

undo clock summer-time

Default

The daylight saving time is not set.

Views

System view

Predefined user roles

network-admin

Parameters

name: Specifies a name for the daylight saving time schedule, a case-sensitive string of 1 to 32 characters.

start-time: Specifies the start time in the *hh:mm:ss* format. The value range for *hh* is 0 to 23. The value range for *mm* is 0 to 59. The value range for *ss* is 0 to 59. The leading zero in a segment can be omitted. If the seconds segment is 0 (*hh*:*mm*:00), you can omit it. If both the minutes and seconds segments are 0 (*hh*:00:00), you can omit both of the segments. For example, to specify 08:00:00, you can enter 8.

start-date: Specifies the start date in one of the following formats:

- *MM/DD*. The value range for *MM* is 1 to 12. The value range for *DD* varies by month.
- *month week day*, where:
  - *month*—Takes **January**, **February**, **March**, **April**, **May**, **June**, **July**, **August**, **September**, **October**, **November** or **December**.
  - *week*—Represents week of the month. It takes **first**, **second**, **third**, **fourth**, **fifth**, or **last**.
  - *day*—Takes **Sunday**, **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, or **Saturday**.

end-time: Specifies the end time in the *hh:mm:ss* format. The value range for *hh* is 0 to 23. The value range for *mm* is 0 to 59. The value range for *ss* is 0 to 59. The leading zero in a segment can be omitted. If the seconds segment is 0 (*hh*:*mm*:00), you can omit it. If both the minutes and seconds segments are 0 (*hh*:00:00), you can omit both of the segments. For example, to specify 08:00:00, you can enter 8.

end-date: Specifies the end date in one of the following formats:

- *MM/DD*. The value range for *MM* is 1 to 12. The value range for *DD* varies by month.
- *month week day*, where:

- *month*—Takes **January**, **February**, **March**, **April**, **May**, **June**, **July**, **August**, **September**, **October**, **November** or **December**.
- *week*—Represents week of the month. It takes **first**, **second**, **third**, **fourth**, **fifth**, or **last**.
- *day*—Takes **Sunday**, **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, or **Saturday**.

add-time: Specifies the time to be added to the standard time, in the *hh:mm:ss* format. The value range for *hh* is 0 to 23. The value range for *mm* is 0 to 59. The value range for *ss* is 0 to 59. The leading zero in a segment can be omitted. If the seconds segment is 0 (*hh*:*mm*:00), you can omit it. If both the minutes and seconds segments are 0 (*hh*:00:00), you can omit both of the segments. For example, to specify 08:00:00, you can enter 8.

Usage guidelines

This command is supported only on the default context.

Correct system time is essential to network management and communication. You must configure the system time correctly before you run the device on the network.

After you set the daylight saving time, the device recalculates the system time. To view the system time, use the **display clock** command.

Make sure all devices on the network are using the same daylight saving time as the local time.

Examples

Set the system time ahead 1 hour for the period between 06:00:00 on 08/01 and 06:00:00 on 09/01.

```
<Sysname> system-view
[Sysname] clock summer-time PDT 6 08/01 6 09/01 1
```

Related commands

clock datetime

clock timezone

display clock

clock timezone

Use **clock timezone** to set the time zone.

Use **undo clock timezone** to restore the default.

Syntax

clock timezone *zone-name* { **add** | **minus** } *zone-offset*

undo clock timezone

Default

The UTC time zone is used.

Views

System view

Predefined user roles

network-admin

Parameters

zone-name: Specifies a time zone by its name, a case-sensitive string of 1 to 32 characters.

add: Adds an offset to the UTC time.

minus: Decreases the UTC time by an offset.

zone-offset: Specifies an offset to the UTC time, in the *hh:mm:ss* format. The value range for *hh* is 0 to 23. The value range for *mm* is 0 to 59. The value range for *ss* is 0 to 59. The leading zero in a segment can be omitted. If the seconds segment is 0 (*hh*:*mm*:00), you can omit it. If both the minutes and seconds segments are 0 (*hh*:00:00), you can omit both of the segments. For example, to specify 08:00:00, you can enter 8.

Usage guidelines

This command is supported only on the default context.

Correct system time is essential to network management and communication. You must configure the system time correctly before you run the device on the network.

After you set the time zone, the device recalculates the system time. To view the system time, use the **display clock** command.

Make sure all devices on the network are using the same time zone as the local time.

Examples

Set the name of the time zone to **Z5**, and add 5 hours to the UTC time.

```
<Sysname> system-view
[Sysname] clock timezone Z5 add 5
```

Related commands

clock datetime

clock summer-time

display clock

command

Use **command** to assign a command to a job.

Use **undo command** to revoke a command.

Syntax

command *id command*

undo command *id*

Default

No command is assigned to a job.

Views

Job view

Predefined user roles

network-admin

context-admin

Parameters

id: Specifies an ID for the command, in the range of 0 to 4294967295. A command ID uniquely identifies a command in a job. Commands in a job are executed in ascending order of their command IDs.

command: Specifies the command to be assigned to the job.

Usage guidelines

To assign a command (command A) to a job, you must first assign the job the command or commands for entering the view of command A.

If you specify the ID of an existing command for another command, the existing command is replaced.

Make sure all commands in a schedule are compliant to the command syntax. The system does not examine the syntax when you assign a command to a job.

If a command requires a yes or no answer, the system always assumes that a **Y** or **Yes** is entered. If a command requires a character string input, the system assumes that either the default character string (if any) or a null string is entered.

A job cannot contain the **telnet**, **ftp**, **ssh2**, or **monitor process** command.

Examples

Assign commands to the **backupconfig** job to back up the **startup.cfg** file to the TFTP server at 192.168.100.11.

```
<Sysname> system-view
[Sysname] scheduler job backupconfig
[Sysname-job-backupconfig] command 2 tftp 192.168.100.11 put flash:/startup.cfg
backup.cfg
```

Assign commands to the **shutdownGE** job to shut down GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] scheduler job shutdownGE
[Sysname-job-shutdownGE] command 1 system-view
[Sysname-job-shutdownGE] command 2 interface gigabitethernet 1/0/1
[Sysname-job-shutdownGE] command 3 shutdown
```

Related commands

scheduler job

copyright-info enable

Use **copyright-info enable** to enable copyright statement display.

Use **undo copyright-info enable** to disable copyright statement display.

Syntax

copyright-info enable

undo copyright-info enable

Default

Copyright statement display is enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Examples

Enable copyright statement display.

```
<Sysname> system-view
[Sysname] copyright-info enable
```

The device will display the following statement when a user logs in:

```
******************************************************************************
* Copyright (c) 2004-2017 New NSFOCUS. All rights reserved.                  *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************
```

display alarm

Use **display alarm** to display alarm information.

Syntax

display alarm [**slot** *slot-number*]

The following compatibility matrix shows the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080,	Yes
NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	No

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays alarm information for all IRF member devices.

Usage guidelines

This command is supported only on the default context.

Examples

Display alarm information.

```
<Sysname> display alarm
Slot CPU Level   Info
1    0   ERROR   faulty
```

Table 1 Command output

Field	Description
Slot	Slot that generated the alarm. If the alarm was generated by the frame, this field displays a hyphen (-).
Level	Alarm severity. Possible values include **ERROR**, **WARNING**, **NOTICE**, and **INFO**, in descending order.

Field	Description
Info	Detailed alarm information: • **faulty**—The slot is starting up or faulty. • **Fan** *n* **is absent**—The specified fan is absent. • **Power** *n* **is absent**—The specified power supply is absent. • **Power** *n* **is faulty**—The specified power supply is faulty. • **The temperature of sensor** *n* **exceeds the lower limit**—The temperature of the specified sensor is lower than the low-temperature threshold. • **The temperature of sensor** *n* **exceeds the upper limit**—The temperature of the specified sensor is higher than the high-temperature warning threshold.

display clock

Use **`display clock`** to display the system time, date, time zone, and daylight saving time.

Syntax

`display clock`

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display the system time and date when the time zone is not specified.

```
<Sysname> display clock
10:09:00.258 UTC Fri 03/16/2015
```

The time is in the *hour*:*minute*:*second*.*milliseconds* format.

Display the system time and date when the time zone Z5 is specified.

```
<Sysname> display clock
15:10:00.152 Z5 Fri 03/16/2015
Time Zone : Z5 add 05:00:00
```

Display the system time and date when the time zone Z5 and daylight saving time PDT are specified.

```
<Sysname> display clock
15:11:00.211 Z5 Fri 03/16/2015
Time Zone : Z5 add 05:00:00
Summer Time : PDT 06:00:00 08/01 06:00:00 09/01 01:00:00
```

Related commands

`clock datetime`

`clock timezone`

`clock summer-time`

display copyright

Use **display copyright** to display the copyright statement.

Syntax

display copyright

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display the copyright statement.

```
<Sysname> display copyright
...
```

display cpu-usage

Use **display cpu-usage** to display the current CPU usage statistics.

Syntax

display cpu-usage [**summary**] [**slot** *slot-number* [**cpu** *cpu-number* [**core** { *core-number* | **all** }]]]

display cpu-usage [**control-plane** | **data-plane**] [**summary**] [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

control-plane: Displays CPU usage statistics for the control plane. If you do not specify this keyword or the **data-plane** keyword, the command displays the total CPU usage statistics.

data-plane: Displays CPU usage statistics for the data plane. If you do not specify this keyword or the **control-plane** keyword, the command displays the total CPU usage statistics.

summary: Displays CPU usage statistics in table form. If you do not specify this keyword, the command displays CPU usage statistics in text form.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays CPU usage statistics for all member devices.

cpu *cpu-number*: Specifies a CPU by its number.

core { *core-number* | **all** }: Displays CPU core usage statistics. If you specify a CPU core by its number, this command displays usage statistics for the CPU core. If you specify the **all** keyword, this command displays average usage statistics for all CPU cores.

Usage guidelines

Executing this command on a context displays the current CPU usage statistics for the context.

If two hyphens (--) are displayed for the CPU usage during the most recent 5-second, 1-minute, and 5-minute intervals, the command might fail to obtain data from the database on the device. Try the command later.

Examples

Display the current CPU usage statistics in text form.

```
<Sysname> display cpu-usage
Slot 1 CPU 0 CPU usage:
       1% in last 5 seconds
       1% in last 1 minute
       1% in last 5 minutes
```

Display the current CPU usage statistics in table form.

```
<Sysname> display cpu-usage
Slot CPU        Last 5 sec        Last 1 min        Last 5 min
1    0          17%               29%               28%
```

Table 2 Command output

Field	Description
x% in last 5 seconds Last 5 sec	Average CPU usage during the most recent 5-second interval.
y% in last 1 minute Last 1 min	Average CPU usage during the most recent 1-minute interval.
z% in last 5 minutes Last 5 min	Average CPU usage during the most recent 5-minute interval.

display cpu-usage configuration

Use **display cpu-usage configuration** to display CPU usage monitoring settings.

Syntax

display cpu-usage configuration [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

context-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the CPU usage monitoring settings for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

Executing this command on a context displays CPU usage monitoring settings for the context.

Examples

Display the CPU usage monitoring settings.

```
<Sysname> display cpu-usage configuration
CPU usage monitor is enabled.
Current monitor interval is 60 seconds.
Current monitor threshold is 70%.
Current monitor recovery threshold is 30%.
Current statistics-interval is 60 seconds for the following cores: 0 to 1.
```

Table 3 Command output

Field	Description
CPU usage monitor is *xxx*.	Whether CPU usage tracking is enabled.
Current monitor interval is *xxx*.	Sampling interval for CPU usage tracking.
Current monitor threshold is *xxx*.	CPU usage threshold.
Current monitor recovery threshold is *xxx*.	CPU usage recovery threshold.
Current statistics-interval is *xxx* seconds for the following cores	CPU core usage statistics interval.

Related commands

monitor cpu-usage enable

monitor cpu-usage interval

monitor cpu-usage threshold

display cpu-usage history

Use **display cpu-usage history** to display the historical CPU usage statistics in a coordinate system.

Syntax

display cpu-usage history [**job** *job-id*] [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

job *job-id*: Specifies a process by its ID. The value range for *job-id* is 1 to 2147483647. If you do not specify a process, this command displays the statistics for the entire system's CPU usage (the

total CPU usage of all processes). To view the IDs and names of the running processes, use the **display process** command. For more information, see *Network Management and Monitoring Configuration Guide*.

slot *slot-number*: Specifies an IRF member device by its member ID. If you specify a process but do not specify a member device, this command displays the statistics for the process on the master device. If you do not specify any options, this command displays the statistics for all processes on all member devices.

cpu *cpu-number*: Specifies a CPU by its number. If you specify a process but do not specify a CPU, this command displays the statistics for the default CPU. If you do not specify a process or CPU, this command displays the historical statistics for all CPUs.

Usage guidelines

After CPU usage monitoring is enabled, the system regularly samples CPU usage and saves the samples to the history record buffer. This command displays the most recent 60 samples in a coordinate system as follows:

The vertical axis represents the CPU usage. If a statistic is not a multiple of the usage step, it is rounded up or down to the closest multiple of the usage step. For example, if the CPU usage step is 5%, the statistic 53% is rounded up to 55%, and the statistic 52% is rounded down to 50%.

The horizontal axis represents the time.

Pound signs (#) indicate the CPU usage. The value on the vertical axis for the topmost pound sign at a specific time represents the CPU usage at that time.

Executing this command on a context displays the historical CPU usage statistics for the context.

Examples

Display the historical CPU usage statistics.

```
<Sysname> display cpu-usage history
100%|
 95%|
 90%|
 85%|
 80%|
 75%|
 70%|
 65%|
 60%|
 55%|
 50%|
 45%|
 40%|
 35%|
 30%|
 25%|
 20%|
 15%|             #
 10%|            ###  #
  5%|           ########
    ------------------------------------------------------------
              10        20        30        40        50        60  (minutes)
                      cpu-usage (Slot 1 CPU 0) last 60 minutes (SYSTEM)
```

The output shows the following items:

- Process name. The name **SYSTEM** represents the entire system.
- CPU that is holding the process: CPU 0 in slot 1.
- Historical CPU usage statistics for the entire system during the last 60 minutes.
  - **12 minutes ago**—Approximately 5%.
  - **13 minutes ago**—Approximately 10%.
  - **14 minutes ago**—Approximately 15%.
  - **15 minutes ago**—Approximately 10%.
  - **16 and 17 minutes ago**—Approximately 5%.
  - **18 minutes ago**—Approximately 10%.
  - **19 minutes ago**—Approximately 5%.
  - **Other time**—2% or lower.

Related commands

`monitor cpu-usage enable`

`monitor cpu-usage interval`

display device

Use **`display device`** to display device information.

Syntax

`display device` [**`harddisk`** | **`usb`**] [**`slot`** *`slot-number`* [**`subslot`** *`subslot-number`*] | **`verbose`**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

`harddisk`: Displays hard disk information.

The following compatibility matrix shows the support of hardware platforms for this keyword:

Models	Parameter compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	Yes
NFNX3-HDB680, NFNX3-HDB1080	No

`usb`: Displays USB interface information.

`slot` *`slot-number`*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all member devices.

subslot *subslot-number*: Specifies an interface module by the number of its slot marked on the device panel. If you do not specify an interface module, this command does not display information about interface modules.

verbose: Displays detailed information. If you do not specify this keyword, this command displays brief information.

Usage guidelines

If you do not specify the **harddisk** or **usb** keyword, this command displays information about member devices.

This command displays information about the physical device, whether you execute it on the default context or a non-default context.

Examples

Display device information.

```
<Sysname> display device
Slot.No   Cpu.Id   Brd Type     Brd Status    Subslot    Sft Ver    Patch Ver
1         0        NFNX3HDB680  Normal        0          9524P07    None
```

Table 4 Command output

Field	Description
Brd Type	Device type.
Brd Status	Role of the device in an IRF fabric: • **Normal**—The member device is operating correctly. • **Fault**—The member device is not operating correctly. • **Absent**—The slot is not installed with a member device.
Sft Ver	Software version of the device.
Patch Ver	Most recently released patch image version that is running on the device. If no patch image is installed, this field displays **None**. If both incremental and non-incremental patch images are running on the device, this field displays the most recently released incremental patch image version. For more information about patch image types, see software upgrade in *Fundamentals Configuration Guide*.

display device manuinfo

Use **display device manuinfo** to display electronic label information for the device.

Syntax

display device manuinfo [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays electronic label information for all member devices.

Usage guidelines

An electronic label contains the permanent configuration information, including the hardware serial number, manufacturing date, MAC address, and vendor name. The data is written to the storage component during hardware debugging or testing. This command displays only part of the electronic label information.

This command is supported only on the default context.

Examples

Display electronic label information for the device.

```
<Sysname> display device manuinfo
 Slot 1 CPU 0:
 DEVICE_NAME           : NFNX3-HDB680
 DEVICE_SERIAL_NUMBER  : 210235A1VNH164000026
 MAC_ADDRESS           : 487A-DA95-91BB
 MANUFACTURING_DATE    : 2016-04-29
 VENDOR_NAME           : NSFOCUS
```

display diagnostic-information

Use **display diagnostic-information** to display or save operating information for features and hardware modules.

Syntax

display diagnostic-information [**hardware** | **infrastructure** | **l2** | **l3** | **service**] [**key-info**] [*filename*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

hardware: Specifies hardware-related operating information.

infrastructure: Specifies operating information for the fundamental features.

l2: Specifies operating information for the Layer 2 features.

l3: Specifies operating information for the Layer 3 features.

service: Specifies operating information for Layer 4 and upper-layer features.

key-info: Displays or saves only critical operating information. The device might have a large amount of operating information if an exception occurs or after the device runs for a long period of time. Specifying this keyword reduces the command execution time and helps you focus on critical operating information. If you do not specify this keyword, the command displays or saves both critical and non-critical operating information.

filename: Saves the information to a file. The *filename* argument must use the **.tar.gz** extension. If you do not specify this argument, the command prompts you to choose whether to save the information to a file or display the information.

Usage guidelines

You can use one of the following methods to collect operating statistics for diagnostics and troubleshooting:

- Use separate **display** commands to collect operating information feature by feature or module by module.
- Use the **display diagnostic-information** command to collect operating information for multiple or all features and hardware modules.

To save storage space, this command automatically compresses the information before saving the information to a file. To view the file content:

1. Use the **tar extract** command to extract the file.
2. Use the **gunzip** command to decompress the extracted file.
3. Use the **more** command to view the content of the decompressed file.

If you abort the **display diagnostic-information** command, the **gunzip** command might not be able to decompress the extracted file. To decompress the extracted file, export the extracted file to a PC that is running Linux, and use the **gunzip -c** command.

If you do not specify a file name for the command, the system prompts you to choose whether to display or save the information. If you choose to save the information, the system automatically assigns a file name and displays the file name in brackets. For file name uniqueness, the file name includes the device name and the current system time. If the device name contains any of the following special characters, the system uses an underscore (_) to replace each special character: forward slashes (/), backward slashes (\), colons (:), asterisks (*), question marks (?), less than signs (<), greater than signs (>), pipeline signs (|), and quotation marks ("). For example, device name **A/B** will change to **A_B** in the file name, as in **flash:/diag_A_B_20160101-000438.tar.gz**.

If you do not specify any feature parameters, this command displays or saves the operating information for all features and modules.

This command does not support the |, **>**, and **>>** options.

While the device is executing this command, do not execute any other commands. Executing other commands might affect the collected operating information.

Examples

Display the operating information for all features and modules.

```
<Sysname> display diagnostic-information
Save or display diagnostic information (Y=save, N=display)? [Y/N]:n
================================================
  ===============display clock===============
14:03:55 UTC Thu 01/05/2015
================================================
  ===============display version===============
...
```

Save the operating information to the default file.

```
<Sysname> display diagnostic-information
Save or display diagnostic information (Y=save, N=display)? [Y/N]:y
Please input the file name(*.tar.gz)[flash:/diag_Sysname_20160101-024601.tar.gz]:
Diagnostic information is outputting to flash:/diag_Sysname_20160101-024601.tar.gz.
Please wait...
```

```
Save successfully.
```

Press **Enter** when the system prompts you to enter the file name.

Save the operating information for all features and modules to file **test.tar.gz**.

```
<Sysname> display diagnostic-information test.tar.gz
Diagnostic information is outputting to flash:/test.tar.gz.
Please wait...
Save successfully.
```

Related commands

gunzip

more

tar extract

display environment

Use **display environment** to display temperature information.

Syntax

display environment [**slot** *slot-number*]

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	Yes
NFNX3-HDB680, NFNX3-HDB1080	No

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays temperature information for all member devices.

This command is supported only on the default context.

Examples

Display information about all temperature sensors on the device.

```
<Sysname> display environment
 System Temperature information (degree centigrade):
-------------------------------------------------------------------------------
---
```

```
 Slot     Sensor   Temperature LowerLimit Warning-UpperLimit  Alarm-UpperLimit
Shutdown-UpperLimit
1      inflow  1      33          -2             52               60               NA
1      outflow 1      37          0              55               65               NA
1      hotspot 1      45          0              70               78               NA
```

Table 5 Command output

Field	Description
System Temperature information (degree centigrade)	Temperature information (°C).
sensor	Temperature sensor: • **hotspot**—Hotspot sensor. • **inflow**—Air inlet sensor. • **outflow**—Air outlet sensor.
Slot	Sensor position.
Temperature	Current temperature.
LowerLimit	Low-temperature threshold. If the device does not support this field, this field displays **NA**.
Warning-UpperLimit	High-temperature warning threshold. If the device does not support this field, this field displays **NA**.
Alarm-UpperLimit	High-temperature alarming threshold. If the device does not support this field, this field displays **NA**.
Shutdown-UpperLimit	High-temperature shutdown temperature threshold. When the sensor temperature reaches the limit, the system shuts down automatically. If the device does not support this field, this field displays **NA**.

display fan

Use **`display fan`** to display fan tray operating status information.

Syntax

`display fan` [**`slot`** *`slot-number`* [*`fan-id`*]]

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	Yes
NFNX3-HDB680, NFNX3-HDB1080	No

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays fan tray operating status information for all member devices.

fan-id: Specifies a fan tray by its ID. If you do not specify a fan tray, this command displays operating status information for all fan trays at the specified position.

The following compatibility matrixes show the value range for the fan tray ID:

Models	Value range
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080	0 to 3
NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	Not supported

Usage guidelines

This command is supported only on the default context.

Examples

Display the operating status of fan tray 1 on member device 1.

```
<Sysname> display fan slot 1 1
SLOT 1 Fan 1      Status: Normal  Speed:2347
```

Table 6 Command output

Field	Description
Status	Fan tray status: • **Absent**—The slot is not installed with a fan tray. • **Faulty**—The fan tray is faulty. • **Normal**—The fan tray is operating correctly. • **NotSupport**—The fan tray is not supported. • **FanDirectionFault**—The actual airflow direction is not the preferred direction.

display memory

Use **display memory** to display memory usage information.

Syntax

display memory [**summary**] [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

summary: Displays brief information about memory usage. If you do not specify this keyword, the command displays detailed information about memory usage.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays memory usage for all member devices.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

Executing this command on a context displays memory usage information for the context.

If two hyphens (--) are displayed for all the fields in a line of the command output, the command might fail to obtain data from the database on the device. Try the command later.

Examples

Display detailed memory usage information.

```
<Sysname> display memory
Memory statistics are measured in KB:
Slot 1:
             Total      Used      Free    Shared   Buffers    Cached   FreeRatio
Mem:        984560    456128    528432         0         4     45616       53.7%
-/+ Buffers/Cache:    410508    574052
Swap:            0         0         0
```

Display brief memory usage information.

```
<Sysname> display memory summary
Memory statistics are measured in KB:
Slot CPU        Total      Used      Free  Buffers    Caches FreeRatio
   1   0       984560    456128    528432        4     45616     53.7%
```

Table 7 Command output

Field	Description
Mem	Memory usage information.
Total	Total size of the physical memory space that can be allocated. The memory space is virtually divided into two parts. Part 1 is solely used for kernel code, kernel management, and ISSU functions. Part 2 can be allocated and used for such tasks as running service modules and storing files. The size of part 2 equals the total size minus the size of part 1.
Used	Used physical memory.
Free	Free physical memory.
Shared	Physical memory shared by processes. If this field is not supported, two hyphens (--) are displayed.
Buffers	Physical memory used for buffers. If this field is not supported, two hyphens (--) are displayed.
Cached Caches	Physical memory used for caches. If this field is not supported, two hyphens (--) are displayed.
FreeRatio	Free memory ratio.
-/+ Buffers/Cache	-/+ Buffers/Cache:used = Mem:Used – Mem:Buffers – Mem:Cached, which indicates the physical memory used by applications. -/+ Buffers/Cache:free = Mem:Free + Mem:Buffers + Mem:Cached, which indicates

Field	Description
	the physical memory available for applications.
Swap	Memory space for swapping.

display memory-threshold

Use **display memory-threshold** to display memory alarm thresholds and statistics.

Syntax

display memory-threshold [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the memory usage thresholds and statistics for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

This command is supported only on the default context.

For more information about memory usage notifications, see log information containing **MEM_EXCEED_THRESHOLD** or **MEM_BELOW_THRESHOLD**.

Examples

Display memory alarm thresholds and statistics.

```
<Sysname> display memory-threshold
Memory usage threshold: 100%
Free memory threshold:
    Minor: 224M
    Severe: 128M
    Critical: 96M
    Normal: 256M
Current memory state: Normal
Event statistics:
 [Back to normal state]
    First notification: 0.0
    Latest notification: 0.0
    Total number of notifications sent: 0
 [Enter minor low-memory state]
    First notification at: 0.0
    Latest notification at: 0.0
```

```
   Total number of notifications sent: 0
 [Back to minor low-memory state]
   First notification at: 0.0
   Latest notification at: 0.0
   Total number of notifications sent: 0
 [Enter severe low-memory state]
   First notification at: 0.0
   Latest notification at: 0.0
   Total number of notifications sent: 0
 [Back to severe low-memory state]
   First notification at: 0.0
   Latest notification at: 0.0
   Total number of notifications sent: 0
 [Enter critical low-memory state]
   First notification at: 0.0
   Latest notification at: 0.0
   Total number of notifications sent: 0
```

display power

Use **display power** to display power supply information.

Syntax

display power [**slot** *slot-number* [*power-id*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays power supply information for all member devices.

power-id: Specifies a power supply by its ID. If you do not specify a power supply, this command displays information about all power supplies at the specified position.

The following compatibility matrixes show the value ranges for the power supply ID:

Models	Value range
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	0 to 1
NFNX3-HDB680, NFNX3-HDB1080	0

Usage guidelines

This command is supported only on the default context.

Examples

Display brief power supply information.

```
<Sysname> display power
Slot  1 Power  0     Status: Absent
Slot  1 Power  1     Status: Normal
```

Table 8 Command output

Field	Description
Status	Power supply status: • **Absent**—The slot is not installed with a power supply. • **Faulty**—The power supply is faulty. • **Normal**—The power supply is operating correctly. • **NotSupport**—The power supply is not supported.

display scheduler job

Use **display scheduler job** to display job configuration information.

Syntax

display scheduler job [*job-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

job-name: Specifies a job by its name, a case-sensitive string of 1 to 47 characters. If you do not specify a job, this command displays configuration information for all jobs.

Examples

Display configuration information for all jobs.

```
<Sysname> display scheduler job
Job name: saveconfig
 copy startup.cfg backup.cfg

Job name: backupconfig

Job name: creat-VLAN100
 system-view
 vlan 100
```

// The output shows that the device has three jobs: the first has one command, the second does not have any commands, and the third has two commands. Jobs are separated by blank lines.

display scheduler logfile

Use **display scheduler logfile** to display job execution log information.

Syntax

display scheduler logfile

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display job execution log information.

```
<Sysname> display scheduler logfile
Logfile Size: 1902 Bytes.

Job name        : shutdown
Schedule name   : shutdown
Execution time  : Tue Dec 27 10:44:42 2015
Completion time : Tue Dec 27 10:44:47 2015
-------------------------------- Job output ----------------------------------
<Sysname>system-view
System View: return to User View with Ctrl+Z.
[Sysname]interface rang gigabitethernet 1/0/1 to gigabitethernet 1/0/3
[Sysname-if-range]shutdown
```

Table 9 Command output

Field	Description
Logfile Size	Size of the log file, in bytes.
Schedule name	Schedule to which the job belongs.
Execution time	Time when the job was started.
Completion time	Time when the job was completed. If the job has never been executed or the job does not have any commands, this field is blank.
Job output	Commands in the job and their output.

Related commands

reset scheduler logfile

display scheduler reboot

Use **display scheduler reboot** to display the automatic reboot schedule.

Syntax

display scheduler reboot

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display the automatic reboot schedule.

```
<Sysname> display scheduler reboot
System will reboot at 16:32:00 05/23/2015 (in 1 hours and 39 minutes).
```

Related commands

scheduler reboot at

scheduler reboot delay

display scheduler schedule

Use **display scheduler schedule** to display schedule information.

Syntax

display scheduler schedule [*schedule-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

schedule-name: Specifies a schedule by its name, a case-sensitive string of 1 to 47 characters. If you do not specify a schedule, this command displays information about all schedules.

Examples

Display information about all schedules.

```
<Sysname> display scheduler schedule
Schedule name        : shutdown
Schedule type        : Run once after 0 hours 2 minutes
Start time           : Tue Dec 27 10:44:42 2015
Last execution time  : Tue Dec 27 10:44:42 2015
Last completion time : Tue Dec 27 10:44:47 2015
Execution counts     : 1
------------------------------------------------------------------------
```

```
Job name                                 Last execution status
shutdown                                 Successful
```

Table 10 Command output

Field	Description
Schedule type	Execution time setting of the schedule. If no execution time is specified, this field is not displayed.
Start time	Time to execute the schedule for the first time. If no execution time is specified, this field is not displayed.
Last execution time	Last time when the schedule was executed. If no execution time is specified, this field is not displayed. If the schedule has never been executed, "Yet to be executed" is displayed for this field.
Last completion time	Last time when the schedule was completed. If no execution time is specified, this field is not displayed.
Execution counts	Number of times the schedule has been executed. If the schedule has never been executed, this field is not displayed.
Job name	Name of a job under the schedule.
Last execution status	Result of the most recent execution: • **Successful**. • **Failed**. • **Waiting**—The device is executing the schedule and the job is waiting to be executed. • **In process**—The job is being executed. • **-NA-**—The execution time has not arrived yet. To view information about whether the commands in the job has been executed and the execution results, execute the **`display scheduler logfile`** command.

display system stable state

Use **`display system stable state`** to display system stability and status information.

Syntax

`display system stable state`

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Usage guidelines

Before performing an ISSU or a switchover, execute this command multiple times to identify whether the system is operating stably. If the value of the **System State** field is not **Stable**, you cannot perform an ISSU. If the value of the **Redundancy Stable** field is not **Stable**, you cannot perform a switchover.

The device startup process takes some time. If the values of the status fields do not change to **Stable**, execute this command multiple times to identify the member devices that are not in **Stable** state. You can also use other commands to identify the faulty components. For example:

- Use the **display device** command to identify the device operating status.
- Use the **display ha service-group** command to display the status of HA service groups and identify the groups in batch backup state.
- Use the **display system internal process state** command in probe view to display service operating status.

Examples

Display system stability and status information.

```
<Sysname> display system stable state
System state    : Stable
Redundancy state: No redundance
  Slot   CPU   Role      State
 1      0     Active    Stable
```

Table 11 Command output

Field	Description
System state	System status: • **Stable**—The system is operating stably. • **Not ready**—The system is not operating stably. You cannot perform an ISSU when the system is in this state.
Redundancy state	System redundancy status: • **Stable**—Member devices are operating stably. You can perform a switchover. • **No redundance**—The system has only one member device. You cannot perform a switchover. • **Not ready**—The system is not operating stably. You cannot perform a switchover.
Role	Role of the member device in the system: • **Active**—The member device is the master. • **Standby**—The member device is a subordinate member.
State	Member device status: • **Stable**—The member device is operating stably. • **Board inserted**—The member device has just been installed. • **Kernel initiating**—Member device kernel is being initialized. • **Service starting**—Services are starting on the member device. • **Service stopping**—Services are stopping on the member device. • **HA Batch backup**—An HA batch backup is going on. • **Interface data batch backup**—An interface data batch backup is in progress. • **Service module data batch backup**—A service module data batch backup is in process.
*	The object is not operating stably.

Related commands

display context (*Virtual Technologies Command Reference*)

display device

display ha service-group (*High Availability Command Reference*)

display transceiver alarm

Use **display transceiver alarm** to display transceiver alarms.

Syntax

display transceiver alarm { controller [*controller-type controller-number* **] | interface [** *interface-type interface-number* **] }**

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

controller [*controller-type controller-number* **]**: Specifies a controller by its type and number. If no controller is specified, this command displays the alarms present on all controllers.

The following compatibility matrixes show the support of hardware platforms for the **controller [** *controller-type controller-number* **]** option:

Models	Parameter compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	No
NFNX3-HDB680, NFNX3-HDB1080	Yes

interface [*interface-type interface-number* **]**: Specifies an interface by its type and number. If no interface is specified, this command displays the alarms present on every transceiver module.

Usage guidelines

Table 12 shows the common transceiver alarm components. If no error occurs, "None" is displayed.

Table 12 Common transceiver alarm components

Field	Description
power	Optical power
RX	Receive
Temp	Temperature
TX	Transmit

Examples

Display the alarms present on the transceiver module in interface GigabitEthernet1/0/1.

```
<Sysname> display transceiver alarm interface gigabitethernet 1/0/1
GigabitEthernet1/0/1 transceiver current alarm information:
  RX loss of signal
```

```
RX power low
```

Table 13 Command output

Field	Description
transceiver current alarm information	Alarms present on the transceiver module.
RX loss of signal	Received signals are lost.
RX power low	Received power is low.

display transceiver diagnosis

Use **display transceiver diagnosis** to display the current values of the digital diagnosis parameters of transceiver modules.

Syntax

display transceiver diagnosis { **controller** [*controller-type controller-number*] | **interface** [*interface-type interface-number*] }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

controller [*controller-type controller-number*] : Specifies a controller by its type and number. If no controller is specified, this command displays the current values of the digital diagnosis parameters on all controllers.

The following compatibility matrixes show the support of hardware platforms for the **controller** [*controller-type controller-number*] option:

Models	Parameter compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	No
NFNX3-HDB680, NFNX3-HDB1080	Yes

interface [*interface-type interface-number*]: Specifies an interface by its type and number. If no interface is specified, this command displays the current values of the digital diagnosis parameters on all interfaces.

Examples

Display the current values of the digital diagnosis parameters on the transceiver module in interface GigabitEthernet1/0/1.

```
<Sysname> display transceiver diagnosis interface gigabitethernet 1/0/1
```

```
GigabitEthernet1/0/1 transceiver diagnostic information:
  Current diagnostic parameters:
    Temp(°C)  Voltage(V)  Bias(mA)  RX power(dBm)  TX power(dBm)
    36        3.31        6.13      -35.64          -5.19
  Alarm thresholds:
            Temp(°C)   Voltage(V)  Bias(mA)  RX power(dBM)  TX power(dBM)
    High    50         3.55        1.44      -10.00         5.00
    Low     30         3.01        1.01      -30.00         0.00
```

Table 14 Command output

Field	Description
transceiver diagnostic information	Digital diagnosis information for the transceiver module in the interface.
Temp.(°C)	Temperature in °C, accurate to 1°C.
Voltage(V)	Voltage in V, accurate to 0.01 V.
Bias(mA)	Bias current in mA, accurate to 0.01 mA.
RX power(dBm)	Receive power in dBm, accurate to 0.01 dBm.
TX power(dBm)	Transmit power in dBm, accurate to 0.01 dBm.

display transceiver interface

Use **display transceiver interface** to display the key parameters of transceiver modules.

Syntax

display transceiver interface [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays the key parameters of every transceiver module.

Examples

Display the key parameters of the transceiver module in interface GigabitEthernet1/0/1.

```
<Sysname> display transceiver interface gigabitethernet 1/0/1
GigabitEthernet 1/0/1 transceiver information:
  Transceiver Type              : 1000_BASE_SX_SFP
  Connector Type                : LC
  Wavelength(nm)                : 850
  Transfer Distance(m)          : 550(50um),270(62.5um)
  Digital Diagnostic Monitoring : YES
  Vendor Name                   : NSFOCUS
```

```
Ordering Name                : SFP-GE-SX-MM850
```

Table 15 Command output

Field	Description
Wavelength(nm)	Central wavelength of the laser in nm. For a fiber transceiver module that supports multiple wavelengths, for example, the 10GBASE-LX4 transceiver module, this field displays all the wavelengths, separating the values by commas (,). For a copper module, this field displays **N/A**.
Transfer Distance(m)	Transmission distance, in km (for single-mode modules) or in m (for other modules). For a module that supports multiple transmission media, this field displays all the transmission distances, separating the values by commas (,). Each transmission distance is followed by the medium name in parentheses. • **9um**—9/125um single-mode optical fiber. • **50um**—50/125um OM2 multi-mode optical fiber. • **62.5um**—62.5/125um OM1 multi-mode optical fiber. • **CX4**—CX4 cables. • **OM3**—50um OM3 multi-mode optical fiber. • **OM4**—50um OM4 multi-mode optical fiber. • **OM5**—50um OM5 multi-mode optical fiber. • **STACK**—Stack cables. • **TP**—Twisted pairs.
Digital Diagnostic Monitoring	Whether digital diagnosis is supported: • **YES**—Digital diagnosis is supported. • **NO**—Digital diagnosis is not supported.

display transceiver manuinfo

Use **display transceiver manuinfo** to display electronic label information for transceiver modules.

Syntax

display transceiver manuinfo { **controller** [*controller-type controller-number*] | **interface** [*interface-type interface-number*] }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

controller [*controller-type controller-number*] : Specifies a controller by its type and number. If no controller is specified, this command displays the electronic label information for the transceiver modules in all controllers.

The following compatibility matrixes show the support of hardware platforms for the **controller** [*controller-type controller-number*] option:

Models	Parameter compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	No
NFNX3-HDB680, NFNX3-HDB1080	Yes

interface [*interface-type interface-number*]: Specifies an interface by its type and number. If no interface is specified, this command displays electronic label information for the transceiver modules in all interfaces.

Examples

Display electronic label information for the transceiver module in interface GigabitEthernet1/0/1.

```
<Sysname> display transceiver manuinfo interface gigabitethernet 1/0/1
GigabitEthernet1/0/1 transceiver manufacture information:
  Manu. Serial Number  : 213410A0000054000251
  Manufacturing Date   : 2017-09-01
  Vendor Name          : NSFOCUS
```

display version

Use **display version** to display system version information.

Syntax

display version

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display system version information.

```
<Sysname> display version
NSFOCUS NF Software, Version 7.1.064, Ess 9333P07
Copyright (c) 2004-2018 NSFOCUS. All rights reserved.
NSFOCUS NFNX3-HDB680 uptime is 0 weeks, 0 days, 1 hour, 57 minutes
Last reboot reason: User reboot

Boot image: flash:/NFNX3HDB680-cmwv6-boot-E9333P07.bin
Boot image version: 7.1.064, Ess 9333P07
  Compiled May 15 2018 16:00:00
System image: flash:/NFNX3HDB680-cmwv6-system-E9333P07.bin
System image version: 7.1.064, Ess 9333P07
```

```
  Compiled May 15 2018 16:00:00
...
```

Table 16 Command output

Field	Description
Last reboot reason	Reason for the last reboot: • **User reboot**—The reboot was manually initiated from a user interface, such as the CLI or SNMP. • **Cold reboot**—The reboot was caused by a power cycle. • **Kernel abnormality reboot**—The reboot was caused by kernel exceptions. • **DeadLoop reboot**—The reboot was caused by a kernel thread dead loop. • **DEV HandShake reboot**—The reboot was caused by a device management handshake failure. • **SlaveSwitch reboot**—The reboot was caused by a master/subordinate switchover. • **IRF Merge reboot**—The reboot was caused by an IRF merge. • **Auto Update reboot**—The reboot was caused by an automatic software upgrade. • **Memory exhaust reboot**—The reboot was caused by a card-memory-exhausted event.

display version-update-record

Use **display version-update-record** to display startup software image upgrade records.

Syntax

display version-update-record

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

This command is supported only on the default context.

The device records its current startup software version information whenever it starts up, and records all software version update information. Such information can survive reboots.

Examples

Display the startup software image upgrade records.

```
<Sysname> display version-update-record
Record 1  (updated on Apr 18 2015 at 06:23:54):
 *Name        : boot-test.bin
  Version     : 7.1.070 Test 0001
  Compile time: Mar 25 2015 15:52:43

 *Name        : system-test.bin
  Version     : 7.1.070 Test 0001
  Compile time: Mar 25 2015 15:52:43
```

Table 17 Command output

Field	Description
Record *n*	Number of the startup software image upgrade record. Record 1 is the most recent record.
Name	Software image file name.
*	The software image version changed during the upgrade.

Related commands

reset version-update-record

header

Use **header** to configure a banner.

Use **undo header** to delete a banner.

Syntax

header { **legal** | **login** | **motd** | **shell** } *text*

undo header { **legal** | **login** | **motd** | **shell** }

Default

The device does not have banners.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

legal: Configures the banner to be displayed before a user inputs the username and password to access the CLI.

login: Configures the banner to be displayed before password or scheme authentication is performed for a login user.

motd: Configures the greeting banner to be displayed before the legal banner appears.

shell: Configures the banner to be displayed before a user accesses user view.

text: Specifies the banner message. You can enter the banner message on the same line as the keywords or on different lines. For more information, see device management in *Fundamentals Configuration Guide*.

Examples

Configure the legal banner.

```
<Sysname> system-view
[Sysname] header legal
Please input banner content, and quit with the character '%'.
Welcome to use the legal banner%
```

job

Use **job** to assign a job to a schedule.

Use **undo job** to revoke a job.

Syntax

job *job-name*

undo job *job-name*

Default

No job is assigned to a schedule.

Views

Schedule view

Predefined user roles

network-admin

context-admin

Parameters

job-name: Specifies the job name, a case-sensitive string of 1 to 47 characters.

Usage guidelines

You can assign multiple jobs to a schedule. The jobs in a schedule are executed concurrently.

The jobs to be assigned to a schedule must already exist. To create a job, use the **scheduler job** command.

Examples

Assign job **save-job** to schedule **saveconfig**.

```
<Sysname> system-view
[Sysname] scheduler schedule saveconfig
[Sysname-schedule-saveconfig] job save-job
```

Related commands

scheduler job

scheduler schedule

locator blink

Use **locator blink** *blink-time* to start LED flashing to locate devices.

Use **locator blink stop** to stop LED flashing.

Syntax

locator [**slot** *slot-number*] **blink** *blink-time*

locator [**slot** *slot-number*] **blink stop**

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, the command applies to all member devices.

blink-time: Specifies the flash duration in seconds. The value range is 5 to 120.

stop: Stops flashing.

Usage guidelines

This command is supported only on the default context.

The device provides a LED for device locating. The **locator blink** *blink-time* command flashes the specified LEDs quickly for a period of time unless you execute the **locator blink stop** command. You can observe the LEDs to locate the devices.

Examples

Start LED flashing to locate devices.

```
<Sysname> locator blink 30
```

Stop LED flashing.

```
<Sysname> locator blink stop
```

memory-threshold

Use **memory-threshold** to set free-memory thresholds.

Use **undo memory-threshold** to restore the default.

Syntax

memory-threshold [**slot** *slot-number* [**cpu** *cpu-number*]] [**ratio**] **minor** *minor-value* **severe** *severe-value* **critical** *critical-value* **normal** *normal-value*

undo memory-threshold [**slot** *slot-number* [**cpu** *cpu-number*]]

Default

The default settings vary by device model. To view the default settings, use the **undo memory-threshold** command to restore the default settings and then execute the **display memory-threshold** command.

Views

System view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command sets free-memory thresholds for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

ratio: Specifies free-memory thresholds in percentage. If you do not specify this keyword, the command sets free-memory thresholds in MB.

minor *minor-value*: Specifies the minor alarm threshold. To view the value range for this threshold, enter a question mark (?) in the place of the *minor-value* argument. Setting this threshold to 0 disables the minor alarm feature.

severe *severe-value*: Specifies the severe alarm threshold. To view the value range for this threshold, enter a question mark (?) in the place of the *severe-value* argument. Setting this threshold to 0 disables the severe alarm feature.

critical *critical-value*: Specifies the critical alarm threshold. To view the value range for this threshold, enter a question mark (?) in the place of the *critical-value* argument. Setting this threshold to 0 disables the critical alarm feature.

normal *normal-value*: Specifies the normal state threshold. To view the value range for this threshold, enter a question mark (?) in the place of the *normal-value* argument.

Usage guidelines

This command is supported only on the default context.

To ensure correct operation and improve memory efficiency, the system monitors the amount of free memory space in real time. If the amount of free memory space decreases to or below the minor, severe, or critical alarm threshold, the system issues an alarm to affected service modules or processes.

The early warning feature warns you of an approaching insufficient-memory condition.

If a memory alarm occurs, delete unused configuration items or disable some features to increase the free memory space. Because the memory space is insufficient, some configuration items might not be able to be deleted.

For more information about the thresholds, see device management in *Fundamentals Configuration Guide*.

Examples

Set the minor alarm, severe alarm, critical alarm, and normal state thresholds to 64 MB, 48 MB, 32 MB, and 96 MB, respectively.

```
<Sysname> system-view
[Sysname] memory-threshold minor 64 severe 48 critical 32 normal 96
```

Related commands

display memory-threshold

memory-threshold usage

Use **memory-threshold usage** to set the memory usage threshold.

Use **undo memory-threshold usage** to restore the default.

Syntax

memory-threshold [**slot** *slot-number* [**cpu** *cpu-number*]] **usage** *memory-threshold*

undo memory-threshold [**slot** *slot-number* [**cpu** *cpu-number*]] **usage**

Default

Models	Default
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280	90%
NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	95%

Views

System view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command sets the memory usage threshold for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

memory-threshold: Specifies the memory usage threshold in percentage. The value range is 0 to 100.

Usage guidelines

This command is supported only on the default context.

The device samples memory usage at 1-minute intervals. If the sample is equal to or greater than the memory usage threshold, the device sends a trap.

Examples

Set the memory usage threshold to 80%.

```
<Sysname> system-view
[Sysname] memory-threshold usage 80
```

Related commands

display memory-threshold

monitor cpu-usage enable

Use **monitor cpu-usage enable** to enable CPU usage monitoring.

Use **undo monitor cpu-usage enable** to disable CPU usage monitoring.

Syntax

monitor cpu-usage enable [**slot** *slot-number* [**cpu** *cpu-number*]]

undo monitor cpu-usage enable [**slot** *slot-number* [**cpu** *cpu-number*]]

Default

CPU usage monitoring is enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command enables CPU usage monitoring for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

After CPU usage monitoring is enabled, the system samples and saves CPU usage at the interval specified by the **monitor cpu-usage interval** command. You can use the **display cpu-usage history** command to view recent CPU usage.

Examples

Enable CPU usage monitoring.

```
<Sysname> system-view
[Sysname] monitor cpu-usage enable
```

Related commands

display cpu-usage configuration

display cpu-usage history

monitor cpu-usage interval

monitor cpu-usage interval

Use **monitor cpu-usage interval** to set the sampling interval for CPU usage monitoring.

Syntax

monitor cpu-usage interval *interval* [**slot** *slot-number* [**cpu** *cpu-number*]]

Default

The system samples CPU usage every 1 minute.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies the sampling interval for CPU usage monitoring. Valid values include **5Sec** (5 seconds), **1Min** (1 minute), and **5Min** (5 minutes), case insensitive.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command sets the interval for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

After CPU usage monitoring is enabled, the system samples and saves CPU usage at the specified interval. You can use the **display cpu-usage history** command to view recent CPU usage.

Examples

Set the sampling interval for CPU usage monitoring to 5 seconds.

```
<Sysname> system-view
[Sysname] monitor cpu-usage interval 5Sec
```

Related commands

display cpu-usage configuration

display cpu-usage history

monitor cpu-usage enable

monitor cpu-usage logging

Use **monitor cpu-usage logging** to enable periodic CPU usage logging.

Use **undo monitor cpu-usage logging** to disable periodic CPU usage logging.

Syntax

monitor cpu-usage logging slot *slot-number* **cpu** *cpu-number* **interval** *interval-time*

undo monitor cpu-usage logging slot *slot-number* **cpu** *cpu-number*

Default

Periodic CPU usage logging is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID.

cpu *cpu-number*: Specifies a CPU by its number.

interval *interval-time*: Specifies the logging interval in seconds, a multiple of five in the range of 5 to 300.

Examples

Enable periodic CPU usage logging for CPU 0 on slot 1 and set the logging interval to 5 seconds.

```
<Sysname> system-view
[Sysname] monitor cpu-usage logging slot 1 cpu 0 interval 5
```

monitor cpu-usage statistics-interval core

Use **monitor cpu-usage statistics-interval core** to set CPU core usage statistics intervals.

Use **undo monitor cpu-usage statistics-interval core** to restore the default.

Syntax

monitor cpu-usage statistics-interval *interval* **slot** *slot-number* **cpu** *cpu-number* **core** *core-id-list*

undo monitor cpu-usage statistics-interval slot *slot-number* **cpu** *cpu-number* **core** *core-id-list*

Default

The CPU core usage statistics interval is 60 seconds.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies the CPU core usage statistics interval in seconds. The value range for this argument is 10 to 3600. As a best practice, set this argument to a multiple of the sampling interval, which is fixed at 5 seconds. If you do not do so, the actual statistics interval is the biggest multiple of the sampling interval that is smaller than the setting. For example, if you set this argument to 12 seconds, the actual statistics interval is 10 seconds.

slot *slot-number*: Specifies an IRF member device by its member ID.

cpu *cpu-number*: Specifies a CPU by its number.

core *core-id-list*: Specifies a space-separated list of up to 10 CPU core items. Each item specifies a CPU core or a range of CPU cores in the form of *core-id1* [**to** *core-id2*]. The value for *core-id2* must be greater than or equal to the value for *core-id1*.

Usage guidelines

The device samples CPU core usage at 5-second intervals and calculates the average value during each CPU core usage statistics interval. If the value during an interval is greater than the CPU core usage threshold, the device issues an alarm and logs the event.

Examples

Set the usage statistics interval to 60 seconds for a CPU core.

```
<Sysname> system-view
[Sysname] monitor cpu-usage statistics-interval 60 slot 1 cpu 0 core 0
```

Related commands

monitor cpu-usage threshold core

monitor resend cpu-usage core-interval

monitor cpu-usage threshold

Use **monitor cpu-usage threshold** to set CPU usage alarm thresholds.

Use **undo monitor cpu-usage threshold** to restore the default.

Syntax

monitor cpu-usage threshold *severe-threshold* **recovery-threshold** *recovery-threshold* [**slot** *slot-number* [**cpu** *cpu-number*]]

undo monitor cpu-usage threshold recovery-threshold [**slot** *slot-number* [**cpu** *cpu-number*]]

Default

The CPU usage alarm threshold is 70%. The CPU usage recovery threshold is 30%.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

severe-threshold: Specifies the severe CPU usage alarm threshold in percentage. The value range for this argument is 2 to 100.

recovery-threshold *recovery-threshold*: Specifies the CPU usage recovery threshold in percentage. The value range for this argument is 0 to the minor CPU usage alarm threshold minus 1.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command sets the CPU usage threshold for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

CAUTION:

If you set the severe CPU usage alarm threshold to a too low value, the device will reach the threshold easily. Normal services will be affected.

The device samples CPU usage at 1-minute intervals. If the sample is greater than the CPU usage threshold, the device sends a trap.

Examples

Set the CPU usage alarm threshold to 90% and the CPU usage recovery threshold to 70%.

```
<Sysname> system-view
[Sysname] monitor cpu-usage threshold 90 recovery-threshold 70
```

Related commands

display cpu-usage configuration

monitor memory-usage logging

Use **monitor memory-usage logging** to enable periodic memory usage logging.

Use **undo monitor memory-usage logging** to disable periodic memory usage logging.

Syntax

monitor memory-usage logging slot *slot-number* **cpu** *cpu-number* **interval** *interval-time*

undo monitor memory-usage logging slot *slot-number* **cpu** *cpu-number*

Default

Periodic memory usage logging is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID.

cpu *cpu-number*: Specifies a CPU by its number.

interval *interval-time*: Specifies the logging interval in seconds, a multiple of five in the range of 5 to 300.

Examples

Enable periodic memory usage logging for CPU 0 on slot 1 and set the logging interval to 5 seconds.

```
<Sysname> system-view
[Sysname] monitor memory-usage logging slot 1 cpu 0 interval 5
```

monitor resend cpu-usage core-interval

Use **monitor resend cpu-usage core-interval** to set CPU core alarm resending intervals.

Use **undo monitor resend cpu-usage core-interval** to restore the default.

Syntax

monitor resend cpu-usage core-interval *core-interval* [**slot** *slot-number* [**cpu** *cpu-number*]]

undo monitor resend cpu-usage core-interval [**slot** *slot-number* [**cpu** *cpu-number*]]

Default

The CPU core alarm resending interval is 300 seconds.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

core-interval: Specifies the CPU core alarm resending interval in seconds, a multiple of 5 in the range of 10 to 3600.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command sets the CPU core alarm resending interval for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Examples

Set the CPU core alarm resending interval to 60 seconds.

```
<Sysname> system-view
[Sysname] monitor resend cpu-usage core-interval 60
```

monitor resource-usage { bridge-aggregation | route-aggregation } threshold

Use **monitor resource-usage { bridge-aggregation | route-aggregation } threshold** to set aggregate interface usage thresholds.

Use **undo monitor resource-usage { bridge-aggregation | route-aggregation } threshold** to restore the default.

Syntax

monitor resource-usage { bridge-aggregation | route-aggregation } threshold *threshold-value*

undo monitor resource-usage { bridge-aggregation | route-aggregation } threshold

Default

No aggregate interface usage thresholds are set. The aggregate interface usage alarm feature is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

bridge-aggregation: Sets the Layer 2 aggregate interface usage threshold.

route-aggregation: Sets the Layer 3 aggregate interface usage threshold.

threshold-value: Specifies the aggregate interface usage threshold in the range of 1 to 4294967295.

Usage guidelines

When the number of created Layer 2 or Layer 3 aggregate interfaces reaches the threshold, the device sends an alarm. If the alarm state persists, the device resends the alarm at 3-hour intervals.

Examples

Set the Layer 2 aggregate interface usage threshold to 100.

```
<Sysname> system-view
[Sysname] monitor resource-usage bridge-aggregation threshold 100
```

Set the Layer 3 aggregate interface usage threshold to 150.

```
<Sysname> system-view
[Sysname] monitor resource-usage route-aggregation threshold 150
```

monitor resource-usage bandwidth inbound threshold

Use **monitor resource-usage bandwidth inbound threshold** to set the total inbound bandwidth usage threshold.

Use **undo monitor resource-usage bandwidth inbound threshold** to restore the default.

Syntax

monitor resource-usage bandwidth inbound threshold *threshold-value* [**duration** *duration-value*]

undo monitor resource-usage bandwidth inbound threshold

Default

The total inbound bandwidth usage threshold is not set. The bandwidth usage alarm feature is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

threshold-value: Specify the total inbound bandwidth usage threshold in Mbps. The value range for this argument is 1 to 4294967295.

duration *duration-value*: Specify the high-usage duration criterion in seconds, a multiple of five in the range of 5 to 300. The default value is 300.

Usage guidelines

This command is supported only on the default context.

If the total inbound traffic remains greater than or equal to the total inbound bandwidth usage threshold for the specified duration, the device sends an alarm. If the alarm state persists, the device resends the alarm at 5-second intervals.

Examples

Set the total inbound bandwidth usage threshold to 1024 Mbps and set the high-usage duration criterion to 60 seconds.

```
<Sysname> system-view
[Sysname] monitor resource-usage bandwidth inbound threshold 1024 duration 60
```

monitor resource-usage context threshold

Use **monitor resource-usage context threshold** to set the global context usage threshold.

Use **undo monitor resource-usage context threshold** to restore the default.

Syntax

monitor resource-usage context threshold *threshold-value*

undo monitor resource-usage context threshold

Default

The global context usage threshold is not set. The context usage alarm feature is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

threshold-value: Specifies the global context usage threshold in the range of 1 to 4294967295.

Usage guidelines

This command is supported only on the default context.

When the number of created contexts on the device reaches the threshold, the device sends an alarm. If the alarm state persists, the device resends the alarm at 6-hour intervals.

Examples

Set the global context usage threshold to 16.

```
<Sysname> system-view
[Sysname] monitor resource-usage context threshold 16
```

monitor resource-usage nat threshold

Use **monitor resource-usage nat threshold** to set the NAT mapping threshold.

Use **undo monitor resource-usage nat threshold** to restore the default.

Syntax

monitor resource-usage nat threshold *threshold-value*

undo monitor resource-usage nat threshold

Default

The NAT mapping threshold is not set. The NAT mapping alarm feature is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

threshold-value: Specifies the NAT mapping threshold in the range of 1 to 4294967295.

Usage guidelines

When the number of NAT mappings reaches the threshold, the device sends an alarm. If the alarm state persists, the device resends the alarm at 3-hour intervals.

In the current software version, this feature counts only static NAT mappings and effective NAT server mappings. To display the status of NAT server mappings, execute the **display nat server** command.

Examples

Set the NAT mapping threshold to 300.

```
<Sysname> system-view
[Sysname] monitor resource-usage nat threshold 300
```

Related commands

display nat server (*Layer 3—IP Services Command Reference*)

monitor resource-usage security-policy threshold

Use **monitor resource-usage security-policy** { **ip** | **ipv6** } **threshold** to set security policy rule usage thresholds.

Use **undo monitor resource-usage security-policy** { **ip** | **ipv6** } **threshold** to restore the default.

Syntax

monitor resource-usage security-policy { **ip** | **ipv6** } **threshold** *threshold-value*

undo monitor resource-usage security-policy { **ip** | **ipv6** } **threshold**

Default

No security policy rule thresholds are set. The security policy rule alarm feature is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ip: Sets the IPv4 security policy rule threshold.

ipv6: Sets the IPv6 security policy rule threshold.

threshold-value: Specifies the security policy rule threshold in the range of 1 to 4294967295.

Usage guidelines

When the number of created security policy rules reaches the threshold, the device sends an alarm. If the alarm state persists, the device resends the alarm at 6-hour intervals.

Examples

Set the IPv4 security policy rule threshold to 500.

```
<Sysname> system-view
[Sysname] monitor resource-usage security-policy ip threshold 500
```

Set the IPv6 security policy rule threshold to 500.

```
<Sysname> system-view
[Sysname] monitor resource-usage security-policy ipv6 threshold 500
```

monitor resource-usage session-count threshold

Use **monitor resource-usage session-count threshold** to set session usage thresholds.

Use **undo monitor resource-usage session-count threshold** to restore the default.

Syntax

monitor resource-usage session-count [**slot** *slot-number*] **threshold** *threshold-value*

undo monitor resource-usage session-count [**slot** *slot-number*] **threshold**

Default

No session usage thresholds are set. The session usage alarm feature is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command sets the session usage threshold for the master device.

threshold-value: Specifies the session threshold in the range of 1 to 4294967295.

Usage guidelines

When the number of sessions reaches the threshold, the device sends an alarm. If the alarm state persists, the device resends the alarm at 10-minute intervals.

Examples

Set the session usage threshold to 100000.

```
<Sysname> system-view
[Sysname] monitor resource-usage session-count threshold 100000
```

monitor resource-usage session-rate threshold

Use **monitor resource-usage session-rate threshold** to set session establishment rate thresholds.

Use **undo monitor resource-usage session-rate threshold** to restore the default.

Syntax

monitor resource-usage session-rate [**slot** *slot-number*] **threshold** *threshold-value*

undo monitor resource-usage session-rate [**slot** *slot-number*] **threshold**

Default

No session establishment rate thresholds are set. The session establishment rate alarm feature is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command sets the session establishment rate threshold for the master device.

threshold-value: Specifies the session establishment rate threshold in the range of 1 to 4294967295.

Usage guidelines

When the session establishment rate reaches the threshold, the device sends an alarm. If the alarm state persists, the device resends the alarm at 10-minute intervals.

Examples

Set the session establishment rate threshold to 500.

```
<Sysname> system-view
[Sysname] monitor resource-usage session-rate threshold 500
```

password-recovery enable

Use **password-recovery enable** to enable password recovery capability.

Use **undo password-recovery enable** to disable password recovery capability.

Syntax

password-recovery enable

undo password-recovery enable

Default

Password recovery capability is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command is supported only on the default context.

Password recovery capability controls console user access to the device configuration and SDRAM from BootWare menus.

If password recovery capability is enabled, a console user can access the device configuration without authentication to configure new passwords.

If password recovery capability is disabled, console users must restore the factory-default configuration before they can configure new passwords. Restoring the factory-default configuration deletes the next-startup configuration files.

To enhance system security, disable password recovery capability.

To access the device configuration without authentication, you must connect to the master device and access the BootWare menu while the master device is starting up.

Availability of BootWare menu options depends on the password recovery capability setting. For more information, see the release notes.

Examples

Disable password recovery capability.

```
<Sysname> system-view
[Sysname] undo password-recovery enable
```

reboot

Use **reboot** to reboot the device.

Syntax

reboot [**slot** *slot-number*] [**force**]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify an IRF member device, the command reboots all IRF member devices.

force: Reboots the device immediately without performing software or hard disk check. If this keyword is not specified, the system first identifies whether the reboot might result in data loss or a system failure. For example, the system identifies whether the main system software image file exists and whether a write operation is in progress on a storage medium. If the reboot might cause problems, the system does not reboot the device.

Usage guidelines

CAUTION:

- A reboot might interrupt network services.
- Use the **force** keyword only when the device fails or a **reboot** command without the **force** keyword cannot perform a reboot correctly. A **reboot** command with the **force** keyword might result in file system corruption because it does not perform data protection.

If the main startup software images are corrupt or missing, you must re-specify a set of main startup software images before executing the **reboot** command.

For data security, the device does not reboot if you reboot the device while the device is performing file operations.

If the IRF fabric has only one member device, rebooting the member device reboots the entire IRF fabric. If the IRF fabric has a subordinate member and the member is operating correctly, rebooting the master triggers a master/subordinate switchover.

To ensure correct operation of the IRF fabric and member devices, do not trigger a switchover by rebooting the master if no subordinate member devices are in **Stable** state. To view the status of subordinate member devices, execute the **display system stable state** command.

Examples

Reboot the device. Save the running configuration at prompt.

```
<Sysname> reboot
Start to check configuration with next startup configuration file, please
wait.........DONE!
Current configuration will be lost after the reboot, save current configuration? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Configuration is saved to mainboard device successfully.
This command will reboot the device. Continue? [Y/N]:y
Now rebooting, please wait...
```

Reboot the device immediately without performing software check.

```
<Sysname> reboot force
A forced reboot might cause the storage medium to be corrupted. Continue? [Y/N]:y
Now rebooting, please wait...
```

Related commands

display system stable state

reset scheduler logfile

Use **reset scheduler logfile** to clear job execution log information.

Syntax

reset scheduler logfile

Views

User view

Predefined user roles

network-admin

Examples

Clear job execution log information.

```
<Sysname> reset scheduler logfile
```

Related commands

display scheduler logfile

reset version-update-record

Use **reset version-update-record** to clear startup software image upgrade records.

Syntax

reset version-update-record

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command is supported only on the default context.

Examples

Clear the startup software image upgrade records.

```
<Sysname> system-view
[Sysname] reset version-update-record
This command will delete all records of version update. Continue? [Y/N]:y
```

Related commands

display version-update-record

restore factory-default

Use **restore factory-default** to restore the factory-default configuration for the device.

Syntax

restore factory-default

Views

User view

Predefined user roles

network-admin

Usage guidelines

CAUTION:

This command restores the device to the factory default settings. Before using this command, make sure you fully understand its impact on your live network.

This command is supported only on the default context.

Use this command only when you cannot troubleshoot the device by using other methods, or you want to use the device in a different scenario.

Examples

Restore the factory-default configuration for the device.

```
<Sysname> restore factory-default
This command will restore the system to the factory default configuration and clear the operation data, and forcibly reboot the system. Continue [Y/N]:y
Restoring the factory default configuration. This process might take a few minutes. Please wait....Done.
The system is rebooting...
```

Related commands

reboot

scheduler job

Use **scheduler job** to create a job and enter its view, or enter the view of an existing job.

Use **undo scheduler job** to delete a job.

Syntax

scheduler job *job-name*

undo scheduler job *job-name*

Default

No job exists.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

job-name: Specifies the job name, a case-sensitive string of 1 to 47 characters.

Usage guidelines

A job can be referenced by multiple schedules. In job view, you can assign commands to the job.

Examples

Create a job named **backupconfig** and enter job view.

```
<Sysname> system-view
[Sysname] scheduler job backupconfig
[Sysname-job-backupconfig]
```

Related commands

command

scheduler schedule

scheduler logfile size

Use **scheduler logfile size** to set the size of the job execution log file.

Syntax

scheduler logfile size *value*

Default

The size of the job execution log file is 16 KB.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

value: Specifies the size of the job execution log file, in KB. The value range is 16 to 1024.

Usage guidelines

The job execution log file stores the execution information of jobs. If the file is full, old records are deleted to make room for new records. If the size of the log information to be written to the file is greater than the file size, the excessive information is not written to the file.

Examples

Set the size of the job execution log file to 32 KB.

```
<Sysname> system-view
[Sysname] scheduler logfile size 32
```

Related commands

display scheduler logfile

scheduler reboot at

Use **scheduler reboot at** to specify the reboot date and time.

Use **undo scheduler reboot** to delete the reboot schedule configuration.

Syntax

scheduler reboot at *time* [*date*]

undo scheduler reboot

Default

No reboot date or time is specified.

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

time: Specifies the reboot time in the *hh:mm* format. The value range for *hh* is 0 to 23. The value range for *mm* is 0 to 59.

date: Specifies the reboot date in the *MM/DD/YYYY* or *YYYY/MM/DD* format. The value range for *YYYY* is 2000 to 2035. The value range for *MM* is 1 to 12. The value range for *DD* varies by month.

Usage guidelines

CAUTION:
This command enables the device to reboot at a scheduled time, which causes service interruption. Before using this command, make sure you fully understand its impact on your live network.

When the *date* argument is not specified, the system uses the following rules to determine the reboot time:

- If the reboot time is later than the current time, a reboot occurs at the reboot time of the current day.
- If the reboot time is earlier than the current time, a reboot occurs at the reboot time the next day.

The device supports only one device reboot schedule. If you execute both the **scheduler reboot delay** and **scheduler reboot at** commands or execute one of the commands multiple times, the most recent configuration takes effect.

For data security, the system does not reboot at the reboot time if a file operation is being performed.

Examples

Configure the device to reboot at 12:00 p.m. This example assumes that the current time is 11:43 a.m. on June 6, 2015.

```
<Sysname> scheduler reboot at 12:00
Reboot system at 12:00:00 06/06/2015 (in 0 hours and 16 minutes). Confirm? [Y/N]:
```

Related commands

scheduler reboot delay

scheduler reboot delay

Use **scheduler reboot delay** to specify the reboot delay time.

Use **undo scheduler reboot** to delete the reboot schedule configuration.

Syntax

scheduler reboot delay *time*

undo scheduler reboot

Default

No reboot delay time is specified.

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

time: Specifies the reboot delay time in the *hh:mm* or *mm* format. This argument can contain up to six characters. When in the *hh:mm* format, *mm* must be in the range of 0 to 59.

Usage guidelines

CAUTION:

This command enables the device to reboot at a scheduled time, which causes service interruption. Before using this command, make sure you fully understand its impact on your live network.

The device supports only one device reboot schedule. If you execute both the **scheduler reboot delay** and **schedule reboot at** commands or execute one of the commands multiple times, the most recent configuration takes effect.

For data security, the system does not reboot at the reboot time if a file operation is being performed.

Examples

Configure the device to reboot after 88 minutes. This example assumes that the current time is 11:48 a.m. on June 6, 2015.

```
<Sysname> scheduler reboot delay 88
Reboot system at 13:16 06/06/2015(in 1 hours and 28 minutes). Confirm? [Y/N]:
```

scheduler schedule

Use **scheduler schedule** to create a schedule and enter its view, or enter the view of an existing schedule.

Use **undo scheduler schedule** to delete a schedule.

Syntax

scheduler schedule *schedule-name*

undo scheduler schedule *schedule-name*

Default

No schedule exists.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

schedule-name: Specifies the schedule name, a case-sensitive string of 1 to 47 characters.

Usage guidelines

You can configure a schedule to have the device automatically run a command or a set of commands without administrative interference.

To configure a schedule:

1. Use the **scheduler job** command to create a job and enter job view.
2. Use the **command** command to assign commands to the job.

3. Use the **scheduler schedule** command to create a schedule and enter schedule view.
4. Use the **job** command to assign the job to the schedule. You can assign multiple jobs to a schedule. The jobs must already exist.
5. Use the **user-role** command to assign user roles to the schedule. You can assign up to 64 user roles to a schedule.
6. Use the **time at**, **time once**, or **time repeating** command to specify an execution time for the schedule. You can specify only one execution time for a schedule.

Examples

Create a schedule named **saveconfig**.

```
<Sysname> system-view
[Sysname] scheduler schedule saveconfig
```

Related commands

job

time at

time once

shutdown-interval

Use **shutdown-interval** to set the port status detection timer.

Use **undo shutdown-interval** to restore the default.

Syntax

shutdown-interval *interval*

undo shutdown-interval

Default

The port status detection timer setting is 30 seconds.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies the port status detection timer value in seconds. The value range is 0 to 300. To disable port status detection, set this argument to 0.

Usage guidelines

The device starts a port status detection timer when a port is shut down by a protocol. Once the timer expires, the device brings up the port so the port status reflects the port's physical status.

If you change the timer setting during port detection, the device compares the new setting (T1) with the time that elapsed since the port was shut down (T).

If T < T1, the port will be brought up after T1 – T seconds.

If T ≥ T1, the port is brought up immediately.

For example, the timer setting is 30 seconds. If you change it to 10 seconds 2 seconds after the port is shut down, the port will come up 8 seconds later. If you change the timer setting to 2 seconds 10 seconds after the port is shut down, the port comes up immediately.

Examples

Set the port status detection timer to 100 seconds.

```
<Sysname> system-view
[Sysname] shutdown-interval 100
```

sysid

Use **sysid** to set the system ID.

Use **undo sysid** to restore the default.

Syntax

sysid *system-id*

undo sysid

Default

The device does not have a system ID.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

system-id: Specifies the system ID for the device. You can use this argument to indicate the position or functionality of the device or any other information.

Examples

Set the system ID of the device to **position-hall**.

```
<Sysname> system-view
[Sysname] sysid positon-hall
```

sysname

Use **sysname** to set the device name.

Use **undo sysname** to restore the default.

Syntax

sysname *sysname*

undo sysname

Default

The device name is NSFOCUS.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

sysname: Specifies a name for the device, a string of 1 to 64 characters.

Usage guidelines

A device name identifies a device in a network and is used in CLI view prompts. For example, if the device name is **Sysname**, the user view prompt is <Sysname>.

Examples

Set the name of the device to **R2000**.

```
<Sysname> system-view
[Sysname] sysname R2000
[R2000]
```

temperature-limit

Use **temperature-limit** to set the temperature alarm thresholds.

Use **undo temperature-limit** to restore the default.

Syntax

temperature-limit slot *slot-number* { **hotspot** | **inflow** | **outflow** } *sensor-number lowlimit warninglimit* [*alarmlimit*]

undo temperature-limit slot *slot-number* { **hotspot** | **inflow** | **outflow** } *sensor-number*

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480,	Yes
NFNX3-HDB680, NFNX3-HDB1080	No

Default

The defaults vary by temperature sensor model. To view the defaults, execute the **undo temperature-limit** and **display environment** commands in turn.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID.

hotspot: Configures temperature alarm thresholds for hotspot sensors. A hotspot sensor is typically near the chip that generates a great amount of heat and used to monitor the chip.

The following compatibility matrixes show the support of hardware platforms for the **hotspot** keyword:

Models	Parameter compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080	Yes
NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	No

inflow: Configures temperature alarm thresholds for inlet sensors. An inlet sensor is near the air inlet and used for monitoring ambient temperature.

outflow: Configures temperature alarm thresholds for outlet sensors. An outlet sensor is near the air outlet for monitoring device temperature.

sensor-number: Specifies a sensor by its number. To view the value range, enter a question mark (?) in the place of this argument.

lowlimit: Specifies the low-temperature threshold in Celsius degrees. The value range varies by temperature sensor. To view the value range, enter a question mark (?) in the place of this argument.

warninglimit: Specifies the high-temperature warning threshold in Celsius degrees. This threshold must be greater than the low-temperature threshold. To view the value range, enter a question mark (?) in the place of this argument.

alarmlimit: Specifies the high-temperature alarming threshold in Celsius degrees. This threshold must be greater than the warning threshold. To view the value range, enter a question mark (?) in the place of this argument.

Usage guidelines

This command is supported only on the default context.

When the device temperature drops below the low-temperature threshold or reaches the high-temperature warning or alarming threshold, the device performs the following operations:

- Sends log messages and traps.
- Sets LEDs on the device panel.

Examples

Set temperature alarm thresholds for hotspot sensor 1 in a slot.

```
<Sysname> system-view
[Sysname] temperature-limit slot 1 hotspot 1 -10 50 60
```

Related commands

display environment

time at

Use **time at** to specify an execution date and time for a non-periodic schedule.

Use **undo time** to delete the execution date and time configuration for a non-periodic schedule.

Syntax

time at *time date*

undo time

Default

No execution time or date is specified for a non-periodic schedule.

Views

Schedule view

Predefined user roles

network-admin

context-admin

Parameters

time: Specifies the schedule execution time in the *hh:mm* format. The value range for *hh* is 0 to 23. The value range for *mm* is 0 to 59.

date: Specifies the schedule execution date in the *MM/DD/YYYY* or *YYYY/MM/DD* format. The value range for *YYYY* is 2000 to 2035. The value range for *MM* is 1 to 12. The value range for *DD* varies by month.

Usage guidelines

The specified time (date plus time) must be later than the current system time.

The **time at** command, the **time once** command, and the **time repeating** command overwrite one another. The most recently executed command takes effect.

Examples

Configure the device to execute schedule **saveconfig** at 01:01 a.m. on May 11, 2015.

```
<Sysname> system-view
[Sysname] scheduler schedule saveconfig
[Sysname-schedule-saveconfig] time at 1:1 2015/05/11
```

Related commands

scheduler schedule

time once

Use **time once** to specify one or more execution days and the execution time for a non-periodic schedule.

Use **undo time** to delete the execution day and time configuration for a non-periodic schedule.

Syntax

time once at *time* [**month-date** *month-day* | **week-day** *week-day*&<1-7>]

time once delay *time*

undo time

Default

No execution time or day is specified for a non-periodic schedule.

Views

Schedule view

Predefined user roles

network-admin

context-admin

Parameters

at *time*: Specifies the execution time in the *hh:mm* format. The value range for *hh* is 0 to 23. The value range for *mm* is 0 to 59.

month-date *month-day*: Specifies a day in the current month, in the range of 1 to 31. If you specify a day that does not exist in the current month, the configuration takes effect on that day in the next month.

week-day *week-day*&<1-7>: Specifies a space-separated list of up to seven week days for the schedule. Valid week day values include **Mon**, **Tue**, **Wed**, **Thu**, **Fri**, **Sat**, and **Sun**.

delay *time*: Specifies the delay time for executing the schedule, in the *hh:mm* or *mm* format. This argument can have up to six characters. When in the *hh:mm* format, *mm* must be in the range of 0 to 59.

Usage guidelines

If the specified time has already occurred, the schedule will be executed at the specified time the following day.

If the day in the month has already occurred, the schedule will be executed at the specified day in the following month.

If the specified day in a week has already occurred, the schedule will be executed at the specified day in the following week.

The **time at** command, the **time once** command, and the **time repeating** command overwrite one another. The most recently executed command takes effect.

Examples

Configure the device to execute schedule **saveconfig** once at 15:00.

```
<Sysname> system-view
[Sysname] scheduler schedule saveconfig
[Sysname-schedule-saveconfig] time once at 15:00
Schedule starts at 15:00 5/11/2011.
```

Configure the device to execute schedule **saveconfig** once at 15:00 on the coming 15th day in a month.

```
<Sysname> system-view
[Sysname] scheduler schedule saveconfig
[Sysname-schedule-saveconfig] time once at 15:00 month-date 15
```

Configure the device to execute schedule **saveconfig** at 12:00 p.m. on the coming Monday and Friday.

```
<Sysname> system-view
[Sysname] scheduler schedule saveconfig
[Sysname-schedule-saveconfig] time once at 12:00 week-day mon fri
```

Configure the device to execute schedule **saveconfig** after 10 minutes.

```
<Sysname> system-view
[Sysname] scheduler schedule saveconfig
[Sysname-schedule-saveconfig] time once delay 10
```

Related commands

scheduler schedule

time repeating

Use **time repeating** to specify an execution time table for a periodic schedule.

Use **undo time** to delete the execution time table configuration for a periodic schedule.

Syntax

time repeating [**at** *time* [*date*]] **interval** *interval*

time repeating at *time* [**month-date** [*month-day* | **last**] | **week-day** *week-day*&<1-7>]

undo time

Default

No execution time table is specified for a periodic schedule.

Views

Schedule view

Predefined user roles

network-admin

context-admin

Parameters

at *time*: Specifies the execution time in the *hh:mm* format. The value range for *hh* is 0 to 23. The value range for *mm* is 0 to 59. If you do not specify this option, the current system time is used as the execution time.

date: Specifies the start date for the periodic schedule, in the *MM/DD/YYYY* or *YYYY/MM/DD* format. The value range for *YYYY* is 2000 to 2035. The value range for *MM* is 1 to 12. The value range for *DD* varies by month. If you do not specify this argument, the execution start date is the first day when the specified time arrives.

interval *interval*: Specifies the execution time interval in the *hh:mm or mm* format. This argument can have up to six characters. When in the *hh:mm* format, *mm* must be in the range of 0 to 59. When in the *mm* format, this argument must be equal to or greater than 1 minute.

month-date [*month-day* | **last**]: Specifies a day in a month, in the range 1 to 31. The **last** keyword indicates the last day of a month. If you specify a day that does not exist in a month, the configuration takes effect on that day in the next month.

week-day *week-day*&<1-7>: Specifies a space-separated list of up to seven week days for the schedule. Valid week day values include **Mon**, **Tue**, **Wed**, **Thu**, **Fri**, **Sat**, and **Sun**.

Usage guidelines

The **time repeating** [**at** *time* [*date*]] **interval** *interval* command configures the device to execute a schedule at intervals from the specified time on.

The **time repeating at** *time* [**month-date** [*month-day* | **last**] | **week-day** *week-day*&<1-7>] command configures the device to execute a schedule at the specified time on every specified day in a month or week.

The **time at** command, the **time once** command, and the **time repeating** command overwrite one another, whichever is executed most recently takes effect.

Examples

Configure the device to execute schedule **saveconfig** once an hour from 8:00 a.m. on.

```
<Sysname> system-view
[Sysname] scheduler schedule saveconfig
[Sysname-schedule-saveconfig] time repeating at 8:00 interval 60
```

Configure the device to execute schedule **saveconfig** at 12:00 p.m. every day.

```
<Sysname> system-view
```

```
[Sysname] scheduler schedule saveconfig
[Sysname-schedule-saveconfig] time repeating at 12:00
```

Configure the device to execute schedule **saveconfig** at 8:00 a.m. on the 5th of every month.

```
<Sysname> system-view
[Sysname] scheduler schedule saveconfig
[Sysname-schedule-saveconfig] time repeating at 8:00 month-date 5
```

Configure the device to execute schedule **saveconfig** at 8:00 a.m. on the last day of every month.

```
<Sysname> system-view
[Sysname] scheduler schedule saveconfig
[Sysname-schedule-saveconfig] time repeating at 8:00 month-date last
```

Configure the device to execute schedule **saveconfig** at 8:00 a.m. every Friday and Saturday.

```
<Sysname> system-view
[Sysname] scheduler schedule saveconfig
[Sysname-schedule-saveconfig] time repeating at 8:00 week-day fri sat
```

Related commands

scheduler schedule

usb disable

Use **usb disable** to disable USB interfaces.

Use **undo usb disable** to enable USB interfaces.

Syntax

usb disable

undo usb disable

Default

All USB interfaces are enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command is supported only on the default context.

You can use USB interfaces to upload or download files or to connect a 3G modem. By default, all USB interfaces are enabled.

Before executing this command, use the **umount** command to unmount all USB file systems.

Examples

Enable USB interfaces.

```
<Sysname> system-view
[Sysname] undo usb disable
```

user-role

Use **user-role** to assign user roles to a schedule.

Use **undo user-role** to remove user roles from a schedule.

Syntax

user-role *role-name*

undo user-role *role-name*

Default

A schedule has the user roles of the schedule creator.

Views

Schedule view

Predefined user roles

network-admin

context-admin

Parameters

role-name: Specifies a user role name, a case-sensitive string of 1 to 63 characters. The user role can be user-defined or predefined. Predefined user roles include network-admin, network-operator, context-admin, context-operator, and level-0 to level-15.

Usage guidelines

A schedule must have one or more user roles. A command in a schedule can be executed if it is permitted by one or more user roles of the schedule. For more information about user roles, see the RBAC configuration in *Fundamentals Configuration Guide*.

A schedule can have a maximum of 64 user roles. After the limit is reached, you cannot assign additional user roles to the schedule.

Examples

Assign user role **rolename** to schedule **test**.

```
<Sysname> system-view
[Sysname] scheduler schedule test
[Sysname-schedule-test] user-role rolename
```

Related commands

command

scheduler **schedule**

Contents

FTP commands

FTP server commands

display ftp-server

Use **display ftp-server** to display FTP server configuration and status information.

Syntax

display ftp-server

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display FTP server configuration and status information.

```
<Sysname> display ftp-server
FTP server is running.
User count:                          1
Idle-timeout timer (in minutes):  30
```

Table 1 Command output

Field	Description
User count	Number of the current logged-in users.
Idle-timeout timer (in minutes)	If no packet is exchanged between the FTP server and client during this period, the FTP connection is closed.

Related commands

ftp server enable

ftp timeout

display ftp-user

Use **display ftp-user** to display detailed information about online FTP users.

Syntax

display ftp-user

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display detailed information about online FTP users.

```
<Sysname> display ftp-user
UserName     HostIP             Port     HomeDir
root         192.168.20.184     46539    flash:
```

A field value is wrapped if its length exceeds the limit. The segments are left justified.

The following are the length limits for fields:

- **UserName**—10 characters.
- **HostIP**—15 characters.
- **HomeDir**—37 characters.

```
<Sysname> display ftp-user
UserName     HostIP             Port     HomeDir
user2        2000:2000:2000:    1499     flash:/user2
             2000:2000:2000:
             2000:2000
administra   100.100.100.100    10001    flash:/123456789/123456789/123456789/
tor                                      123456789/123456789/123456789/1234567
                                         89/123456789
```

Table 2 Command output

Field	Description
UserName	Name of the user.
HostIP	IP address of the user.
Port	Port number of the user.
HomeDir	Authorized directory for the user.

free ftp user

Use **free ftp user** to manually release the FTP connections established by using a specific user account.

Syntax

free ftp user *username*

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

username: Specifies a username. To display online FTP users, execute the **display ftp-user** command.

Examples

Release the FTP connections established by using user account **ftpuser**.

```
<Sysname> free ftp user ftpuser
Are you sure to free FTP connection? [Y/N]:y
<Sysname>
```

free ftp user-ip

Use **free ftp user-ip** to manually release the FTP connections established from a specific IPv4 address.

Syntax

free ftp user-ip *ip-address* [**port** *port*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the source IP address of an FTP connection. To view the source IP addresses of FTP connections, execute the **display ftp-user** command.

port *port*: Specifies the source port of an FTP connection. To view the source ports of FTP connections, execute the **display ftp-user** command.

Examples

Release the FTP connections established from the IP address 192.168.20.184.

```
<Sysname> free ftp user-ip 192.168.20.184
Are you sure to free FTP connection? [Y/N]:y
<Sysname>
```

free ftp user-ip ipv6

Use **free ftp user-ip ipv6 to** manually release the FTP connections established from a specific IPv6 address.

Syntax

free ftp user-ip ipv6 *ipv6-address* [**port** *port*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address: Specifies the source IPv6 address of an FTP connection. To view the source IPv6 addresses of FTP connections, execute the **display ftp-user** command.

port *port*: Specifies the source port of an FTP connection. To view the source ports of FTP connections, execute the **display ftp-user** command.

Examples

Release the FTP connections established from IPv6 address 2000::154.

```
<Sysname> free ftp user-ip ipv6 2000::154
Are you sure to free FTP connection? [Y/N]:y
<Sysname>
```

ftp server acl

Use **ftp server acl** to apply an ACL to control IPv4 FTP clients' access to the FTP server.

Use **undo ftp server acl** to restore the default.

Syntax

ftp server acl { *advanced-acl-number* | *basic-acl-number* | **mac** *mac-acl-number* }

undo ftp server acl

Default

No ACL is used to control IPv4 FTP clients' access to the FTP server.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

advanced-acl-number: Specifies the number of an IPv4 advanced ACL, in the range of 3000 to 3999.

basic-acl-number: Specifies the number of an IPv4 basic ACL, in the range of 2000 to 2999.

mac *mac-acl-number*: Specifies the number of a Layer 2 ACL, in the range of 4000 to 4999.

Usage guidelines

When no ACL is applied, all IPv4 FTP clients can access the FTP server. To control FTP access, specify an ACL that exists and has rules so only IPv4 FTP clients permitted by the ACL can access the FTP server. If you specify an ACL that does not exist or does not have rules, no IPv4 FTP clients can access the FTP server.

If a VPN instance is specified in an ACL rule, the ACL rule applies only to the packets of the VPN instance. If no VPN instance is specified in an ACL rule, the ACL rule applies only to the packets on the public network.

The ACL takes effect only for FTP connections to be established. It does not impact existing FTP connections.

If you execute this command multiple times, the most recent configuration takes effect.

For more information about ACLs, see *ACL and QoS Configuration Guide.*

Examples

Use ACL 2001 to allow only client 1.1.1.1 to access the FTP server.

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule 0 permit source 1.1.1.1 0
[Sysname-acl-ipv4-basic-2001] rule 1 deny source any
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] ftp server acl 2001
```

ftp server acl ipv6

Use **ftp server acl** to apply an ACL to control IPv6 FTP clients' access to the FTP server.

Use **undo ftp server acl** to restore the default.

Syntax

ftp server acl ipv6 { *advanced-acl-number* | *basic-acl-number* | **mac** *mac-acl-number* }

undo ftp server acl ipv6

Default

No ACL is used to control IPv6 FTP clients' access to the FTP server.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

advanced-acl-number: Specifies the number of an IPv6 advanced ACL, in the range of 3000 to 3999.

basic-acl-number: Specifies the number of an IPv6 basic ACL, in the range of 2000 to 2999.

mac *mac-acl-number*: Specifies the number of a Layer 2 ACL, in the range of 4000 to 4999.

Usage guidelines

When no ACL is applied, all IPv6 FTP clients can access the FTP server. To control FTP access, specify an ACL that exists and has rules so only IPv6 FTP clients permitted by the ACL can access the FTP server. If you specify an ACL that does not exist or does not have rules, no IPv6 FTP clients can access the FTP server.

If a VPN instance is specified in an ACL rule, the ACL rule applies only to the packets of the VPN instance. If no VPN instance is specified in an ACL rule, the ACL rule applies only to the packets on the public network.

The ACL takes effect only for FTP connections to be established. It does not impact existing FTP connections.

If you execute this command multiple times, the most recent configuration takes effect.

For more information about ACLs, see *ACL and QoS Configuration Guide.*

Examples

Use ACL 2001 to allow only IPv6 client 1:1::1:1/64 to access the FTP server.

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2001
[Sysname-acl-ipv6-basic-2001] rule 0 permit source 1:1::1:1 64
[Sysname-acl-ipv6-basic-2001] rule 1 deny source any
[Sysname-acl-ipv6-basic-2001] quit
[Sysname] ftp server acl ipv6 2001
```

ftp server acl-deny-log enable

Use **ftp server acl-deny-log enable** to enable logging for FTP login attempts that are denied by the FTP login control ACL.

Use **undo ftp server acl-deny-log enable** to disable logging for FTP login attempts that are denied by the FTP login control ACL.

Syntax

ftp server acl-deny-log enable

undo ftp server acl-deny-log enable

Default

Logging is disabled for FTP login attempts that are denied by the FTP login control ACL.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

Only clients permitted by the FTP login control ACL can use FTP to access the device. This logging feature generates log messages for FTP login attempts that are denied by the FTP login control ACL.

For information about log message output, see the information center in *Network Management and Monitoring Configuration Guide*. For information about configuring an FTP login control ACL, see the **ftp server acl** or **ftp server acl ipv6** command.

Examples

Enable logging for FTP login attempts that are denied by the FTP login control ACL.

```
<Sysname> system-view
[Sysname] FTP server acl-deny-log enable
```

Related commands

ftp server acl

- **ftp server acl ipv6**

ftp server dscp

Use **ftp server dscp** to set the DSCP value for IPv4 to use for FTP packets sent to an FTP client.

Use **undo ftp server dscp** to restore the default.

Syntax

ftp server dscp *dscp-value*

undo ftp server dscp

Default

IPv4 uses the DSCP value 0 for FTP packets sent to an FTP client.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

dscp-value: Specifies a DSCP value in the range of 0 to 63.

Usage guidelines

The DSCP value is carried in the ToS field of an IP packet to indicate the transmission priority of the packet.

Examples

Set the DSCP value for IPv4 to use for outgoing FTP packets to 30 on an FTP server.

```
<Sysname> system-view
[Sysname] ftp server dscp 30
```

ftp server enable

Use **ftp server enable** to enable the FTP server.

Use **undo ftp server enable** to disable the FTP server.

Syntax

ftp server enable

undo ftp server enable

Default

The FTP server is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Examples

Enable the FTP server.

```
<Sysname> system-view
[Sysname] ftp server enable
```

ftp server ipv6 dscp

Use **ftp server ipv6 dscp** to set the DSCP value for IPv6 to use for FTP packets sent to an FTP client.

Use **undo ftp server ipv6 dscp** to restore the default.

Syntax

ftp server ipv6 dscp *dscp-value*

undo ftp server ipv6 dscp

Default

IPv6 uses the DSCP value 0 for FTP packets sent to an FTP client.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

dscp-value: Specifies a DSCP value in the range of 0 to 63.

Usage guidelines

The DSCP value is carried in the Traffic class field of an IPv6 packet to indicate the transmission priority of the packet.

Examples

Set the DSCP value for IPv6 to use for outgoing FTP packets to 30 on an FTP server.

```
<Sysname> system-view
[Sysname] ftp server ipv6 dscp 30
```

ftp server ssl-server-policy

Use **ftp server ssl-server-policy** to associate an SSL server policy with the FTP server.

Use **undo ftp server ssl-server-policy** to restore the default.

Syntax

ftp server ssl-server-policy *policy-name*

undo ftp server ssl-server-policy

Default

No SSL server policy is associated with the FTP server.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies an SSL server policy by its name, a string of 1 to 31 characters.

Usage guidelines

After you associate an SSL server policy with the device, a client that supports SFTP will establish a secure connection to the device to ensure data security.

Examples

Associate SSL server policy **myssl** with the FTP server.

```
<Sysname> system-view
[Sysname] ftp server ssl-server-policy myssl
```

Related commands

ftp server enable

ssl server-policy (*Security Command Reference*)

ftp timeout

Use **ftp timeout** to set the FTP connection idle-timeout timer.

Use **undo ftp timeout** to restore the default.

Syntax

ftp timeout *minute*

undo ftp timeout

Default

The FTP connection idle-timeout timer is 30 minutes.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

Minute: Specifies a time interval in the range of 1 to 35791 minutes.

Usage guidelines

If no data transfer occurs on an FTP connection within the idle-timeout interval, the FTP server closes the FTP connection to release resources.

Examples

Set the FTP connection idle-timeout timer to 36 minutes.

```
<Sysname> system-view
[Sysname] ftp timeout 36
```

FTP client commands

For FTP users to execute FTP client configuration commands, you must configure authorization settings for users on the FTP server. Authorized operations include viewing the files in the working directory, reading/downloading/uploading/renaming/removing files, and creating directories.

The FTP client commands in this section are supported by the device, but whether they can be executed successfully depends on the FTP server.

The output in the examples of this section varies by FTP server type.

?

Use **?** to display all commands supported by an FTP client.

Use **?** *command-name* to display the help information for a command.

Syntax

? [*command-name*]

Views

FTP client view

Predefined user roles

network-admin

context-admin

Parameters

command-name: Specifies a command supported by the FTP client.

Usage guidelines

In FTP client view, entering **?** is the same as executing the **help** command.

Examples

Display all commands supported by the FTP client.

```
ftp> ?
Commands may be abbreviated.  Commands are:

append          delete          ls              quit            rmdir
ascii           debug           mkdir           reget           status
binary          dir             newer           rstatus         system
bye             disconnect      open            rhelp           user
cd              get             passive         rename          verbose
cdup            help            put             reset           ?
close           lcd             pwd             restart
```

Display the help information for the **dir** command.

```
ftp> ? dir
dir              list contents of remote directory
```

Related commands

help

append

Use **append** to add the content of a file on the FTP client to a file on the FTP server.

Syntax

append *localfile* [*remotefile*]

Views

FTP client view

Predefined user roles

network-admin

context-admin

Parameters

localfile: Specifies a file on the FTP client.

remotefile: Specifies a file on the FTP server.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

Examples

Append the content of the local **a.txt** file to the **b.txt** file on the FTP server.

```
ftp> append a.txt b.txt
local: a.txt remote: b.txt
150 Connecting to port 50190
226 File successfully transferred
1657 bytes sent in 0.000736 seconds (2.15 Mbyte/s)
```

ascii

Use **ascii** to set the file transfer mode to ASCII.

Syntax

ascii

Default

The file transfer mode is binary.

Views

FTP client view

Predefined user roles

network-admin

context-admin

Usage guidelines

You can perform this operation only after you log in to the FTP server.

FTP transfers files in either of the following modes:

- **Binary mode**—Transfers non-text files.
- **ASCII mode**—Transfers text files.

When the device acts as the FTP server, the transfer mode is determined by the FTP client. When the device acts as the FTP client, you can set the transfer mode. The transfer mode is binary by default.

Examples

Set the file transfer mode to ASCII.

```
ftp> ascii
200 TYPE is now ASCII
```

Related commands

binary

binary

Use **binary** to set the file transfer mode to binary, which is also called the flow mode.

Syntax

binary

Default

The file transfer mode is binary.

Views

FTP client view

Predefined user roles

network-admin

context-admin

Usage guidelines

You can perform this operation only after you log in to the FTP server.

FTP transfers files in either of the following modes:

- **Binary mode**—Transfers program file or pictures.
- **ASCII mode**—Transfers text files.

When the device acts as the FTP server, the transfer mode is determined by the FTP client. When the device acts as the FTP client, you can set the transfer mode. The default transfer mode is binary.

Examples

Set the file transfer mode to binary.

```
ftp> binary
200 TYPE is now 8-bit binary
```

Related commands

ascii

bye

Use **bye** to terminate the connection to the FTP server and return to user view. If no connection is established between the device and the FTP server, use this command to return to user view.

Syntax

bye

Views

FTP client view

Predefined user roles

network-admin

context-admin

Examples

Terminate the connection to the FTP server and return to user view.

```
ftp> bye
221-Goodbye. You uploaded 2 and downloaded 2 kbytes.
221 Logout.
<Sysname>
```

Related commands

quit

cd

Use **cd** to change the current working directory to another directory on the FTP server.

Syntax

cd { *directory* | **..** | **/** }

Views

FTP client view

Predefined user roles

network-admin

context-admin

Parameters

directory: Specifies the target directory. If the target directory does not exist, the **cd** command does not change the current working directory.

..: Specifies the upper directory. Executing the **cd ..** command is the same as executing the **cdup** command. If the current working directory is the FTP root directory, the **cd ..** command does not change the current working directory.

/: Specifies the FTP root directory.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

The directory that can be accessed must be authorized by the FTP server.

Examples

Change the working directory to the **logfile** subdirectory of the current directory.

```
ftp> cd logfile
250 OK. Current directory is /logfile
```

Change the working directory to the **folder** subdirectory of the FTP root directory.

```
ftp> cd /folder
250 OK. Current directory is /folder
```

Change the working directory to the upper directory of the current directory.

```
ftp> cd ..
250 OK. Current directory is /
```

Change the working directory to the FTP root directory.

```
ftp> cd /
250 OK. Current directory is /
```

Related commands

cdup

pwd

cdup

Use **cdup** to enter the upper directory of the FTP server.

Syntax

cdup

Views

FTP client view

Predefined user roles

network-admin

context-admin

Usage guidelines

You can perform this operation only after you log in to the FTP server.

This command does not change the working directory if the current directory is the FTP root directory.

Examples

Change the working directory to the upper directory.

```
ftp> pwd
257 "/ftp/subdir" is your current location
ftp> cdup
250 OK. Current directory is /ftp
ftp> pwd
257 "/ftp" is your current location
```

Related commands

cd

pwd

close

Use **close** to terminate the connection to the FTP server without exiting FTP client view.

Syntax

close

Views

FTP client view

Predefined user roles

network-admin

context-admin

Usage guidelines

You can perform this operation only after you log in to the FTP server.

Examples

Terminate the connection to the FTP server without exiting the FTP client view.

```
ftp> close
221-Goodbye. You uploaded 0 and downloaded 0 kbytes.
221 Logout.
ftp>
```

Related commands

disconnect

debug

Use **debug** to enable or disable FTP client debugging.

Syntax

debug

Default

FTP client debugging is disabled.

Views

FTP client view

Predefined user roles

network-admin

context-admin

Usage guidelines

When FTP client debugging is enabled, executing this command disables FTP client debugging.

When FTP client debugging is disabled, executing this command enables FTP client debugging.

Examples

Enable and then disable FTP client debugging.

```
ftp> debug
Debugging on (debug=1).
ftp> debug
Debugging off (debug=0).
```

delete

Use **delete** to permanently delete a file from the FTP server.

Syntax

delete *remotefile*

Views

FTP client view

Predefined user roles

network-admin

context-admin

Parameters

remotefile: Specifies a file on the FTP server.

Usage guidelines

CAUTION:

Permanently delete a file from the FTP server with caution. When you permanently delete a file from the FTP server, make sure the file is no longer in use.

You can perform this operation only after you log in to the FTP server.

To perform this operation, you must have delete permission on the FTP server.

Examples

Delete the **b.txt** file.

```
ftp> delete b.txt
250 Deleted b.txt
```

dir

Use **dir** to display or save detailed information about files and directories on the FTP server.

Syntax

dir [*remotefile* [*localfile*]]

Views

FTP client view

Predefined user roles

network-admin

context-admin

Parameters

remotefile: Specifies a file or directory on the FTP server.

localfile: Specifies the name of the local file used to save the displayed information.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

To display detailed information about the files and subdirectories in the working directory on the FTP server, use the **dir** command.

To display detailed information about a file or directory on the FTP server, use the **dir** *remotefile* command.

To save detailed information about a file or directory on the FTP server to a local file, use the **dir** *remotefile localfile* command.

In FTP client view, executing the **dir** command is the same as executing the **ls** command.

Examples

Display detailed information about the files and subdirectories in the working directory on the FTP server.

```
ftp> dir
150 Connecting to port 50201
```

```
-rwxr-xr-x    1 0          0               1481 Jul  7 15:36 a.txt
drwxr-xr-x    2 0          0               8192 Jul  2 14:33 diagfile
drwxr-xr-x    3 0          0               8192 Jul  7 15:21 ftp
drwxr-xr-x    2 0          0               8192 Jul  5 09:15 logfile
drwxr-xr-x    2 0          0               8192 Jul  2 14:33 seclog
-rwxr-xr-x    1 0          0           40808448 Jul  2 14:33 system-a1801.bin
-rwxr-xr-x    1 0          0               3050 Jul  7 12:26 startup.cfg
-rwxr-xr-x    1 0          0              54674 Jul  4 09:24 startup.mdb
-rwxr-xr-x    1 0          0               1481 Jul  7 12:34 x.cfg
226 9 matches total
```

Save detailed information about file **a.txt** to **s.txt**.

```
ftp> dir a.txt s.txt
output to local-file: s.txt ? [Y/N]y
150 Connecting to port 50203
226-Glob: a.txt
```

Display the content of the file **s.txt**.

```
ftp> bye
221-Goodbye. You uploaded 0 and downloaded 2 kbytes.
221 Logout.
<Sysname> more s.txt
-rwxr-xr-x    1 0          0               1481 Jul  7 12:34 a.txt
```

Related commands

ls

disconnect

Use **disconnect** to terminate the connection to the FTP server without exiting FTP client view.

Syntax

disconnect

Views

FTP client view

Predefined user roles

network-admin

context-admin

Usage guidelines

You can perform this operation only after you log in to the FTP server.

Examples

Terminate the connection to the FTP server without exiting the FTP client view.

```
ftp> disconnect
221-Goodbye. You uploaded 0 and downloaded 0 kbytes.
221 Logout.
ftp>
```

Related commands

close

display ftp client source

Use **display ftp client source** to display the source address settings on the FTP client.

Syntax

display ftp client source

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display the source address settings on the FTP client.

```
<Sysname> display ftp client source
The source IP address of the FTP client is 1.1.1.1.
```

ftp

Use **ftp** to log in to an IPv4 FTP server and enter FTP client view.

Syntax

ftp [*ftp-server* [*service-port*] [**vpn-instance** *vpn-instance-name*] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* }]] *

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

ftp-server: Specifies the IPv4 address or host name of an FTP server. A host name can be a case-insensitive string of 1 to 253 characters. Valid characters for a host name include letters, digits, hyphens (-), underscores (_), and dots (.).

service-port: Specifies the TCP port number of the FTP server, in the range of 0 to 65535. The default is 21.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the FTP server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the FTP server belongs to the public network, do not specify this option.

dscp *dscp-value*: Specifies the DSCP value for IPv4 to use in outgoing FTP packets to indicate the packet transmission priority. The value range is 0 to 63. The default is 0.

source { **interface** *interface-type interface-number* | **ip** *source-ip-address* }: Specifies the source address used to establish the FTP connection.

- **interface** *interface-type interface-number*: Specifies an interface by its type and number. The device will use the interface's primary IPv4 address as the source address. To establish the FTP connection successfully, make sure the interface is up and has the primary IPv4 address configured.
- **ip** *source-ip-address*: Specifies an IPv4 address. To establish the FTP connection successfully, make sure this address is the IPv4 address of an interface in up state on the device.

Usage guidelines

This command is only applicable to IPv4 networks.

If no parameters are specified, this command enters the FTP client view without logging in to an FTP server.

If the server parameters are specified, you are prompted to enter the username and password for logging in to the FTP server.

Examples

Log in to FTP server 192.168.0.211. Use 192.168.0.212 as the source IPv4 address for outgoing FTP packets.

```
<Sysname> ftp 192.168.0.211 source ip 192.168.0.212
Press CTRL+C to abort.
Connected to 192.168.0.211 (192.168.0.211).
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User (192.168.0.211:(none)): abc
331 Give me your password, please
Password:
230 Logged in successfully
Remote system type is MSDOS.
ftp>
```

ftp client ipv6 source

Use **ftp client ipv6 source** to specify the source IPv6 address for FTP packets sent to an IPv6 FTP server.

Use **undo ftp client ipv6 source** to restore the default.

Syntax

ftp client ipv6 source { **interface** *interface-type interface-number* | **ipv6** *source-ipv6-address* }

undo ftp client ipv6 source

Default

No source address is specified for FTP packets sent to an IPv6 FTP server. The device selects a source IPv6 address as defined in RFC 3484.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. The device will use the interface's IPv6 address as the source address. For successful FTP packet transmission, make sure the interface is up and is configured with an IPv6 address.

ipv6 *source-ipv6-address*: Specifies an IPv6 address. For successful FTP packet transmission, make sure this address is the IPv6 address of an interface in up state on the device.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

The source address specified with the **ftp ipv6** command takes precedence over the source address specified with the **ftp client ipv6 source** command.

The source address specified with the **ftp client ipv6 source** command applies to all FTP connections. The source address specified with the **ftp ipv6** command applies only to the FTP connection that is being established.

Examples

Specify the source IPv6 address of 2000::1 for FTP packets sent to an IPv6 FTP server.

```
<Sysname> system–view
[Sysname] ftp client ipv6 source ipv6 2000::1
```

Related commands

ftp ipv6

ftp client source

Use **ftp client source** to specify the source IPv4 address for FTP packets sent to an IPv4 FTP server.

Use **undo ftp client source** to restore the default.

Syntax

ftp client source { **interface** *interface-type interface-number* | **ip** *source-ip-address* }

undo ftp client source

Default

No source IPv4 address is specified for FTP packets sent to an IPv4 FTP server. The device uses the primary IPv4 address of the output interface for the route to the server as the source address.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. The device will use the interface's primary IPv4 address as the source address. For successful FTP packet transmission, make sure the interface is up and has the primary IPv4 address configured.

ip *source-ip-address*: Specifies an IPv4 address. For successful FTP packet transmission, make sure this address is the IPv4 address of an interface in up state on the device.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

The source address specified with the **ftp** command takes precedence over the source address specified with the **ftp client source** command.

The source address specified with the **ftp client source** command applies to all FTP connections. The source address specified with the **ftp** command applies only to the FTP connection that is being established.

Examples

Specify the source IPv4 address of 192.168.20.222 for FTP packets sent to an IPv4 FTP server.

```
<Sysname> system-view
[Sysname] ftp client source ip 192.168.20.222
```

Related commands

ftp

ftp ipv6

Use **ftp ipv6** to log in to an IPv6 FTP server and enter FTP client view.

Syntax

ftp ipv6 [*ftp-server* [*service-port*] [**vpn-instance** *vpn-instance-name*] [**dscp** *dscp-value* | **source** { **ipv6** *source-ipv6-address* | **interface** *interface-type interface-number* }] * [**-i** *interface-type interface-number*]]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

ftp-server: Specifies the IPv6 address or host name of an FTP server. A host name can be a case-insensitive string of 1 to 253 characters. Valid characters for a host name include letters, digits, hyphens (-), underscores (_), and dots (.).

service-port: Specifies the TCP port number of the FTP server, in the range of 0 to 65535. The default is 21.

dscp *dscp-value*: Specifies the DSCP value for IPv6 to use in outgoing FTP packets to indicate the packet transmission priority. The value range is 0 to 63. The default is 0.

source { **ipv6** *source-ipv6-address* | **interface** *interface-type interface-number* }: Specifies the source address used to establish the FTP connection.

- **interface** *interface-type interface-number*: Specifies an interface by its type and number. This option can be used only when the FTP server address is a link local address and the specified output interface has a link local address. For information about link local addresses, see IPv6 basics in *Layer 3—IP Services Configuration Guide*.
- **ipv6** *source-ipv6-address*: Specifies an IPv6 address. To establish the FTP connection successfully, make sure this address is the IPv6 address of an interface in up state on the device.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the FTP server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the FTP server belongs to the public network, do not specify this option.

-i *interface-type interface-number*: Specifies an output interface by its type and number. This option can be used only when the FTP server address is a link local address and the specified output interface has a link local address.

Usage guidelines

This command is only applicable to IPv6 networks.

If no parameters are specified, this command enters the FTP client view.

If the FTP server parameters are specified, you are prompted to enter the username and password for logging in to the FTP server.

Examples

Log in to FTP server 2000::154.

```
<Sysname>ftp ipv6 2000::154
Press CTRL+C to abort.
Connected to 2000::154 (2000::154).
220 FTP service ready.
User (2000::154): root
331 Password required for root.
Password:
230 User logged in
Remote system type is NSFOCUS
```

get

Use **get** to download a file from the FTP server and save the file.

Syntax

get *remotefile* [*localfile*]

Views

FTP client view

Predefined user roles

network-admin

context-admin

Parameters

remotefile: Specifies the file to be downloaded.

localfile: Specifies a name for the downloaded file. If you do not specify this argument, the system uses the name of the source file.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

To save the downloaded file to the working directory accessed by the **ftp** command, perform one of the following tasks:

- Execute the command without specifying the *localfile* argument.

- Specify a file name without any path information for the *localfile* argument, for example, a.cfg.

To save the downloaded file to some other directory, you must specify a fully qualified file name for the *localfile* argument, for example, flash:/subdirectory/a.cfg.

Examples

Download the **a.txt** file and save it as **b.txt** in the working directory accessed by the **ftp** command.

```
ftp> get a.txt b.txt
local: b.txt remote: a.txt
150 Connecting to port 47457
226 File successfully transferred
1569 bytes received in 0.00527 seconds (290.6 kbyte/s)
```

Download the **a.txt** file to the **test** directory in the working directory accessed by the **ftp** command.

```
ftp> get a.txt flash:/test/b.txt
local: flash:/test/b.txt remote: a.txt
150 Connecting to port 47457
226 File successfully transferred
1569 bytes received in 0.00527 seconds (290.6 kbyte/s)
```

Download the **a.txt** file to the root directory of the flash memory on a member device. Save the file as **c.txt**.

```
ftp> get a.txt slot1#flash:/c.txt
local: slot1#flash:/c.txt remote: a.txt
150 Connecting to port 47460
226 File successfully transferred
1569 bytes received in 0.0564 seconds (27.2 kbyte/s)
```

Related commands

put

help

Use **help** to display all commands supported by the FTP client.

Use **help** *command-name* to display the help information for a command.

Syntax

help [*command-name*]

Views

FTP client view

Predefined user roles

network-admin

context-admin

Parameters

command-name: Specifies a command supported by the FTP client.

Usage guidelines

In FTP client view, executing the **help** command is the same as entering **?**.

Examples

Display all commands supported by the FTP client.

```
ftp> help

append          delete          ls              quit            rmdir
ascii           debug           mkdir           reget           status
binary          dir             newer           rstatus         system
bye             disconnect      open            rhelp           user
cd              get             passive         rename          verbose
cdup            help            put             reset           ?
close           lcd             pwd             restart
```

Display the help information for the **dir** command.

```
ftp> help dir
dir              list contents of remote directory
```

Related commands

?

lcd

Use **lcd** to display or change the local working directory of the FTP client.

Syntax

lcd [*directory* | **/**]

Views

FTP client view

Predefined user roles

network-admin

context-admin

Parameters

directory: Changes the local working directory of the FTP client to the specified local directory. There must be a slash sign (/) before the name of the storage medium, for example, /flash:/logfile.

/: Changes the local working directory of the FTP client to the local root directory.

Usage guidelines

To display the local working directory of the FTP client, do not specify the *directory* or **/** argument.

Examples

Display the local working directory.

```
ftp> lcd
Local directory now /flash:
```

Change the local working directory to **flash:/logfile**.

```
ftp> lcd /flash:/logfile
Local directory now /flash:/logfile
```

ls

Use **ls** to display or save detailed information about files and directories on the FTP server.

Syntax

ls [*remotefile* [*localfile*]]

Views

FTP client view

Predefined user roles

network-admin

context-admin

Parameters

remotefile: Specifies a file or directory on the FTP server.

localfile: Specifies the name of the local file used to save the displayed information.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

To display detailed information about the files and subdirectories in the working directory on the FTP server, use the **ls** command.

To display detailed information about a file or directory on the FTP server, use the **ls** *remotefile* command.

To save detailed information about a file or directory on the FTP server to a local file, use the **ls** *remotefile localfile* command.

In FTP client view, executing the **ls** command is the same as executing the **dir** command.

Examples

Display detailed information about the files and subdirectories in the working directory on the FTP server.

```
ftp> ls
150 Connecting to port 50201
-rwxr-xr-x    1 0          0               1481 Jul  7 15:36 a.txt
drwxr-xr-x    2 0          0               8192 Jul  2 14:33 diagfile
drwxr-xr-x    3 0          0               8192 Jul  7 15:21 ftp
drwxr-xr-x    2 0          0               8192 Jul  5 09:15 logfile
drwxr-xr-x    2 0          0               8192 Jul  2 14:33 seclog
-rwxr-xr-x    1 0          0           40808448 Jul  2 14:33 system-a1801.bin
-rwxr-xr-x    1 0          0               3050 Jul  7 12:26 startup.cfg
-rwxr-xr-x    1 0          0              54674 Jul  4 09:24 startup.mdb
-rwxr-xr-x    1 0          0               1481 Jul  7 12:34 x.cfg
226 9 matches total
```

Save detailed information about the file **a.txt** to **s.txt**.

```
ftp> ls a.txt s.txt
output to local-file: s.txt ? [Y/N]y
150 Connecting to port 50203
226-Glob: s.txt
```

Display the content of the file **s.txt**.

```
ftp> bye
221-Goodbye. You uploaded 0 and downloaded 2 kbytes.
221 Logout.
<Sysname> more s.txt
-rwxr-xr-x    1 0          0               1481 Jul  7 12:34 a.txt
```

Related commands

dir

mkdir

Use **mkdir** to create a subdirectory in the current directory on the FTP server.

Syntax

mkdir *directory*

Views

FTP client view

Predefined user roles

network-admin

context-admin

Parameters

directory: Specifies the name for the directory to be created.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

You must have permission to perform this operation on the FTP server.

Examples

Create a subdirectory named **newdir** in the current directory of the FTP server.

```
ftp> mkdir newdir
257 "newdir" : The directory was successfully created
```

newer

Use **newer** to update a local file by using a file on the FTP server.

Syntax

newer *remotefile* [*localfile*]

Views

FTP client view

Predefined user roles

network-admin

context-admin

Parameters

remotefile: Specifies a file on the FTP server.

localfile: Specifies the local file to be updated.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

If the local file does not exist, this command downloads the file from the FTP server and saves it locally.

If the file on the FTP server is not newer than the local file, this command does not update the local file.

Examples

Update the local file with the **a.txt** file on the FTP server.

```
ftp> newer a.txt
local: a.txt remote: a.txt
150 Connecting to port 63513
226 File successfully transferred
1573 bytes received in 0.0293 seconds (52.3 kbyte/s)
```

open

Use **open** to log in to an FTP server from FTP client view.

Syntax

open *server-address* [*service-port*]

Views

FTP client view

Predefined user roles

network-admin

context-admin

Parameters

server-address: Specifies the IPv4 address, IPv6 address, or host name of the FTP server.

service-port: Specifies the TCP port number of the FTP server, in the range of 0 to 65535. The default is 21.

Usage guidelines

After you issue this command, the system will prompt you to enter the username and password.

After you log in to one FTP server, you must disconnect from the server before you can use the **open** command to log in to another server.

Examples

In FTP client view, log in to FTP server 192.168.40.7.

```
<Sysname>ftp
ftp> open 192.168.40.7
Press CTRL+C to abort.
Connected to 192.168.40.7 (192.168.40.7).
220 FTP service ready.
User (192.168.40.7:(none)): root
331 Password required for root.
Password:
230 User logged in.
Remote system type is NSFOCUS.
```

```
ftp>
```

passive

Use **passive** to change the FTP operation mode.

Syntax

passive

Default

The FTP operation mode is passive.

Views

FTP client view

Predefined user roles

network-admin

context-admin

Usage guidelines

FTP can operate in either of the following modes:

- **Active mode**—The FTP server initiates the TCP connection.
- **Passive mode**—The FTP client initiates the TCP connection.

When the FTP operation mode is passive, executing this command changes the mode to active.

When the FTP operation mode is active, executing this command changes the mode to passive.

This command is typically used together with a firewall to control FTP session establishment between private network users and public network users.

Examples

Change the FTP operation mode to passive.

```
ftp> passive
Passive mode on.
ftp> passive
Passive mode off.
```

put

Use **put** to upload a file from the FTP client to the FTP server.

Syntax

put *localfile* [*remotefile*]

Views

FTP client view

Predefined user roles

network-admin

context-admin

Parameters

localfile: Specifies the local file to be uploaded.

remotefile: Specifies the name of the file for saving the uploaded file on the FTP server.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

To upload a file in the current working directory, specify a file name without the path for the *localfile* argument, for example, a.cfg.

To upload a file in some other directory, specify a fully qualified file name for the *localfile* argument, for example, flash:/subdirectory/a.cfg.

Examples

Upload the **a.txt** file from the local working directory to the FTP server. Save the file as **b.txt**.

```
ftp> put a.txt b.txt
local: a.txt remote: b.txt
150 Connecting to port 47461
226 File successfully transferred
1569 bytes sent in 0.000671 seconds (2.23 Mbyte/s)
```

Upload the **a.txt** file from the **test** directory of the local working directory to the FTP server. Save the file as **b.txt**.

```
ftp> put flash:/test/a.txt b.txt
local: flash:/test/a.txt remote: b.txt
150 Connecting to port 47461
226 File successfully transferred
1569 bytes sent in 0.000671 seconds (2.23 Mbyte/s)
```

Upload file **a.txt** from the **test** directory of the storage medium on a member device. Save the file as **b.txt** on the FTP server.

```
ftp> put slot2#flash:/test/a.txt b.txt
local: slot2#flash:/test/a.txt remote: b.txt
150 Connecting to port 47461
226 File successfully transferred
1569 bytes sent in 0.000671 seconds (2.23 Mbyte/s)
```

Related commands

get

pwd

Use **pwd** to display the currently accessed directory on the FTP server.

Syntax

pwd

Views

FTP client view

Predefined user roles

network-admin

context-admin

Usage guidelines

You can perform this operation only after you log in to the FTP server.

Examples

Display the currently accessed directory on the FTP server.

```
ftp> cd subdir
250 OK. Current directory is /subdir
ftp> pwd
257 "/subdir" is your current location
```

quit

Use **quit** to terminate the connection to the FTP server and return to user view.

Syntax

quit

Views

FTP client view

Predefined user roles

network-admin

context-admin

Examples

Terminate the connection to the FTP server and return to user view.

```
ftp> quit
221-Goodbye. You uploaded 0 and downloaded 0 kbytes.
221 Logout.
<Sysname>
```

Related commands

bye

reget

Use **reget** to get the missing part of a file from the FTP server.

Syntax

reget *remotefile* [*localfile*]

Views

FTP client view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

remotefile: Specifies a file on the FTP server.

localfile: Specifies a local file.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

If a file download is not completed due to network or storage space problems, use this command to get the part that has not been downloaded yet.

Examples

Get the part of the **s.bin** file that has not been downloaded yet.

```
ftp> reget s.bin
local: s.bin remote: s.bin
350 Restarting at 1749706
150-Connecting to port 47429
150 38143.3 kbytes to download
226 File successfully transferred
39058742 bytes received in 66.2 seconds (576.1 kbyte/s)
```

rename

Use **rename** to rename a file.

Syntax

rename [*oldfilename* [*newfilename*]]

Views

FTP client view

Predefined user roles

network-admin

context-admin

Parameters

oldfilename: Specifies the original file name.

newfilename: Specifies the new file name.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

Examples

Rename the **a.txt** file as **b.txt**.

- Method 1:

  ```
  ftp> rename
  (from-name) a.txt
  (to-name) b.txt
  350 RNFR accepted - file exists, ready for destination
  250 File successfully renamed or moved
  ```

- Method 2:

  ```
  ftp> rename a.txt
  (to-name) b.txt
  350 RNFR accepted - file exists, ready for destination
  250 File successfully renamed or moved
  ```

- Method 3:

```
ftp> rename a.txt b.txt
350 RNFR accepted - file exists, ready for destination
250 File successfully renamed or moved
```

reset

Use **reset** to clear the reply information received from the FTP server in the buffer.

Syntax

reset

Views

FTP client view

Predefined user roles

network-admin

context-admin

Examples

Clear the reply information received from the FTP server.

```
ftp> reset
```

restart

Use **restart** to specify the file retransmission offset.

Syntax

restart *marker*

Views

FTP client view

Predefined user roles

network-admin

context-admin

Parameters

marker: Specifies the retransmission offset, in bytes.

Usage guidelines

Use this command to continue with a file retransmission. The file retransmission starts from the (offset+1)th byte.

You can perform this operation only after you log in to the FTP server.

Support for this command depends on the FTP server.

Examples

Set retransmission offset to 2 bytes and retransmit the **h.c** file. The file has 82 bytes in total.

```
ftp> restart 2
restarting at 2. execute get, put or append to initiate transfer
ftp> put h.c h.c
local: h.c remote: h.c
350 Restart position accepted (2).
```

```
150 Ok to send data.
226 File receive OK.
80 bytes sent in 0.000445 seconds (175.6 kbyte/s)
ftp> dir
150 Here comes the directory listing.
-rw-r--r--    1 0        0              82 Jul 18 02:58 h.c
```

rhelp

Use **rhelp** to display the FTP commands supported by the FTP server.

Use **rhelp** *protocol-command* to display the help information for an FTP command supported by the FTP server.

Syntax

rhelp [*protocol-command*]

Views

FTP client view

Predefined user roles

network-admin

context-admin

Parameters

protocol-command: Specifies an FTP command.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

Examples

Display the FTP-related commands supported by the FTP server.

```
ftp> rhelp
214-The following FTP commands are recognized
 USER PASS NOOP QUIT SYST TYPE
 HELP CWD  XCWD PWD  CDUP XCUP
 XPWD LIST NLST MLSD PORT EPRT
 PASV EPSV REST RETR STOR APPE
 DELE MKD  XMKD RMD  XRMD ABOR
 SIZE RNFR RNTO
214 UNIX Type: L8
```

Table 3 Command output

Field	Description
USER	Username.
PASS	Password.
NOOP	Null operation.
SYST	System parameters.
TYPE	Request type.
CWD	Changes the current working directory.

Field	Description
XCWD	Extended command with the meaning of CWD.
PWD	Prints the working directory.
CDUP	Changes the directory to the upper directory.
XCUP	Extended command with the meaning of CDUP.
XPWD	Extended command with the meaning of PWD.
LIST	Lists files.
NLST	Lists brief file description.
MLSD	Lists file content.
PORT	Active mode (IPv4).
EPRT	Active mode (IPv6).
PASV	Passive mode (IPv4).
EPSV	Passive mode (IPv6).
REST	Restarts.
RETR	Downloads files.
STOR	Uploads files.
APPE	Appends uploading.
DELE	Deletes files.
MKD	Creates folders.
XMKD	Extended command with the meaning of MKD.
RMD	Deletes folders.
XRMD	Extended command with the meaning of RMD.
ABOR	Aborts the transmission.
SIZE	Size of the transmission file.
RNFR	Original name.
RNTO	New name.

rmdir

Use **`rmdir`** to permanently delete a directory from the FTP server.

Syntax

`rmdir` *`directory`*

Views

FTP client view

Predefined user roles

network-admin

context-admin

Parameters

directory: Specifies a directory on the FTP server.

Usage guidelines

CAUTION:

Permanently delete a directory from the FTP server with caution. When you permanently delete a directory from the FTP server, make sure the directory is no longer in use.

You can perform this operation only after you log in to the FTP server.

To perform this operation, you must have delete permission on the FTP server.

Delete all files and subdirectories in a directory before you delete the directory. For more information about how to delete files, see the **delete** command.

The **rmdir** command does not delete the files of the specified directory from the recycle bin.

Examples

Delete empty directory **subdir1**.

```
ftp>rmdir subdir1
250 The directory was successfully removed
```

Related commands

delete

rstatus

Use **rstatus** to display FTP server status information.

Use **rstatus** *remotefile* to display detailed information about a directory or file on the FTP server.

Syntax

rstatus [*remotefile*]

Views

FTP client view

Predefined user roles

network-admin

context-admin

Parameters

remotefile: Specifies a directory or file on the FTP server.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

Support for this command depends on the FTP server.

Examples

Display FTP server status information.

```
ftp> rstatus
211-FTP server status:
     Connected to 192.168.20.177
     Logged in as root
```

```
     TYPE: ASCII
     No session bandwidth limit
     Session timeout in seconds is 300
     Control connection is plain text
     Data connections will be plain text
     At session startup, client count was 1
     vsFTPd 2.0.6 - secure, fast, stable
211 End of status
```

Table 4 Command output

Filed	Description
211-FTP server status:	Beginning of the display of FTP server status, where 211 specifies the FTP command.
Connected to 192.168.20.177	IP address of the FTP client.
Logged in as root	Login username root.
TYPE: ASCII	File transfer mode ASCII.
Session timeout in seconds is 300	FTP connection idle-timeout interval is 300 seconds.
Control connection is plain text	Control connection type is plain text.
Data connections will be plain text	Data connection type is plain text.
At session startup, client count was 1	FTP connection number is 1.
vsFTPd 2.0.6 - secure, fast, stable	FTP version is 2.0.6.
211 End of status	End of the display of FTP server status.

Display the file **a.txt**.

```
ftp> rstatus a.txt
213-Status follows:
-rw-r--r--    1 0        0             80 Jul 18 02:58 a.txt
213 End of status
```

Table 5 Command output

Field	Description
213-Status follows:	Beginning of the display of the file, where 213 specifies the FTP command.
-rw-r--r--	The first bit specifies the file type. • **-**—Common. • **B**—Block. • **c**—Character. • **d**—Directory. • **l**—Symbol connection file. • **p**—Pipe. • **s**—socket. The second bit through the tenth bit are divided into three groups. Each group contains three characters, representing the access permission of the owner, group, and other users. • **-**—No permission. • **r**—Read permission. • **w**—Write permission. • **x**—Execution permission.

Field	Description
1	Number of connections.
0	Name of the file owner.
0	Group number of the file owner.
80	File size, in bytes.
Jul 18 02:58	Date and time when the file was most recently modified.
a.txt	File name.
213 End of status	End of the display of the file information.

status

Use **status** to display FTP status information.

Syntax

status

Views

FTP client view

Predefined user roles

network-admin

context-admin

Examples

Display FTP status information.

```
ftp> status
Connected to 192.168.1.56.
No proxy connection.
Not using any security mechanism.
Mode: stream; Type: ascii; Form: non-print; Structure: file
Verbose: on; Bell: off; Prompting: on; Globbing: off
Store unique: off; Receive unique: off
Case: off; CR stripping: on
Ntrans: off
Nmap: off
Hash mark printing: off; Use of PORT cmds: on
```

Table 6 Command output

Field	Description
Connected to 192.168.1.56.	IP address of the FTP server that is connected to the FTP client.
Verbose: on; Bell: off; Prompting: on; Globbing: off	Displays debugging information.
Store unique: off; Receive unique: off	The name of the file on the FTP server is unique and the name of the local file is unique.
Case: off; CR stripping: on	Does not support obtaining multiple files once and deletes "\r" when downloading text files.

Field	Description
Ntrans: off	Does not use the input-output transmission table.
Nmap: off	The file name does not use the input-to-output mapping template.
Hash mark printing: off; Use of PORT cmds: on	Does not end with a pound sign (#) and uses "PORT" data transmission.

system

Use **system** to display the system information of the FTP server.

Syntax

system

Views

FTP client view

Predefined user roles

network-admin

context-admin

Usage guidelines

You can perform this operation only after you log in to the FTP server.

Examples

Display the system information of the FTP server.

```
ftp> system
215 UNIX Type: L8
```

user

Use **user** to initiate an FTP authentication on the current FTP connection.

Syntax

user *username* [*password*]

Views

FTP client view

Predefined user roles

network-admin

context-admin

Parameters

username: Specifies the username.

password: Specifies the password.

Usage guidelines

If you tried to access an FTP server but failed to pass the authentication when the device acts as an FTP client, use this command to try again before the connection to the FTP server expires.

Make sure the specified username and password have been configured on the FTP server. If the username or password is not configured, this command fails and the FTP connection is closed.

Examples

After a login failure, log in again to the FTP server before the connection expires.

- Method 1:

```
ftp> user ftp hello12345
331 Password required for ftp.
230 User logged in.
```

- Method 2:

```
ftp> user ftp
331 Password required for ftp.
Password:
230 User logged in.
```

verbose

Use **verbose** to enable or disable the device to display detailed information about FTP operations.

Syntax

verbose

Default

The device displays detailed information about FTP operations.

Views

FTP client view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command affects only the current FTP session.

Examples

Disable the device from displaying detailed information about FTP operations.

```
ftp> verbose
Verbose mode off.
```

Execute the **get** command.

```
ftp> get a.cfg 1.cfg
```

Enable the device to display detailed information about FTP operations.

```
ftp> verbose
Verbose mode on.
```

Execute the **get** command.

```
ftp> get a.cfg 2.cfg
227 Entering Passive Mode (192,168,1,58,68,14)
150-Accepted data connection
150 The computer is your friend. Trust the computer
226 File successfully transferred
```

```
3796 bytes received in 0.00762 seconds (486.5 kbyte/s)
```

TFTP commands

TFTP server commands

tftp server enable

Use **tftp server enable** to enable the TFTP server.

Use **undo tftp server enable** to disable the TFTP server.

Syntax

tftp server enable

undo tftp server enable

Default

The TFTP server is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Examples

Enable the TFTP server.

```
<Sysname> system-view
[Sysname] tftp server enable
```

Related commands

tftp server work-directory

tftp server work-directory

Use **tftp server work-directory** to set the TFTP server working directory.

Use **undo tftp server work-directory** to restore the default.

Syntax

tftp server work-directory *directory*

undo tftp server work-directory

Default

The TFTP server working directory is the root directory of the default file system.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

directory: Specifies a directory on the TFTP server. It must be the absolute path of an existing directory, a case-insensitive string of 1 to 255 characters.

Usage guidelines

TFTP clients have read and write rights to all files and directories in the TFTP server working directory.

Examples

Set the TFTP server working directory to **flash:/tftp**.

```
<Sysname> system-view
[Sysname] tftp server work-directory flash:/tftp
```

Related commands

tftp server enable

TFTP client commands

tftp

Use **tftp** to download a file from a TFTP server or upload a file to a TFTP server in an IPv4 network.

Syntax

tftp *tftp-server* { **get** | **put** | **sget** } *source-filename* [*destination-filename*] [**vpn-instance** *vpn-instance-name*] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* }] *

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

tftp-server: Specifies the IPv4 address or host name of a TFTP server. The host name can be a case-insensitive string of 1 to 253 characters and can contain only letters, digits, hyphens (-), underscores (_), and dots (.).

get: Downloads a file and writes the file directly to the destination folder. If the destination folder already has a file with the same name, the system deletes the existing file before starting the download operation. The existing file is permanently deleted even if the download operation fails.

put: Uploads a file.

sget: Downloads a file and saves the file to memory before writing it to the destination folder. The system starts to write the file to the destination folder only after the file is downloaded and saved to memory successfully. If the destination folder already has a file with the same name, the system overwrites the existing file. If the download or save-to-memory operation fails, the existing file in the destination folder is not overwritten.

source-filename: Specifies the source file name, a case-insensitive string of 1 to 1 to 255 characters.

destination-filename: Specifies the destination file name, a case-insensitive string of 1 to 255 characters. If this argument is not specified, the file uses the source file name.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the TFTP server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the TFTP server belongs to the public network, do not specify this option.

dscp *dscp-value*: Specifies the DSCP value for IPv4 to use for outgoing TFTP packets to indicate the packet transmission priority. The value range is 0 to 63. The default is 0.

source { **interface** *interface-type interface-number* | **ip** *source-ip-address* }: Specifies the source address for outgoing TFTP packets. If you do not specify this option, the device uses the primary IPv4 address of the output interface for the route to the TFTP server as the source address.

- **interface** *interface-type interface-number*: Specifies an interface by its type and number. The device will use the interface's primary IPv4 address as the source IPv4 address. For successful TFTP packet transmission, make sure the interface is up and has the primary IPv4 address configured.
- **ip** *source-ip-address*: Specifies an IPv4 address. For successful TFTP packet transmission, make sure this address is the IPv4 address of an interface in up state on the device.

Usage guidelines

The source address specified with the **tftp** command takes precedence over the source address specified with the **tftp client source** command.

The source address specified with the **tftp client source** command applies to all TFTP connections. The source address specified with the **tftp** command applies only to the current TFTP connection.

Examples

Download the **new.bin** file from TFTP server 192.168.1.1 and save the file as **new.bin**.

```
<Sysname> tftp 192.168.1.1 get new.bin
Press CTRL+C to abort.
   % Total    % Received % Xferd  Average Speed   Time    Time     Time   Current
                                  Dload  Upload   Total   Spent    Left   Speed
100 13.9M  100 13.9M    0     0  1206k      0  0:00:11  0:00:11  --:--:-- 1206k
Writing file...Done.
<Sysname>
```

Table 7 Command output

Field	Description
%	Percentage of file transmission progress.
Total	Size of files to be transmitted, in bytes.
%	Percentage of received file size to total file size.
Received	Received file size, in bytes.
%	Percentage of sent file size to total file size.
Xferd	Sent file size, in bytes.
Average Dload	Average download speed, in bps.
Speed Upload	Average upload speed, in bps.

Field	Description
Writing file…	The system was writing the downloaded file to the storage medium. This field is displayed only when the **get** or **sget** keyword is specified. If the operation succeeded, this command displays **Done** at the end of this field. If the operation failed, this command displays **Failed**.

Related commands

tftp client source

tftp client ipv6 source

Use **tftp client ipv6 source** to specify the source IPv6 address for TFTP packets sent to an IPv6 TFTP server.

Use **undo tftp client ipv6 source** to restore the default.

Syntax

tftp client ipv6 source { **interface** *interface-type interface-number* | **ipv6** *source-ipv6-address* }

undo tftp client ipv6 source

Default

No source address is specified for TFTP packets sent to an IPv6 TFTP server. The device selects a source IPv6 address as defined in RFC 3484.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. The device will use the interface's IPv6 address as the source address. For successful TFTP packet transmission, make sure the interface is up and is configured with an IPv6 address.

ipv6 *source-ipv6-address*: Specifies an IPv6 address . For successful TFTP packet transmission, make sure this address is the IPv6 address of an interface in up state on the device.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

The source address specified with the **tftp ipv6** command takes precedence over the source address specified with the **tftp client ipv6 source** command.

The source address specified with the **tftp client ipv6 source** command applies to all TFTP connections. The source address specified with the **tftp ipv6** command applies only to the TFTP connection that is being established.

Examples

Specify the source IPv6 address of 2000::1 for TFTP packets sent to an IPv6 TFTP server.

```
<Sysname> system–view
[Sysname] tftp client ipv6 source ipv6 2000::1
```

Related commands

tftp ipv6

tftp client source

Use **tftp client source** to specify the source IPv4 address for TFTP packets sent to an IPv4 TFTP server.

Use **undo tftp client source** to restore the default.

Syntax

tftp client source { **interface** *interface-type interface-number* | **ip** *source-ip-address* }

undo tftp client source

Default

No source IPv4 address is specified for TFTP packets sent to an IPv4 TFTP server. The device uses the primary IPv4 address of the output interface for the route to the server as the source address.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. The device will use the interface's primary IPv4 address as the source address. For successful TFTP packet transmission, make sure the interface is up and has the primary IPv4 address configured.

ip *source-ip-address*: Specifies an IPv4 address. For successful TFTP packet transmission, make sure this address is the IPv4 address of an interface in up state on the device.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

The source address specified with the **tftp** command takes precedence over the source address specified with the **tftp client source** command.

The source address specified with the **tftp client source** command applies to all TFTP connections. The source address specified with the **tftp** command applies only to the TFTP connection that is being established.

Examples

Specify the source IP address of 192.168.20.222 for TFTP packets sent to an IPv4 TFTP server.

```
<Sysname> system-view
[Sysname] tftp client source ip 192.168.20.222
```

Related commands

tftp

tftp ipv6

Use **tftp ipv6** to download a file from a TFTP server or upload a file to a TFTP server in an IPv6 network.

Syntax

tftp ipv6 *tftp-server* [**-i** *interface-type interface-number*] { **get** | **put** | **sget** } *source-filename* [*destination-filename*] [**vpn-instance** *vpn-instance-name*] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ipv6** *source-ipv6-address* }] *

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

tftp-server: Specifies the IPv6 address or host name of a TFTP server. The host name can be a case-insensitive string of 1 to 253 characters and can contain only letters, digits, hyphens (-), underscores (_), and dots (.).

-i *interface-type interface-number*: Specifies an output interface by its type and number. This option can be used only when the TFTP server address is a link local address and the specified output interface has a link local address. For information about link local addresses, see IPv6 basics in *Layer 3—IP Services Configuration Guide*.

get: Downloads a file and writes the file directly to the destination folder. If the destination folder already has a file with the same name, the system deletes the existing file before starting the download operation. The existing file is permanently deleted even if the download operation fails.

put: Uploads a file.

sget: Downloads a file and saves the file to memory before writing it to the destination folder. The system starts to write the file to the destination folder only after the file is downloaded and saved to memory successfully. If the destination folder already has a file using the same name, the system overwrites the existing file. If the download or save-to-memory operation fails, the existing file in the destination folder is not overwritten.

source-filename: Specifies the source file name, a case-insensitive string of 1 to 255 characters.

destination-filename: Specifies the destination file name, a case-insensitive string of 1 to 255 characters. If this argument is not specified, the file uses the source file name.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the TFTP server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the TFTP server belongs to the public network, do not specify this option.

dscp *dscp-value*: Specifies the DSCP value for IPv6 to use in outgoing TFTP packets to indicate the packet transmission priority. The value range is 0 to 63. The default is 0.

source { **interface** *interface-type interface-number* | **ipv6** *source-ipv6-address* }: Specifies the source address for outgoing TFTP packets. If you do not specify this option, the device selects a source IPv6 address as defined in RFC 3484.

- **interface** *interface-type interface-number*: Specifies an interface by its type and number. The device will use the interface's IPv6 address as the source IPv6 address. For

successful TFTP packet transmission, make sure the interface is up and is configured with an IPv6 address.

- **ipv6** *source-ipv6-address*: Specifies an IPv6 address. For successful TFTP packet transmission, make sure this address is the IPv6 address of an interface in up state on the device.

Usage guidelines

The source address specified with the **tftp ipv6** command takes precedence over the source address specified with the **tftp client ipv6 source** command.

The source address specified with the **tftp client ipv6 source** command applies to all TFTP connections. The source address specified with the **tftp ipv6** command applies only to the current TFTP connection.

Examples

Download the **new.bin** file from TFTP server 2001::1 and save the file as **new.bin**.

```
<Sysname> tftp ipv6 2001::1 get new.bin new.bin
Press CTRL+C to abort.
   % Total    % Received % Xferd  Average Speed   Time    Time     Time   Current
                                  Dload  Upload   Total   Spent    Left   Speed
100 13.9M  100 13.9M    0     0  1206k      0  0:00:11  0:00:11  --:--:-- 1206k
Writing file...Done.
```

For more information about the command output, see Table 7.

tftp-server acl

Use **tftp-server acl** to use an ACL to control the device's access to TFTP servers in an IPv4 network.

Use **undo tftp-server acl** to restore the default.

Syntax

tftp-server acl *acl-number*

undo tftp-server acl

Default

No ACL is used to control the device's access to TFTP servers.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

acl-number: Specifies the number of a basic ACL, in the range of 2000 to 2999.

Usage guidelines

You can use an ACL to deny or permit the device's access to specific TFTP servers.

If the ACL does not exist or does not have rules, the device can access all TFTP servers in the network.

If a VPN instance is specified in an ACL rule, the ACL rule applies only to the packets of the VPN instance. If no VPN instance is specified in an ACL rule, the ACL rule applies only to the packets on the public network.

Examples

Allow the device to access only TFTP server 1.1.1.1.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule permit source 1.1.1.1 0
[Sysname-acl-ipv4-basic-2000] quit
[Sysname] tftp-server acl 2000
```

tftp-server ipv6 acl

Use **tftp-server ipv6 acl** to use an ACL to control the device's access to TFTP servers in an IPv6 network.

Use **undo tftp-server ipv6 acl** to restore the default.

Syntax

tftp-server ipv6 acl *ipv6-acl-number*

undo tftp-server ipv6 acl

Default

No ACL is used to control the device's access to TFTP servers.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-acl-number: Specifies the number of a basic ACL, in the range of 2000 to 2999.

Usage guidelines

You can use an ACL to deny or permit the device's access to specific TFTP servers.

If the ACL does not exist or does not have rules, the device can access all TFTP servers in the network.

If a VPN instance is specified in an ACL rule, the ACL rule applies only to the packets of the VPN instance. If no VPN instance is specified in an ACL rule, the ACL rule applies only to the packets on the public network.

Examples

Allow the device to access only TFTP server 2001::1.

```
<Sysname> System-view
[Sysname] acl ipv6 basic 2001
[Sysname-acl-ipv6-basic-2001] rule permit source 2001::1/128
[Sysname-acl-ipv6-basic-2001] quit
[Sysname] tftp-server ipv6 acl 2001
```

Contents

File system management commands

IMPORTANT:

- Before managing storage media, file systems, directories, and files, make sure you know the possible impact.
- A file or directory whose name starts with a dot character (.) is a hidden file or directory. To prevent the system from hiding a file or directory, make sure the file or directory name does not start with a dot character.
- Some system files and directories are hidden. For correct system operation and full functionality, do not modify or delete hidden files or directories.

File system names, directory names, and file names must be compliant with the naming conventions. For more information about the naming conventions and the methods for specifying the names, see file system management in *Fundamentals Configuration Guide*.

Before you use the **copy**, **delete**, **fixdisk**, **format**, **gunzip**, **gzip**, **mkdir**, **move**, **rename**, **rmdir**, or **undelete** command on a file system, make sure the file system is not write protected.

You cannot access a storage medium that is being partitioned, or a file system that is being formatted or repaired. To access the file system, wait for the ongoing operation to be completed and then use one of the following methods:

- Use the absolute path to specify a file or directory. For example, use the **dir flash:/** command to display the files and directories in the **flash:** file system.
- Use the **cd** command to change the working directory to the root directory of the file system before accessing a file or directory in the file system. For example, to display the files and directories in the root directory of the **flash:** file system, perform the following tasks:
  a. Use the **cd flash:/** command to change the working directory to the root directory of the file system.
  b. Execute the **dir** command.

cd

Use **cd** to change the working directory.

Syntax

cd { *directory* | **..** }

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

directory: Specifies the destination directory.

..: Specifies the parent directory. If the working directory is the root directory, an error message appears when you execute the **cd ..** command. No online help information is available for this keyword.

Examples

Access the **test** directory after logging in to the device.

```
<Sysname> cd test
```

Change to the parent directory.

```
<Sysname> cd ..
```

copy

Use **copy** to copy a file.

Syntax

copy *source-file* { *dest-file* | *dest-directory* } [**vpn-instance** *vpn-instance-name*] [**source interface** *interface-type interface-number*] [**append**]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

source-file: Specifies the name or URL of the file to be copied. If the file resides on a remote file server rather than on the device, specify the URL of the file. Whether a URL is case sensitive depends on the server.

dest-file: Specifies the name or URL for the destination file. To copy the source file to a remote file server, specify a URL. Whether a URL is case sensitive depends on the server.

dest-directory: Specifies the destination directory or URL. To copy the source file to a remote file server, specify a URL. The device copies the source file to the destination location and saves the file with its original file name. Whether a URL is case sensitive depends on the server.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the destination remote file server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the server belongs to the public network, do not specify this option.

source interface *interface-type interface-number*: Specifies the source interface used to connect to the server. After you specify the source interface, the device uses the primary IP address of the source interface as the source IP address for outgoing packets. If you do not specify this option, the device uses the outgoing interface as the source interface.

append: Saves the content that has been correctly transmitted when a transmission failure or interruption occurs, and continues to copy the missing part when the command is executed again. If you do not specify this keyword and a transmission failure or interruption occurs, the device discards the content that has been correctly transmitted. This keyword is supported only when you copy a file from or to an FTP or HTTP file server.

Usage guidelines

You can use the **copy** command to perform the following tasks:

- Copy a local file and save it locally.
- Copy a local file and save it to an FTP, TFTP, or HTTP server.
- Copy a file from an FTP, TFTP, or HTTP server and save it locally.

To specify a file or directory, use the following guidelines:

Location	Name format	Remarks
On the device	Use the file name guidelines in *Fundamentals Configuration Guide*.	N/A
On an FTP server	Enter the URL in the format of **ftp://***FTP username*[**:***password*]*@server address*[**:***port number*]**/***file path*[**/***file name*].	The username and password must be the same as the username and password configured on the FTP server. If the server authenticates users only by the username, you are not required to enter the password. For example, to use the username a and password 1 and specify the startup.cfg file in the authorized working directory on the FTP server 1.1.1.1, enter ftp://a:1@1.1.1.1/startup.cfg.
On a TFTP server	Enter the URL in the format of **tftp://***server address*[**:***port number*]**/***file path*[**/***file name*].	For example, to specify the startup.cfg file in the working directory on TFTP server 1.1.1.1, enter the URL tftp://1.1.1.1/startup.cfg.
On an HTTP server	Enter the URL in the format of **http://**[*HTTP username*[**:***password*]@]*server address*[**:***port number*]**/***filepath*[**/***file name*].	The username and password in the URL must be the same as the username and password configured on the server. If only the username is required for authentication, you do not need to enter the password. If authentication is not required, you do not need to enter the username or password. For example, the **startup.cfg** file is saved in the authorized directory on the HTTP server at 1.1.1.1. The HTTP account username and password are **a** and **1**, respectively. To copy the file, enter the URL http://a:1@1.1.1.1/startup.cfg. If authentication is not required, enter the URL http://1.1.1.1/startup.cfg.

To specify an IPv6 address, enclose the IPv6 address in square brackets ([ ]), for example, ftp://test:test@[2001::1]:21/test.cfg.

Examples

Copy the **test.cfg** file in the current directory and save it to the current directory as **testbackup.cfg**.

```
<Sysname> copy test.cfg testbackup.cfg
Copy flash:/test.cfg to flash:/testbackup.cfg? [Y/N]:y
Copying file flash:/test.cfg to flash:/testbackup.cfg...Done.
```

Copy the **1.cfg** file in the **flash:/test** directory and save it to the **testbackup** directory of a USB file system as **1backup.cfg**.

```
<Sysname> copy flash:/test/1.cfg usba0:/testbackup/1backup.cfg
Copy flash:/test/1.cfg to usba0:/testbackup/1backup.cfg? [Y/N]:y
Copying file flash:/test/1.cfg to usba0:/testbackup/1backup.cfg...Done.
```

Copy the **test.cfg** file in the current directory and save it to the root directory of a file system in a specific slot as **testbackup.cfg**.

```
<Sysname> copy test.cfg slot2#flash:/
Copy flash:/test.cfg to slot2#flash:/test.cfg? [Y/N]:y
Copying file flash:/test.cfg to slot2#flash:/test.cfg...Done.
```

Copy **test.cfg** from the working directory on FTP server 1.1.1.1. Save the copy to the local current directory as **testbackup.cfg.** The FTP username is **user**. The password is **private**.

```
<Sysname> copy ftp://user:private@1.1.1.1/test.cfg testbackup.cfg
```

```
Copy ftp://user:private@1.1.1.1/test.cfg to flash:/testbackup.cfg? [Y/N]:y
Copying file ftp://user:private@1.1.1.1/test.cfg to flash:/testbackup.cfg... Done.
```

Copy **test.cfg** from the current directory. Save the copy to the working directory on FTP server 1.1.1.1 as **testbackup.cfg**. The FTP username is **user**. The password is **private**.

```
<Sysname> copy test.cfg ftp://user:private@1.1.1.1/testbackup.cfg
Copy flash:/test.cfg to ftp://user:private@1.1.1.1/testbackup.cfg? [Y/N]:y
Copying file flash:/test.cfg to ftp://user:private@1.1.1.1/testbackup.cfg... Done.
```

Copy **test.cfg** from the working directory on TFTP server 1.1.1.1. Save the copy to the local current directory as **testbackup.cfg**.

```
<Sysname> copy tftp://1.1.1.1/test.cfg testbackup.cfg
Copy tftp://1.1.1.1/test.cfg to flash:/testbackup.cfg? [Y/N]:y
Copying file tftp://1.1.1.1/test.cfg to flash:/testbackup.cfg... Done.
```

Copy **test.cfg** from the current directory. Save the copy to the working directory on TFTP server 1.1.1.1 as **testbackup.cfg**.

```
<Sysname> copy test.cfg tftp://1.1.1.1/testbackup.cfg
Copy flash:/test.cfg to tftp://1.1.1.1/testbackup.cfg? [Y/N]:y
Copying file flash:/test.cfg to tftp://1.1.1.1/testbackup.cfg... Done.
```

Copy **test.cfg** from the working directory on FTP server 1.1.1.1. Save the copy to the local current directory as **testbackup.cfg**. The FTP username is **user**. The password is **private**. The FTP server belongs to VPN instance **vpn1**.

```
<Sysname> copy ftp://user:private@1.1.1.1/test.cfg testbackup.cfg vpn-instance vpn1
Copy ftp://user:private@1.1.1.1/test.cfg to flash:/testbackup.cfg? [Y/N]:y
Copying file ftp://user:private@1.1.1.1/test.cfg to flash:/testbackup.cfg... Done.
```

Copy **test.cfg** from the working directory on TFTP server 1.1.1.1. Save the copy to the local current directory as **testbackup.cfg**. The TFTP server belongs to VPN instance **vpn1**.

```
<Sysname> copy tftp://1.1.1.1/test.cfg testbackup.cfg vpn-instance vpn1
Copy tftp://1.1.1.1/test.cfg to flash:/testbackup.cfg? [Y/N]:y
Copying file tftp://1.1.1.1/test.cfg to flash:/testbackup.cfg... Done.
```

Copy **test.cfg** from the working directory on FTP server 2001::1. Save the copy to the local current directory as **testbackup.cfg**. The FTP username is **user**. The password is **private**.

```
<Sysname> copy ftp://user:private@[2001::1]/test.cfg testbackup.cfg
Copy ftp://user:private@[2001::1]/test.cfg to flash:/testbackup.cfg? [Y/N]:y
Copying file ftp://user:private@[2001::1]/test.cfg to flash:/testbackup.cfg... Done.
```

Copy **test.cfg** from the working directory on TFTP server 2001::1. Save the copy to the local current directory as **testbackup.cfg**.

```
<Sysname> copy tftp://[2001::1]/test.cfg testbackup.cfg
Copy tftp://[2001::1]/test.cfg to flash:/testbackup.cfg? [Y/N]:y
Copying file tftp://[2001::1]/test.cfg to flash:/testbackup.cfg... Done.
```

Copy **test.cfg** from the authorized directory on HTTP server 1.1.1.1. Save the copy to the local current directory as **testbackup.cfg**. The HTTP login username is **user**. The password is **private**.

```
<Sysname> copy http://user:private@1.1.1.1/test.cfg testbackup.cfg
Copy http://user:private@1.1.1.1/test.cfg to flash:/testbackup.cfg? [Y/N]:y
Copying file http://user:private@1.1.1.1/test.cfg to flash:/testbackup.cfg... Done.
```

Copy **test.cfg** from the current directory. Save the copy to the authorized directory on HTTP server 1.1.1.1 as **testbackup.cfg**. The HTTP login username is **user**. The password is **private**.

```
<Sysname> copy test.cfg http://user:private@1.1.1.1/testbackup.cfg
Copy flash:/test.cfg to http://user:private@1.1.1.1/testbackup.cfg? [Y/N]:y
Copying file flash:/test.cfg to http://user:private@1.1.1.1/testbackup.cfg... Done.
```

Copy **test.cfg** from the authorized directory on HTTP server 2001::1. Save the copy to the local current directory as **testbackup.cfg**. The HTTP login username is **user**. The password is **private**.

```
<Sysname> copy http://user:private@[2001::1]/test.cfg testbackup.cfg
Copy http://user:private@[2001::1]/test.cfg to flash:/testbackup.cfg? [Y/N]:y
Copying file http://user:private@[2001::1]/test.cfg to flash:/testbackup.cfg... Done.
```

Copy **test.cfg** from the working directory on FTP server 1.1.1.1 in append mode. Save the copy to the local current directory as **testbackup.cfg**. The FTP username is **user**. The password is **private**.

```
<Sysname> copy ftp://user:private@1.1.1.1/test.cfg testbackup.cfg append
Copy ftp://user:private@1.1.1.1/test.cfg to flash:/testbackup.cfg? [Y/N]:y
Copying file ftp://user:private@1.1.1.1/test.cfg to flash:/testbackup.cfg... Done
```

Copy **test.cfg** from the authorized directory on HTTP server 1.1.1.1 in append mode. Save the copy to the local current directory as **testbackup.cfg**. The HTTP login username is **user**. The password is **private**.

```
<Sysname> copy http://user:private@1.1.1.1/test.cfg testbackup.cfg append
Copy http://user:private@1.1.1.1/test.cfg to flash:/testbackup.cfg? [Y/N]:y
Copying file http://user:private@1.1.1.1/test.cfg to flash:/testbackup.cfg... Done.
```

delete

Use **delete** to delete a file.

Syntax

delete [**/unreserved**] *file*

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

/unreserved: Permanently deletes the specified file. If you do not specify this keyword, the command moves the file to the recycle bin.

file: Specifies the name of the file to be deleted. Asterisks (*) are acceptable as wildcards. For example, to remove files with the **.txt** extension in the current directory, enter **delete *.txt**.

Usage guidelines

CAUTION:

- The **delete /unreserved** *file* command deletes a file permanently. The file cannot be restored.

A file moved to the recycle bin can be restored by using the **undelete** command.

Do not use the **delete** command to delete files from the recycle bin. To delete files from the recycle bin, use the **reset recycle-bin** command.

If you delete two files that have the same name from different directories, both files are retained in the recycle bin. If you successively delete two files that have the same name from the same directory, only the most recently deleted file is retained in the recycle bin.

Examples

Remove the **1.cfg** file from the current directory.

```
<Sysname> delete 1.cfg
Delete flash:/1.cfg? [Y/N]:y
Deleting file flash:/1.cfg...Done.
```

Permanently delete the **1.cfg** file from the current directory.

```
<Sysname> delete /unreserved 1.cfg
The file cannot be restored. Delete flash:/1.cfg? [Y/N]:y
Deleting the file permanently will take a long time. Please wait...
Deleting file flash:/1.cfg...Done.
```

Related commands

reset recycle-bin

undelete

dir

Use **dir** to display files or directories.

Syntax

dir [**/all**] [*file* | *directory* | **/all-filesystems**]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

/all: Displays all files and directories in the current directory, visible or hidden. If you do not specify this option, only visible files and directories are displayed.

file: Displays a specific file. This argument can use the asterisk (*) as a wildcard. For example, to display files with the **.txt** extension in the current directory, enter **dir *.txt**.

directory: Displays a specific directory.

/all-filesystems: Displays files and directories in the root directories of all file systems on the device.

Usage guidelines

If no option is specified, the command displays all visible files and directories in the current directory.

The directory name of the recycle bin is **.trash**. To display files in the recycle bin, use either of the following methods:

- Execute the **dir /all .trash** command.
- Execute the **cd .trash** command and then the **dir** command.

In an ext4 file system, 1% space is reserved. This command does not take account of the reserved space in the amount of free space.

If multiple users perform file operations (for example, creating or deleting files or directories) at the same time, the output for this command might be incorrect.

Examples

Display information about all files and directories in the current directory.

```
<Sysname> dir /all
Directory of flash: (YAFFS2)
...
```

Display files and directories in the root directories of all file systems on the device.

```
<Sysname> dir /all-filesystems
Directory of flash: (YAFFS2)
...
```

Table 1 Command output

Field	Description
Directory of *xx* (*yy*)	Current directory. The *xx* indicates the directory name. The *yy* indicates the type of the current file system.
0 -rwh 3144 Apr 26 2014 13:45:28 xx.xx	File or directory information: • **0**—File or directory number, which is automatically allocated by the system. • **-rwh**—Attributes of the file or directory. The first character is the directory indicator (**d** for directory and **–** for file). The second character indicates whether the file or directory is readable (**r** for readable). The third character indicates whether the file or directory is writable (**w** for writable). The fourth character indicates whether the file or directory is hidden (**h** for hidden, **-** for visible). Modifying, renaming, or deleting hidden files might affect functions. • **3144**—File size in bytes. For a directory, a hyphen (-) is displayed. • **Apr 26 2014 13:45:28**—Last date and time when the file or directory was modified. • **xx.xx**—File or directory name.

fdisk

Use **fdisk** to partition a storage medium.

Syntax

fdisk *medium* [*partition-number*]

Views

User view

Predefined user roles

network-admin

Parameters

medium: Specifies the name of the storage medium to be partitioned.

partition-number: Specifies the number of partitions, in the range of 1 to 4. If you specify this argument, the storage medium is divided evenly into the specified number of partitions. To customize the sizes of partitions, do not provide this argument.

Usage guidelines

This command is supported only on the default context.

The flash memory cannot be partitioned. A partition cannot be partitioned.

Before partitioning a storage medium, perform the following tasks:

- Back up the files in the storage medium. The partition operation clears all data on the medium.
- Make sure no other users are accessing the medium.
- Make sure the storage medium to be partitioned is not write protected. If the storage medium is write protected, the operation will fail, and you must remount or reinstall the storage medium to restore access to the storage medium.

After partitioning a storage medium, you must format the partitions to create the file systems before you can access the file systems.

The actual partition size and the specified partition size might have a difference of less than 5% of the storage medium's total size.

To change the sizes of partitions on a storage medium, partition the storage medium again and specify the required sizes for the partitions.

Before removing a partitioned storage medium, you must unmount all file systems on the storage medium.

Examples

Divide the USB disk on the device evenly into three partitions.

```
<Sysname> fdisk usba: 3
Capacity of usba: : 256M bytes
cfa: will be divided into the following partitions:
DeviceName      Capacity
usba0:            85MB
usba1:            85MB
usba2:            86MB
All data on usba: will be lost, continue? [Y/N]:y
Partitioning usba:...Done.
```

file prompt

Use **file prompt** to set the operation mode for files and directories.

Use **undo file prompt** to restore the default.

Syntax

file prompt { **alert** | **quiet** }

undo file prompt

Default

The operation mode is **alert**. The system prompts for confirmation when you perform a destructive file or directory operation.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

alert: Prompts for confirmation when a destructive file or directory operation is being performed.

quiet: Gives no confirmation prompt for file or directory operations except the recycle bin emptying operation.

Usage guidelines

In quiet mode, the system does not prompt for confirmation when a user performs a file or directory operation except the recycle bin emptying operation. The **alert** mode provides an opportunity to cancel a disruptive operation.

Examples

Set the file and directory operation mode to **alert**.

```
<Sysname> system-view
[Sysname] file prompt alert
```

fixdisk

Use **fixdisk** to check a file system for damage and repair any damage.

Syntax

fixdisk *filesystem*

Views

User view

Predefined user roles

network-admin

Parameters

filesystem: Specifies the name of a file system.

Usage guidelines

This command is supported only on the default context.

Use this command to fix a file system when space in the file system cannot be used or released.

You can repair a file system only when no other users are accessing the file system.

Examples

Repair file system **flash:**.

```
<Sysname> fixdisk flash:
Restoring flash: may take some time...
Restoring flash:...Done.
```

format

Use **format** to format a file system.

Syntax

format *filesystem* [**ext4** | **vfat**]

Views

User view

Predefined user roles

network-admin

Parameters

filesystem: Specifies the name of a file system.

ext4: Formats the file system as an EXT4 file system.

vfat: Formats the file system as a VFAT file system.

Usage guidelines

CAUTION:

Formatting a file system permanently deletes all files and directories in the file system. You cannot restore the deleted files or directories. If a startup configuration file exists in the file system, back up the file if necessary.

This command is supported only on the default context.

The flash memory does not support the **ext4** or **vfat** keyword. The file system on the flash memory can be formatted only as a file system of the default type.

File systems on storage media except the flash memory can and must be formatted as EXT4 or VFAT file systems.

You can use the **dir** command to display the types of the file systems.

You can format a file system only when no other users are accessing the file system.

A file system to be formatted cannot contain security log files. Only a user with the security-audit user role can delete security log files. For more information about the security-audit user role, see RBAC in *Fundamentals Configuration Guide*.

Examples

Format file system **flash:**.

```
<Sysname> format flash:
All data on flash: will be lost, continue? [Y/N]:y
Formatting flash:... Done.
```

Format the file system on the third partition of the USB disk.

```
<Sysname> format usba2:
All data on usba2: will be lost, continue? [Y/N]:y
Formatting usba2:... Done.
```

fuser

Use **fuser** to display processes that are using a file system, directory, or file.

Syntax

fuser { *directory* | *file* | *filesystem* }

Views

User view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

directory: Specifies a directory by its name.

file: Specifies a file by its name.

filesystem: Specifies a file system by its name.

Usage guidelines

Execute this command if you fail to execute a command such as **fdisk**, **fixdisk, format**, **umount, rmdir**, **rename**, **delete**, or **copy** command for a file system, directory, or file. View the command output to identify whether a process is using the file system, directory, or file.

When a user logs in to the CLI of the device, a process named **comsh** starts to monitor the user's behavior. Such a process uses file system resources but does not affect management of file systems, directories, or files.

Examples

Display processes that are using file system **flash:**.

```
<Sysname> fuser flash:
Job ID      PID         Process name
198         198         comsh
223         223         ttymgrd
332         332         ntopd
```

Table 2 Command output

Field	Description
Job ID	Task ID, which uniquely identifies a process. This ID does not change when the process reboots.
PID	Process ID, which identifies a process. This ID changes when the process reboots.

gunzip

Use **gunzip** to decompress a file.

Syntax

gunzip *file*

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

file: Specifies the name of the file to be decompressed. This argument must use the **.gz** extension.

Usage guidelines

This command deletes the specified file after decompressing it.

Examples

Decompress file **system.bin.gz**:

1. Before decompressing the file, you can display files whose names start with the **system.** string.

```
<Sysname> dir system.*
Directory of flash:
   1 -rw-          20 Jun 14 2012 10:18:53   system.bin.gz
```

```
252164 KB total (251820 KB free)
```

2. Decompress the file **system.bin.gz**.

```
<Sysname> gunzip system.bin.gz
Decompressing file flash:/system.bin.gz..... Done.
```

3. Verify the decompress operation.

```
<Sysname> dir system.*
Directory of flash:
   1 -rw-           0 May 30 2012 11:42:25   system.bin


252164 KB total (251820 KB free)
```

gzip

Use **gzip** to compress a file.

Syntax

gzip *file*

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

file: Specifies the name of the file to be compressed.

Usage guidelines

This command saves the compressed file to the *file***.gz** file and deletes the source file.

Examples

Compress file **system.bin**:

1. Before compressing the file, you can display files whose names start with the **system.** string.

```
<Sysname> dir system.*
Directory of flash:
   1 -rw-           0 May 30 2012 11:42:24   system.bin


252164 KB total (251820 KB free)
```

2. Compress the file **system.bin**.

```
<Sysname> gzip system.bin
Compressing file flash:/system.bin..... Done.
```

3. Verify the compress operation.

```
<Sysname> dir system.*
Directory of flash:
   1 -rw-          20 Jun 14 2012 10:18:53   system.bin.gz
```

```
252164 KB total (251820 KB free)
```

md5sum

Use **md5sum** to use the MD5 algorithm to calculate the digest of a file.

Syntax

md5sum *file*

Views

User view

Predefined user roles

network-admin

network-operator

Parameters

file: Specifies the name of a file.

Usage guidelines

You can use file digests to verify file integrity.

Examples

Use the MD5 algorithm to calculate the digest of file **system.bin**.

```
<Sysname> md5sum system.bin
MD5 digest:
4f22b6190d151a167105df61c35f0917
```

mkdir

Use **mkdir** to create a directory.

Syntax

mkdir *directory*

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

directory: Specifies a directory.

Usage guidelines

The name of the directory to be created must be unique in the parent directory.

You can create a directory only in an existing directory. For example, to create the **flash:/test/mytest** directory, make sure the **test** directory already exists.

Examples

Create the **test** directory in the current directory.

```
<Sysname> mkdir test
Creating directory flash:/test... Done.
```

Create the **test/subtest** directory in the current directory.

```
<Sysname> mkdir test/subtest
Creating directory flash:/test/subtest... Done.
```

more

Use **more** to display the contents of a text file.

Syntax

more *file*

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

file: Specifies the name of a file.

Examples

Display the contents of the **test.txt** file.

```
<Sysname> more test.txt
Have a nice day.
```

Display the contents of the **testcfg.cfg** file.

```
<Sysname> more testcfg.cfg

#
 version 7.1.070, Release 1201
#
 sysname Sysname
#
vlan 2
#
return
<Sysname>
```

mount

Use **mount** to mount a file system.

Syntax

mount *filesystem*

Views

User view

Predefined user roles

network-admin

Parameters

filesystem: Specifies the name of a file system.

Usage guidelines

This command is supported only on the default context.

Generally, file systems on a hot-swappable storage medium are automatically mounted when the storage medium is connected to the device. If the system cannot recognize a file system, however, you must mount the file system before you can access it.

To avoid file system corruption, do not perform the following tasks while the system is mounting a file system:

- Reboot, power cycle, or power off the device.
- Install or remove storage media.
- Perform a switchover.

To remove a hot-swappable storage medium from the device, you must first unmount all file systems on the storage medium. Removing a mounted hot-swappable storage medium might damage files on the storage medium or even the storage medium.

Examples

Mount a file system on a USB disk.

```
<Sysname> mount usba0:
```

Related commands

umount

move

Use **move** to move a file.

Syntax

move *source-file* { *dest-file* | *dest-directory* }

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

source-file: Specifies the name of the source file.

dest-file: Specifies the name of the destination file.

dest-directory: Specifies the name of the destination directory.

Usage guidelines

If you specify a destination directory, the system moves the source file to the specified directory without changing the file name.

Examples

Move the **flash:/test/sample.txt** file to **flash:/**, and save it as **1.txt**.

```
<Sysname> move test/sample.txt 1.txt
Move flash:/test/sample.txt to flash:/1.txt? [Y/N]:y
Moving file flash:/test/sample.txt to flash:/1.txt ...Done.
```

Move the **b.cfg** file to the **test2** directory.

```
<Sysname> move b.cfg test2
Move flash:/b.cfg to flash:/test2/b.cfg? [Y/N]:y
Moving file flash:/b.cfg to flash:/test2/b.cfg... Done.
```

pwd

Use **pwd** to display the working directory.

Syntax

pwd

Views

User view

Predefined user roles

network-admin

context-admin

Examples

Display the working directory.

```
<Sysname> pwd
flash:
```

rename

Use **rename** to rename a file or directory.

Syntax

rename { *source-file* | *source-directory* } { *dest-file* | *dest-directory* }

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

source-file: Specifies the name of the source file.

source-directory: Specifies the name of the source directory.

dest-file: Specifies the name of the destination file.

dest-directory: Specifies the name of the destination directory.

Usage guidelines

This command is not executed if the destination file or directory name is already used by an existing file or directory in the working directory.

Examples

Rename the **copy.cfg** file as **test.cfg**.

```
<Sysname> rename copy.cfg test.cfg
Rename flash:/copy.cfg as flash:/test.cfg? [Y/N]:y
Renaming flash:/copy.cfg as flash:/test.cfg... Done.
```

reset recycle-bin

Use **reset recycle-bin** to delete files from the recycle bin.

Syntax

reset recycle-bin [**/force**]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

/force: Deletes all files in the recycle bin without prompting for confirmation. If you do not specify this option, the command prompts you to confirm the deletion operation for each file.

Usage guidelines

CAUTION:

The files in a recycle bin can be restored by using the **undelete** command. If you delete a file from the recycle bin, that file cannot be restored. Before you delete files from a recycle bin, make sure the files are no longer in use.

The **delete** *file* command only moves a file to the recycle bin. To permanently delete the file, use the **reset recycle-bin** command to delete the file from the recycle bin.

Examples

Empty the recycle bin. (In this example there are two files in the recycle bin.)

```
<Sysname> reset recycle-bin
Clear flash:/a.cfg? [Y/N]:y
Clearing file flash:/a.cfg... Done.
Clear flash:/b.cfg? [Y/N]:y
Clearing file flash:/b.cfg... Done.
```

Delete the **b.cfg** file from the recycle bin. (In this example there are two files in the recycle bin.)

```
<Sysname> reset recycle-bin
Clear flash:/a.cfg? [Y/N]:n
Clear flash:/b.cfg? [Y/N]:y
Clearing file flash:/b.cfg... Done.
```

Related commands

delete

rmdir

Use **rmdir** to delete a directory.

Syntax

rmdir *directory*

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

directory: Specifies a directory.

Usage guidelines

CAUTION:

To delete a directory, you must first delete all files and subdirectories in the directory permanently or move them to the recycle bin. If you move them to the recycle bin, executing the **rmdir** command to delete the directory will delete them permanently. Before you use the **rmdir** command to delete a directory, you must make sure the directory and its files and subdirectories are no longer in use.

Examples

Delete the **subtest** directory.

```
<Sysname> rmdir subtest/
Remove directory flash:/test/subtest and the files in the recycle-bin under this directory
will be deleted permanently. Continue? [Y/N]:y
Removing directory flash:/test/subtest... Done.
```

sha256sum

Use **sha256sum** to use the SHA-256 algorithm to calculate the digest of a file.

Syntax

sha256sum *file*

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

file: Specifies the name of a file.

Usage guidelines

You can use file digests to verify file integrity.

Examples

Use the SHA-256 algorithm to calculate the digest of file **system.bin**.

```
<Sysname> sha256sum system.bin
SHA256 digest:
0851e0139f2770e87d01ee8c2995ca9e59a8f5f4062e99af14b141b1a36ca152
```

tar create

Use **tar create** to archive files and directories.

Syntax

tar create [**gz**] **archive-file** *dest-file* [**verbose**] **source** { *source-file* | *source-directory* }&<1-5>

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

gz: Uses gzip to compress the files and directories before archiving them. If you do not specify this keyword, the command archives the files and directories without compressing them.

archive-file *dest-file*: Specifies the archive file name. If you specified the **gz** keyword, the extension of the archive file name must be **.tar.gz**. If you did not specify the **gz** keyword, the extension of the archive file name must be **.tar**.

verbose: Displays the names of the successfully archived files and directories. If you do not specify this keyword, the command does not display the names of the successfully archived files and directories.

source { *source-file* | *source-directory* }&<1-5>: Specifies the files and directories to be archived. The argument can be a space-separated list of up to five items. Each item can be a file or directory name. The files and directories must be in the current working directory.

Examples

Archive the **1.cfg** and **2.cfg** files and the **test** directory to **a.tar**.

```
<Sysname> tar create archive-file a.tar source 1.cfg 2.cfg test
Creating archive flash:/a.tar Done.
```

Compress and archive the **1.cfg** and **2.cfg** files and the **test** directory to **b.tar.gz**.

```
<Sysname> tar create gz archive-file b.tar.gz source 1.cfg 2.cfg test
Creating archive flash:/b.tar.gz Done.
```

Compress and archive files and directories, and display the successfully archived files and directories.

```
<Sysname> tar create gz archive-file c.tar.gz verbose source 1.cfg 2.cfg test
1.cfg
2.cfg
test/
test/a.log
```

```
test/subtest/
test/subtest/aa.log
```

Related commands

tar extract

tar list

tar extract

Use **tar extract** to extract files and directories.

Syntax

tar extract archive-file *file* [**verbose**] [**screen** | **to** *directory*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

archive-file *file*: Specifies the archive file name. The extension can be **.tar** or **.tar.gz**.

verbose: Displays the names of the successfully extracted files and directories.

screen: Displays the content of the extracted files and directories on the screen. The extracted files are not saved.

to *directory*: Saves the extracted files and directories to a different directory. The *directory* argument specifies the directory.

Usage guidelines

IMPORTANT:

Before specifying the **screen** keyword for this command, use the **tar list** command to identify the types of the archived files. As a best practice, specify the keyword only if all archived files are text files. Displaying the content of an archived non-text file that contains terminal control characters might result in garbled characters and even cause the terminal unable to operate correctly. To use the terminal again, you must close the current connection and log in to the device again.

If you do not specify the **screen** keyword or the **to** *directory* option, the command saves the extracted files and directories to the working directory.

The command saves the extracted files and directories by using their original names. If a file or directory that has the same name as an extracted file or directory already exists in the destination directory, the file or directory is overwritten.

Examples

Extract files and directories from archive file **a.tar**.

```
<Sysname> tar extract archive-file a.tar
Extracting archive flash:/a.tar Done.
```

Extract files and directories from archive file **b.tar.gz**, and display the names of the successfully extracted files and directories.

```
<Sysname> tar extract archive-file b.tar.gz verbose
1.cfg
```

```
2.cfg
test/
test/a.log
test/subtest/
test/subtest/aa.log
```

Extract files and directories from archive file **c.tar.gz**, and display the content of the files on the screen.

```
<Sysname> tar extract archive-file c.tar.gz screen
#
 version 7.1.070, Release 1201
#
 sysname Sysname
#
...
```

Related commands

tar create

tar list

tar list

Use **tar list** to display the names of archived files and directories.

Syntax

tar list archive-file *file*

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

archive-file *file*: Specifies the archive file name. The extension can be **.tar** or **.tar.gz**.

Examples

Display the names of archived files and directories.

```
<Sysname> tar list archive-file a.tar
1.cfg
2.cfg
test/
test/a.log
test/subtest/
test/subtest/aa.log
```

Related commands

tar create

tar extract

umount

Use **umount** to unmount a file system.

Syntax

umount *filesystem*

Views

User view

Predefined user roles

network-admin

Parameters

filesystem: Specifies the name of a file system.

Usage guidelines

This command is supported only on the default context.

File systems on a storage medium are automatically mounted when the storage medium is connected to the device. To remove a hot-swappable storage medium from the device, you must first unmount all file systems on the storage medium. Removing a mounted hot-swappable storage medium might damage files on the storage medium or even the storage medium.

You can unmount a file system only when no other users are accessing the file system.

To avoid file system corruption, do not perform the following tasks while the system is unmounting a file system:

- Reboot, power cycle, or power off the device.
- Install, remove, or access storage media.
- Perform a switchover.

Examples

Unmount a file system on a USB disk.

```
<Sysname> umount usba0:
```

Related commands

mount

undelete

Use **undelete** to restore a file from the recycle bin.

Syntax

undelete *file*

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

file: Specifies the name of the file to be restored.

Usage guidelines

If a file with the same name already exists in the directory, the system prompts whether or not you want to overwrite the existing file. If you enter **Y**, the existing file is overwritten. If you enter **N**, the command is not executed.

Examples

Restore the **copy.cfg** file, which was moved from the root directory of the **flash:** file system to the recycle bin.

```
<Sysname> undelete copy.cfg
Undelete flash:/copy.cfg? [Y/N]:y
Undeleting file flash:/copy.cfg... Done.
```

Restore the **startup.cfg** file, which was moved from the **flash:/seclog** directory to the recycle bin.

- Method 1:

  ```
  <Sysname> undelete seclog/startup.cfg
  Undelete flash:/seclog/startup.cfg? [Y/N]:y
  Undeleting file flash:/seclog/startup.cfg... Done.
  <Sysname>
  ```

- Method 2:

  ```
  <Sysname> cd seclog
  <Sysname> undelete startup.cfg
  Undelete flash:/seclog/startup.cfg? [Y/N]:y
  Undeleting file flash:/seclog/startup.cfg... Done.
  ```

Contents

Configuration file management commands

archive configuration

Use **archive configuration** to manually archive the running configuration to the configuration archive directory.

Syntax

archive configuration

Views

User view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command saves the running configuration to the specified configuration archive directory with file names generated from the specified name prefix.

Before executing this command, you must use one of the following methods to specify a directory and a name prefix for the configuration archives:

- For local archiving, use the **archive configuration location** command to specify a local configuration archive directory and a name prefix.
- For remote archiving, use the **archive configuration server** command to configure server parameters.

If you specify a local configuration archive directory, manual configuration archiving saves the running configuration only on the master device.

Examples

Archive the running configuration.

```
<Sysname> archive configuration
Save the running configuration to an archive file. Continue? [Y/N]: Y
The archive configuration file myarchive_1.cfg is saved.
```

Related commands

archive configuration interval

archive configuration location

archive configuration max

archive configuration server

archive configuration server password

archive configuration server user

display archive configuration

archive configuration interval

Use **archive configuration interval** to enable automatic running-configuration archiving and set the archiving interval for local archiving.

Use **undo archive configuration interval** to disable automatic running-configuration archiving for local archiving.

Syntax

archive configuration interval *interval*

undo archive configuration interval

Default

The automatic running-configuration archiving feature is disabled for local archiving.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies the interval for automatically saving the running configuration. The value range is 10 to 525600, in minutes.

Usage guidelines

Automatic configuration archiving enables the system to periodically save the running configuration to the archive directory. After the system finishes an automatic archive, it resets the archiving interval timer.

Before enabling automatic configuration archiving, you must use the **archive configuration location** command to specify a directory and a name prefix for the configuration archives.

Automatic configuration archiving saves the running configuration only on the master device.

Examples

Set the system to archive the running configuration every 60 minutes.

```
<Sysname> system-view
[Sysname] archive configuration interval 60
Archive file will be saved every 60 minutes.
```

Related commands

archive configuration

archive configuration location

archive configuration max

display archive configuration

archive configuration location

Use **archive configuration location** to specify a local directory and file name prefix for archiving the running configuration.

Use **undo archive configuration location** to restore the default.

Syntax

archive configuration location *directory* **filename-prefix** *filename-prefix*

undo archive configuration location

Default

No local directory or file name prefix is specified on the device for archiving the running configuration.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

directory: Specifies the archive directory, a string of 1 to 63 characters. The value for this argument must take the format of *storage-medium-name:/folder-name*. The directory must already exist on the master.

filename-prefix: Specifies a file name prefix for configuration archives, a case-insensitive string of 1 to 30 characters. Valid characters are letters, digits, underscores (_), and hyphens (-).

Usage guidelines

Before archiving the running configuration, either manually or automatically, you must specify a directory and file name prefix for configuration archives.

The configuration archives are named in the format of *prefix_serial number***.cfg**, for example, **archive_1.cfg** and **archive_2.cfg**. The serial number is automatically assigned from 1 to 1000, increasing by 1. After the serial number reaches 1000, it restarts from 1.

If you change the file directory or file name prefix, the following events occur:

- The old configuration archives change to common configuration files.
- The configuration archive counter is reset. The serial number for new configuration archives starts at 1.
- The **display archive configuration** command no longer displays the old configuration archives.

The configuration archive counter does not restart when you delete configuration archives from the archive directory. However, if the device reboots after all configuration archives have been deleted, the configuration archive counter restarts. The serial number for new configuration archives starts at 1.

The **undo archive configuration location** command removes the local configuration archive directory and file name prefix settings. The command also performs the following operations:

- Disables the configuration archive feature (both manual and automatic methods).
- Restores the default settings of the **archive configuration interval** and **archive configuration max** commands.
- Clears the configuration archive information displayed by using the **display archive configuration** command.

Examples

Set the configuration archive directory as **flash:/archive** and the archive file name prefix as **my_archive**.

```
<Sysname> mkdir flash:/archive
Creating directory flash:/archive... Done.
```

```
<Sysname> system-view
[Sysname] archive configuration location flash:/archive filename-prefix my_archive
```

Related commands

archive configuration

archive configuration interval

archive configuration max

display archive configuration

archive configuration max

Use **archive configuration max** to set the maximum number of configuration archives that can be saved on the device.

Use **undo archive configuration max** to restore the default.

Syntax

archive configuration max *file-number*

undo archive configuration max

Default

The maximum number is 5.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

file-number: Specifies the maximum number of configuration archives that can be saved on the device. The value range is 1 to 10. Adjust the setting depending on the amount of storage space available.

Usage guidelines

Before you execute this command, use the **archive configuration location** command to specify a configuration archive directory and archive file name prefix on the device.

After the maximum number of configuration archives is reached, the system deletes the oldest archive for the new archive.

Changing the limit setting to a lower value does not cause immediate deletion of excess archives. Instead, the configuration archive feature deletes the oldest *n* files when a new archive is manually or automatically saved, where *n* = current archive count – new archive limit + 1. For example, seven configuration archives have been saved before the archive limit is set to four. When saving a new configuration archive, the system first deletes the oldest four (7 – 4 + 1) archives.

If you execute the **undo archive configuration location** command, the default archive limit is restored.

Examples

Set the maximum number of configuration archives to 10.

```
<Sysname> system-view
[Sysname] archive configuration max 10
```

Related commands

archive configuration

archive configuration location

archive configuration interval

display archive configuration

archive configuration server

Use **archive configuration server** to configure the parameters for archiving the running configuration to a remote server.

Use **undo archive configuration server** to restore the default.

Syntax

archive configuration server { **ftp** | **tftp** | **scp** } { *ipv4-address* | **ipv6** *ipv6-address* } [**port** *port-number*] [**vpn-instance** *vpn-instance-name*] [**directory** *directory*] **filename-prefix** *filename-prefix* [**interval** *interval*]

undo archive configuration server

Default

No parameters are configured for archiving the running configuration to a remote server.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ftp: Specifies a remote FTP server.

tftp: Specifies a remote TFTP server.

scp: Specifies a remote SCP server.

ipv4-address: Specifies the IPv4 address of the remote server.

ipv6 *ipv6-address*: Specifies the IPv6 address of the remote server.

port *port-number*: Specifies the TCP port number of the remote server, in the range of 1 to 65535. By default, the FTP port number is 21 and the TFTP port number is 69.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If the remote server is on the public network, do not specify this option.

directory *directory*: Specifies the remote archive directory, a case-insensitive string. If you do not specify this option, the archive directory is the root directory of the remote server.

filename-prefix *filename-prefix*: Specifies a file name prefix for configuration archives, a case-insensitive string of 1 to 30 characters. Valid characters are letters, digits, underscores (_), and hyphens (-).

interval *interval*: Enables automatic running-configuration remote archiving and sets the archiving interval. The value range for the *interval* argument is 10 to 525600 minutes.

Usage guidelines

Local archiving (the **archive configuration location** command) and remote archiving (the **archive configuration server** command) are mutually exclusive. You cannot use the two features at the same time.

If you use a remote FTP or SCP server, make sure the device is consistent with that server in FTP or SCP settings. If a login username and password is configured on the server, you must use the **archive configuration server user** and **archive configuration server password** commands to specify that login username and password on the device.

If you use the **archive configuration server** command multiple times to configure parameters for remote archiving, the most recent configuration takes effect.

After you configure the remote archiving parameters, you can use the **archive configuration** command to manually archive the running configuration.

By default, automatic running-configuration remote archiving is disabled. To enable automatic running-configuration remote archiving, specify the **interval** *interval* option when you use the **archive configuration server** command. To disable automatic running-configuration remote archiving, use the **undo archive configuration server** command.

On the specified remote server, configuration archives are named in the format of *filename-prefix*_*YYYYMMDD*_*HHMMSS***.cfg** (for example, **archive_20170526_203430.cfg**).

Examples

Set the configuration archive directory as **archive/** on the server at 192.168.1.1 and configure the archive file name prefix as **my_archive**.

```
<Sysname> system-view
[Sysname] archive configuration server ftp 192.168.1.1 port 22 directory /archive/
filename-prefix my_archive
```

Related commands

archive configuration

archive configuration location

archive configuration server password

archive configuration server user

display archive configuration

archive configuration server password

Use **archive configuration server password** to configure the password for accessing the FTP or SCP server that stores the configuration archives.

Use **undo archive configuration server password** to restore the default.

Syntax

archive configuration server password { **cipher** | **simple** } *string*

undo archive configuration server password

Default

No password is configured for accessing the FTP or SCP server that stores the configuration archives.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 63 characters. Its encrypted form is a case-sensitive string of 33 to 117 characters.

Examples

Set the password to **admin** in plaintext form for accessing the FTP or SCP server that stores the configuration archives.

```
<Sysname> system-view
[Sysname] archive configuration server password simple admin
```

Related commands

archive configuration server

archive configuration server user

display archive configuration

archive configuration server user

Use **archive configuration server user** to configure the username for accessing the FTP or SCP server that stores the configuration archives.

Use **undo archive configuration server user** to restore the default.

Syntax

archive configuration server user *user-name*

undo archive configuration server user

Default

No username is configured for accessing the FTP or SCP server that stores the configuration archives.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

user-name: Specifies the username, a case-sensitive string of 1 to 63 characters.

Usage guidelines

If no username is configured, the username will be **anonymous**.

Examples

Set the username to **admin** for accessing the FTP or SCP server that stores the configuration archives.

```
<Sysname> system-view
[Sysname] archive configuration server user admin
```

Related commands

archive configuration server

archive configuration server password

display archive configuration

backup startup-configuration

Use **backup startup-configuration** to back up the main next-startup configuration file to a TFTP server.

Syntax

backup startup-configuration to { *ipv4-server* | **ipv6** *ipv6-server* } [*dest-filename*] [**vpn-instance** *vpn-instance-name*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-server: Specifies a TFTP server by its IPv4 address or host name. The host name is a case-insensitive string of 1 to 253 characters. Valid characters include letters, digits, hyphens (-), underscores (_), and dots (.).

ipv6 *ipv6-server*: Specifies a TFTP server by its IPv6 address or host name. The host name is a case-insensitive string of 1 to 253 characters. Valid characters include letters, digits, hyphens (-), underscores (_), and dots (.).

dest-filename: Specifies the name of the target file used for saving the file on the server. The file must be a .cfg file. The file name is a case-insensitive string of up to 255 characters. If you do not specify a target file name, the source file name is used.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If the TFTP server is on the public network, do not specify this option.

Examples

Back up the main next-startup configuration file to the IPv4 TFTP server at 2.2.2.2 in the public network, and set the target file name to **192-168-1-26.cfg**.

```
<Sysname> backup startup-configuration to 2.2.2.2 192-168-1-26.cfg
Backing up the main startup configuration file to 2.2.2.2...
Done.
```

Back up the main next-startup configuration file to the IPv4 TFTP server at 2.2.2.2 in MPLS L3VPN instance **VPN1**, and set the target file name to **192-168-1-26.cfg**.

```
<Sysname> backup startup-configuration to 2.2.2.2 192-168-1-26.cfg vpn-instance VPN1
Backing up the main startup configuration file to 2.2.2.2 in VPN VPN1...
```

```
Done.
```

Back up the main next-startup configuration file to the IPv6 TFTP server at 2001::2 in the public network, and set the target file name to **192-168-1-26.cfg**.

```
<Sysname> backup startup-configuration to ipv6 2001::2 192-168-1-26.cfg
Backing up the main startup configuration file to 2001::2...
Done.
```

Related commands

`restore startup-configuration`

configuration encrypt

Use **`configuration encrypt`** to enable configuration encryption.

Use **`undo configuration encrypt`** to disable configuration encryption.

Syntax

`configuration encrypt` { **`private-key`** | **`public-key`** }

`undo configuration encrypt`

Default

Configuration encryption is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

`private-key`: Encrypts configuration with a private key. All devices running NF software use the same private key.

`public-key`: Encrypts configuration with a public key. All devices running NSFOCUS software use the same public key.

Usage guidelines

Configuration encryption enables the device to automatically encrypt a configuration file when saving the running configuration to the file.

Any devices running NSFOCUS software can decrypt the encrypted configuration file. To prevent an encrypted file from being decoded by unauthorized users, make sure the file is accessible only to authorized users.

Examples

Enable the public-key method for configuration encryption.

```
<Sysname> system-view
[Sysname] configuration encrypt public-key
```

configuration replace file

Use **`configuration replace file`** to roll the running configuration back by using a local replacement configuration file.

Syntax

configuration replace file *filename*

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

filename: Specifies the path of the replacement configuration file, a string of up to 255 characters. The file must be a .cfg file. The file and file path must be valid and on the local system.

Usage guidelines

CAUTION:

The configuration rollback feature replaces the running configuration with the configuration in a configuration file without rebooting the device. This operation will cause settings not in the replacement configuration file to be lost, which might cause service interruption. When you perform configuration rollback, make sure you fully understand its impact on your network.

This command helps you revert to a previous configuration state or adapt the running configuration to different network environments.

To ensure a successful rollback, follow these guidelines:

- Make sure the replacement configuration file is created by using the configuration archive feature or the **save** command on the device.
- If the configuration file is not created on the device, make sure the command lines in the configuration file are fully compatible with the device.
- Make sure the replacement configuration file is not encrypted.

Examples

Replace the running configuration with the configuration in the **my_archive_1.cfg** configuration file.

```
<Sysname> system-view
[Sysname] configuration replace file my_archive_1.cfg
Current configuration will be lost, save current configuration? [Y/N]:n
Now replacing the current configuration. Please wait...
Succeeded in replacing current configuration with the file my_archive_1.cfg.
```

configuration replace server

Use **configuration replace server** to roll the running configuration back by using a configuration file on a remote server.

Use **undo configuration replace server** to restore the default.

Syntax

configuration replace server { **ftp** | **tftp** } { *ipv4-address* | **ipv6** *ipv6-address* } [**port** *port-number*] [**vpn-instance** *vpn-instance-name*] [**directory** *directory*] **file** *filename*

undo configuration replace server

Default

No parameters are configured for remote configuration rollback.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ftp: Specifies a remote FTP server.

tftp: Specifies a remote TFTP server.

ipv4-address: Specifies the IPv4 address of the remote server.

ipv6 *ipv6-address*: Specifies the IPv6 address of the remote server.

port *port-number*: Specifies the TCP port number of the remote server, in the range of 1 to 65535. By default, the FTP port number is 21 and the TFTP port number is 69.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If the remote server is on the public network, do not specify this option.

directory *directory*: Specifies the remote rollback directory. The *directory* argument is a case-insensitive string. If you do not specify this option, the rollback directory is the root directory of the remote server.

file *filename*: Specifies the default replacement configuration file for running-configuration remote rollback. The *filename* argument is a case-insensitive string. The file must be a .cfg file.

Usage guidelines

If you use a remote FTP server, make sure the device is consistent with that FTP server in FTP settings. If a login username and password is configured on the FTP server, you must use the **configuration replace server user** and **configuration replace server password** commands to specify that login username and password on the device.

Examples

Replace the running configuration with the configuration in the **archive/** directory of the FTP server at 192.168.1.1.

```
<Sysname> system-view
[Sysname] configuration replace server ftp 192.168.1.1 port 22 directory /archive/
```

Related commands

configuration replace server file

configuration replace server password

configuration replace server user

display configuration replace server

configuration replace server file

Use **configuration replace server file** to enable remote configuration rollback.

Use **undo configuration replace server file** to disable remote configuration rollback.

Syntax

configuration replace server file [*filename*] [**at** *time* [*date*]]

undo configuration replace server file

Default

Remote configuration rollback is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

filename: Specifies a replacement configuration file by its name, a string of up to 255 characters. The file must be a .cfg file. If you do not specify a replacement configuration file, this command uses the default replacement configuration file specified by using the **configuration replace server** command for a rollback.

at *time*: Specifies the time at which the system downloads the replacement configuration file and performs configuration rollback. The *time* argument is in the format of HH:MM. HH represents the hours, in the range of 0 to 23. MM represents the minutes, in the range of 0 to 59.

date: Specifies the date on which the system downloads the replacement configuration file and performs configuration rollback. This argument is in the format of MM/DD/YYYY or YYYY/MM/DD. YYYY represents the year, in the range of 2000 to 2035. MM represents the month, in the range of 1 to 12. DD represents the day, in the range of 1 to N. The value for N depends on the month.

Usage guidelines

CAUTION:

The remote configuration rollback feature replaces the running configuration with the configuration in a remote configuration file without rebooting the device. This operation will cause settings not in the replacement configuration file to be lost, which might cause service interruption. When you perform configuration rollback, make sure you fully understand its impact on your network.

This command enables the device to perform the following operations:

1. Downloads the replacement configuration file from the remote rollback server.
2. Saves the downloaded file as a temporary file.
3. Replaces the running configuration with the configuration in the temporary file.
4. Deletes the temporary file after the configuration rollback finishes.

To perform an immediate configuration rollback, do not specify a rollback time or date. An immediate configuration rollback cannot be canceled.

To schedule a configuration rollback, specify a rollback time and optionally a date. A configuration rollback schedule can be canceled before the specified rollback time. When you schedule a rollback, follow these restrictions and guidelines:

- If you specify a rollback date with the rollback time, the specified date must be the same or later than the current system date. If the specified date is the same as the current system date, the specified time must be later than the current system time. After you create the rollback schedule, be careful with changing the system clock backward. The rollback schedule will be canceled automatically if it expires before it could be executed because the system date or time is changed backward.

- If you do not specify a rollback date with the rollback time, the device compares the specified rollback time with the current system time.
  - If the specified rollback time is later than the current system time, the device performs a rollback at the specified time on the current day.
  - If the specified rollback time is earlier than the current system time, the device performs a rollback at the specified time on the next day.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Roll back the running configuration immediately with the specified replacement configuration file on the remote server for configuration rollback.

```
<Sysname> system-view
[Sysname] configuration replace server file my_archive_2017-05-09.cfg
The running configuration will be lost. Do you want to save the running configuration?
[Y/N]: N
Now replacing the running configuration...
Successfully replaced running configuration with file my_archive_2017-05-09.cfg.
```

Related commands

configuration replace server

configuration replace server password

configuration replace server user

configuration replace server password

Use **configuration replace server password** to configure the password for accessing the remote FTP server for configuration rollback.

Use **undo configuration replace server password** to restore the default.

Syntax

configuration replace server password { **cipher** | **simple** } *string*

undo configuration replace server password

Default

No password is configured for accessing the remote FTP server for remote configuration rollback.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 63 characters. Its encrypted form is a case-sensitive string of 33 to 117 characters.

Examples

Set the password to **admin** in plaintext form for accessing the remote FTP server for configuration rollback.

```
<Sysname> system-view
[Sysname] configuration replace server password simple admin
```

Related commands

configuration replace server

configuration replace server file

configuration replace server user

configuration replace server user

Use **configuration replace server user** to specify the username for accessing the remote FTP server for configuration rollback.

Use **undo configuration replace server user** to restore the default.

Syntax

configuration replace server user *user-name*

undo configuration replace server user

Default

No username is configured for accessing the remote FTP server for configuration rollback.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

user-name: Specifies the username, a case-sensitive string of 1 to 63 characters.

Usage guidelines

If no username is configured, the username will be **anonymous**.

Examples

Set the username to **admin** for accessing the remote FTP server for configuration rollback.

```
<Sysname> system-view
[Sysname] configuration replace server user admin
```

Related commands

configuration replace server

configuration replace server file

configuration replace server password

display configuration replace server

display archive configuration

Use **display archive configuration** to display configuration archive information.

Syntax

display archive configuration

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Usage guidelines

If you use remote archiving, this command displays configuration archive information on the remote server. If you use local archiving, this command displays configuration archive information on the local device.

Examples

Display information about the configuration archives. The sample output was created based on local archiving.

```
<Sysname> display archive configuration
Location: flash:/archive
Filename prefix: my_archive
Archive interval in minutes: 120
Maximum number of archive files: 10
Archive history:
  No. TimeStamp               FileName
   1  Sat Oct 20 22:50:26 2018 my_archive_1.cfg
   2  Sat Oct 20 22:50:31 2018 my_archive_2.cfg
 # 3  Sat Oct 20 22:50:35 2018 my_archive_3.cfg
The pound sign (#) indicates the most recent archive file.
Next archive file to be saved: my_archive_4.cfg
```

Display information about the configuration archives. The sample output was created based on remote archiving.

```
<Sysname> display archive configuration
Username: test
Location: ftp://192.168.21.21:21/archive
VPN instance: VPN1
Filename prefix: my_archive
Archive interval in minutes: 120
Archive history:
  No. TimeStamp               FileName
 ! 1  Thu Oct 18 14:23:51 2018 my_archive_20181018_142351.cfg
 ! 2  Sat Oct 20 22:46:44 2018 my_archive_20181020_224644.cfg
#! 3  Sat Oct 20 22:46:49 2018 my_archive_20181020_224649.cfg
The exclamation mark (!) indicates that the remote archiving attempt failed.
```

```
The pound sign (#) indicates the most recent archive file.
```

Table 1 Command output

Field	Description
Username	Username for accessing the remote FTP or SCP server that stores the configuration archives. If the remote server is a TFTP server, this field is not available.
Location	Absolute path of the directory for saving running-configuration archives.
VPN instance	VPN instance to which the remote server belongs.
Filename prefix	File name prefix for configuration archives.
Archive interval in minutes	Interval (in minutes) for the system to automatically archive the running configuration. If automatic configuration archiving is disabled, this field is not available.
Maximum number of archive files	Maximum number of configuration archives that can be saved on the device.
Archive history	History configuration archive information.
No.	Number of a configuration archive.
TimeStamp	Time when the configuration archive was created.

Related commands

archive configuration

archive configuration interval

archive configuration location

archive configuration max

archive configuration server

display configuration replace server

Use **display configuration replace server** to display information about remote configuration rollback.

Syntax

display configuration replace server

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Usage guidelines

The device stores only the most recent 10 remote rollback records.

Examples

Display information about remote configuration rollback.

```
<Sysname> display configuration replace server
Username: test
Location: ftp://192.168.21.21:22/test/
VPN instance: VPN1
Next replacement file: my_archive_20180509_143018.cfg
Next replacement time: 22:00 2018/6/12
Replacement history:
  No. Time                    FileName
 ! 1  20:21:09 2018/10/18     my_archive_20180509_142018.cfg
 ! 2  20:25:00 2018/10/18     my_archive_20180509_143018.cfg
#! 3  22:52:23 2018/10/20     my_archive_20180509_144018.cfg
The exclamation mark (!) indicates that the remote replacing attempt failed.
The pound sign (#) indicates the most recent replacement file.
```

Table 2 Command output

Field	Description
Username	Username for accessing the remote server to download a configuration file for configuration rollback.
Location	Absolute path of the replacement configuration file.
VPN instance	VPN instance to which the remote server belongs.
Next replacement file	Configuration file for the next remote configuration rollback. If no remote configuration rollback schedule is waiting for execution, this field is not available.
Next replacement time	Time and date for the next remote configuration rollback. If no remote configuration rollback schedule is waiting for execution, this field is not available.
Replacement history	Remote configuration rollback history.
No.	Number of a configuration rollback.
Time	Time and date when the configuration rollback was performed.
Filename	Name of the replacement configuration file.

Related commands

`configuration replace server`

`configuration replace server file`

`configuration replace server password`

`configuration replace server user`

display current-configuration

Use **`display current-configuration`** to display the running configuration.

Syntax

display current-configuration [**configuration** [*module-name*] | **interface** [*interface-type* [*interface-number*]] | **vpn-instance** [*vpn-instance-name*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

configuration [*module-name*]: Displays the feature configuration. The *module-name* argument specifies a feature module. If you do not specify a feature module, the command displays all feature settings you have made.

interface [*interface-type* [*interface-number*]]: Displays interface configuration, where the *interface-type* argument represents the interface type and the *interface-number* argument represents the interface number. If you do not specify the *interface-type interface-number* arguments, the command displays the running configuration for all interfaces. If you specify only the *interface-type* argument, the command displays the running configuration for all interfaces of this type.

vpn-instance [*vpn-instance-name*]: Specifies one or all MPLS L3VPN instances. Use the *vpn-instance-name* argument to specify one MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you specify the **vpn-instance** keyword without specifying the *vpn-instance-name* argument, this command displays the running configuration for all VPN instances. If you do not specify VPN instances, this command displays the running configuration for all VPN instances and the public network.

Usage guidelines

Use this command to verify the configuration you have made.

If the system has automatically changed the setting you have made for a parameter, this command displays the effective setting instead of the configured one. An automatic change typically occurs because of system restrictions.

This command does not display parameters that are using the default settings.

Executing this command with the **vpn-instance** [*vpn-instance-name*] option displays only part of the running configuration for the specified VPN instances. The displayed information includes settings made on the VPN instances, interfaces associated with the VPN instances, and routing protocol settings. To obtain the complete running configuration, execute the **display current-configuration** command without specifying any parameters. To obtain the desired running configuration related to VPN instances, use the **| include** *regular-expression* option. With the **include** *regular-expression* option, you can specify a regular expression to identify the configuration you want to display.

Examples

Display local user configuration.

```
<Sysname> display current-configuration configuration local-user
#
local-user ftp class manage
```

```
 password hash
$h$6$D5A6pqcGpnZXxFUO$OJqnqffG7m1wTNSFOCUS6v+FBCjZZBzqgJjTZlbATl1dnKNlYwFMJcWDMbDn8HD
1j4XzuKggDp2LrP40kGIOvQGYhQ==
 service-type ftp
 authorization-attribute user-role network-operator
#
local-user root class manage
 password hash
$h$6$GcTZyXO04qmom21z$GjeAeDMjP/xtknMLf9NHUNIvebNYR3tkd5aWS6sKbkFh/ECFJZOjh2FVUI0GW7u
44fNK6Ke7ANE7dhhAFcytUQ==
 service-type ssh telnet terminal
 authorization-attribute user-role network-admin
#
return
```

Display Ethernet interface configuration.

```
<Sysname> display current-configuration interface gigabitethernet
#
interface GigabitEthernet1/0/1
 port link-mode route
#
return
```

display current-configuration diff

Use **display current-configuration diff** to display the differences that the running configuration has as compared with the next-startup configuration.

Syntax

display current-configuration diff

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Usage guidelines

This command searches for the next-startup configuration in the following order:

1. The .cfg main next-startup configuration file.
2. The .cfg backup next-startup configuration file if the .cfg main next-startup configuration file is unavailable.

If both configuration files are unavailable, the system displays a message indicating that no next-startup configuration files exist.

Examples

Display the differences that the running configuration has as compared with the next-startup configuration.

```
<Sysname> display current-configuration diff
--- Startup configuration
+++ Current configuration
@@ -5,7 +5,7 @@
 #
  sysname Sysname
 #
-alias dhc display history-command
+alias dh display hotkey
<Sysname>
```

Table 3 Command output

Field	Description
- - - *A* +++ *B*	• *A* represents the source configuration for comparison, which can be **Startup configuration**, **Current configuration**, or the name of the source configuration file with its directory information. • *B* represents the target configuration for comparison, which can be **Current configuration**, **Startup configuration**, or the name of the target configuration file with its directory information. In this example, the startup configuration and the current configuration are the source and target, respectively.
@@ -*linenumber1*,*number1* +*linenumber2*,*number2* @@	Location information for identifying the command line differences: • -*linenumber1*,*number1*—Source configuration section that contains differences. The *linenumber1* argument represents the start line of the section. The *number1* argument represents the number of lines between the start line and the end line of the section. • +*linenumber2*,*number2*—Target configuration section that contains differences. The *linenumber2* argument represents the start line of the section. The *number2* argument represents the number of lines between the start line and the end line of the section.
cmd1 - *cmd2* + *cmd3* *cmd4*	Displays command differences. • *cmd1* and *cmd4*—Command lines are contained in both source and target configurations if they are not prefixed with a minus (-) or plus (+) sign. They provide a context for locating command line differences. • - *cmd2*—Command lines are prefixed with a minus sign if they are contained in the source configuration but not in the target configuration. • + *cmd3*—Command lines are prefixed with a plus sign if they are contained in the target configuration but not in the source configuration. In this example, the sample output shows that the **`alias dhc display history-command`** command is contained only in the source configuration, and the **`alias dh display hotkey`** command is contained only in the target configuration.

Related commands

`display current-configuration`

`display diff`

`display saved-configuration`

display default-configuration

Use **`display default-configuration`** to display the factory defaults.

Syntax

display default-configuration

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Usage guidelines

Factory defaults are custom basic settings that came with the device. Factory defaults vary by device models and might differ from the initial default settings for the commands.

The device starts up with the factory defaults if no next-startup configuration files are available.

Examples

Display the factory defaults.

```
<Sysname> display default-configuration
```

display diff

Use **display diff** to display differences between configurations.

Syntax

display diff configfile *file-name-s* { **configfile** *file-name-d* | **current-configuration** | **startup-configuration** }

display diff current-configuration { **configfile** *file-name-d* | **startup-configuration** }

display diff startup-configuration { **configfile** *file-name-d* | **current-configuration** }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

configfile *file-name-s*: Specifies the source configuration file for comparison.

configfile *file-name-d*: Specifies the target configuration file for comparison.

current-configuration: Specifies the running configuration. In the **display diff current-configuration** command, this keyword specifies the source configuration for comparison. In the **display diff configfile** *file-name-s* and **display diff startup-configuration** commands, this keyword specifies the target configuration.

startup-configuration: Specifies the next-startup configuration. In the **display diff startup-configuration** command, this keyword specifies the source configuration for comparison. In the **display diff configfile** *file-name-s* and **display diff current-configuration** commands, this keyword specifies the target configuration.

Usage guidelines

If you specify the **startup-configuration** keyword, the system searches for the next-startup configuration in the following order:

1. The .cfg main next-startup configuration file.
2. The .cfg backup next-startup configuration file if the .cfg main next-startup configuration file is unavailable.

If both configuration files are unavailable, the system displays a message indicating that no next-startup configuration files exist.

Examples

Display the differences between **startup.cfg** and **test.cfg**.

```
<Sysname> display diff configfile startup.cfg configfile test.cfg
--- flash:/startup.cfg
+++ flash:/test.cfg
@@ -5,7 +5,7 @@
 #
  sysname Sysname
 #
-alias dhc display history-command
+alias dh display hotkey
<Sysname>
```

The output shows that the **alias dhc display history-command** command is contained only in **startup.cfg**, and the **alias dh display hotkey** command is contained only in **test.cfg**.

Display the differences between the running configuration and the next-startup configuration.

```
<Sysname> display diff current-configuration startup-configuration
--- Current configuration
+++ Startup configuration
@@ -5,7 +5,7 @@
 #
  sysname Sysname
 #
-alias dhc display history-command
+alias dh display hotkey
<Sysname>
```

The output shows that the **alias dhc display history-command** command is contained only in the running configuration, and the **alias dh display hotkey** command is contained only in the next-startup configuration.

For the command output description, see Table 3.

Related commands

display current-configuration

display current-configuration diff

display saved-configuration

display saved-configuration

Use **display saved-configuration** to display the contents of the configuration file for the next system startup.

Syntax

display saved-configuration

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Usage guidelines

Use this command to verify that important settings have been saved to the configuration file for the next system startup.

This command selects the configuration file to display in the following order:

1. If the main startup configuration file is available, this command displays the contents of the main startup configuration file.
2. If only the backup startup configuration file is available, this command displays the contents of the backup file.
3. If both the main and backup startup configuration files are not available, this command does not display anything.

Examples

Display the contents of the configuration file for the next system startup.

```
<Sysname> display saved-configuration
#
 version 7.1.070, Release 1201
#
 sysname Sysname
#
 ftp server enable
#
 telnet server enable
#
 domain default enable system
#
vlan 1
#
domain system
#
...
```

Related commands

reset saved-configuration

save

display startup

Use **display startup** to display the names of the current startup configuration file and the next-startup configuration files.

Syntax

display startup

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Usage guidelines

All IRF members use the same current startup configuration file as the master.

After a master/subordinate switchover, it is normal that the current startup configuration files on all IRF members are displayed as NULL. This is because the new master continues to run with the running configuration rather than rebooting with a startup configuration file.

Examples

Display names of the startup configuration files.

```
<Sysname> display startup
 Current startup saved-configuration file: flash:/startup.cfg(*)
 Next main startup saved-configuration file: flash:/startup.cfg
 Next backup startup saved-configuration file: NULL
```

Table 4 Command output

Field	Description
Current startup saved-configuration file	Configuration file that the device has started up with. If the field is suffixed with an asterisk (*), the startup configuration file is a binary configuration file.
Next main startup saved-configuration file	Primary configuration file to be used at the next startup.
Next backup startup saved-configuration file	Backup configuration file to be used at the next startup.

Related commands

startup saved-configuration

display this

Use **display this** to display the running configuration in the current view.

Syntax

display this

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Usage guidelines

Use this command to verify the configuration you have made in a certain view.

This command does not display parameters that are using the default settings.

Some parameters can be successfully set even if their dependent features are not enabled. For these parameters, this command displays their settings after the dependent features are enabled.

This command can be executed in any user line view to display the running configuration of all user lines.

Examples

Display the running configuration on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
#
return
```

reset saved-configuration

Use **reset saved-configuration** to delete a next-startup configuration file.

Syntax

reset saved-configuration [**backup** | **main**]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

backup: Specifies the backup next-startup configuration file.

main: Specifies the main next-startup configuration file.

Usage guidelines

CAUTION:

This command permanently deletes the specified next-startup configuration file from all IRF member devices. As a best practice, make sure you have a configuration backup before you use this command.

You can delete the main file, the backup file, or both.

To delete a file that is set as both main and backup next-startup configuration files, you must execute both the **reset saved-configuration backup** command and the **reset saved-configuration main** command. Using only one of the commands sets the target file attribute to NULL instead of deleting the file.

If you do not specify a configuration file attribute, the **reset saved-configuration** command deletes the main next-startup configuration file.

Examples

Delete the main next-startup configuration file.

```
<Sysname> reset saved-configuration
The saved configuration file will be erased. Are you sure? [Y/N]:y
Configuration file in flash: is being cleared.
Please wait ..........
Configuration file is cleared.
```

Related commands

display saved-configuration

restore startup-configuration

Use **restore startup-configuration** to download a configuration file from a TFTP server and specify it as the main next-startup configuration file.

Syntax

restore startup-configuration from { *ipv4-server* | **ipv6** *ipv6-server* } *src-filename* [**vpn-instance** *vpn-instance-name*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-server: Specifies a TFTP server by its IPv4 address or host name. The host name is a case-insensitive string of 1 to 253 characters. Valid characters include letters, digits, hyphens (-), underscores (_), and dots (.).

ipv6 *ipv6-server*: Specifies a TFTP server by its IPv6 address or host name. The host name is a case-insensitive string of 1 to 253 characters. Valid characters include letters, digits, hyphens (-), underscores (_), and dots (.).

src-filename: Specifies the name of the configuration file to be downloaded. The file must be a .cfg file. The file name is a case-insensitive string of up to 255 characters.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If the TFTP server is on the public network, do not specify this option.

Usage guidelines

Before restoring the configuration file for the next startup, make sure the following requirements are met:

- The server is reachable.
- The server is enabled with TFTP service.
- You have read and write permissions to the server.

This command downloads the configuration file to the root directory of the default storage medium on each member device and specifies the file as the main next-startup configuration file. If the default storage medium has been partitioned, the configuration file is saved on the first partition. Make sure all IRF members use the same type of default storage media. If a subordinate device uses a different type of default storage medium than the master, the command cannot propagate the configuration file to the subordinate device. For example, the subordinate device uses a USB disk, but the master uses a flash memory. In this situation, you must manually restore the main next-startup configuration file on the subordinate device.

Examples

Download **test.cfg** from the IPv4 TFTP server at 2.2.2.2 in the public network, and specify the file as the main next-startup configuration file.

```
<Sysname> restore startup-configuration from 2.2.2.2 test.cfg
Restoring the next startup-configuration file from 2.2.2.2...
Done.
```

Download **test.cfg** from the IPv4 TFTP server at 2.2.2.2 in MPLS L3VPN instance **VPN1**, and specify the file as the main next-startup configuration file.

```
<Sysname> restore startup-configuration from 2.2.2.2 test.cfg vpn-instance VPN1
Restoring the next startup-configuration file from 2.2.2.2...
Done.
```

Download **test.cfg** from the IPv6 TFTP server at 2001::2 in the public network, and specify the file as the main next-startup configuration file.

```
<Sysname> restore startup-configuration from ipv6 2001::2 test.cfg
Restoring the next startup-configuration file from 2001::2...
Done.
```

Related commands

backup startup-configuration

save

Use **save** *file-url* [**all** | **slot** *slot-number*] to save the running configuration to a configuration file, without specifying the file as a next-startup configuration file.

Use **save** [**safely**] [**backup** | **main**] [**force**] [**context-all** | **changed**] to save the running configuration to a file in the root directory of the storage medium. This command automatically saves the file on each IRF member device and specifies the file as a next-startup configuration file.

Syntax

save *file-url* [**all** | **slot** *slot-number*]

save [**safely**] [**backup** | **main**] [**force**] [**context-all** | **changed**]

Views

Any view

Predefined user roles

network-admin

context-admin

Parameters

file-url: Specifies a file path, a string of up to 255 characters. The file must be a .cfg file. If you specify the **all** keyword or the **slot** *slot-number* option, the file path cannot include a member ID. If the file path includes a folder name, the folder must already exist on all IRF member devices.

all: Saves the running configuration to all member devices. If you do not specify this keyword or the **slot** *slot-number* option, the command saves the running configuration only to the master.

slot *slot-number*: Specifies a subordinate device by its member ID. If you do not specify a subordinate device or the **all** keyword, this command saves the running configuration only to the master.

safely: Saves the configuration file in safe mode. If you do not specify this keyword, the device saves the configuration file in fast mode.

backup: Saves the running configuration to a configuration file, and specifies the file as the backup next-startup configuration file. If you do not specify this keyword or the **main** keyword, the command specifies the saved file as the main next-startup configuration file.

main: Saves the running configuration to a configuration file, and specifies the file as the main next-startup configuration file. If you do not specify this keyword or the **backup** keyword, the command specifies the saved file as the main next-startup configuration file.

force: Saves the running configuration to the existing next-startup configuration file without prompting for confirmation. If you do not specify this keyword, the system prompts you to confirm the operation. If you do not confirm the operation within 30 seconds, the system automatically aborts the operation. If you enter **Y** within the time limit, you can continue the save process and change the target file name during the process.

context-all: Saves the running configuration for each context. The running configuration for each context is saved to the storage medium of the firewall module. If you do not specify this keyword, the **save** command saves the running configuration only for the context where you are logged in.

changed: Overwrites the target configuration file with the running configuration if an inconsistency is detected between the settings in the configuration file and the running configuration. The **save** command does not take effect if no inconsistency is detected. If you do not specify this keyword, the **save** command always overwrites the target configuration file with the running configuration.

Usage guidelines

CAUTION:

Use the **save** command with caution. This command will overwrite the settings in the target configuration file. When you execute this command, carefully read the messages displayed by the system and make sure you fully understand the impact of this command on services.

If the file specified for this command does not exist, the system creates the file before saving the configuration. If the file already exists, the system prompts you to confirm whether to overwrite the file. If you choose to not overwrite the file, the system cancels the save operation.

This command saves the running configuration to an .mdb binary file as well as a .cfg text file. The two files use the same file name. An .mdb file takes less time to load than a .cfg file.

When you use the **save** [**safely**] [**backup** | **main**] [**force**] [**context-all** | **changed**] command, follow these guidelines:

- In safe mode, the system saves configuration in a temporary file and starts overwriting the target next-startup configuration file after the save operation is complete. If a reboot, power failure, or out of memory or storage space event occurs during the save operation, the next-startup configuration file is retained.

- In fast mode, the device directly overwrites the target next-startup configuration file. If a reboot, power failure, or out of memory or storage space event occurs during this process, all settings in the next-startup configuration file are lost.

Safe mode is slower than fast mode, but more secure. As a best practice, specify the **safely** keyword for reliable configuration saving.

Examples

Save the running configuration to **backup.cfg**, without specifying the file as a next-startup configuration file.

```
<Sysname> save backup.cfg
The current configuration will be saved to flash:/backup.cfg. Continue? [Y/N]:y
Now saving current configuration to the device.
Saving configuration flash:/backup.cfg. Please wait...
Configuration is saved to device successfully.
```

Save the running configuration to the main next-startup configuration file without any confirmation required.

```
<Sysname> save force
Validating file. Please wait....
Saved the current configuration to mainboard device successfully.
```

Save the running configuration to a file in the root directory of the default storage medium, and specify the file as the main next-startup configuration file.

```
<Sysname> save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/backup.cfg]
(To leave the existing filename unchanged, press the enter key):test.cfg
Validating file. Please wait.....
Saved the current configuration to mainboard device successfully.
```

Save the running configuration to a file in the root directory of the storage medium for each context, and specify the file as the main next-startup configuration file.

```
<Sysname> save context-all
Save current configuration in all context? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Saved the current configuration of context Admin to mainboard device successfully.
```

Related commands

display current-configuration

display saved-configuration

startup saved-configuration

Use **startup saved-configuration** to specify a file as a next-startup configuration file.

Use **undo startup saved-configuration** to configure the system to start up with the factory defaults at the next startup.

Syntax

startup saved-configuration *cfgfile* [**backup** | **main**]

undo startup saved-configuration

Default

No next-startup configuration files are specified.

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

cfgfile: Specifies the path of a configuration file, a string of up to 255 characters. The file must be a .cfg file. The file path can include only the file name, or the storage medium information and file name. If the file is not on the default storage medium, you must specify the file name with storage medium information.

backup: Specifies the configuration file as the backup next-startup configuration file.

main: Specifies the configuration file as the main next-startup configuration file. This is the primary configuration file that the device attempts to load at startup. If the loading attempt fails, the device tries the backup next-startup configuration file.

Usage guidelines

CAUTION:

In an IRF fabric, the **undo startup saved-configuration** command can cause an IRF split after the IRF fabric or an IRF member reboots.

The **startup saved-configuration** command applies to all IRF members. To successfully execute this command, make sure the specified file has been saved in the root directory of the storage medium on each member.

If you do not specify the **backup** or **main** keyword, the **startup saved-configuration** command specifies the main next-startup configuration file.

As a best practice, specify different files as the main and backup next-startup configuration files.

The **undo startup saved-configuration** command changes the file attribute of the main and backup next-startup configuration files to NULL. However, the command does not delete the two configuration files.

You can also specify a configuration file as a next startup file when you use the **save** command to save the running configuration.

Examples

Specify the main next-startup configuration file.

```
<Sysname> startup saved-configuration testcfg.cfg
Please wait ....... Done.
```

Related commands

display startup

Contents

Software upgrade commands

As a best practice, store the startup images in the factory default file system. If you store the startup images in a hot swappable storage medium, do not remove the hot swappable storage medium during the startup process.

boot-loader file

Use **boot-loader file** to specify startup image files.

Syntax

boot-loader file boot *filename* **system** *filename* [**feature** *filename*&<1-30>] { **all** | **slot** *slot-number* } { **backup** | **main** }

boot-loader file *ipe-filename* { **all** | **slot** *slot-number* } { **backup** | **main** }

Views

User view

Predefined user roles

network-admin

Parameters

boot: Specifies a boot image file.

system: Specifies a system image file.

feature: Specifies a space-separated list of up to 30 feature image files.

filename: Specifies a .bin file in the *filesystemnameIfilename***.bin** format. The file must be stored in the root directory of a file system on the device. Excluding the file system location section (if any), the value string can have a maximum of 63 characters. For more information about specifying a file, see file system management in *Fundamentals Configuration Guide*.

ipe-filename: Specifies an .ipe image package file in the *filesystemnameIfilename***.ipe** format. The file must be stored in the root directory of a file system on the device. Excluding the file system location section (if any), the value string can have a maximum of 63 characters. For more information about specifying a file, see file system management in *Fundamentals Configuration Guide*.

all: Specifies all hardware components to which the specified images apply.

slot *slot-number*: Specifies the IRF member ID of a member device.

backup: Specifies the files as backup startup image files. Backup images are used only when main images are not available.

main: Specifies the files as main startup image files. The device always first attempts to start up with main startup files.

Usage guidelines

The **boot-loader file** command overwrites the entire startup image list. To add new startup feature images, specify all feature image files in the old startup image list, including feature image files. The new startup image list will contain only the feature image files that are specified in the command.

Before you specify startup image files, register and activate a license for each upgrade image that requires a license. If a license-based software image lacks a license, the command execution result is as follows:

- If .bin files are specified, the command cannot be executed.
- If an .ipe file is specified, the command sets all images as startup images except for the image that does not have a license.

For more information about licensing, see *Fundamentals Configuration Guide*.

To load the specified startup software images, you must reboot the system.

If the upgrade images are not found in the file system on the slot specified to upgrade, the system automatically copies the images to that file system. The destination directory is the root directory of the file system. If the destination root directory already contains a startup image with the same name as an upgrade image, you must choose whether to overwrite the image.

Incremental patches cannot be installed by using the **boot-loader file** command.

NOTE:

The system will verify the digital signature of the specified images before it updates the startup image list with the specified images. If the digital signature verification fails, the system will not update the startup image list and you will receive a digital signature verification failure message.

Examples

Specify **flash:/all.ipe** as the main startup image file for slot 1.

```
<Sysname> boot-loader file flash:/all.ipe slot 1 main
Verifying the file flash:/all.ipe on slot 1.............Done.
NSFOCUS NFNX3-HDB680 images in IPE:
  boot.bin
  system.bin
This command will set the main startup software images. Please do not reboot any
 MPU during the upgrad. Continue? [Y/N]:Y
Add images to slot 1.
File flash:/boot.bin already exists on slot 1.
File flash:/system.bin already exists on slot 1.
Overwrite the existing files? [Y/N]:Y
Decompressing file boot.bin to flash:/boot.bin.....................Done.
Decompressing file system.bin to flash:/system.bin.............................Done.
Verifying the file flash:/boot.bin on slot 1...Done.
Verifying the file flash:/system.bin on slot 1.............Done.
The images that have passed all examinations will be used as the main startup software
images at the next reboot on slot 1.
```

Specify **flash:/all.ipe** as the main startup image file for all IRF member devices.

```
<Sysname> boot-loader file slot1#flash:/all.ipe all main
Verifying the file flash:/all.ipe on slot 1.................................Done.
NSFOCUS NFNX3-HDB680 images in IPE:
  Boot.bin
  System.bin
This command will set the main startup software images. Please do not reboot any
 MPU during the upgrad. Continue? [Y/N]:y
Add images to slot 1.
File flash:/Boot.bin already exists on slot 1.
File flash:/System.bin already exists on slot 1.
Overwrite the existing files? [Y/N]:y
Decompressing file Boot.bin to flash:/Boot.bin.....................Done.
```

```
Decompressing file System.bin to flash:/System.bin.....................Done.
The images that have passed all examinations will be used as the main startup software
images at the next reboot on slot 1.
File flash:/Boot.bin already exists on slot 2.
Do you want to overwrite the file?
 Y: Overwrite the file.
 N: Not overwrite the file.
 A: From now on, overwrite or not overwrite without prompt.
Please make a choice. [Y/N/A]:a
What type of overwrite operation do you want to perform?
 Y: Overwrite without prompt.
 N: Not overwrite or display prompt.
 Q: Return to the previous step.
Please make a choice. [Y/N/Q]:y
An existing file will be overwritten without prompt if it has the same name as any upgrade
file.
Loading.....................Done.
Loading.....................Done.
Loading.....................Done.
Loading.....................Done.
Loading.....................Done.
Loading.....................Done.
The images that have passed all examinations will be used as the main startup software
images at the next reboot on slot 2.
Decompression completed.
Do you want to delete flash:/all.ipe now? [Y/N]:n
```

Related commands

display boot-loader

boot-loader update

Use **boot-loader update** to synchronize startup images.

Syntax

boot-loader update { **all** | **slot** *slot-number* }

Views

User view

Predefined user roles

network-admin

Parameters

all: Synchronizes startup images from the master to all subordinate devices.

slot *slot-number*: Specifies the IRF member ID of a subordinate device.

Usage guidelines

You can use this command to synchronize startup images after adding new member devices.

If any of the startup software images require a license, register and activate a license for the image on the new subordinate device before executing this command. Use the **display license feature** command to verify the licensing state of software images.

The startup images synchronized to the subordinate device are set as main startup images, regardless of whether the source startup images are main or backup.

- If the master device has started up with main startup images, its main startup images are synchronized to the subordinate device, regardless of whether any main startup image has been respecified on the master device.
- If the master device has started up with backup startup images, its backup startup images are synchronized to the subordinate device, regardless of whether any backup startup image has been respecified on the master device.

If a patch installation or ISSU has been performed on the master, use the **install commit** command to update the set of main startup images on the master before software synchronization. This command ensures startup image consistency between the master and the subordinate device.

Do not reboot any member device during the execution of the **boot-loader update** command. Member devices might not be able to come up.

Startup image synchronization fails if any software image being synchronized is not available or is corrupted.

Examples

Synchronize startup images from the active MPU to the standby MPU in slot 1.

```
<Sysname> boot-loader update slot 1
This command will update the specified standby MPU. Please do not reboot any MPU during
the upgrade. Continue? [Y/N]:y
Updating. Please wait...
Verifying the file flash:/BOOT.bin on slot 1.............Done.
Verifying the file flash:/SYSTEM.bin on slot 1.....................Done.
Successfully updated the startup software images of slot 1.
```

Related commands

display boot-loader

install commit

bootrom backup

Use **bootrom backup** to back up the BootWare image in the Normal area to the Backup area on a BootWare.

Syntax

bootrom backup slot *slot-number-list* [**all** | **part**]

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number-list*: Specifies a space-separated list of up to seven slot number items. An item specifies an IRF member device by its member ID or a range of IRF member devices in the form of *start-slot-number* **to** *end-slot-number*. The end slot number must be equal to or greater than the start slot number.

all: Backs up the entire BootWare image, including the basic segment and the extended segment. If you do not specify the **all** or **part** keyword, this command backs up the entire BootWare image.

part: Backs up the extended BootWare image section.

Usage guidelines

A BootWare is divided into a Normal area and a Backup area. The BootWare image is stored in the Normal area and backed up to the Backup area. At startup, the system reads the BootWare image automatically from the Normal area. If the image is inaccessible, the system reads the BootWare image from the Backup area.

If the BootWare image in the Normal area is corrupted or requires a version rollback, use the **bootrom restore** command to copy the BootWare image in the Backup area to the Normal area.

Examples

Back up the entire BootWare image from the Normal area to the Backup area.

```
<Sysname> bootrom backup slot 1
Now backing up the Boot ROM, please wait...
......Done.
```

Related commands

bootrom restore

bootrom read

Use **bootrom read** to back up the BootWare image in the Normal area of a BootWare to the default file system.

Syntax

bootrom read slot *slot-number-list* [**all** | **part**]

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number-list*: Specifies a space-separated list of up to seven slot number items. An item specifies an IRF member device by its member ID or a range of IRF member devices in the form of *start-slot-number* **to** *end-slot-number*. The end slot number must be equal to or greater than the start slot number.

all: Backs up the entire BootWare image, including the basic segment and the extended segment. If you do not specify the **all** or **part** keyword, this command backs up the entire BootWare image.

part: Backs up the extended BootWare image section.

Usage guidelines

For each BootWare image you are backing up, this command creates two files in the default file system: **basicbtm.bin** for the basic segment and **extendbtm.bin** for the extended segment.

Examples

Back up the BootWare image from the Normal area of BootWare to the flash memory.

```
<Sysname> bootrom read slot 1
  Now reading the Boot ROM, please wait...
.........Done.
```

Related commands

bootrom update

bootrom restore

Use **bootrom restore** to replace the BootWare image in the Normal area with the BootWare image in the Backup area for image restoration or version rollback.

Syntax

bootrom restore slot *slot-number-list* [**all** | **part**]

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number-list*: Specifies a space-separated list of up to seven slot number items. An item specifies an IRF member device by its member ID or a range of IRF member devices in the form of *start-slot-number* **to** *end-slot-number*. The end slot number must be equal to or greater than the start slot number.

all: Restores the entire BootWare image, including the basic segment and the extended segment. If you do not specify the **all** or **part** keyword, this command restores the entire BootWare image.

part: Restores the extended BootWare image section.

Examples

Restore the entire BootWare image.

```
<Sysname> bootrom restore slot 1
  This command will restore the Boot ROM file on the specified board(s), Continue? [Y/N]:y
  Now restoring the Boot ROM, please wait...
......Done.
```

Related commands

bootrom backup

bootrom update

Use **bootrom update** to load the BootWare image from a file system to the Normal BootWare area.

Syntax

bootrom update file *file* **slot** *slot-number-list* [**all** | **part**]

Views

User view

Predefined user roles

network-admin

Parameters

file *file*: Specifies the file that contains the BootWare image. The *file* argument represents the file name, a string of 1 to 63 characters.

slot *slot-number-list*: Specifies a space-separated list of up to seven slot number items. An item specifies an IRF member device by its member ID or a range of IRF member devices in the form of *start-slot-number* **to** *end-slot-number*. The end slot number must be equal to or greater than the start slot number.

all: Loads the entire BootWare image, including the basic segment and the extended segment. If you do not specify the **all** or **part** keyword, this command restores the entire BootWare image.

part: Loads the extended BootWare image section.

Usage guidelines

BootWare images are contained in the .bin NF boot image file. You can specify a NF boot image file in this command to upgrade the BootWares in the system before you upgrade the NF images. If you do not upgrade BootWares before upgrading NF images, the system automatically upgrades BootWares as necessary when loading NF images.

The new BootWare images take effect after you reboot the device.

NOTE:

The system verifies a BootWare image before it loads that image to the Normal area of BootWare. If the digital signature verification fails, the system will not load the image and you will receive a digital signature verification failure message.

Examples

Use the file **a.bin** in the root directory of the flash memory to upgrade the BootWare image.

```
<Sysname> bootrom update file flash:/a.bin slot 1
   This command will update the Boot ROM file on the specified board(s), Continue? [Y/N]:y
   Now updating the Boot ROM, please wait..............Done.
```

Related commands

boot-loader file

bootrom-update security-check enable

Use **bootrom-update security-check enable** to enable BootWare image validity check.

Use **undo bootrom-update security-check enable** to disable BootWare image validity check.

Syntax

bootrom-update security-check enable

undo bootrom-update security-check enable

Default

BootWare image validity check is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Before a BootWare image upgrade starts, this feature examines the upgrade BootWare image for file validity and incompatibility with hardware. If the BootWare image passes the check, the upgrade process starts. If the check fails, the system does not perform the upgrade.

Examples

Enable BootWare image validity check.

```
<Sysname> system-view
[Sysname] bootrom-update security-check enable
```

display boot-loader

Use **display boot-loader** to display current software images and startup software images.

Syntax

display boot-loader [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies the member ID of an IRF member device. If you do not specify a member device, this command displays the software images on each IRF member device.

Examples

Display the current software images and startup software images.

```
<Sysname> display boot-loader
Software images on slot 1:
Current software images:
  flash:/boot.bin
  flash:/system.bin
Main startup software images:
  flash:/boot.bin
  flash:/system.bin
Backup startup software images:
  flash:/boot.bin
  flash:/system.bin
```

Display the current software images and startup software images.

```
<Sysname> display boot-loader
Software images on slot 1:
Current software images:
  Image              Version
  flash:/boot.bin      Release 0053
  flash:/system.bin    Release 0053
Main startup software images:
  Image              Version
  flash:/boot.bin      Release 0054
  flash:/system.bin    Release 0054
Backup startup software images:
  Image              Version
  flash:/boot.bin      --
```

```
flash:/system.bin    --
```

Table 1 Command output

Field	Description
Current software images	NF images that have been loaded.
Main startup software images	Primary NF images for the next startup.
Image	Image name.
Version	Image version. If an image is corrupted or deleted, this field displays two hyphens (**--**).
Backup startup software images	Backup NF images for the next startup. If the backup startup software images are not specified, this field displays **None**.

Related commands

boot-loader file

Contents

ISSU commands

display install active

Use **display install active** to display active software images.

Syntax

display install active [**slot** *slot-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all IRF members.

verbose: Displays detailed information. If you do not specify this keyword, the command displays only image names.

Examples

Display active software images.

```
<Sysname> display install active
Active packages on slot 1:
  flash:/boot.bin
  flash:/system.bin
  flash:/feature1.bin
```

Display detailed information about active software images.

```
<Sysname> display install active verbose
Active packages on slot 1:
flash:/boot.bin
 [Package]
 Vendor: NFNX3-HDB680
 Product: xxxx
 Service name: boot
 Platform version: 7.1.070
 Product version: Test 0001015
 Supported board: mpu
 [Component]
 Component: boot
 Description: boot package

flash:/system.bin
 [Package]
 Vendor: NFNX3-HDB680
 Product: xxxx
```

```
 Service name: system
 Platform version: 7.1.070
 Product version: Test 0001015
 Supported board: mpu
 [Component]
 Component: system
 Description: system package

flash:/feature1.bin
 [Package]
 Vendor: NFNX3-HDB680
 Product: xxxx
 Service name: test
 Platform version: 7.1.070
 Product version: Test 0001015
 Supported board: mpu
 [Component]
 Component: test
 Description: test package
```

Table 1 Command output

Field	Description
[Package]	Detailed information about the software image.
Service name	Image type: • **boot**—Boot image. • **system**—System image. • **boot patch**—Patch image for the boot image. • **system patch**—Patch image for the system image. • Any other value indicates a feature image.
Supported board	Hardware types supported by the software image: **mpu**—Member device.
[Component]	Information about components included in the image file.

Related commands

`install active`

display install backup

Use **`display install backup`** to display backup startup software images.

Syntax

`display install backup` [**`slot`** *`slot-number`*] [**`verbose`**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all IRF members.

verbose: Displays detailed information. If you do not specify this keyword, the command displays only image names.

Usage guidelines

Backup startup images are used only when the main boot or system image is missing or corrupt. For more information, see *Fundamentals Configuration Guide*.

To modify the backup startup image list, use the **boot-loader file** command.

Examples

Display the backup startup software images.

```
<Sysname> display install backup
Backup startup software images on slot 1:
  flash:/boot.bin
  flash:/system.bin
```

Display detailed information about backup startup software images.

```
<Sysname> display install backup verbose
Backup startup software images on slot 1:
 flash:/boot.bin
 [Package]
 Vendor: NFNX3-HDB680
 Product: xxxx
 Service name: boot
 Platform version: 7.1.070
 Product version: Test 0001015
 Supported board: mpu
 [Component]
 Component: boot
 Description: boot package

 flash:/system.bin
 [Package]
 Vendor: NFNX3-HDB680
 Product: xxxx
 Service name: system
 Platform version: 7.1.070
 Product version: Test 0001015
 Supported board: mpu
 [Component]
 Component: system
 Description: system package
```

For information about the command output, see Table 1.

Related commands

boot-loader file

display install committed

display install committed

Use **display install committed** to display main startup software images.

Syntax

display install committed [**slot** *slot-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all member devices.

verbose: Displays detailed information. If you do not specify this keyword, the command displays only image names.

Usage guidelines

Some **install** commands modify the current software image list but do not modify the main startup image list. For the software image changes to take effect after a reboot, you must execute the **install commit** command to update the main startup image list with the image changes. You can use the **display install committed** command to verify the operation results.

Both the **install commit** and **boot-loader file** commands modify the main startup software image list.

Examples

Display the main startup software images.

```
<Sysname> display install committed
Committed packages on slot 1:
 flash:/boot.bin
 flash:/system.bin
 flash:/feature1.bin
```

Display detailed information about main startup software images.

```
<Sysname> display install committed verbose
Committed packages on slot 1:
 flash:/boot.bin
 [Package]
 Vendor: NFNX3-HDB680
 Product: xxxx
 Service name: boot
 Platform version: 7.1.070
 Product version: Test 0001015
 Supported board: mpu
 [Component]
 Component: boot
 Description: boot package
```

```
 flash:/system.bin
 [Package]
 Vendor: NFNX3-HDB680
 Product: xxxx
 Service name: system
 Platform version: 7.1.070
 Product version: Test 0001015
 Supported board: mpu
 [Component]
 Component: system
 Description: system package

flash:/feature1.bin
 [Package]
 Vendor: NFNX3-HDB680
 Product: xxxx
 Service name: feature1
 Platform version: 7.1.070
 Product version: Test 0001015
 Supported board: mpu
 [Component]
 Component: feature1
 Description: feature1 package
```

For information about the command output, see Table 1.

Related commands

boot-loader file

display install backup

install commit

display install inactive

Use **display install inactive** to display inactive software images in the root directories of file systems.

Syntax

display install inactive [**slot** *slot-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all member devices.

verbose: Displays detailed information. If you do not specify this keyword, the command displays only image names.

Examples

Display brief information about inactive software images in the root directories of the file systems.

```
<Sysname> display install inactive
Inactive packages on slot 1:
 flash:/feature1.bin
```

Display detailed information about inactive software images in the root directories of the file systems.

```
<Sysname> display install inactive verbose
Inactive packages on slot 1:
flash:/feature1.bin
 [Package]
 Vendor: NFNX3-HDB680
 Product: xxxx
 Service name: feature1
 Platform version: 7.1.070
 Product version: Test 0001015
 Supported board: mpu
 [Component]
 Component: feature1
 Description: feature1 package
```

For information about the command output, see Table 1.

Related commands

install deactivate

display install ipe-info

Use **display install ipe-info** to display the software images included in an .ipe file.

Syntax

display install ipe-info *ipe-filename*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipe-filename: Specifies an .ipe file in the *filesystemname*/*filename*.**ipe** format. The file must be stored in the root directory of a file system on the device. The value string excluding the file system location section (if any) can have a maximum of 63 characters. For more information about specifying a file, see file system management in *Fundamentals Configuration Guide.*

Examples

Display information about .ipe file **flash:/test.ipe**.

```
<Sysname> display install ipe-info flash:/test.ipe
Verifying the file flash:/test.ipe on slot 1.............Done.
```

```
XX images in IPE:
  boot.bin
  system.bin
```

Related commands

display install package

display install job

Use **display install job** to display ongoing ISSU activate, deactivate, and rollback operations.

Syntax

display install job

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display ongoing ISSU activate, deactivate, and rollback operations.

```
<Sysname> display install job
 JobID:5
  Action:install activate flash:/feature1.bin on slot 1
```

The output shows that the device is executing the **install activate flash:/feature1.bin slot 1** command.

display install log

Use **display install log** to display ISSU log information.

Syntax

display install log [*log-id*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

log-id: Specifies a log entry by its ID. If you do not specify this argument, the command displays all ISSU log entries.

verbose: Displays detailed ISSU log information. If you do not specify this keyword, the command displays brief ISSU log information.

Usage guidelines

The device creates one log entry for each ISSU operation to track the ISSU process and operation result.

The ISSU log can contain a maximum of 50 entries. The latest entry overwrites the oldest entry if the log is full.

Examples

Display all ISSU log entries.

```
<Sysname> display install log
Install job 1 started by user root at 04/28/2001 08:39:29.
Job 1 completed successfully at 04/28/2001 08:39:30.
Install job 1 started by user root at 04/28/2001 08:39:29.
    Install activate flash:/feature1.bin on slot 1
Job 1 completed successfully at 04/28/2001 08:39:30.
Install job 1 started by user root at 04/28/2001 08:39:29.
Job 1 completed successfully at 04/28/2001 08:39:30.
------------------------------------------------------------
Install job 2 started by user root at 04/28/2001 08:40:29.
Job 2 completed successfully at 04/28/2001 08:40:30.
Install job 2 started by user root at 04/28/2001 08:40:29.
    Install activate flash:/route.bin on slot 1
Job 2 completed successfully at 04/28/2001 08:40:30.
Install job 2 started by user root at 04/28/2001 08:40:29.
Job 2 completed successfully at 04/28/2001 08:40:30.
```

Displays detailed information about ISSU log entry 1.

```
<Sysname> display install log 1 verbose
Install job 1 started by user root at 04/28/2001 08:39:29.
Job 1 completed successfully at 04/28/2001 08:39:30.
Install job 1 started by user root at 04/28/2001 08:39:29.
    Install activate flash:/feature1.bin on slot 1
Job 1 completed successfully at 04/28/2001 08:39:30.
Install job 1 started by user root at 04/28/2001 08:39:29.
Job 1 completed successfully at 04/28/2001 08:39:30.
Detail of activating packages on slot 1.
    Get upgrade policy successfully.
Detail of activating packages on slot 1.
    Uncompress package to system successfully.
    Remove files from system successfully.
```

Table 2 Command output

Field	Description
Detail of xxx	Detailed information about an ISSU operation.
Get upgrade policy successfully.	Obtained the upgrade policy.
Uncompress package to system successfully.	Decompressed the package successfully.
Remove files from system successfully.	Deleted files from the system successfully.

Related commands

reset install log-history oldest

display install package

Use **display install package** to display software image file information.

Syntax

display install package { *filename* | **all** } [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

filename: Specifies a .bin file in the *filesystemnameIfilename***.bin** format. The file must be stored in the root directory of a file system on the device. The value string excluding the file system location section (if any) can have a maximum of 63 characters. For more information about specifying a file, see file system management in *Fundamentals Configuration Guide.*

all: Specifies all software image files in the root directories of the master's file systems.

verbose: Displays detailed information. If you do not specify this keyword, the command displays only basic software image information.

Examples

Display information about **system.bin**.

```
<Sysname> display install package flash:/system.bin
  flash:/system.bin
  [Package]
  Vendor: NFNX3-HDB680
  Product: xxxx
  Service name: system
  Platform version: 7.1.070
  Product version: Test 0001015
  Supported board: mpu
```

Display detailed information about **system.bin**.

```
<Sysname> display install package flash:/system.bin verbose
  flash:/system.bin
  [Package]
  Vendor: NFNX3-HDB680
  Product: xxxx
  Service name: system
  Platform version: 7.1.070
  Product version: Test 0001015
  Supported board: mpu
  [Component]
  Component: system
  Description: system package
```

For information about the command output, see Table 1.

display install rollback

Use **display install rollback** to display rollback point information.

Syntax

display install rollback [*point-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

point-id: Specifies a rollback point ID. If you do not specify a rollback point ID, the command displays all rollback points.

Usage guidelines

Use this command to identify available rollback points during an ISSU that uses **install** commands. The system does not record rollback points during an ISSU that uses **issu** commands.

Examples

Display all rollback points.

```
<Sysname> display install rollback
Install rollback information 1 on slot 1:
  Updating from flash:/route-1.bin
         to flash:/route-2.bin.

Install rollback information 2 on slot 1:
   Deactivating flash:/route-2.bin
```

The output shows that the device has two rollback points.

- At rollback point 1, **flash:/route-1.bin** was upgraded to **flash:/route-2.bin**.
- At rollback point 2, **flash:/route-2.bin** was deactivated.

Related commands

install rollback

reset install rollback oldest

display install which

Use **display install which** to display all software image files that include a specific component or file.

Syntax

display install which { **component** *name* | **file** *filename* } [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

component *name*: Specifies a component name.

file *filename*: Specifies a file in the *filename.extension* format, a case-insensitive string of up to 63 characters. It cannot contain path information.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all IRF members.

Usage guidelines

A component is a collection of features. The features of a component are installed or uninstalled at the same time.

When the system displays a component or file error, use this command to identify the image files that include the component or file. Then, you can use the **install verify** command to identify image file problems.

This command searches only the root directories of the file systems at the specified location.

Examples

Display the software image file that includes **pkg_ctr**.

```
<Sysname> display install which file pkg_ctr
Verifying the file flash:/system-t0001015.bin on slot 1.......................Done.
Found pkg_ctr in flash:/system-t0001015.bin on slot 1.
  flash:/system-t0001015.bin
  [Package]
  Vendor: NFNX3-HDB680
  Product: xxxx
  Service name: system
  Platform version: 7.1.070
  Product version: Test 0001015
  Supported board: mpu

Verifying the file flash:/boot-d2601007.bin on slot 1....Done.
```

Table 3 Command output

Field	Description
Verifying the file	The system was verifying the validity of the file.
[Package]	Detailed information about the software image.
Service name	Image type: • **boot**—Boot image. • **system**—System image. • **patch**—Patch image. • Any other value indicates a feature image.
Supported board	Hardware types supported by the software image: **mpu**—Member device.

display issu rollback-timer

Use **display issu rollback-timer** to display automatic rollback timer information.

Syntax

display issu rollback-timer

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

Change to the automatic rollback interval does not take effect on the ongoing ISSU process. The current remaining rollback time might be greater than the specified automatic rollback interval.

Examples

Display automatic rollback timer information after the **issu run switchover** command is executed.

```
<Sysname> display issu rollback-timer
Rollback timer: Working
Rollback interval: 45 minutes
Rollback time remaining : 40 minutes
```

Display automatic rollback timer information after the **issu accept** command is executed.

```
<Sysname> display issu rollback-timer
Rollback timer: Not working
Rollback interval: 30 minutes
```

Display automatic rollback timer information when no ISSU process is taking place.

```
<Sysname> display issu rollback-timer
Rollback timer: Not working
Rollback interval: 45 minutes
```

Related commands

issu rollback-timer

display issu state

Use **display issu state** to display ISSU status information.

Syntax

display issu state

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

During an ISSU that uses **issu** commands, you can use this command to verify the ISSU status and determine what to do next.

This command does not apply to an ISSU that uses **install** commands, because the ISSU state machine is not involved.

Examples

Display ISSU status information when no upgrade is taking place.

```
<Sysname> display issu state
ISSU state: Init
Compatibility: Unknown
Work state: Normal
Upgrade method: Card by card
Upgraded slot: None
Current upgrading slot: None
Current version list:
  boot: 7.1.070, Test 0001015
  system: 7.1.070, Test 0001015
  feature1: 7.1.070, Test 0001015
Current software images:
  flash:/boot-t0001015.bin
  flash:/system-t0001015.bin
  flash:/feature1-t0001015.bin
```

Display ISSU status information while the **issu load** command is being executed.

```
<Sysname> display issu state
ISSU state: Loading
Compatibility: Incompatible
Work state: Normal
Upgrade method: Card by card
Upgraded slot: None
Current upgrading slot:
  slot 1
Previous version list:
  boot: 7.1.070, Test 0001015
  system: 7.1.070, Test 0001015
  feature1: 7.1.070, Test 0001015
Previous software images:
  flash:/boot-t0001015.bin
  flash:/system-t0001015.bin
  flash:/feature1-t0001015.bin
Upgrade version list:
  boot: 7.1.070, Test 0001016
  system: 7.1.070, Test 0001016
  feature1: 7.1.070, Test 0001016
Upgrade software images:
  flash:/boot-t0001016.bin
  flash:/system-t0001016.bin
  flash:/feature1-t0001016.bin
```

Table 4 Command output

Field	Description
ISSU state	ISSU status: • **Init**—The ISSU process has not started or has finished. • **Loading**—The system is executing the **issu load** command. • **Loaded**—The **issu load** command is completed. • **Switching**—The system is executing the **issu run switchover** command. • **Switchover**—The **issu run switchover** command is completed. • **Accepted**—The **issu accept** command is completed. • **Committing**—The system is executing the **issu commit** command. • **Rollbacking**—A rollback is in progress. • **Unknown**—An upgrade is in progress. This value is displayed if you execute the command on an original subordinate member.
Compatibility	Version compatibility: • **Compatible**—Upgrade to a compatible version. • **Incompatible**—Upgrade to an incompatible version. • **Unknown**—No upgrade is in progress.
Work state	Operating status of the device: • **Normal**—The device is operating correctly. • **Independent active**—When you perform an ISSU to an incompatible version, a subordinate member that is upgraded first enters this state. In this state, member devices are not running the same software versions.
Upgrade method	Upgrade mode. The value of this field is fixed at **Card by card**. In this mode, member devices are upgraded one by one.
Upgraded slot	Upgraded members. During a rollback, this field displays **Unknown**.
Current upgrading slot	Members that are being upgraded. During a rollback, this field displays **Unknown**.
Current version list	Versions of currently running images. This field is displayed if no upgrade is taking place.
Current software images	File names of currently running images. This field is displayed if no upgrade is taking place.
Previous version list	Versions of the images that were running on the device before the ISSU. If you execute the command on an original subordinate member while the member is being upgraded to an incompatible version, this field displays **Unknown**.
Previous software images	File names of the images that were running on the device before the ISSU. If you execute the command on an original subordinate member while the member is being upgraded to an incompatible version, this field displays **Unknown**.
Upgrade version list	Versions of the upgrade images. If you execute the command on an original subordinate member while the member is being upgraded to an incompatible version, this field displays **Unknown**.
Upgrade software images	File names of the upgrade images. If you execute the command on an original subordinate member while the member is being upgraded to an incompatible version, this field displays **Unknown**.

Related commands

issu accept

issu commit

issu load

issu rollback

issu run switchover

display version comp-matrix

Use **display version comp-matrix** to display the recommended ISSU methods.

Syntax

display version comp-matrix file { **boot** *filename* | **system** *filename* | **feature** *filename*&<1-30> | **patch** *filename*&<1-30> } *

display version comp-matrix file ipe *ipe-filename* [**patch** *filename*&<1-30>]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

boot: Specifies a boot image file.

system: Specifies a system image file.

feature: Specifies a space-separated list of up to 30 feature image files.

patch: Specifies a space-separated list of up to 30 patch image files.

filename: Specifies a .bin file in the *filesystemnameIfilename***.bin** format. The file must be stored in the root directory of a file system on the device. The value string excluding the file system location section (if any) can have a maximum of 63 characters. For more information about specifying a file, see file system management in *Fundamentals Configuration Guide.*

ipe-filename: Specifies an .ipe file in the *filesystemnameIfilename***.ipe** format. The file must be stored in the root directory of a file system on the device. The value string excluding the file system location section (if any) can have a maximum of 63 characters. For more information about specifying a file, see file system management in *Fundamentals Configuration Guide.*

Usage guidelines

If one or more images are incompatible, the incompatible upgrade method applies. The entire system needs to be rebooted during an incompatible upgrade.

Examples

Display the recommended ISSU methods. In this example, the specified images are compatible with the running images.

```
<Sysname> display version comp-matrix file boot flash:/boot-t0001015.bin system
flash:/system-t0001015.bin feature flash:/feature1-t0001015.bin
Verifying the file flash:/boot-t0001015.bin on slot 1.....Done.
Verifying the file flash:/system-t0001015.bin on slot 1.....Done.
```

```
Verifying the file flash:/feature1-t0001015.bin on slot 1.....Done.


  Slot     Upgrade Way
  1        File Upgrade
```

Table 5 Command output

Field	Description
Verifying the file	The system was verifying the validity of the file.
Influenced service according to following table	Services that will be affected by the upgrade. This field is displayed only for compatible versions.
Incompatible upgrade	You are upgrading the software to an incompatible version.
Upgrade Way	ISSU method: • **Service Upgrade**. • **File Upgrade**. • **Reboot**. This field is displayed only for compatible versions. For more information about ISSU methods, see *Fundamentals Configuration Guide*.

Related commands

`issu load`

install abort

Use **`install abort`** to abort an ongoing activate or deactivate operation.

Syntax

`install abort` [*`job-id`*]

Views

User view

Predefined user roles

network-admin

Parameters

`job-id`: Specifies the job ID of an ISSU operation. If you do not specify this argument, the command aborts all ongoing software image activate and deactivate operations.

Usage guidelines

The system creates a software image management job each time you use the **`install activate`**, **`install add`**, **`install commit`**, **`install deactivate`**, **`install remove`**, or **`install rollback to`** command. Each job represents one command and is assigned a unique job ID. To obtain the ID of a job, use the **`display install job`** command.

When you abort an ongoing activate or deactivate operation, the system rolls back to the status it was in before the operation was started.

Examples

Abort all ongoing software image activate and deactivate operations.

```
<Sysname> install abort
```

Related commands

display install job

install activate

Use **install activate** to activate software images, or identify the ISSU method and the possible impact on the device.

Syntax

install activate { **boot** *filename* | **system** *filename* | **feature** *filename*&<1-30> } * **slot** *slot-number* [**test**]

install activate patch *filename* { **all** | **slot** *slot-number* }

Views

User view

Predefined user roles

network-admin

Parameters

boot: Specifies a boot image file.

system: Specifies a system image file.

feature: Specifies a space-separated list of up to 30 feature image files

patch: Specifies a patch image file. You can specify only one patch image file for the command at a time. However, you can execute the command multiple times to activate multiple patch image files. You can specify both incremental and non-incremental patch image files. The device can use a maximum of 30 incremental patch image files. Because the boot, system, and feature images each can have one non-incremental patch image file, the device can use a maximum of 16 non-incremental patch image files. For more information about incremental and non-incremental patch image files, see software upgrade in *Fundamentals Configuration Guide*.

filename: Specifies a .bin file in the *filesystemnameIfilename***.bin** format. The file must be stored in the root directory of a file system on the device. The value string excluding the file system location section (if any) can have a maximum of 63 characters. For more information about specifying a file, see file system management in *Fundamentals Configuration Guide.*

all: Specifies all member devices.

slot *slot-number*: Specifies an IRF member device by its member ID.

test: Only identifies the ISSU method to be used for the upgrade. If you do not specify this keyword, the command activates the specified software images.

Usage guidelines

Before you use this command to activate a software image, read the release notes to identify the licensing requirements for the image. If the image requires a license, make sure the device has a valid license installed for the image.

Images run in memory immediately after they are activated. However, only images activated by using the **install activate patch** *filename* **all** command still run in memory after a reboot. For other images to take effect after a reboot, you must commit the software change by using the **install commit** command.

If the specified files are not stored on the member device to be upgraded, the command copies the images to the member device automatically.

At reboot, a subordinate device automatically synchronizes the master device's configuration and status data. You must wait for the synchronization to complete before using the **install activate** command on the subordinate device. To identify whether the synchronization is complete, use the **display system stable state** command. The synchronization is complete if the **System State** field displays **Stable**.

Examples

Identify the ISSU method for feature upgrade with **feature1.bin** on subordinate member 2 and the upgrade impact.

```
<Sysname> install activate feature flash:/feature1.bin slot 2 test
Copying file flash:/feature1.bin to slot2#flash:/feature1.bin......Done.
Verifying the file flash:/feature1.bin on slot 2.....Done.
Upgrade summary according to following table:

flash:/feature1.bin
  Running Version             New Version
  Test 0001015                Test 0001016

  Slot                        Upgrade Way
  2                           Reboot

Influenced service according to following table:
flash:/feature1.bin
     Feature1
```

The output shows that a reboot upgrade is recommended.

Activate the system image in **system.bin** and the feature images in **feature1.bin** on member device 2.

```
<Sysname> install activate system flash:/system.bin feature flash:/feature1.bin slot 2
Copying file flash:/system.bin to slot2#flash:/system.bin......Done.
Verifying the file flash:/system.bin on slot 2.....Done.
Copying file flash:/feature1.bin to slot2#flash:/feature1.bin......Done.
Verifying the file flash:/feature1.bin on slot 2.....Done.
Upgrade summary according to following table:

flash:/system.bin
  Running Version             New Version
  Test 0001015                Test 0001016

flash:/feature1.bin
  Running Version             New Version
  None                        Test 0001016

  Slot                        Upgrade Way
  2                           Service Upgrade
Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait...Done.
```

Table 6 Command output

Field	Description
Verifying the file	The system was verifying the validity of the file.
Upgrade summary according to following table	Upgrade summary.
Running Version	Version number of the running software.
New Version	Version number of the new software.
Upgrade Way	ISSU methods: • **Service Upgrade**. • **File Upgrade**. • **Reboot**. This field is displayed only for an upgrade to a compatible version. For more information about ISSU methods, see *Fundamentals Configuration Guide*.
Influenced service according to following table	Services influenced by the upgrade.

Related commands

`display install active`

`install commit`

`install deactivate`

install add

Use **`install add`** to decompress an .ipe file.

Syntax

`install add` *`ipe-filename filesystem`*

Views

User view

Predefined user roles

network-admin

Parameters

`ipe-filename`: Specifies an .ipe file in the *filesystemnameIfilename***.ipe** format. The file must be stored in the root directory of a file system on the device. The value string excluding the file system location section (if any) can have a maximum of 63 characters. For more information about specifying a file, see file system management in *Fundamentals Configuration Guide.*

`filesystem`: Specifies the destination file system for the software images, in the *filesystemname* format.

Usage guidelines

To use the **`install activate`** command to activate software images, you must use .bin image files. If the upgrade file is an .ipe file, use this command to decompress the .ipe file before you start the upgrade.

To identify software images that are included in an .ipe file, use the **display install ipe-info** command.

Examples

Decompress **all.ipe** to the flash memory.

```
<Sysname> install add flash:/all.ipe flash:
Verifying the file flash:/all.ipe on slot 1...Done.
Decompressing file boot.bin to flash:/boot.bin.....................Done.
Decompressing file system.bin to
flash:/system.bin.............................Done.
```

install commit

Use **install commit** to commit software changes.

Syntax

install commit

Views

User view

Predefined user roles

network-admin

Usage guidelines

Before you use this command, read the release notes to identify software image licensing requirements. Make sure the device has valid licenses for all license-based images.

This command adds the patch image file to the startup software image list that the device used at startup.

- If the device used the main startup software image list at startup, this command adds the patch image file to the main startup software image list.
- If the device used the backup startup software image list at startup, this command adds the patch image file to the backup startup software image list.

You must execute this command after using the following commands:

- The **install activate** command in an incremental upgrade.
- The **install deactivate** command.
- The **install rollback** command.

In a reboot or ISSU reboot upgrade, the **install activate** command modifies both the current and startup software image lists. You do not need to commit software changes.

Both the **install commit** and **boot-loader file** commands modify the main startup software image list. To modify the backup startup image list or add inactive images as main startup images, however, you must use the **boot-loader file** command.

For more information about main and backup startup software images, see *Fundamentals Configuration Guide*.

Examples

Commit software changes.

```
<Sysname> install commit
This operation will take several minutes, please wait.........................Done.
```

Related commands

install activate

install deactivate

install rollback

install deactivate

Use **install deactivate** to deactivate feature images and patch images.

Syntax

install deactivate feature *filename*&<1-30> **slot** *slot-number*

install deactivate patch *filename* { **all** | **slot** *slot-number* }

Views

User view

Predefined user roles

network-admin

Parameters

feature: Specifies a space-separated list of up to 30 feature image files.

patch: Specifies a patch image file. You can specify only one patch image file for the command at a time. However, you can execute the command multiple times to deactivate multiple patch image files.

filename: Specifies a .bin file in the *filesystemname*/*filename*.**bin** format. The value string can have a maximum of 63 characters. The file system name cannot contain file system location information. For more information about specifying a file, see file system management in *Fundamentals Configuration Guide.*

all: Specifies all member devices on which the specified patch image file has been activated.

slot *slot-number*: Specifies an IRF member device by its member ID.

Usage guidelines

At reboot, a subordinate device automatically synchronizes the master device's configuration and status data. You must wait for the synchronization to complete before using the **install deactivate** command on the subordinate device. To identify whether the synchronization is complete, use the **display system stable state** command. The synchronization is complete if the **System State** field displays **Stable**.

You can deactivate only active feature and patch images.

Images deactivated by using the **install deactivate patch** *filename* **all** command do not run after a reboot. To prevent other deactivated images from running after a reboot, you must commit the software change by using the **install commit** command.

Examples

Deactivate the patch images in the **route-patch.bin** file for a slot.

```
<Sysname> install deactivate patch flash:/route-patch.bin slot 1
This operation might take several minutes, please wait...Done.
```

Related commands

display install active

display install inactive

install remove

Use **install remove** to delete an inactive software image file.

Syntax

install remove [**slot** *slot-number*] { *filename* | **inactive** }

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command deletes inactive software images from all IRF members.

filename: Specifies a .bin file in the *filesystemnameIfilename***.bin** format. The value string can have a maximum of 63 characters. The file must be stored in the root directory of a file system on the device. The file system name cannot contain file system location information. For more information about specifying a file, see file system management in *Fundamentals Configuration Guide.*

inactive: Deletes all inactive software image files in the root directories of the specified file systems.

Usage guidelines

This command permanently deletes the image files from the device. You cannot use the **install rollback to** command to revert the operation, or use the **install abort** command to abort the operation.

Examples

Delete inactive software image file **flash:/feature1.bin**.

```
<Sysname> install remove flash:/feature1.bin
```

install rollback to

Use **install rollback to** to roll back the software to an earlier rollback point.

Syntax

install rollback to { *point-id* | **original** }

Views

User view

Predefined user roles

network-admin

Parameters

point-id: Specifies a rollback point ID. This option is supported only when there are two or more rollback points. To identify available rollback points, use the **display install rollback** command.

original: Rolls back to the status before any activate or deactivate operations were performed.

Usage guidelines

During an incremental upgrade, the system creates a rollback point for each activate or deactivate operation of a boot, system, or feature image. The device supports a maximum of 50 rollback points. The earliest rollback point is deleted if this limit has been reached when a rollback point is created.

During a reboot or ISSU reboot upgrade, the system does not create rollback points. After the upgrade, you can roll back the software only to the status before any activate or deactivate operations were performed.

For a rollback to take effect after a reboot, you must perform a commit operation to update the main startup software image list.

After a commit operation is performed, you cannot perform a rollback.

Patch images do not support rollback.

Examples

Roll back the software to rollback point 1.

```
<Sysname>install rollback to 1
This operation might take several minutes, please wait...Done.
```

Roll back the software to the original software versions and observe the change made by the rollback.

```
<Sysname> display install active
Active packages on slot 1:
  flash:/boot-t0001015.bin
  flash:/system-t0001015.bin
  flash:/feature1-t0001015.bin
<Sysname> display install rollback
Install rollback information 1 on slot 1:
  Updating from no package
         to flash:/feature1-t0001015.bin.
```

The output shows that currently three image files are active but only two of them are confirmed. Image file flash:/feature1-t0001015.bin is not confirmed yet.

```
<Sysname> install rollback to original
This operation might take several minutes, please wait...Done.
<Sysname> display install active
Active packages on slot 1:
  flash:/boot-t0001015.bin
  flash:/system-t0001015.bin
<Sysname> display install committed
Committed packages on slot 1:
  flash:/boot-t0001015.bin
  flash:/system-t0001015.bin
```

The output shows the software has been rolled back to the original version. Image file flash:/feature1-t0001015.bin has been removed.

Related commands

`display install rollback`

install verify

Use **`install verify`** to verify the software change commit status, image integrity, and image consistency.

Syntax

`install verify`

Views

User view

Predefined user roles

network-admin

Usage guidelines

To ensure a successful ISSU and make sure that the system can start up and operate correctly after an ISSU, execute this command to verify the following items:

- **Integrity**—Verify that the boot, system, and feature images are integral.
- **Consistency**—Verify that the same active images are running across the entire system.
- **Software commit status**—Verify that the active images are committed as needed.

If a software image fails the verification, perform the following tasks to resolve the problem:

- To ensure software integrity, download and install the software images again.
- To guarantee software image consistency or change software commit status, use the **`install activate`**, **`install deactivate`**, and **`install commit`** commands as appropriate.

Examples

Verify the software change confirmation status and software image integrity and consistency.

```
<Sysname> install verify
Active packages on slot 1 are the reference packages.
Packages will be compared with the reference packages.
This operation will take several minutes, please wait...
  Verifying packages on slot 1:
  Start to check active package completeness.
Verifying the file flash:/boot-t0001015.bin on slot 1.....................Done.
    flash:/boot-t0001015.bin verification successful.
Verifying the file flash:/system-t0001015.bin on slot 1.....................Done.
    flash:/system-t0001015.bin verification successful.
  Start to check active package consistency.
    Active packages are consistent with committed packages on their own board.
    Active packages are consistent with the reference packages.
  Verifying packages on slot 2:
  Start to check active package completeness.
Verifying the file flash:/boot-t0001015.bin on slot 2.....................Done.
    flash:/boot-t0001015.bin verification successful.
Verifying the file flash:/system-t0001015.bin on slot 2.....................Done.
    flash:/system-t0001015.bin verification successful.
  Start to check active package consistency.
    Active packages are consistent with committed packages on their own board.
    Active packages are consistent with the reference packages.
Verification is done.
```

issu accept

Use **issu accept** to accept the upgrade to a compatible version and delete the automatic rollback timer.

Syntax

issu accept

Views

User view

Predefined user roles

network-admin

Usage guidelines

The system cannot perform automatic rollback for the ISSU process after you execute this command. However, you can use the **issu rollback** command to perform a manual rollback.

The **issu accept** command does not apply to an ISSU to an incompatible version.

Examples

Accept the upgrade to a compatible version.

```
<Sysname> issu accept
```

Related commands

issu load

issu run switchover

issu commit

Use **issu commit** to upgrade the original master and the subordinate members that have not been upgraded and complete the ISSU upgrade.

Syntax

issu commit slot *slot-number*

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies the member ID of the original master or a subordinate member that has not been upgraded.

Usage guidelines

CAUTION:

Use this command to upgrade the original master and the subordinate members that have not been upgraded, one by one. You must wait for one upgraded member to start up again and join the IRF fabric before upgrading another member. The ISSU process cannot be rolled back automatically or manually after you execute this command. After all members are upgraded, the ISSU status changes to Init.

At reboot, a subordinate device automatically synchronizes the master device's configuration and status data. You must wait for the synchronization to complete before using the **issu commit** command on the subordinate device. To identify whether the synchronization is complete, use the **display system stable state** command. The synchronization is complete if the **System State** field displays **Stable**.

Examples

After member 2 is upgraded and becomes the new master, upgrade the original master (member 3) and the other subordinate members that have not been upgraded (member 4 and member 1).

```
<Sysname> issu commit slot 3
Upgrade summary according to following table:

flash:/feature1.bin
  Running Version             New Version
  Test 0001015                Test 0001016

  Slot                        Upgrade Way
  3                           Service Upgrade
Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait...Done.
<Sysname> issu commit slot 4
Verifying the file flash:/feature1.bin on slot 4.............Done.
Copying file flash:/feature1.bin to slot4#flash:/feature1.bin...Done.
Upgrade summary according to following table:

flash:/feature1.bin
  Running Version             New Version
  Test 0001015                Test 0001016

  Slot                        Upgrade Way
  4                           Service Upgrade
Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait...Done.
<Sysname> issu commit slot 1
Verifying the file flash:/feature1.bin on slot 1.............Done.
Copying file flash:/feature1.bin to slot1#flash:/feature1.bin...Done.
Upgrade summary according to following table:

flash:/feature1.bin
  Running Version             New Version
  Test 0001015                Test 0001016

  Slot                        Upgrade Way
  1                           Service Upgrade
Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait...Done.
```

For information about the command output, see Table 5.

Related commands

issu accept

issu load

issu run switchover

issu load

Use **issu load** to upgrade the software images of subordinate members and configure the new images as main startup software images for those members.

Syntax

issu load file { **boot** *filename* | **system** *filename* | **feature** *filename*&<1-30> | **patch** *filename*&<1-30> } * **slot** *slot-number*&<1-9> [**reboot**]

issu load file ipe *ipe-filename* **slot** *slot-number*&<1-9> [**patch** *filename*&<1-30>] [**reboot**]

Views

User view

Predefined user roles

network-admin

Parameters

boot: Specifies a boot image file.

system: Specifies a system image file.

feature: Specifies a space-separated list of up to 30 feature image files.

patch: Specifies a space-separated list of up to 30 patch image files. You can specify both incremental and non-incremental patch image files. The device can use a maximum of 30 incremental patch image files. Because the boot, system, and feature images each can have one non-incremental patch image file, the device can use a maximum of 16 non-incremental patch image files. For more information about incremental and non-incremental patch image files, see software upgrade in *Fundamentals Configuration Guide*.

filename: Specifies a .bin file in the *filesystemnameIfilename***.bin** format. The file must be stored in the root directory of a file system on the master device. The value string excluding the file system location section (if any) can have a maximum of 63 characters. For more information about specifying a file, see file system management in *Fundamentals Configuration Guide.*

ipe-filename: Specifies an .ipe file in the *filesystemnameIfilename***.ipe** format. The file must be stored in the root directory of a file system on the master device. The value string excluding the file system location section (if any) can have a maximum of 63 characters. For more information about specifying a file, see file system management in *Fundamentals Configuration Guide.*

slot *slot-number*: Specifies the member ID of a subordinate member. You can specify a space-separated list of up to nine member IDs. On a single-chassis IRF fabric, enter the member ID of the member device to upgrade the entire fabric. On a multichassis IRF fabric, you can specify only one member ID for a compatible upgrade and can specify multiple member IDs for an incompatible upgrade. As a best practice, specify half of the subordinate members if the member devices form a ring. Make sure the specified subordinate members are directly connected by physical links.

reboot: Uses the reboot method for the upgrade. For an incremental upgrade or ISSU reboot upgrade, specify this keyword if you want to use the reboot upgrade method. If you do not specify this keyword, the recommended upgrade method is used.

Usage guidelines

NOTE:

The software images for the device are digitally signed. The system verifies the digital signatures of

the specified software images for authenticity and integrity before it sets or loads them as main startup images. If the digital signature verification fails, the system will not set or load the specified images as main startup images and you will receive a digital signature verification failure message.

You may upgrade all or some of the software images. If you are upgrading only some of the images, make sure the new images are compatible with the images that are not to be upgraded. The upgrade will fail if a conflict exists.

This command performs the following operations:

- Checks the version compatibility.
- Identifies the upgrade method.
- Loads the new images to upgrade the member devices.
- Sets the new images as the main startup software images so the upgrade can survive a reboot.

At reboot, a subordinate device automatically synchronizes the master device's configuration and status data. You must wait for the synchronization to complete before using the **issu load** command on the subordinate device. To identify whether the synchronization is complete, use the **display system stable state** command. The synchronization is complete if the **System State** field displays **Stable**.

Examples

Upgrade member device 2 (a subordinate member) with feature image file **flash:/feature1.bin**. (In this example, the image is compatible with the running images.)

```
<Sysname> issu load file feature flash:/feature1.bin slot 2
This operation will delete the rollback point information for the previous upgrade and maybe get unsaved configuration lost. Continue? [Y/N]:Y
Verifying the file flash:/feature1.bin on slot 1...Done.
Copying file flash:/feature1.bin to slot2#flash:/feature1.bin......Done.
Verifying the file flash:/feature1.bin on slot 2...Done.
Identifying the upgrade methods….Done.
Upgrade summary according to following table:

flash:/feature1.bin
  Running Version             New Version
  Test 0001015                Test 0001016

  Slot                        Upgrade Way
  2                           Service Upgrade
Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait...Done.
```

Use the reboot method to upgrade member device 2 (a subordinate member) when the incremental upgrade method is recommended.

```
<Sysname> issu load file feature flash:/feature1.bin slot 2 reboot
This operation will delete the rollback point information for the previous upgrade and maybe get unsaved configuration lost. Continue? [Y/N]:Y
Verifying the file flash:/feature1.bin on slot 1...Done.
Copying file flash:/feature1.bin to slot2#flash:/feature1.bin......Done.
Verifying the file flash:/feature1.bin on slot 2...Done.
Identifying the upgrade methods….Done.
Upgrade summary according to following table:

flash:/feature1.bin
```

```
  Running Version             New Version
  Test 0001015                Test 0001016

  Slot                        Upgrade Way
  2                           Reboot
Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait...Done.
```

Upgrade member devices 3 and 4 (subordinate members) with feature image file **flash:/feature1.bin**. (In this example, the image is incompatible with the running images.)

```
<Sysname> issu load file feature flash:/feature1.bin slot 3 4
This operation will delete the rollback point information for the previous upgrade and
maybe get unsaved configuration lost. Continue? [Y/N]:Y
Verifying the file flash:/feature1.bin on slot 1...Done.
Copying file flash:/feature1.bin to slot3#flash:/feature1.bin......Done.
Verifying the file flash:/feature1.bin on slot 3...Done.
Copying file flash:/feature1.bin to slot4#flash:/feature1.bin......Done.
Verifying the file flash:/feature1.bin on slot 4...Done.
Identifying the upgrade methods….Done.
Upgrade summary according to following table:

flash:/feature1.bin
  Running Version             New Version
  Test 0001015                Test 0001016

  Slot                        Upgrade Way
  3                           Reboot
  4                           Reboot
Upgrading software images to incompatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait...Done.
```

Table 7 Command output

Field	Description
Verifying the file	The system was verifying the validity of the file.
Copying file	The system was copying the upgrade file to a subordinate member. This field is displayed if you specified a subordinate member for the command.
Upgrade Way	ISSU method: • **Service Upgrade**. • **File Upgrade**. • **Reboot**. This field is displayed only for an upgrade to a compatible version. For more information about ISSU methods, see *Fundamentals Configuration Guide*.

issu quit

Use **issu quit** to terminate the ongoing ISSU process forcibly.

Syntax

issu quit

Views

System view

Predefined user roles

network-admin

Usage guidelines

Use this command to terminate the ISSU process if one of the following exceptions occurs and you cannot perform an upgrade or rollback:

- The ISSU status is not **Init** but the upgrade has stopped.
- The ISSU status is **Init** but the upgrade has not completed.

After using this command to terminate the ISSU process, identify whether the requirements for an ISSU are met. If yes, use **boot-loader** or **install** commands as needed to restore the device to the state prior to the terminated ISSU and then try an ISSU again. If the ISSU fails again, contact the technical support.

Examples

Terminate the ongoing ISSU process forcibly.

```
<Sysname> system-view
[Sysname] issu quit
This command stops the ongoing ISSU process. Execute this command only under the guidance
of the technical support. Continue? [Y/N]:y

Succeeded.
```

Related commands

install activate

issu load

issu rollback

Use **issu rollback** to cancel the ISSU and roll back to the original software versions.

Syntax

issu rollback

Views

User view

Predefined user roles

network-admin

Usage guidelines

The device supports automatic rollback and manual rollback. This command performs a manual rollback.

You can perform a manual rollback while an ISSU is in one of the following states:

- Loaded.
- Switching (during an upgrade to a compatible version).
- Switchover (during an upgrade to a compatible version).

- Accepted.

As a best practice, do not perform a manual rollback while an ISSU is in Switching state and specify a value that is great enough for the automatic rollback timer. If a rollback occurs for a reboot ISSU in Switching state or an automatic rollback occurs for an incompatible ISSU in Switching state, you might have the following issues:

- The upgraded subordinate members reboot. If a master/subordinate switchover is in progress, a service outage occurs.
- The rollback cannot ensure that the member devices have the same master/subordinate roles as they have before the ISSU.

Examples

Roll back to the original software versions.

```
<Sysname> issu rollback
This command will quit the ISSU process and roll back to the previous version. Continue? [Y/N]:y
```

Related commands

issu accept

issu commit

issu load

issu run switchover

issu rollback-timer

Use **issu rollback-timer** to set the automatic rollback timer.

Use **undo issu rollback-timer** to restore the default.

Syntax

issu rollback-timer *minutes*

undo issu rollback-timer

Default

The automatic rollback timer is set to 45 minutes.

Views

System view

Predefined user roles

network-admin

Parameters

minutes: Specifies the automatic rollback interval, in the range of 0 to 120 minutes. Setting it to 0 disables automatic rollback.

Usage guidelines

The automatic software version rollback feature is available only during an ISSU to a compatible version when the IRF fabric has multiple members.

The system starts the automatic rollback timer when you execute the **issu run switchover** command in a scenario where automatic rollback is supported. If you do not execute the **issu accept** or **issu commit** command before the timer expires, the system automatically rolls back to the software version used before the ISSU.

Change to the automatic rollback interval does not take effect on the ongoing ISSU process.

Examples

Set the automatic rollback timer to 50 minutes.

```
<Sysname> system-view
[Sysname] issu rollback-timer 50
```

Related commands

issu rollback

issu run switchover

Use **issu run switchover** to perform an ISSU switchover.

Syntax

issu run switchover

Views

User view

Predefined user roles

network-admin

Usage guidelines

Use this command on a multichassis IRF fabric.

- For a compatible upgrade, this command performs operations depending on the ISSU method.
  - **Incremental upgrade**—Performs a process-level master/subordinate switchover for the processes to be upgraded.
  - **Reboot upgrade** or **ISSU upgrade**—Reboots the current master with the old software version, causing the upgraded subordinate member to be elected as the new master.
- For an incompatible upgrade, the **issu load** command splits the IRF fabric into two fabrics, with the upgraded members forming a new fabric. The **issu run switchover** command reboots the members in the old IRF fabric with the upgrade images to upgrade the members. After startup, the members join the new IRF fabric as subordinate members.

At reboot, a subordinate device automatically synchronizes the master device's configuration and status data. You must wait for the synchronization to complete before using the **issu run switchover** command on the subordinate device. To identify whether the synchronization is complete, use the **display system stable state** command. The synchronization is complete if the **System State** field displays **Stable**.

When you execute the **issu run switchover** command during an ISSU to a compatible version, the system starts the automatic rollback timer. If you do not execute the **issu accept** or **issu commit** command before the timer expires, the system automatically rolls back to the original software versions.

Examples

On a multichassis IRF fabric, perform a master/subordinate switchover during an ISSU to a compatible version.

```
<Sysname> issu run switchover
Upgrade summary according to following table:

flash:/feature1.bin
  Running Version             New Version
```

```
  Test 0001015                Test 0001016

  Slot                        Switchover Way
  1                           Active standby process switchover
Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait...Done.
```

On a multichassis IRF fabric, perform a master/subordinate switchover, and upgrade members that have not been upgraded (member 1 and member 2) during an ISSU to an incompatible version.

```
<Sysname> issu run switchover
Upgrade summary according to following table:

flash:/feature1.bin
  Running Version             New Version
  Test 0001015                Test 0001016

  Slot                        Upgrade Way
  1                           Reboot
  2                           Reboot
Upgrading software images to incompatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait...Done.
```

Table 8 Command output

Field	Description
Switchover Way	Switchover method: • **Active standby process switchover**—Switch from the active process to the standby process. • **Master subordinate switchover**—Switch from the master to a subordinate member.

For more information about the command output, see Table 5.

Related commands

`issu load`

reset install log-history oldest

Use **`reset install log-history oldest`** to clear ISSU log entries.

Syntax

`reset install log-history oldest` *`log-number`*

Views

User view

Predefined user roles

network-admin

Parameters

`log-number`: Specifies the number of ISSU log entries to be deleted.

Usage guidelines

This command clears the specified number of log entries, beginning with the oldest log entry.

Examples

Clear the two oldest ISSU log entries.

```
<Sysname> reset install log-history oldest 2
```

Related commands

`display install log`

reset install rollback oldest

Use **`reset install rollback oldest`** to clear ISSU rollback points.

Syntax

`reset install rollback oldest` *`point-id`*

Views

User view

Predefined user roles

network-admin

Parameters

`point-id`: Specifies a rollback point by its ID.

Usage guidelines

CAUTION:

This command clears the specified rollback point and all rollback points earlier than the specified rollback point.

Examples

Clear rollback point 2 and all rollback points older than rollback point 2.

```
<Sysname> reset install rollback oldest 2
```

Related commands

`display install rollback`

Contents

Automatic configuration commands

autodeploy udisk enable

Use **autodeploy udisk enable** to enable USB-based automatic configuration.

Use **undo autodeploy udisk enable** to disable USB-based automatic configuration.

Syntax

autodeploy udisk enable

undo autodeploy udisk enable

Default

USB-based automatic configuration is enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Examples

Disable USB-based automatic configuration.

```
<Sysname> system-view
[Sysname] undo autodeploy udisk enable
```

Contents

Tcl commands

cli

Use **cli** to enable a NF command to be executed in Tcl configuration view when it conflicts with a Tcl command.

Syntax

cli *command*

Views

Tcl configuration view

Predefined user roles

network-admin

context-admin

Parameters

command: Specifies the commands to be executed. They must be complete command lines.

Usage guidelines

In Tcl configuration view, if a NF command conflicts with a Tcl command, the Tcl command will be executed. To execute the NF command when a conflict occurs, execute the **cli** command.

Examples

Perform the following steps to execute a NF command that conflicts with a Tcl command in Tcl configuration view.

1. Execute a NF command in Tcl configuration view. The output shows that the NF command cannot be executed because it conflicts with a Tcl command.

```
<Sysname> tclsh
<Sysname-tcl> system-view
[Sysname-tcl] route-policy 1 permit node 10
[Sysname-tcl-route-policy-1-10] apply cost 10
can't interpret "cost" as a lambda expression
```

2. Configure the **cli** command to execute the NF command again.

```
[Sysname-tcl-route-policy-1-10] cli apply cost 10
```

Execute multiple NF commands in one operation to enter OSPF area view.

Method 1:

```
[Sysname-tcl] cli "ospf 100 ; area 0"
[Sysname-tcl-ospf-100-area-0.0.0.0]
```

Method 2:

```
[Sysname-tcl] cli ospf 100 ; cli area 0
[Sysname-tcl-ospf-100-area-0.0.0.0]
```

tclquit

Use **tclquit** to return from Tcl configuration view to user view.

Syntax

tclquit

Views

Tcl configuration view

Predefined user roles

network-admin

context-admin

Usage guidelines

To return from Tcl configuration view to user view, you can also use the **quit** command.

To return to the upper-level view after you execute NF commands to enter system view or a NF feature view, use the **quit** command.

Examples

Return from Tcl configuration view to user view.

```
<Sysname-tcl> tclquit
<Sysname>
```

Related commands

tclsh

tclsh

Use **tclsh** to enter Tcl configuration view from user view.

Syntax

tclsh

Views

User view

Predefined user roles

network-admin

context-admin

Usage guidelines

In Tcl configuration view, you can execute the following commands:

- All Tcl 8.5 commands.
- NF commands. The Tcl configuration view is equivalent to the user view. You can use NF commands in Tcl configuration view in the same way they are used in user view.

Examples

Enter Tcl configuration view from user view.

```
<Sysname> tclsh
<Sysname-tcl>
```

Related commands

tclquit

Contents

Python commands

exit()

Use **exit()** to exit the Python shell.

Syntax

exit()

Views

Python shell

Predefined user roles

network-admin

context-admin

Usage guidelines

To return to user view from the Python shell, you cannot use the **quit** command. You must use the **exit()** command.

Examples

Exit the Python shell.

```
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>>
>>> exit()
<Sysname>
```

python

Use **python** to enter the Python shell.

Syntax

python

Views

User view

Predefined user roles

network-admin

context-admin

Usage guidelines

In the Python shell, you can use the following items:

- Python 2.7 commands.
- Python 2.7 standard API.
- NF extended API.

Examples

Enter the Python shell.

```
<Sysname> python
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

python *filename*

Use **python** *filename* to execute a Python script.

Syntax

python *filename* [*param*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

filename: Specifies the name of a Python script on a storage medium of the device. The script name is case sensitive and must use the extension .py. The extension .py is case insensitive.

param: Specifies the parameters to be passed to the script. To enter multiple parameters, use spaces as the delimiter.

Usage guidelines

You cannot perform any operations while you are executing a Python script.

Make sure the statements in the script meet the syntax requirements. The system stops executing a Python script if it finds a statement with syntax errors.

When executing a script, the system uses the defaults for interactive statements. The system does not stop for human input.

Examples

Execute Python script **test.py**.

```
<Sysname> python test.py 1 2
['/flash:/test.py', '1', '2']
```

NSFOCUS Firewall Series

NF Virtual Technologies

Command Reference

NSFOCUS Technologies, Inc.

Document version: 6W600-20230221

Preface

This command reference describes the commands for configuring virtual technologies features, including IRF, context and Reth interface and redundancy group.

This preface includes the following topics about the documentation:

- Audience.
- Conventions.

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators.

Conventions

The following information describes the conventions used in the documentation.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select a minimum of one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
CAUTION:	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Contents

IRF commands

The following compatibility matrixes show the support of hardware platforms for IRF:

Models	IRF compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	Yes
NFNX3-HDB680, NFNX3-HDB1080	No

All IRF commands are available only on the default context, except for the commands in Table 1.

Table 1 IRF commands available on both default and non-default contexts

Command category	Commands
Display commands	**display irf link** **display mad**
MAD commands	**mad arp enable** **mad enable** **mad nd enable** **mad exclude interface**

For more information about contexts, see *Virtual Technologies Configuration Guide*.

display irf

Use **display irf** to display IRF fabric information.

Syntax

display irf

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display IRF fabric information.

```
<Sysname> display irf
MemberID   Role     Priority    CPU-Mac           Description
   1       Loading  1           00e0-fcbe-3102    F1Num001
 *+2       Master   1           00e0-fcb1-ade2    F1Num002
-------------------------------------------------------

 * indicates the device is the master.
 + indicates the device through which the user logs in.
```

```
The Bridge MAC of the IRF is: 00e0-fc00-1000
Auto upgrade                  : yes
Mac persistent                : always
Domain ID                     : 30
```

Table 2 Command output

Field	Description
MemberID	IRF member ID: • ID of the master is prefixed with an asterisk (*) sign. • ID of the device where you are logged in is prefixed with a plus (+) sign.
Role	Role of the member device in the IRF fabric: • **Standby**—Subordinate device. • **Master**—Master device. • **Loading**—The device is loading software images.
Priority	IRF member priority.
CPU-MAC	MAC address of the CPU in the device.
Description	Description you have configured for the member device. • If no description is configured, this field displays a dashed line (-----). • If the description exceeds the maximum number of characters that can be displayed, an ellipsis (…) is displayed in place of the exceeding text. To display the complete description, use the **`display current-configuration`** command.
Auto upgrade	Status of the software auto-update feature: • **yes**—Enabled. • **no**—Disabled.
MAC persistent	IRF bridge MAC persistence setting: • ***n*** **min**—Bridge MAC address of the IRF fabric remains unchanged for *n* minutes after the address owner leaves. • **always**—Bridge MAC address of the IRF fabric does not change after the address owner leaves. • **no**—Bridge MAC address of the current master replaces the original bridge MAC address as soon as the owner of the original address leaves.
Domain ID	Domain ID of the IRF fabric. The domain ID you assign to an IRF fabric must uniquely identify the fabric in a multi-IRF fabric network.

Related commands

`display irf configuration`

`display irf topology`

display irf configuration

Use **`display irf configuration`** to display basic IRF settings for each member device.

Syntax

`display irf configuration`

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display basic IRF settings for all members.

```
<Sysname> display irf configuration
 MemberID  NewID    IRF-Port1                  IRF-Port2
 1         1        Ten-GigabitEthernet1/0/1   Ten-GigabitEthernet1/0/2
 2         2        Ten-GigabitEthernet2/0/1   Ten-GigabitEthernet2/0/2
```

Table 3 Command output

Field	Description
MemberID	Current member ID of the device.
NewID	Member ID assigned to the device. This member ID takes effect at reboot.
IRF-Port1	Physical interfaces bound to IRF-port 1. This field displays **disable** if no physical interfaces are bound to the IRF port.
IRF-Port2	Physical interfaces bound to IRF-port 2. This field displays **disable** if no physical interfaces are bound to the IRF port.

Related commands

display irf

display irf topology

display irf link

Use **display irf link** to display IRF link information.

Syntax

display irf link

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display IRF link information.

```
<Sysname> display irf link
Member 1
 IRF Port    Interface                     Status
 1           disable                       --
 2           Ten-GigabitEthernet1/0/1      UP
             Ten-GigabitEthernet1/0/2      ADM
```

```
             Ten-GigabitEthernet1/0/3           DOWN
Member 2
 IRF Port    Interface                          Status
 1           Ten-GigabitEthernet2/0/1           UP
             Ten-GigabitEthernet2/0/2           DOWN
             Ten-GigabitEthernet2/0/3           ADM
 2           disable                            --
```

Table 4 Command output

Field	Description
Member *ID*	IRF member ID.
IRF Port	IRF port number: • **1**—IRF-port 1. • **2**—IRF-port 2.
Interface	Physical interfaces bound to the IRF port. This field displays **disable** if no physical interfaces have been bound to the IRF port.
Status	Link state of the IRF physical interface: • **UP**—The link is up. • **DOWN**—The link is down. • **ADM**—The interface has been manually shut down by using the **shutdown** command. • **ABSENT**—Interface module or expansion interface card that hosts the interface is not present.

display irf topology

Use **display irf topology** to display IRF fabric topology information.

Syntax

display irf topology

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the IRF fabric topology.

```
<Sysname> display irf topology
                          Topology Info
 -------------------------------------------------------------------------
              IRF-Port1                 IRF-Port2
 MemberID   Link        neighbor      Link        neighbor     Belong To
 1          DOWN        ---           UP          2            000f-cbb8-1a82
 2          UP          1             DIS         ---          000f-cbb8-1a82
```

Table 5 Command output

Field	Description
IRF-Port1	Information about IRF-port 1, including its link state and neighbor.
IRF-Port2	Information about IRF-port 2, including its link state and neighbor.
MemberID	IRF member ID.

Link	Link state of the IRF port:
	• **UP**—The IRF link is up.
	• **DOWN**—The IRF link is down because the port has no physical link or has not been activated by the **irf-port-configuration active** command.
	• **DIS**—No physical interfaces have been bound to the IRF port.
	• **TIMEOUT**—IRF hello interval has timed out.
	• **ISOLATE**—The device is isolated from the IRF fabric. This issue might be caused by the following reasons:
	  ○ The IRF fabric does not support the device model.
	  ○ The maximum number of member devices has exceeded the upper limit.

neighbor	IRF member ID of the device connected to the IRF port. This field displays three hyphens (---) if no device is connected to the port.
Belong To	IRF fabric that has the device, represented by the CPU MAC address of the master in the IRF fabric.

Related commands

display irf

display irf configuration

display irf-port load-sharing mode

Use **display irf-port load-sharing mode** to display IRF link load sharing mode.

Syntax

display irf-port load-sharing mode [**irf-port** [*member-id/irf-port-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

irf-port: Displays IRF port-specific load sharing modes. If you do not specify this keyword, the command displays the global load sharing mode for IRF links.

member-id/irf-port-number: Specifies an IRF port number. The *member-id* argument represents an IRF member ID. The *irf-port-number* argument represents the index number (1 or 2) of the IRF port on the member device. If you do not specify the *member-id* and *irf-port-number* arguments, this command displays the load sharing mode used on each IRF port in the IRF fabric. If no IRF ports are in up state, this command displays **No IRF link exists**.

Usage guidelines

To display the global load sharing mode for IRF links, execute this command without any keywords or arguments.

To display the load sharing mode used on each IRF port in the IRF fabric, specify the **irf-port** keyword without specifying an IRF port.

To display the load sharing mode used on a specific IRF port, specify both the **irf-port** keyword and the port number of that IRF port.

Examples

Display the global load sharing mode for IRF links. In this example, because no user-defined global load sharing mode has been configured, the default global load sharing mode applies.

```
<Sysname> display irf-port load-sharing mode
irf-port Load-Sharing Mode:
Layer 2 traffic: packet type-based sharing
Layer 3 traffic: packet type-based sharing
```

Display the global load sharing mode for IRF links. In this example, because a global load sharing mode has been configured, the configured mode applies.

```
<Sysname> display irf-port load-sharing mode
irf-port Load-Sharing Mode:
destination-mac address, source-mac address
```

Display the load sharing mode of IRF-port 1/1. In this example, because neither port-specific load sharing mode nor user-defined global load sharing mode has been configured, the default global load sharing mode applies.

```
<Sysname> display irf-port load-sharing mode irf-port 1/1
irf-port1/1 Load-Sharing Mode:
Layer 2 traffic: packet type-based sharing
Layer 3 traffic: packet type-based sharing
```

Display the load sharing mode of IRF-port 1/1 after a load sharing mode is configured on the port.

```
<Sysname> display irf-port load-sharing mode irf-port 1/1
irf-port 1/1 Load-Sharing Mode:
destination-mac address, source-mac address
```

Display the load sharing mode used on each IRF port.

```
<Sysname> display irf-port load-sharing mode irf-port
irf-port 1/2 Load-Sharing Mode:
  destination-ip address,  source-ip address

irf-port 2/1 Load-Sharing Mode:
Layer 2 traffic: destination-mac address, source-mac address
Layer 3 traffic: destination-ip address,  source-ip address
```

Table 6 Command output

Field	Description
irf-port Load-Sharing Mode	Global load sharing mode for IRF links: • If no global IRF link load sharing mode has been configured, the default global load sharing mode applies. • If a user-defined global load sharing mode has been configured, the configured mode applies.

Field	Description
irf-port1/1 Load-Sharing Mode	Link load sharing mode of IRF-port 1/1: • If you have not configured a port-specific load sharing mode, the global IRF link load sharing mode applies. • If you have configured a port-specific load sharing mode, the configured mode applies.
Layer 2 traffic: packet type-based sharing	Default load sharing mode for traffic that has no IP header. By default, packets are distributed based on the load sharing mode automatically selected depending on the packet type.
Layer 3 traffic: packet type-based sharing	Default load sharing mode for non-TCP/-UDP IP packets. By default, packets are distributed based on the load sharing mode automatically selected depending on the packet type.

display mad

Use **display mad** to display MAD status and settings.

Syntax

display mad [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

verbose: Displays detailed MAD information. If you do not specify this keyword, the command only displays whether a MAD mechanism is enabled or disabled.

Examples

Display brief MAD information.

```
<Sysname> display mad
MAD ARP disabled.
MAD ND disabled.
MAD LACP enabled.
MAD BFD enabled.
```

Display detailed MAD information.

```
<Sysname> display mad verbose
Multi-active recovery state: No
Excluded ports (user-configured):
  GigabitEthernet1/0/1
  GigabitEthernet2/0/1
Excluded ports (system-configured):
  GigabitEthernet1/0/2
  GigabitEthernet2/0/2
MAD ARP disabled.
```

```
MAD ND disabled.
MAD LACP enabled interface: Route-Aggregation2
  MAD status                 : Normal
  Member ID       Port                              MAD status
  1               GigabitEthernet1/0/3              Normal
  2               GigabitEthernet2/0/3              Normal
MAD BFD enabled interface: Route-Aggregation2
  MAD status                 : Normal
  Member ID   MAD IP address       Neighbor    MAD status
  1           192.168.1.1/24       2           Normal
  2           192.168.1.2/24       1           Normal
```

Table 7 Command output

Field	Description
MAD ARP disabled.	Status of ARP MAD. This field displays **MAD ARP enabled** if ARP MAD is enabled.
MAD ND disabled.	Status of ND MAD. This field displays **MAD ND enabled** if ND MAD is enabled.
MAD LACP enabled.	Status of LACP MAD. This field displays **MAD LACP disabled** if LACP MAD is disabled.
MAD BFD enabled.	Status of BFD MAD. This field displays **MAD BFD disabled** if BFD MAD is disabled.
Multi-active recovery state	Whether the IRF fabric is in Recovery state: • **Yes**—The IRF fabric is in Recovery state. When MAD detects that an IRF fabric has split into multiple IRF fabrics, it allows one fabric to forward traffic. All the other IRF fabrics are set to the Recovery state. In Recovery state, MAD shuts down all network interfaces in the fabric except for the system- and user-excluded network interfaces. • **No**—The IRF fabric is not in Recovery state. It is active and can forward traffic.
Excluded ports (user-configured)	Network interfaces manually configured to not shut down when the IRF fabric transits to the Recovery state.
Excluded ports (system-configured)	Network interfaces set to not shut down by the system when the IRF fabric transits to the Recovery state. These network interfaces are not manually configured. • IRF physical interfaces. • Member interfaces of a Layer 2 aggregate interface if the aggregate interface is excluded from the MAD shutdown action. • Member interfaces of a Layer 3 aggregate interface if the aggregate interface is excluded from the MAD shutdown action.
MAD ARP enabled interface:	Interfaces on which ARP MAD is enabled. This field displays **MAD ARP disabled** if ARP MAD is disabled.
MAD ND enabled interface:	Interfaces on which ND MAD is enabled. This field displays **MAD ND disabled** if ND MAD is disabled.
MAD LACP enabled interface	Interface on which LACP MAD is enabled. This field is displayed for each interface enabled with LACP MAD. This field displays **MAD LACP disabled** if LACP MAD is disabled.

Field	Description

MAD status	LACP MAD operating status:
	• **Normal**—LACP MAD is operating correctly.
	• **Faulty**—LACP MAD is not operating correctly. Verify the following items:
	  ◦ Verify that the ports on LACP MAD links are up.
	  ◦ Verify that the intermediate device supports extended LACPDUs.
	  ◦ Verify that all member devices have member ports used for LACP MAD.

Member ID Port MAD status	LACP MAD details: • **Member ID**—IRF member ID of a device. • **Port**—Member ports of the aggregate interface used for LACP MAD. • **MAD status**—LACP MAD operating state on a member port. Values include **Normal** and **Faulty**.
MAD BFD enabled interface:	Layer 3 interface on which BFD MAD is enabled. This field displays **MAD BFD disabled** if BFD MAD is disabled.
MAD status	BFD MAD operating status: • **Normal**—BFD MAD is operating correctly. • **Faulty**—BFD MAD is not operating correctly. Check the BFD MAD link for connectivity issues. • **N/A**—BFD MAD link status cannot be detected.

Member ID
MAD IP address
Neighbor
MAD status
	BFD MAD details:
	• **Member ID**—IRF member ID of the local device.
	• **MAD IP address**—MAD IP address of a member device.
	• **Neighbor**—IRF member ID of the neighboring member device.
	• **MAD status**—BFD MAD link state. Available states:
	  ◦ **Normal**—BFD MAD is operating correctly.
	  ◦ **Faulty**—BFD MAD is not operating correctly. Check the BFD MAD link for connectivity issues.

easy-irf

Use **easy-irf** to bulk-configure basic IRF settings for an IRF member device.

Syntax

easy-irf [**member** *member-id* [**renumber** *new-member-id*] **domain** *domain-id* [**priority** *priority*] [**irf-port1** *interface-list1*] [**irf-port2** *interface-list2*]]

Views

System view

Predefined user roles

network-admin

Parameters

member *member-id*: Specifies the member ID of a member device. The member ID can be 1 or 2.

renumber *new-member-id*: Specifies a new member ID for the device. The member ID can be 1 or 2. The member device automatically reboots for the new member ID to take effect. If you do not specify this option, the command does not change the member ID.

domain *domain-id*: Specifies an IRF domain ID in the range of 0 to 4294967295. Assign the same domain ID to all devices you are adding to the same IRF fabric.

priority *priority*: Specifies an IRF priority in the range of 1 to 32. The greater the priority value, the higher the priority. A member with higher priority is more likely to be the master.

irf-port1 *interface-list1*: Specifies interfaces bound to IRF-port 1. The *interface-list1* argument represents a space-separated list of up to *n* interface items. Each interface item specifies one interface in the *interface-type interface-number* form.

irf-port2 *interface-list2*: Specifies interfaces bound to IRF-port 2. A physical interface can be bound to only one IRF port. The *interface-list2* argument represents a space-separated list of up to *n* interface items. Each interface item specifies one interface in the *interface-type interface-number* form.

The following compatibility matrixes show the values for the *n* argument in the **irf-port1** *interface-list1* and **irf-port2** *interface-list2* options:

Models	Value for the n argument (maximum number of physical interfaces for each IRF port)
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	8
NFNX3-HDB680, NFNX3-HDB1080	Not supported

Usage guidelines

This command bulk-configures basic IRF settings for a member device, including the member ID, domain ID, priority, and IRF port bindings.

The easy IRF feature provides the following configuration methods:

- **Interactive method**—Enter the **easy-irf** command without parameters. The system will guide you to set the parameters step by step.
- **Non-interactive method**—Enter the **easy-irf** command with parameters.

As a best practice, use the interactive method if you are new to IRF.

If you execute this command multiple times, the following settings take effect:

- The most recent settings for the member ID, domain ID, and priority.
- IRF port bindings added through repeated executions of the command.

When you specify physical interfaces for an IRF port, you must follow the IRF port binding requirements in *Virtual Technologies Configuration Guide*.

If you specify physical interfaces by using the interactive method, you must also follow these restrictions and guidelines:

- Do not enter spaces between the interface type and interface number.
- Use a comma (,) to separate two physical interfaces. No spaces are allowed between interfaces.

To remove an IRF physical interface from an IRF port, you must use the **undo port group interface** command in IRF port view.

Examples

Bulk-configure basic IRF settings by using the non-interactive method. Change the member ID from 2 to 1, set the domain ID to 10, configure the member priority as 10, and bind Ten-GigabitEthernet 2/0/1 and Ten-GigabitEthernet 2/0/2 to IRF-port 1.

```
<Sysname> system-view
```

```
[Sysname] easy-irf member 2 renumber 1 domain 10 priority 10 irf-port1 ten-gigabitethernet
2/0/1 ten-gigabitethernet 2/0/2
*************************************************************************
                 Configuration summary for member 2
IRF new member ID: 1
IRF domain ID    : 10
IRF priority     : 10
IRF-port 1       : Ten-GigabitEthernet2/0/1, Ten-GigabitEthernet2/0/2
IRF-port 2       : Disabled
*************************************************************************
Are you sure to use these settings to set up IRF? [Y/N] y
Starting to configure IRF...
Configuration succeeded.
The device will reboot for the new member ID to take effect. Continue? [Y/N] y
```

Bulk-configure basic IRF settings by using the interactive method. Change the member ID from 2 to 1, set the domain ID to 10, configure the member priority as 10, and bind Ten-GigabitEthernet 2/0/1 and Ten-GigabitEthernet 2/0/2 to IRF-port 1.

```
<Sysname> system-view
[Sysname] easy-irf
*************************************************************************
Welcome to use easy IRF.
To skip the current step, enter a dot sign (.).
To return to the previous step, enter a minus sign (-).
To use the default value (enclosed in []) for each parameter, press Enter without
entering a value.
To quit the setup procedure, press CTRL+C.
*************************************************************************
Select a member by its ID <2> [2]:2
Specify a new member ID <1~10> [1]: 1
Specify a domain ID <0~4294967295> [0]: 10
Specify a priority <1~32> [1]: 10
Specify IRF-port 1 bindings (a physical interface or a comma-separated physical
interface list)[Disabled]: ten-gigabitethernet2/0/1,ten-gigabitethernet2/0/2
Specify IRF-port 2 bindings (a physical interface or a comma-separated physical
interface list)[Disabled]:
*************************************************************************
                 Configuration summary for member 2
IRF new member ID: 1
IRF domain ID    : 10
IRF priority     : 10
IRF-port 1       : Ten-GigabitEthernet2/0/1, Ten-GigabitEthernet2/0/2
IRF-port 2       : Disabled
*************************************************************************
Are you sure to use these settings to set up IRF? [Y/N] y
Starting to configure IRF...
Configuration succeeded.
The device will reboot for the new member ID to take effect. Continue? [Y/N] y
```

irf auto-update enable

Use **irf auto-update enable** to enable the software auto-update feature.

Use **undo irf auto-update enable** to disable the software auto-update feature.

Syntax

irf auto-update enable

undo irf auto-update enable

Default

Software auto-update is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command automatically propagates the current software images of the master device in the IRF fabric to any devices you are adding to the IRF fabric.

To ensure a successful software update, verify that the new device you are adding to the IRF fabric has sufficient storage space for the new software images. If sufficient storage space is not available, the device automatically deletes the current software images. If the reclaimed space is still insufficient, the device cannot complete the auto-update. You must reboot the device, and then access the BootWare menu to delete files.

Examples

Enable the software auto-update feature.

```
<Sysname> system-view
[Sysname] irf auto-update enable
```

irf domain

Use **irf domain** to assign a domain ID to the IRF fabric.

Use **undo irf domain** to restore the default.

Syntax

irf domain *domain-id*

undo irf domain

Default

The IRF domain ID is 0.

Views

System view

Predefined user roles

network-admin

Parameters

domain-id: Specifies a domain ID for the IRF fabric. The value range is 0 to 4294967295.

Usage guidelines

CAUTION:

Changing the IRF domain ID of an IRF member device will remove that member device from the IRF fabric. This member device will be unable to exchange IRF protocol packets with the remaining member devices in the IRF fabric.

One IRF fabric forms one IRF domain. IRF uses IRF domain IDs to uniquely identify IRF fabrics and prevent IRF fabrics from interfering with one another.

If one IRF fabric uses another IRF fabric as the intermediate device for LACP MAD, ARP MAD, or ND MAD, you must assign the two IRF fabrics different domain IDs for correct split detection. False detection causes IRF split.

An IRF fabric has only one IRF domain ID. You can change the IRF domain ID by using the following commands: **irf domain**, **mad enable**, **mad arp enable**, or **mad nd enable**. The IRF domain IDs configured by using these commands overwrite each other.

The **irf domain** command is available only on the default context. The **mad enable**, **mad arp enable**, and **mad nd enable** commands are available on all contexts. If you change the IRF domain ID in one context, the IRF domain IDs in all other contexts change automatically.

Examples

Set the IRF domain ID to 10.

```
<Sysname> system-view
[Sysname] irf domain 10
```

irf mac-address persistent

Use **irf mac-address persistent** to configure IRF bridge MAC persistence.

Use **undo irf mac-address persistent** to disable IRF bridge MAC persistence.

Syntax

irf mac-address persistent { **always** | **timer** }

undo irf mac-address persistent

Default

The IRF bridge MAC address remains unchanged for 6 minutes after the address owner leaves.

Views

System view

Predefined user roles

network-admin

Parameters

always: Enables the IRF bridge MAC address to be permanent. The IRF bridge MAC address does not change after the address owner leaves the fabric.

timer: Enables the IRF bridge MAC address to remain unchanged for 6 minutes after the address owner leaves. If the owner rejoins the IRF fabric within the time limit, the IRF bridge MAC address does not change. If the owner does not rejoin the IRF fabric within the time limit, the IRF fabric uses the bridge MAC address of the current master as the bridge MAC address.

Usage guidelines

CAUTION:

IRF bridge MAC address change will cause transient traffic disruption.

If the **undo** form of this command is used, bridge MAC address of the current master replaces the original IRF bridge MAC as soon as the original address owner leaves.

If the IRF fabric uses a daisy-chain topology and has aggregate links with upstream or downstream devices, do not execute the **undo irf mac-address persistent** command. Use of this command might result in transmission delay or packet loss after the address owner leaves or reboots.

If the IRF fabric has multichassis aggregate links, do not use the **undo irf mac-address persistent** command. Use of this command might cause traffic disruption.

By default, an IRF fabric uses the bridge MAC address of the master device as its bridge MAC address.

On a switched LAN, the IRF bridge MAC address must be unique for correct traffic transmission.

When IRF fabrics merge, IRF ignores the IRF bridge MAC address and checks the bridge MAC address of each member device in the IRF fabrics. IRF merge fails if any two member devices have the same bridge MAC address.

Examples

Enable the IRF bridge MAC address to persist forever.

```
<Sysname> system-view
[Sysname] irf mac-address persistent always
```

irf member description

Use **irf member description** to configure a description for an IRF member device.

Use **undo irf member description** to restore the default.

Syntax

irf member *member-id* **description** *text*

undo irf member *member-id* **description**

Default

No description is configured for an IRF member device.

Views

System view

Predefined user roles

network-admin

Parameters

member-id: Specifies the ID of an IRF member.

text: Specifies a description, a string of 1 to 127 characters.

Examples

Configure the description as **F1Num001** for IRF member 1.

```
<Sysname> system-view
[Sysname] irf member 1 description F1Num001
```

irf member priority

Use **irf member priority** to change the priority of an IRF member device.

Use **undo irf member priority** to restore the default.

Syntax

irf member *member-id* **priority** *priority*

undo irf member *member-id* **priority**

Default

The IRF member priority is 1.

Views

System view

Predefined user roles

network-admin

Parameters

member-id: Specifies an IRF member ID. The member ID can be 1 or 2.

priority: Sets priority in the range of 1 to 32. The greater the priority value, the higher the priority. A member with higher priority is more likely to be the master.

Usage guidelines

The new priority setting takes effect at the next master election, but it does not trigger a master election.

Examples

Set the priority of IRF member 2 to 32.

```
<Sysname> system-view
[Sysname] irf member 2 priority 32
```

irf member renumber

Use **irf member renumber** to change the member ID of an IRF member device.

Use **undo irf member renumber** to restore the previous IRF member ID of the device.

Syntax

irf member *member-id* **renumber** *new-member-id*

undo irf member *member-id* **renumber**

Default

The IRF member ID is 1.

Views

System view

Predefined user roles

network-admin

Parameters

member-id: Specifies the ID of an IRF member. The IRF member ID can be 1 or 2.

new-member-id: Assigns a new ID to the IRF member. The IRF member ID can be 1 or 2.

Usage guidelines

CAUTION:

IRF member ID change can invalidate member ID-related settings, including interface and file path settings, and cause data loss. Make sure you fully understand its impact on your live network.

To have the new ID take effect, you must reboot the IRF member. To cancel the member ID change before you reboot the member device, use the **undo irf member renumber** command. In the command, set the new member ID to be the same as the old member ID.

When adding a device into an IRF fabric, you must assign a unique IRF member ID to the device. If its IRF member ID has been used in the IRF fabric, the device cannot join the IRF fabric.

Interchanging member IDs between IRF member devices might cause undesirable configuration changes and data loss. For example, the IRF member IDs of Device A and Device B are 2 and 1, respectively. After you interchange their member IDs, their port settings also interchange.

Examples

Change the ID of an IRF member device from 1 to 2.

```
<Sysname> display irf
[Sysname] irf member 1 renumber 2
Renumbering the member ID may result in configuration change or loss. Continue?[Y/N]Y
```

Before rebooting the device, cancel the change in the preceding example.

```
[Sysname] undo irf member 1 renumber
Renumbering the member ID may result in configuration change or loss. Continue?[Y/N]y
```

If you reboot the device after executing the **irf member 1 renumber 2** command, the device member ID changes to 2 at system reboot. Using **undo irf member 1 renumber** cannot restore the member ID to 1. You must use the **irf member 2 renumber 1** command to reconfigure the member ID.

irf-port

Use **irf-port** to enter IRF port view.

Use **undo irf-port** to remove all port bindings on an IRF port.

Syntax

irf-port *member-id/irf-port-number*

undo irf-port *member-id/irf-port-number*

Views

System view

Predefined user roles

network-admin

Parameters

member-id: Specifies an IRF member device by its member ID.

irf-port-number: Specifies an IRF port on the member device. The *irf-port-number* argument represents the IRF port index and must be 1 or 2.

Usage guidelines

To bind physical interfaces to an IRF port, you must enter IRF port view.

Examples

Enter IRF-port 2/1 view.

```
<Sysname> system-view
[Sysname] irf-port 2/1
[Sysname-irf-port2/1]
```

Related commands

port group interface

irf-port global load-sharing mode

Use **irf-port global load-sharing mode** to set the global load sharing mode for IRF links.

Use **undo irf-port global load-sharing mode** to restore the default.

Syntax

irf-port global load-sharing mode { **destination-ip** | **destination-mac** | **source-ip** | **source-mac** } *

undo irf-port global load-sharing mode

Default

Packets are distributed based on the load sharing mode automatically selected depending on the packet type.

Views

System view

Predefined user roles

network-admin

Parameters

destination-ip: Distributes traffic across IRF member links based on destination IP address.

destination-mac: Distributes packets across IRF member links based on destination MAC address.

source-ip: Distributes packets across IRF member links based on source IP address.

source-mac: Distributes packets across IRF member links based on source MAC address.

Usage guidelines

The global IRF link load sharing mode applies to all IRF ports in the IRF fabric. You can also configure a port-specific load sharing mode for an IRF port in IRF port view by using the **irf-port load-sharing mode** command.

An IRF port preferentially uses the port-specific load sharing mode. If no port-specific load sharing mode is available, the port uses the global load sharing mode.

You can configure the sharing mode to include a combination of multiple criteria for making traffic distribution decisions. If your device does not support a criterion combination, the system displays an error message.

If you configure the global load sharing mode multiple times, the most recent configuration takes effect.

Examples

Configure the global IRF link load sharing mode to distribute traffic based on destination MAC address.

```
<Sysname> system-view
[Sysname] irf-port global load-sharing mode destination-mac
```

Related commands

irf-port load-sharing mode

irf-port load-sharing mode

Use **irf-port load-sharing mode** to configure a port-specific load sharing mode for an IRF port to distribute traffic across its physical links.

Use **undo irf-port load-sharing mode** to restore the default.

Syntax

irf-port load-sharing mode { **destination-ip** | **destination-mac** | **source-ip** | **source-mac** } *

undo irf-port load-sharing mode

Default

Packets are distributed based on the load sharing mode automatically selected depending on the packet type.

Views

IRF port view

Predefined user roles

network-admin

Parameters

destination-ip: Distributes traffic across IRF member links based on destination IP address.

destination-mac: Distributes packets across IRF member links based on destination MAC address.

source-ip: Distributes packets across IRF member links based on source IP address.

source-mac: Distributes packets across IRF member links based on source MAC address.

Usage guidelines

To successfully configure a port-specific load sharing mode for an IRF port, make sure you have bound a minimum of one physical interface to the IRF port.

You can configure an IRF port-specific load sharing mode to include a combination of multiple criteria for making traffic distribution decisions. If your device does not support a criterion combination, the system displays an error message.

If you configure the port-specific load sharing mode multiple times on an IRF port, the most recent configuration takes effect.

An IRF port preferentially uses the port-specific load sharing mode. If no port-specific load sharing mode is available, the port uses the global load sharing mode.

Examples

Configure a port-specific load sharing mode for IRF-port 1/1 to distribute traffic based on destination MAC address.

```
<Sysname> system-view
[Sysname] irf-port 1/1
[Sysname-irf-port1/1] irf-port load-sharing mode destination-mac
```

Related commands

`irf-port global load-sharing mode`

irf-port-configuration active

Use **`irf-port-configuration active`** to activate IRF ports.

Syntax

`irf-port-configuration active`

Views

System view

Predefined user roles

network-admin

Usage guidelines

After connecting the physical interfaces between two devices and binding them to the correct IRF ports, you must use this command to activate the settings on the IRF ports. This command merges the two devices into one IRF fabric.

The system activates the IRF port settings automatically in the following situations:

- The configuration file that the device starts with contains IRF port bindings.
- You are binding physical interfaces to an IRF port after an IRF fabric is formed.

Examples

To configure and activate IRF-port 1/2 when the port is in DIS state:

Bind a physical interface to IRF-port 1/2.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] shutdown
[Sysname-Ten-GigabitEthernet1/0/1] quit
[Sysname] irf-port 1/2
[Sysname-irf-port1/2] port group interface ten-gigabitethernet 1/0/1
You must perform the following tasks for a successful IRF setup:
Save the configuration after completing IRF configuration.
Execute the "irf-port-configuration active" command to activate the IRF ports.
[Sysname-irf-port1/2] quit
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] undo shutdown
[Sysname-Ten-GigabitEthernet1/0/1] quit
```

Save the configuration so the IRF port settings can take effect after the device reboots.

```
[Sysname] save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait.........................
Saved the current configuration to mainboard device successfully.
```

Activate the IRF port.

```
[Sysname] irf-port-configuration active
```

mad arp enable

Use **mad arp enable** to enable ARP MAD.

Use **undo mad arp enable** to disable ARP MAD.

Syntax

mad arp enable

undo mad arp enable

Default

ARP MAD is disabled.

Views

VLAN interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

Do not configure ARP MAD together with LACP MAD or BFD MAD, because they handle collisions differently.

When you configure ARP MAD, follow these restrictions and guidelines:

Category	Restrictions and guidelines

ARP MAD VLAN	• Do not enable ARP MAD on VLAN-interface 1.
	• If you are using an intermediate device, perform the following tasks:
	  ○ On the IRF fabric and the intermediate device, create a VLAN for ARP MAD.
	  ○ On the IRF fabric and the intermediate device, assign the ports of ARP MAD links to the ARP MAD VLAN.
	  ○ On the IRF fabric, create a VLAN interface for the ARP MAD VLAN.
	• As a best practice, do not use the ARP MAD VLAN for any other purposes.

ARP MAD and feature configuration	If an intermediate device is used, make sure the following requirements are met: • Run the spanning tree feature between the IRF fabric and the intermediate device to ensure that there is only one ARP MAD link in forwarding state. For more information about the spanning tree feature and its configuration, see *Layer 2—LAN Switching Configuration Guide*. • Enable the IRF fabric to change its bridge MAC address as soon as the address owner leaves. • If the intermediate device is also an IRF fabric, assign the two IRF fabrics different domain IDs for correct split detection.

When you use the **mad arp enable** command, the system prompts you to enter a domain ID. If you do not want to change the current domain ID, press **enter** at the prompt.

An IRF fabric has only one IRF domain ID. You can change the IRF domain ID by using the following commands: **irf domain**, **mad enable**, **mad arp enable**, or **mad nd enable**. The IRF domain IDs configured by using these commands overwrite each other.

You can execute the **mad arp enable** command on any contexts. If you change the IRF domain ID in one context, the new IRF domain ID takes effect immediately on all contexts.

Examples

Enable ARP MAD on VLAN-interface 3.

```
<Sysname> system-view
[Sysname] interface vlan-interface 3
[Sysname-Vlan-interface3] mad arp enable
You need to assign a domain ID (range: 0-4294967295)
[Current domain is: 0]: 1
The assigned domain ID is: 1
```

Related commands

irf domain

mad bfd enable

Use **mad bfd enable** to enable BFD MAD.

Use **undo mad bfd enable** to disable BFD MAD.

Syntax

mad bfd enable

undo mad bfd enable

Default

BFD MAD is disabled.

Views

Layer 3 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

Do not configure BFD MAD together with ARP MAD or ND MAD, because they handle collisions differently.

When you configure BFD MAD on a Layer 3 aggregate interface, follow these restrictions and guidelines:

Category	Restrictions and guidelines
BFD MAD-enabled Layer 3 aggregate interface	• Make sure the Layer 3 aggregate interface operates in static aggregation mode. • Make sure the member ports in the aggregation group do not exceed the maximum number of Selected ports allowed for an aggregation group. If the number of member ports exceeds the maximum number of Selected ports, some member ports cannot become Selected. BFD MAD will be unable to work correctly and its state will change to Faulty.

Category	Restrictions and guidelines
BFD MAD VLAN	• On the intermediate device (if any), assign the ports on the BFD MAD links to the same VLAN. Do not assign the ports to an aggregate interface. If the ports are hybrid ports, make sure these ports are untagged members of their PVIDs. • If the intermediate device acts as a BFD MAD intermediate device for multiple IRF fabrics, assign different BFD MAD VLANs to the IRF fabrics. • Do not use the BFD MAD VLAN on the intermediate device for any purposes other than BFD MAD. • Make sure the BFD MAD VLAN on the intermediate device contains only ports on the BFD MAD links. Exclude a port from the BFD MAD VLAN if that port is not on a BFD MAD link. If you have assigned that port to all VLANs by using the **port trunk permit vlan all** command, use the **undo port trunk permit** command to exclude that port from the BFD MAD VLAN.
BFD MAD-enabled Layer 3 aggregate interface and feature compatibility	Use only the **mad bfd enable** and **mad ip address** commands on the BFD MAD-enabled interface. If you configure other features, both BFD MAD and other features on the interface might run incorrectly.
MAD IP address	• To avoid network issues, only use the **mad ip address** command to configure IP addresses on the BFD MAD-enabled interface. Do not configure an IP address by using the **ip address** command on the BFD MAD-enabled interface. • Make sure all the MAD IP addresses are on the same subnet.

Examples

Enable BFD MAD on Route-Aggregation 3.

```
<Sysname> system-view
[Sysname] interface route-aggregation 3
[Sysname-Route-Aggregation3] mad bfd enable
```

mad enable

Use **mad enable** to enable LACP MAD.

Use **undo mad enable** to disable LACP MAD.

Syntax

mad enable

undo mad enable

Default

LACP MAD is disabled.

Views

Aggregate interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

LACP MAD handles collisions differently than ARP MAD and ND MAD. To avoid conflicts, do not enable LACP MAD together with ARP MAD and ND MAD on an IRF fabric.

LACP MAD requires a device that supports extended LACPDUs for MAD to act as the intermediate device. You must set up a dynamic link aggregation group that spans all IRF member devices between the IRF fabric and the intermediate device. To enable dynamic link aggregation, configure the **link-aggregation mode dynamic** command on the aggregate interface.

If one IRF fabric uses another IRF fabric as the intermediate device for LACP MAD, you must assign the two IRF fabrics different domain IDs for correct split detection. False detection causes IRF split.

When you use the **mad enable** command, the system prompts you to enter a domain ID. If you do not want to change the current domain ID, press **enter** at the prompt.

An IRF fabric has only one IRF domain ID. You can change the IRF domain ID by using the following commands: **irf domain**, **mad enable**, **mad arp enable**, or **mad nd enable**. The IRF domain IDs configured by using these commands overwrite each other.

Examples

Enable LACP MAD on Bridge-Aggregation 1, a Layer 2 dynamic aggregate interface.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] link-aggregation mode dynamic
[Sysname-Bridge-Aggregation1] mad enable
You need to assign a domain ID (range: 0-4294967295)
[Current domain is: 0]: 1
The assigned domain ID is: 1
MAD LACP only enable on dynamic aggregation interface.
```

Enable LACP MAD on Route-Aggregation 1, a Layer 3 dynamic aggregate interface.

```
<Sysname> system-view
[Sysname] interface route-aggregation 1
[Sysname-Route-Aggregation1] link-aggregation mode dynamic
[Sysname-Route-Aggregation1] mad enable
You need to assign a domain ID (range: 0-4294967295)
[Current domain is: 0]: 1
The assigned domain ID is: 1
MAD LACP only enable on dynamic aggregation interface.
```

Related commands

irf domain

mad exclude interface

Use **mad exclude interface** to exclude an interface from being shut down when the IRF fabric transits to the Recovery state upon detection of a multi-active collision.

Use **undo mad exclude interface** to configure the IRF fabric to shut down an interface when it transits to the Recovery state upon detection of a multi-active collision.

Syntax

mad exclude interface *interface-type interface-number*

undo mad exclude interface *interface-type interface-number*

Default

All network interfaces on a Recovery-state IRF fabric are shut down, except for the network interfaces automatically excluded by the system.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

If an interface must be kept in up state for special purposes such as Telnet connection, exclude the interface from the shutdown action. As a best practice to avoid incorrect traffic forwarding, do not exclude any interfaces except the interfaces used for Telnet.

The interfaces that have been shut down by MAD come up when the member devices reboot to join the recovered IRF fabric. If the active IRF fabric fails before the IRF link is recovered, use the **mad restore** command on the inactive IRF fabric to recover the inactive IRF fabric. This command also brings up all interfaces that were shut down by MAD.

Examples

Exclude GigabitEthernet 1/0/1 from being shut down when the MAD status transits to Recovery.

```
<Sysname> system-view
[Sysname] mad exclude interface gigabitethernet 1/0/1
```

Related commands

mad restore

mad ip address

Use **mad ip address** to assign a MAD IP address to an IRF member device for BFD MAD.

Use **undo mad ip address** to delete the MAD IP address for an IRF member device.

Syntax

mad ip address *ip-address* { *mask* | *mask-length* } **member** *member-id*

undo mad ip address *ip-address* { *mask* | *mask-length* } **member** *member-id*

Default

No MAD IP address is configured for an IRF member device.

Views

VLAN interface view

Layer 3 aggregate interface view

Predefined user roles

network-admin

Parameters

ip-address: Specifies an IP address in dotted decimal notation.

mask: Specifies a subnet mask in decimal dotted notation.

mask-length: Specifies a subnet mask in length, in the range of 0 to 32.

member *member-id*: Specifies the ID of an IRF member.

Usage guidelines

To use BFD MAD, configure a MAD IP address for each IRF member. Make sure all the MAD IP addresses are on the same subnet.

Do not configure a MAD IP address by using the **ip address** command on the BFD MAD-enabled port or interface.

The master attempts to establish BFD sessions with other member devices by using its MAD IP address as the source IP address.

- If the IRF fabric is integrated, only the MAD IP address of the master takes effect. The master cannot establish a BFD session with any other member. If you execute the **display bfd session** command, the state of the BFD sessions is **Down**.
- When the IRF fabric splits, the IP addresses of the masters in the partitioned IRF fabrics take effect. The masters can establish a BFD session. If you execute the **display bfd session** command, the state of the BFD session between the two devices is **Up**.

Examples

Assign a MAD IP address to IRF member 1 on Route-Aggregation 3.

```
<Sysname> system-view
[Sysname] interface route-aggregation 3
[Sysname-Route-Aggregation3] mad ip address 192.168.0.1 255.255.255.0 member 1
```

Assign a MAD IP address to IRF member 2 on Route-Aggregation 3.

```
[Sysname-Route-Aggregation 3] mad ip address 192.168.0.2 255.255.255.0 member 2
```

Related commands

mad bfd enable

mad nd enable

Use **mad nd enable** to enable ND MAD.

Use **undo mad nd enable** to disable ND MAD.

Syntax

mad nd enable

undo mad nd enable

Default

ND MAD is disabled.

Views

VLAN interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

Do not configure ND MAD together with LACP MAD or BFD MAD, because they handle collisions differently.

Do not configure ND MAD on VLAN-interface 1.

If one IRF fabric uses another IRF fabric as the intermediate device for ND MAD, you must assign the two IRF fabrics different domain IDs for correct split detection. False detection causes IRF split.

When you use the **mad nd enable** command, the system prompts you to enter a domain ID. If you do not want to change the current domain ID, press **enter** at the prompt.

An IRF fabric has only one IRF domain ID. You can change the IRF domain ID by using the following commands: **irf domain**, **mad enable**, **mad arp enable**, or **mad nd enable**. The IRF domain IDs configured by using these commands overwrite each other.

You can execute the **mad nd enable** command on any contexts. If you change the IRF domain ID in one context, the new IRF domain ID takes effect immediately on all contexts.

Examples

Enable ND MAD on VLAN-interface 3.

```
<Sysname> system-view
[Sysname] interface vlan-interface 3
[Sysname-Vlan-interface3] mad nd enable
You need to assign a domain ID (range: 0-4294967295)
[Current domain is: 0]: 1
The assigned domain ID is: 1
```

Related commands

irf domain

mad restore

Use **mad restore** to restore the normal MAD state of the IRF fabric in Recovery state.

Syntax

mad restore

Views

System view

Predefined user roles

network-admin

Usage guidelines

If the active IRF fabric has failed to work before the IRF split problem is fixed, use this command to restore an IRF fabric in Recovery state. The recovered IRF fabric will take over the active IRF fabric role.

Examples

Restore the normal MAD state of the IRF fabric in Recovery state.

```
<Sysname> system-view
[Sysname] mad restore
This command will restore the device from multi-active conflict state. Continue? [Y/N]:Y
Restoring from multi-active conflict state, please wait...
```

port group interface

Use **port group interface** to bind a physical interface to an IRF port.

Use **undo port group interface** to remove the binding of a physical interface to an IRF port.

Syntax

port group interface *interface-type interface-number*

undo port group interface *interface-name*

Default

No physical interfaces are bound to an IRF port.

Views

IRF port view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies a physical interface by its type and number.

interface-name: Specifies a physical interface in the *interface-typeinterface-number* format. No space is allowed between the *interface-type* and *interface-number* arguments.

Usage guidelines

CAUTION:

Use the **undo port group interface** command with caution. If the physical interface is the only up member interface of the IRF port, the IRF fabric will split after you remove the binding.

Execute this command multiple times to bind multiple physical interfaces to an IRF port. The following compatibility matrix shows the maximum number of physical interfaces for each IRF port on different hardware platforms:

Models	Maximum number of physical interfaces for each IRF port
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	8
NFNX3-HDB680, NFNX3-HDB1080	Not supported

Use the **shutdown** command to shut down a physical interface before you bind it to or remove it from an IRF port. To bring up the physical interface after a binding or binding removal operation, use the **undo shutdown** command.

The system does not dynamically remove IRF port bindings when IRF links are lost, for example, because an interface card is removed. To remove IRF port bindings, you must use the **undo port group interface** command.

For more information about IRF port binding requirements, see *Virtual Technologies Configuration Guide*.

Examples

Bind Ten-GigabitEthernet 1/0/1 to IRF-port 1/1 on IRF member 1.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] shutdown
[Sysname-Ten-GigabitEthernet1/0/1] quit
[Sysname] irf-port 1/1
[Sysname-irf-port1/1] port group interface ten-gigabitethernet 1/0/1
[Sysname-irf-port1/1] quit
```

```
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] undo shutdown
```

Related commands

irf-port

Contents

Context commands

The following compatibility matrixes show the support of hardware platforms for context configuration:

Models	Context compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080	Yes
NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	No

Context commands for the default context

This section describes the context commands that you can use after logging in to the default context (the physical device).

allocate interface

Use **`allocate interface`** to assign interfaces to a context.

Use **`undo allocate interface`** to reclaim interfaces assigned to a context.

Syntax

`allocate interface` { *`interface-type interface-number`* }&<1-24> [**`share`**]

`undo allocate interface` { *`interface-type interface-number`* }&<1-24>

`allocate interface` *`interface-type interface-number1`* **`to`** *`interface-type interface-number2`* [**`share`**]

`undo allocate interface` *`interface-type interface-number1`* **`to`** *`interface-type interface-number2`*

Default

All interfaces on the firewall belong to the default context. A non-default context cannot use any interfaces.

Views

Context view

Predefined user roles

network-admin

Parameters

{ *`interface-type interface-number`* }&<1-24>: Assigns 1 to 24 individual interfaces to the context.

`interface-type interface-number1` **`to`** *`interface-type interface-number2`*: Assigns a range of interfaces to the context. The specified interfaces must be the same interface type and must belong to the same interface card.

`share`: Assigns the interfaces in shared mode. If you do not specify this keyword, the command assigns the interfaces exclusively to the context.

Usage guidelines

IMPORTANT:

- Do not assign IRF physical interfaces to a non-default context.
- If a subinterface of a Layer 3 interface is a member interface of a Reth interface, do not assign the Layer 3 interface to a non-default context.
- Logical interfaces support only shared mode, and physical interfaces support both exclusive mode and shared mode.

You can assign interfaces in exclusive or shared mode.

- **Exclusive mode**—You assign an interface exclusively to a context, and only the context can use the interface. The administrator of the context can see the interface and use all commands supported on the interface.
- **Shared mode**—You assign an interface to multiple contexts in shared mode, and the system creates a virtual interface for each context. The virtual interfaces use the same name as the physical interface but have different MAC addresses and IP addresses. They forward and receive packets through the physical interface. The shared mode improves interface usage.

  You can see the physical interface and perform all commands supported on the interface from the default context. The administrator of a context can only see the context's virtual interface and use the **shutdown**, **description**, and network- and security-related commands.

Examples

Assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to context **sub1** in shared mode.

```
<Sysname> system-view
[Sysname] context sub1
[Sysname-context-2-sub1] allocate interface gigabitethernet 1/0/1 gigabitethernet 1/0/3
share
```

allocate vlan

Use **allocate vlan** to assign VLANs to a context.

Use **undo allocate vlan** to reclaim VLANs assigned to a context.

Syntax

allocate vlan *vlan-id*&<1-24>

undo allocate vlan *vlan-id*&<1-24>

allocate vlan *vlan-id1* **to** *vlan-id2*

undo allocate vlan *vlan-id1* **to** *vlan-id2*

Default

No VLAN is assigned to a context.

Views

Context view

Predefined user roles

network-admin

Parameters

vlan-id&<1-24>: Assigns 1 to 24 individual VLANs to the context.

vlan-id1 **to** *vlan-id2*: Assigns a range of VLANs to the context.

Usage guidelines

You assign static VLANs except for VLAN 1 to contexts without the VLAN-unshared attribute. Before doing so, you must create the VLANs on the default context. A VLAN can be assigned only to one context. After the assignment to a context, you can use only the **display** commands on the context, but you can use all VLAN commands on the default context.

A context with the VLAN-unshared attribute has its own VLAN resources (VLAN 2 through VLAN 4094). It does not share VLAN resources with any other context. To create VLANs for the context, log in to the context and use the **vlan** command. VLAN 1 is system defined. You cannot create or delete VLAN 1.

Examples

Assign VLAN 100 to context **sub1**.

```
<Sysname> system-view
[Sysname] context sub1
[Sysname-context-2-sub1] allocate vlan 100
```

Related commands

display context vlan

capability security-policy-rule maximum

Use **capability security-policy-rule maximum** to set the maximum number of security policy rules for a context.

Use **undo capability security-policy-rule maximum** to restore the default.

Syntax

capability security-policy-rule maximum *max-number*

undo capability security-policy-rule maximum

Default

The number of security policy rules is not limited for a context.

Views

Context view

Predefined user roles

network-admin

Parameters

max-number: Specifies the maximum number of security policy rules for the context, in the range of 1 to 4294967295.

Usage guidelines

A large number of rules occupy too much memory, affecting other features on the context. This command sets the maximum number of security policy rules for a context. When the maximum number is reached, you cannot add new rules.

If the maximum number you set is smaller than the number of existing security policy rules, this setting takes effect. The context does not delete extra existing security policy rules and allows new security policy rules to be created only when the number of security policy rules drops below the maximum number.

Examples

Set the maximum number of security policy rules to 1000 for context **cnt2**.

```
<Sysname> system-view
[Sysname] context cnt2
[Sysname-context-2-cnt2] capability security-policy-rule maximum 1000
```

Related commands

display security-policy ip (*Security Command Reference*)

capability session maximum

Use **capability session maximum** to set the maximum number of concurrent unicast sessions for a context.

Use **undo capability session maximum** to restore the default.

Syntax

capability session maximum *max-number*

undo capability session maximum

Default

The number of concurrent unicast sessions is not limited for a context.

Views

Context view

Predefined user roles

network-admin

Parameters

max-number: Specifies the maximum number of concurrent unicast sessions for the context. The value range is 1 to 4294967295.

Usage guidelines

A large number of concurrent unicast sessions occupy too much memory, affecting other features on the context. This command sets the maximum number of concurrent unicast sessions for a context. When the maximum number is reached, you cannot establish additional unicast sessions.

If the maximum number you set is smaller than the number of existing concurrent unicast sessions, this setting takes effect. The context does not delete extra existing concurrent unicast sessions and allows new unicast sessions to be created only when the number of concurrent unicast sessions drops below the maximum number.

This command does not affect local traffic, such as FTP traffic, Telnet traffic, SSH traffic, HTTP traffic, and HTTP-based load balancing traffic.

Examples

Set the maximum number of concurrent unicast sessions to 1000000 for context **cnt2**.

```
<Sysname> system-view
[Sysname] context cnt2
[Sysname-context-2-cnt2] capability session maximum 1000000
```

Related commands

context

display session statistics (*Security Command Reference*)

capability session rate

Use **capability session rate** to set the upper limit of the session establishment rate for a context.

Use **undo capability session rate** to restore the default.

Syntax

capability session rate *max-value*

undo capability session rate

Default

The session establishment rate is not limited for a context.

Views

Context view

Predefined user roles

network-admin

Parameters

max-value: Specifies the maximum number of sessions that can be established per second.

Usage guidelines

Establishing sessions too frequently consumes too much CPU resources. If a context establishes sessions too frequently, other contexts in the same security engine will not be able to establish sessions. This command sets the number of sessions that can be established per second for a context. When the limit is reached, no additional sessions can be established.

This command does not affect local traffic, such as FTP traffic, Telnet traffic, SSH traffic, HTTP traffic, and HTTP-based load balancing traffic.

Examples

Configure context **cnt2** to establish a maximum of 20000 sessions per second.

```
<Sysname> system-view
[Sysname] context cnt2
[Sysname-context-2-cnt2] capability session rate 20000
```

Related commands

context

display session statistics (*Security Command Reference*)

capability sslvpn-user maximum

Use **capability sslvpn-user maximum** to set the maximum number of SSL VPN users for a context.

Use **undo capability sslvpn-user maximum** to restore the default.

Syntax

capability sslvpn-user maximum *max-number*

undo capability sslvpn-user maximum

Default

The number of SSL VPN users is not limited for a context. The number is determined by the usage of the SSL VPN licenses installed on the device.

Views

Context view

Predefined user roles

network-admin

Parameters

max-number: Specifies the maximum number of SSL VPN users for the context. The value range is 1 to 1048575.

Usage guidelines

This command limits the number of SSL VPN users that can log in to a context. When the maximum number is reached, the context will reject the login requests of new SSL VPN users.

If the maximum number you set is smaller than the number of SSL VPN users that already have logged in to a context, this setting takes effect. The context does not log out the currently logged-in users and allows new users to log in only when the number of the logged-in users drops below the maximum number.

Examples

Set the maximum number of SSL VPN users to 1000000 for context **cnt2**.

```
<Sysname> system-view
[Sysname] context cnt2
[Sysname-context-2-cnt2] capability sslvpn-user maximum 1000000
```

Related commands

context

capability throughput

Use **capability throughput** to set the outbound throughput threshold for a context.

Use **undo capability throughput** to restore the default.

Syntax

capability throughput { **kbps** | **pps** } *threshold*

undo capability throughput

Default

The outbound throughput of a context is not limited on a context.

Views

Context view

Predefined user roles

network-admin

Parameters

kbps: Specifies the throughput in kilobits per second.

pps: Specifies the throughput in number of packets per second.

threshold: Specifies the throughput threshold in the range of 1000 to 100000000.

Examples

Set the outbound throughput threshold to 100000 kbps for context **cnt2**.

```
<Sysname> system-view
[Sysname] context cnt2
[Sysname-context-2-cnt2] capability throughput kbps 100000
```

Set the outbound throughput threshold to 10000 pps for context **cnt3**.

```
<Sysname> system-view
[Sysname] context cnt3
[Sysname-context-3-cnt3] capability throughput pps 10000
```

context

Use **context** to create a context and enter its view, or enter the view of an existing context.

Use **undo context** to delete a context.

Syntax

context *context-name* [**id** *context-id*] [**vlan-unshared**]

undo context *context-name*

Default

A default context exists. The context name is **Admin** and the context ID is 1.

Views

System view

Predefined user roles

network-admin

Parameters

context-name: Specifies the context name, a case-sensitive string of 1 to 15 characters.

id *context-id*: Specifies the context ID. If you do not specify this option, the system assigns the lowest ID among the available IDs to the context.

vlan-unshared: Configures the context to not share VLAN resources with any contexts. If you do not specify this keyword, the context shares the same VLAN resources with other contexts.

Usage guidelines

A context with the VLAN-unshared attribute has its own VLAN resources (VLAN 1 through VLAN 4094). It does not share VLAN resources with any other contexts. You log in to the context and use the **vlan** command to create VLANs for the context.

All contexts without the VLAN-unshared attribute share the same VLAN resources (VLAN 1 through VLAN 4094). You create VLANs on the default context and use the **allocate vlan** command to assign VLANs to the contexts. A VLAN can be assigned only to one context.

Examples

Create a context named **test**.

```
<Sysname> system-view
[Sysname] context test
[Sysname-context-2-test]
```

Create a context named **test**. Set its ID to 2.

```
<Sysname> system-view
```

```
[Sysname] context test id 2
[Sysname-context-2-test]
```

context start

Use **context start** to start a context.

Use **undo context start** to stop a context.

Syntax

context start [**force**]

undo context start [**force**]

Default

A context is not started.

Views

Context view

Predefined user roles

network-admin

Parameters

force: Forcibly starts or stops a context. If you do not specify this keyword, the command starts or stops a context through normal procedures.

Usage guidelines

CAUTION:

Stop a context with caution. Stopping a context stops all services on the context and logs out all users on the context. To avoid configuration data loss, save the running configuration of a context before you stop the context.

You must use this command to initiate a newly created context. You can configure a context only after it is started.

Examples

Start context **cnt2**.

```
<Sysname> system-view
[Sysname] context cnt2
[Sysname-context-2-cnt2] context start
```

context-capability inbound broadcast single

Use **context-capability inbound broadcast single** to set the inbound broadcast rate limit for a context.

Use **undo context-capability inbound broadcast single** to restore the default.

Syntax

context-capability inbound broadcast single pps *threshold*

undo context-capability inbound broadcast single

Default

The inbound broadcast rate limit for a context is the total inbound broadcast rate limit divided by the number of active contexts that share interfaces with other contexts.

Views

System view

Context view

Predefined user roles

network-admin

Parameters

pps *threshold*: Specifies the inbound broadcast rate limit in pps, in the range of 1000 to 100000.

Usage guidelines

The rate limit takes effect only on active contexts that share interfaces with other contexts on the device.

If you execute this command in system view, you set the limit for the default context. If you execute this command in context view, you set the limit for the non-default context.

When both a per-context inbound broadcast rate limit and the total inbound broadcast rate limit are reached, the device drops subsequent broadcast packets that arrive at the context. To set the total inbound broadcast rate limit, use the **context-capability inbound broadcast total** command.

Examples

Set the inbound broadcast rate limit for the default context to 10000 pps.

```
<Sysname> system-view
[Sysname] context-capability inbound broadcast single pps 10000
```

Set the inbound broadcast rate limit to 10000 pps on context **ctx1**.

```
<Sysname> system-view
[Sysname] context ctx1
[Sysname-context-1-ctx1] context-capability inbound broadcast single pps 10000
```

Related commands

context-capability inbound broadcast total

context-capability inbound broadcast total

Use **context-capability inbound broadcast total** to set the total inbound broadcast rate limit for all contexts.

Use **undo context-capability inbound broadcast total** to restore the default.

Syntax

context-capability inbound broadcast total pps *threshold*

undo context-capability inbound broadcast total

Default

The total inbound broadcast rate limit for all contexts is 20000 pps.

Views

System view

Predefined user roles

network-admin

Parameters

pps *threshold*: Specifies the total inbound broadcast rate limit in pps. The limit can be 0 or a value in the range of 1000 to 100000. Setting the limit to 0 disables inbound broadcast rate limiting.

Usage guidelines

The rate limit takes effect only on active contexts that share interfaces with other contexts.

The total inbound broadcast rate is the sum of the inbound broadcast rates on all active contexts that share interfaces with other contexts.

When both a per-context inbound broadcast rate limit and the total inbound broadcast rate limit are reached, the device drops subsequent broadcast packets that arrive at the context. To set the inbound broadcast rate limit for a context, use the **context-capability inbound broadcast single** command.

Examples

Set the total inbound broadcast rate limit to 10000 pps.

```
<Sysname> system-view
[Sysname] context-capability inbound broadcast total pps 10000
```

Related commands

context-capability inbound broadcast single

context-capability inbound drop-logging enable

Use **context-capability inbound drop-logging enable** to enable logging for incoming packets dropped because of rate limiting on contexts.

Use **undo context-capability inbound drop-logging enable** to disable logging for incoming packets dropped because of rate limiting on contexts.

Syntax

context-capability inbound drop-logging enable

undo context-capability inbound drop-logging enable

Default

Logging is disabled for incoming packets that are dropped because of rate limiting on contexts.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This logging feature generates and sends a log message to the information center when an incoming packet is dropped because of broadcast or multicast rate limiting on contexts. For more information about how the information center manages log messages, see information center configuration in *Network Management and Monitoring Configuration Guide*.

Examples

Enable logging for incoming packets dropped because of rate limiting on contexts.

```
<Sysname> system-view
```

```
[Sysname] context-capability inbound drop-logging enable
```

context-capability inbound multicast single

Use **context-capability inbound multicast single** to set the inbound multicast rate limit for a context.

Use **undo context-capability inbound multicast single** to restore the default.

Syntax

context-capability inbound multicast single pps *threshold*

undo context-capability inbound multicast single

Default

The inbound multicast rate limit for a context is the total inbound multicast rate limit divided by the number of active contexts that share interfaces with other contexts.

Views

System view

Context view

Predefined user roles

network-admin

Parameters

pps *threshold*: Specifies the inbound multicast rate limit in pps, in the range of 1000 to 100000.

Usage guidelines

The rate limit takes effect only on active contexts that share interfaces with other contexts on the device.

If you execute this command in system view, you set the limit for the default context. If you execute this command in context view, you set the limit for the non-default context.

When both a per-context inbound multicast rate limit and the total inbound multicast rate limit are reached, the device drops subsequent multicast packets that arrive at the context. To set the total inbound multicast rate limit, use the **context-capability inbound multicast total** command.

Examples

Set the inbound multicast rate limit to 10000 pps for the default context.

```
<Sysname> system-view
[Sysname] context-capability inbound multicast single pps 10000
```

Set the inbound multicast rate limit to 10000 pps for context **ctx1**.

```
<Sysname> system-view
[Sysname] context ctx1
[Sysname-context-1-ctx1] context-capability inbound multicast single pps 10000
```

Related commands

context-capability inbound multicast total

context-capability inbound multicast total

Use **context-capability inbound multicast total** to set the total inbound multicast rate limit for all contexts.

Use **undo context-capability inbound multicast total** to restore the default.

Syntax

context-capability inbound multicast total pps *threshold*

undo context-capability inbound multicast total

Default

The total inbound multicast rate limit for all contexts is 0 pps.

Views

System view

Predefined user roles

network-admin

Parameters

pps *threshold*: Specifies the total inbound multicast rate limit in pps. The limit can be 0 or a value in the range of 1000 to 100000. Setting the limit to 0 disables inbound multicast rate limiting.

Usage guidelines

The rate limit takes effect only on active contexts that share interfaces with other contexts.

The total inbound multicast rate is the sum of the inbound multicast rates on all active contexts that share interfaces with other contexts.

When both a per-context inbound multicast rate limit and the total inbound multicast rate limit are reached, the device drops subsequent multicast packets that arrive at the context. To set the inbound multicast rate limit for a context, use the **context-capability inbound multicast single** command.

Examples

Set the total inbound multicast rate limit to 10000 pps.

```
<Sysname> system-view
[Sysname] context-capability inbound multicast total pps 10000
```

Related commands

context-capability inbound multicast single

context-capability inbound unicast total

Use **context-capability inbound unicast total** to set the CPU usage threshold per CPU core for all inbound packets from all contexts.

Use **undo context-capability inbound unicast total** to restore the default.

Syntax

context-capability inbound unicast total cpu-usage *threshold*

undo context-capability inbound unicast total

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280	Yes

Models	Command compatibility
NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	No

Default

The CPU usage threshold per CPU core for all inbound packets is 95%.

Views

System view

Predefined user roles

network-admin

Parameters

cpu-usage *threshold*: Specifies the CPU usage threshold per CPU core for inbound packets, in percentage. The value range for the *threshold* argument is 1 to 100.

Usage guidelines

The threshold set by using this command applies to all inbound packets, including broadcast, unicast, and multicast packets.

If the shared queue in the driver is full when the total usage of a CPU core reaches the specified threshold, the system determines that an attack risk is present. Then, it takes the attack prevention action configured by using the **attack-defense cpu-core action** command until the attack risk is eliminated. For more information about the **attack-defense cpu-core action** command, see attack detection and prevention commands in *Security Command Reference*.

Examples

Set the CPU usage threshold per CPU core for all inbound packets to 70%.

```
<Sysname> system-view
[Sysname] context-capability inbound unicast total cpu-usage 70
```

Related commands

attack-defense cpu-core action (*Security Command Reference*)

description

Use **description** to configure the description of the default context, or configure a description for a non-default context.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

The default context uses the description **DefaultContext**. A non-default context does not have a description.

Views

Context view

Predefined user roles

network-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 255 characters.

Usage guidelines

You can configure a description for each context, which is useful when there are a number of contexts.

Examples

Configure a description for context **cnt2**.

```
<Sysname> system-view
[Sysname] context cnt2
[Sysname-context-2-cnt2] description test
```

display context

Use **display context** to display contexts.

Syntax

display context [**name** *context-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *context-name*: Specifies a context by its name, a case-sensitive string of 1 to 15 characters.

Usage guidelines

On the default context, this command displays the context specified by the **name** *context-name* option. Without the option, this command displays all contexts on the device.

Examples

Display all contexts.

```
<Sysname> display context
ID     Name          Status          Description
1      cnt1          active          context1
2      cnt2          inactive        context2
3      cnt3          inactive        context3
```

Table 1 Command output

Field	Description
Status	Status of the context: • **active**—The context is operating correctly. • **inactive**—The context is not started. • **starting**—The context is starting up.

Field	Description
	• **stopping**—The context is being stopped.

display context capability

Use **display context capability** to display usage of allocable service resources on contexts.

Syntax

display context [**name** *context-name*] **capability** [**security-policy** | **session** [**slot** *slot-number*] | **sslvpn-user**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *context-name*: Specifies a context by its name, a case-sensitive string of 1 to 15 characters. If you do not specify a context, this command displays usage of allocable service resources on all contexts.

security-policy: Displays usage of allocable security policy rule resources.

session: Displays usage of allocable session resources.

sslvpn-user: Displays usage of allocable SSL VPN user resources.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the usage on all member devices.

Usage guidelines

This command is supported only on the default context.

Examples

Display usage of allocable service resources on all contexts.

```
<Sysname> display context capability
Session usage and establishment rate:
 Slot 1 CPU 0:
  ID    Name     Maximum    Used    Free    Total(/s)  Rate(/s)   Usage(%)
  1    Admin     NA         500     NA      NA         1000       NA
  2    context1  10000      300     9700    1000       100        10
  3    context2  2000       1000    1000    2000       1000       50
Security policy rule usage:
  ID    Name            Maximum        Used                Free
  1     Admin           NA             500                 NA
  2     context1        10000          300                 9700
  3     context2        2000           1000                1000
Online SSL VPN users:
  ID    Name            Maximum        Used          Free
  1     Admin           NA             0             NA
```

```
2     conetxt1        10000          3000           7000
3     context2        2000           0              2000
```

Table 2 Command output

Field	Description
ID	Context ID.
Name	Context name.
Maximum	Maximum number of allocable resources.
Used	Number of used resources.
Free	Number of available resources.
Total	Maximum session establishment rate, which is the maximum number of sessions that can be established in a second.
Rate	Current session establishment rate.
Usage	Ratio of the current session establishment rate to the maximum session establishment rate, in percentage.

Related commands

- **capability security-policy-rule maximum**
- **capability session maximum**
- **capability session rate**
- **capability sslvpn-user maximum**

display context capability inbound broadcast

Use **display context capability inbound broadcast** to display the inbound broadcast rate limit statistics for a context.

Syntax

display context name *context-name* **capability inbound broadcast slot** *slot-number*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *context-name*: Specifies a context by its name, a case-sensitive string of 1 to 15 characters.

slot *slot-number*: Specifies an IRF member device by its member ID.

Examples

Display the inbound broadcast rate limit statistics for context **abc** on a slot.

```
<Sysname> display context name abc capability inbound broadcast slot 1
Context name: abc
Context ID: 2
```

```
 Drop Rate: 1000 pps
 Inbound throughput limit: 8000 pps
 Total inbound throughput limit: 10000 pps
```

Table 3 Command output

Field	Description
Drop Rate	Broadcast packet drop rate of the context.
Inbound throughput limit	Inbound broadcast rate limit for the context.
Total inbound throughput limit	Total inbound broadcast rate limit.

display context capability inbound multicast

Use **display context capability inbound multicast** to display the inbound multicast rate limit statistics for a context.

Syntax

display context name *context-name* **capability inbound multicast slot** *slot-number*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *context-name*: Specifies a context by its name, a case-sensitive string of 1 to 15 characters.

slot *slot-number*: Specifies an IRF member device by its member ID.

Examples

Display the inbound multicast rate limit statistics for context **abc** on a slot.

```
<Sysname> display context name abc capability inbound multicast slot 1
Context name: abc
Context ID: 2
 Drop Rate: 1000 pps
 Inbound throughput limit: 8000 pps
 Total inbound throughput limit: 10000 pps
```

Table 4 Command output

Field	Description
Drop Rate	Multicast packet drop rate of the context.
Inbound throughput limit	Inbound multicast rate limit for the context.
Total inbound throughput limit	Total inbound multicast rate limit.

display capability inbound unicast

Use **display capability inbound unicast** to display attack prevention statistics for CPU cores.

Syntax

display capability inbound unicast slot *slot-number*

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280	Yes
NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	No

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID.

Examples

Display attack prevention statistics for CPU cores on a slot.

```
<Sysname> display capability inbound unicast slot 1
CPU usage threshold: 95%
Current attack-defense cpu-core action: Per-packet-balance
CPU ID          Up rate         Packet rate    CPU usage      Effective percentage
CPU0            0/s             0/s            1%             95%
CPU1            0/s             0/s            2%             95%
CPU2            0/s             0/s            1%             95%
CPU3            0/s             0/s            3%             95%
CPU4            0/s             0/s            1%             95%
CPU5            0/s             0/s            2%             95%
CPU6            0/s             0/s            1%             95%
CPU7            50000/s         40000/s        90%            70%
CPU8            0/s             0/s            1%             95%
CPU9            0/s             0/s            5%             95%
CPU10           0/s             0/s            2%             95%
CPU11           0/s             0/s            1%             95%
CPU12           0/s             0/s            6%             95%
CPU13           0/s             0/s            1%             95%
CPU14           0/s             0/s            3%             95%
CPU15           0/s             0/s            1%             95%
```

Table 5 Command output

Field	Description
CPU usage threshold	Total CPU usage threshold per CPU core for all inbound broadcast, multicast, and unicast packets from all contexts, in percentage. When this threshold is reached, attack prevention action will be taken on excessive packets to protect the CPU core.
Current attack-defense cpu-core action	Attack prevention action on excessive packets for CPU core protection. Options: • **Drop**—Drops the packets in the driver. • **Per-packet-balance**—Distributes the packets across CPU cores on a per-packet basis in the driver. • **Isolate**—Puts the packets in the isolation queue in hardware for future processing.
CPU ID	CPU core ID.
Pass rate	Number of packets permitted per second when the attack prevention action is drop or isolate.
Drop rate	Number of packets dropped per second when the attack prevention action is drop or isolate.
Up rate	Number of packets that are delivered to the CPU core per second when the attack prevention action is **Per-packet-balance**.
Balance rate	Number of packets sent to the CPU core per second when the attack prevention action is per-packet-balance.
CPU usage	Current usage of the CPU core, in percentage. When this value reaches the CPU usage threshold per CPU core, the attack prevention action is triggered.
Effective percentage	Maximum percentage of CPU time available for packet processing. The CPU core will use all its available processing capability to process packets after the attack prevention action is triggered, in order to minimize the impact of the action and decrease the CPU usage as quickly as possible. The attack prevention action will take on a packet only if it is beyond the maximum available capability of the CPU core.

display context configuration

Use **display context configuration** to display or save context configuration information.

Syntax

display context [**name** *context-name*] **configuration** [**file** *filename*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *context-name*: Specifies a context by its name, a case-sensitive string of 1 to 15 characters. If you do not specify this option, the command displays the configurations of all contexts.

file *filename*: Saves the information to a file. The *filename* argument specifies the file name, a case-insensitive string of 1 to 255 characters. The file name must use the .tar.gz extension, and

cannot be **..tar.gz** or **…tar.gz**. It cannot start with a hyphen (-) or contain any of the following characters: quote marks ("), forward slashes (/), colons (:), backward slashes (\), question marks (?), less than signs (<), greater than signs (>), vertical bars (|), and asterisks (*). If you do not specify this option, the system prompts you to choose whether to display or save the information.

Usage guidelines

This command is supported only on the default context.

This command does not take effect on contexts that have not started up.

Executing this command is equivalent to executing the **display current-configuration** command on the specified context or each context.

Examples

Display the configurations of all contexts.

```
<Sysname> display context configuration
Save or display context configuration(Y=save, N=display)? [Y/N]:n
===========inner configuration of context Admin===========

============================================================
display current-configuration
#
 version 7.1.064, Feature 9321
#
sysname Sysname
#
context Admin id 1
#
context cnt1 id 2
#
return
<Sysname>

===========inner configuration of context cnt1===========

============================================================
display current-configuration
#
 version 7.1.064, Feature 9321
#
sysname Sysname
#
context Admin id 1
#
context cnt1 id 2
---- More ----
```

Save the configurations of all contexts to a file in interactive mode.

```
<Sysname> display context configuration
Save or display context configuration (Y=save, N=display)? [Y/N]:y
Please input the file name(*.tar.gz)[flash:/diag.tar.gz]: test.tar.gz
Saving context configuration to flash:/test.tar.gz. Please wait....
```

Save the configurations of all contexts to a file by specifying a file name for the command.

```
<Sysname> display context configuration file test.tar.gz
Saving context configuration to flash:/test.tar.gz. Please wait...
```

display context interface

Use **display context interface** to display interfaces assigned to contexts.

Syntax

display context [**name** *context-name*] **interface**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *context-name*: Specifies a context by its name, a case-sensitive string of 1 to 15 characters.

Usage guidelines

This command cannot display interfaces created on non-default contexts.

On the default context, this command displays the interfaces allocated to the non-default context specified by using the **name** *context-name* option. If you do not specify the option, this command displays the interfaces allocated to all non-default contexts on the device.

Examples

Display the interfaces allocated to all non-default contexts.

```
<Sysname> display context interface
Context stub1's interfaces:
  GigabitEthernet1/0/2
Context stub2's interfaces:
  GigabitEthernet1/0/3
```

Related commands

allocate interface

display context online-users sslvpn

Use **display context online-users sslvpn** to display the number of online SSL VPN users on all contexts.

Syntax

display context online-users sslvpn

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

The number of online SSL VPN users collected by this command equals to the number of SSL VPN sessions.

Examples

Display the number of online SSL VPN users on all contexts.

```
<Sysname> display context online-users sslvpn
Total number of SSL VPN online users: 50
```

display context reboot

Use **display context name reboot** to display non-default context reboot information.

Syntax

display context name *context-name* **reboot** *show-number* [*offset*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *context-name*: Specifies a non-default context by its name, a case-sensitive string of 1 to 15 characters.

show-number: Specifies the number of non-default context reboot records to be displayed, in the range of 1 to 20.

offset: Specifies the offset of the first non-default context reboot record to be displayed, starting from the most recent record. The value range is 0 to 19. The default value is 0, which means starting from the most recent record.

Usage guidelines

To view the reboot information about the default context, execute the **display version** command and view the **Last reboot reason** field. For more information about this command, see *Fundamentals Command Reference*.

Examples

Display the most recent reboot record of context **test**.

```
<Sysname> display context name test reboot 1
----------------- Reboot record 1 -----------------
Recorded at          : 2019-05-01  11:16:00
Reason               : 0x0
Process              : comsh (PID: 120) from Context 3 on slot 1 cpu 0
```

Table 6 Command output

Field	Description
Reason	Reboot reason.
Process	Process that triggered the reboot, in the format of *process-name* **(PID:** *process-ID***) from Context** *context-ID* **on slot** *slot-number* **CPU** *CPU-number*.

Related commands

display version (*Fundamentals Command Reference*)

reset context name reboot

display context resource

Use **display context resource** to display CPU, disk space, and memory usage for contexts.

Syntax

display context [**name** *context-name*] **resource** [**cpu** | **disk** | **memory**] [**slot** *slot-number* **cpu** *cpu-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *context-name*: Specifies a context by its name, a case-sensitive string of 1 to 15 characters. If you do not specify this option, the command displays the usage for all contexts.

cpu: Displays the CPU usage.

disk: Displays the disk space usage.

memory: Displays the memory usage.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the usage on all member devices.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

If you do not specify the **cpu**, **disk**, or **memory** keyword, the command displays the CPU, disk space, and memory space usage.

Examples

Display the CPU usage for all contexts on all member devices.

```
<Sysname> display context resource cpu
CPU usage:
Slot 1 CPU 0:
  ID   Name        Weight       Usage(%)
  1    cnt1        10           24
  2    cnt2        10           0

Slot 2 CPU 0:
  ID   Name        Weight       Usage(%)
  1    cnt3        10           0
  2    cnt4        10           0
```

Related commands

limit-resource cpu

limit-resource disk

limit-resource memory

display context statistics

Use **display context statistics** to display or save resource statistics for contexts.

Syntax

display context [**name** *context-name*] **statistics** [**file** *filename*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *context-name*: Specifies a context by its name, a case-sensitive string of 1 to 15 characters. If you do not specify this option, the command displays or saves resource statistics for all contexts.

file *filename*: Saves the information to a file. The *filename* argument specifies the file name, a case-insensitive string of 1 to 255 characters. The file name must use the .tar.gz extension, and cannot be **..tar.gz** or **…tar.gz**. It cannot start with a hyphen (-) or contain any of the following characters: quote marks ("), forward slashes (/), colons (:), backward slashes (\), question marks (?), less than signs (<), greater than signs (>), vertical bars (|), and asterisks (*). If you do not specify this argument, the system prompts you to choose whether to display or save the information.

Usage guidelines

This command is supported only on the default context.

Executing this command is equivalent to executing the following commands:

- **display context capability**
- **display counters inbound interface**
- **display counters outbound interface**
- **display counters rate inbound interface**
- **display counters rate outbound interface**
- **display interface**
- **display ip statistics**
- **display ipv6 statistics**
- **display nat statistics**
- **display session statistics**

Examples

Display resource statistics for all contexts.

```
<Sysname> display context statistics
Save or display context statistics (Y=save, N=display)? [Y/N]:n
=======================================================
    =============== display session statistics =================
Slot 1:
Current sessions: 0
```

```
          TCP sessions:                   0
          UDP sessions:                   0
         ICMP sessions:                   0
       ICMPv6 sessions:                   0
     UDP-Lite sessions:                   0
         SCTP sessions:                   0
         DCCP sessions:                   0
        RAWIP sessions:                   0
...
```

Save resource statistics for all contexts to a file in interactive mode.

```
<Sysname> display context statistics
Save or display context statistics(Y=save, N=display)? [Y/N]:y
Please input the file name(*.tar.gz)[flash:/diag.tar.gz]: test.tar.gz
Saving context statistics to flash:/test.tar.gz. Please wait....
```

Save resource statistics for all contexts to a file by specifying a file name for the command.

```
<Sysname> display context statistics file test.tar.gz
Saving context statistics to flash:/test.tar.gz. Please wait...
```

Related commands

display context capability

display counters inbound interface (*Interface Command Reference*)

display counters outbound interface (*Interface Command Reference*)

display counters rate inbound interface (*Interface Command Reference*)

display counters rate outbound interface (*Interface Command Reference*)

display interface (*Interface Command Reference*)

display ip statistics (*Layer 3—IP Services Command Reference*)

display ipv6 statistics (*Layer 3—IP Services Command Reference*)

display nat statistics (*NAT Command Reference*)

display session statistics (*Security Command Reference*)

display context vlan

Use **display context vlan** to display VLAN lists for contexts.

Syntax

display context [**name** *context-name*] **vlan**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *context-name*: Specifies a context by its name, a case-sensitive string of 1 to 15 characters.

Usage guidelines

On the default context, if you specify the **name** *context-name* option, this command displays the VLAN list for the specified context. If you do not specify the **name** *context-name* option, this command displays VLAN lists for all contexts.

Examples

Display VLAN lists for all contexts.

```
<Sysname> display context vlan
Context stub1's VLAN(s):

Context stub2's VLAN(s):
  2,4094
Context stub3's VLAN(s):
5,6,800-3000,3400
```

Display the VLAN list for context **sub1**.

```
<Sysname> display context name sub1 vlan
Context stub1's VLAN(s):
  5,6,11-23,3400
```

Related commands

allocate vlan

limit-resource cpu

Use **limit-resource cpu** to set a CPU weight for a context.

Use **undo limit-resource cpu** to restore the default.

Syntax

limit-resource cpu weight *weight-value*

undo limit-resource cpu

Default

Each context has a CPU weight of 10.

Views

Context view

Predefined user roles

network-admin

Parameters

weight *weight-value*: Specifies a CPU weight value in the range of 1 to 10.

Examples

Set the CPU weight to 2 for context **cnt2**.

```
<Sysname> system-view
[Sysname] context cnt2
[Sysname-context-2-cnt2] limit-resource cpu weight 2
```

limit-resource memory

Use **limit-resource memory** to set a memory space percentage for a context. A memory space percentage defines the maximum memory space that the context can use.

Use **undo limit-resource memory** to restore the default.

Syntax

limit-resource memory slot *slot-number* **cpu** *cpu-number* **ratio** *limit-ratio*

undo limit-resource memory slot *slot-number* **cpu** *cpu-number*

Default

All contexts share the memory space in the system. A context can use all free memory space.

Views

Context view

Predefined user roles

network-admin

Parameters

slot *slot-number* **cpu** *cpu-number*: Specifies a security engine on an IRF member device. The *slot-number* argument represents the member ID of the IRF member device. The *cpu-number* argument represents the CPU number.

ratio *limit-ratio*: Specifies the ratio of the memory space that the context can use on the specified security engine to the total memory space of the engine. The value range is 1 to 100.

Usage guidelines

When you assign a context to a security engine group, the system automatically assigns memory space resources on the security engines to the context. All contexts residing on the same security engine share and compete for the engine's free memory resources. To prevent one context from occupying too many memory space resources, assign memory space resources to the contexts. When the limit for a context is reached, the context cannot apply for more memory space.

When you assign memory space to a context, follow these guidelines:

- Use the **display context resource** command to view the amount of memory space that has been used by the context before assigning memory space to the context.
- Assign an amount of memory space that is larger than the memory space used by the context to avoid the following problems:
  - The context cannot apply for more memory space.
  - The context cannot create, copy, or save additional folders or files.

Examples

Configure context **cnt2** to use up to 30% of the memory space on CPU 0 of member device 1.

```
<Sysname> system-view
[Sysname] context cnt2
[Sysname-context-2-cnt2] limit-resource memory slot 1 cpu 0 ratio 30
```

reset context capability inbound broadcast

Use **reset context capability inbound broadcast** to clear the inbound broadcast rate limit statistics for a context.

Syntax

reset context name *context-name* **capability inbound broadcast slot** *slot-number*

Views

User view

Predefined user roles

network-admin

Parameters

name *context-name*: Specifies a context by its name, a case-sensitive string of 1 to 15 characters.

slot *slot-number*: Specifies an IRF member device by its member ID.

Examples

Clear the inbound broadcast rate limit statistics for context **abc** on a slot.

```
<Sysname> reset context name abc capability inbound broadcast slot 1
```

reset context capability inbound multicast

Use **reset context capability inbound multicast** to clear the inbound multicast rate limit statistics for a context.

Syntax

reset context name *context-name* **capability inbound multicast slot** *slot-number*

Views

User view

Predefined user roles

network-admin

Parameters

name *context-name*: Specifies a context by its name, a case-sensitive string of 1 to 15 characters.

slot *slot-number*: Specifies an IRF member device by its member ID.

Examples

Clear the inbound multicast rate limit statistics for context **abc** on a slot.

```
<Sysname> reset context name abc capability inbound multicast slot 1
```

reset context reboot

Use **reset context name reboot** to clear non-default context reboot information.

Syntax

reset context [**name** *context-name*] **reboot**

Views

User view

Predefined user roles

network-admin

Parameters

name *context-name*: Specifies a non-default context by its name, a case-sensitive string of 1 to 15 characters. If you do not specify a non-default context, this command clears reboot information for all non-default contexts.

Examples

Clear reboot information about non-default context **test**.

```
<Sysname> reset context name test reboot
```

Related commands

display context name reboot

switchto context

Use **switchto context** to log in to a context.

Syntax

switchto context *context-name*

Views

System view

Predefined user roles

network-admin

network-operator

Parameters

context-name: Specifies a context that has been started.

Usage guidelines

Use this command to log in to a non-default context from the system view of the default context. The connection uses the internal interfaces between the physical device and the context.

Examples

Log in to context **test2**.

```
<Sysname> system-view
[Sysname] switchto context test2
******************************************************************************
* Copyright (c) 2004-2018 NSFOCUS. All rights reserved.                      *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

<NSFOCUS>
```

tar context log

Use **tar context log** to archive log messages for contexts.

Syntax

tar context [**name** *context-name*] **log file** *filename*

Views

User view

Predefined user roles

network-admin

Parameters

name *context-name*: Specifies a context by its name, a case-sensitive string of 1 to 15 characters. If you do not specify this option, the command archives log messages for all contexts.

file *filename*: Specifies a file name, a case-insensitive string of 1 to 255 characters. The file name must use the .tar.gz extension, and cannot be **..tar.gz** or **…tar.gz**. It cannot start with a hyphen (-) or contain any of the following characters: quote marks ("), forward slashes (/), colons (:), backward slashes (\), question marks (?), less than signs (<), greater than signs (>), vertical bars (|), and asterisks (*).

Usage guidelines

This command is supported only on the default context.

This command does not take effect on contexts that have never started up.

This command archives all files in the **logfile** directory and **diagfile** directory.

Examples

Archive log messages for all contexts to file **test.tar.gz**.

```
<Sysname> tar context log file test.tar.gz
```

Context commands for non-default contexts

This section describes the context commands that you can use after logging in to a non-default context.

display context interface

Use **display context interface** to display interfaces assigned to the current context.

Syntax

display context interface

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the interfaces assigned to the current context.

```
<Sysname> display context interface
Context stub1's interfaces:
  GigabitEthernet1/0/2
```

Related commands

allocate interface

display context reboot

Use **display context reboot** to display reboot information about the current context.

Syntax

display context reboot *show-number* [*offset*]

Views

Any view

Predefined user roles

context-admin

context-operator

Parameters

show-number: Specifies the number of context reboot records to be displayed, in the range of 1 to 20.

offset: Specifies the offset of the first context reboot record to be displayed, starting from the most recent record. The value range is 0 to 19. The default value is 0, which means starting from the most recent record.

Examples

Display the most recent reboot record of the current CONTEXT.

```
<Sysname> display context reboot 1
----------------- Reboot record 1 -----------------
Recorded at          : 2019-05-01  11:16:00
Reason               : 0x0
Process              : comsh (PID: 120) from Context 3 on slot 1 cpu 0
```

For information about the command output fields, see Table 6.

Related commands

reset context reboot

reset context reboot

Use **reset context reboot** to clear reboot information about the current context.

Syntax

reset context reboot

Views

User view

Predefined user roles

context-admin

Examples

Clear reboot information about the current context.

```
<Sysname> reset context reboot
```

Related commands

display context reboot

Contents

Reth interface commands

The following matrixes show the compatibility of hardware and the Reth interface feature:

Models	Reth interface compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	Yes
NFNX3-HDB680, NFNX3-HDB1080	No

bandwidth

Use **bandwidth** to set the expected bandwidth for a Reth interface or subinterface.

Use **undo bandwidth** to restore the default.

Syntax

bandwidth *bandwidth-value*

undo bandwidth

Default

The expected bandwidth is 10000 kbps for a Reth interface or subinterface.

Views

Reth interface view

Reth subinterface view

Predefined user roles

network-admin

context-admin

Parameters

bandwidth-value: Specifies the expected bandwidth in the range of 1 to 400000000 kbps.

Usage guidelines

The expected bandwidth is an informational parameter used only by higher-layer protocols for calculation. You cannot adjust the actual bandwidth of an interface by using this command.

Examples

Set the expected bandwidth to 50 kbps for Reth 1.

```
<Sysname> system-view
[Sysname] interface reth 1
[Sysname-Reth1] bandwidth 50
```

default

Use **default** to restore the default settings for a Reth interface or subinterface.

Syntax

default

Views

Reth interface view

Reth subinterface view

Predefined user roles

network-admin

context-admin

Usage guidelines

CAUTION:

The **default** command might interrupt ongoing network services. Make sure you are fully aware of the impacts of this command when you execute it on a live network.

This command might fail to restore the default settings for some commands for reasons such as command dependencies and system restrictions.

To resolve this problem:

1. Use the **display this** command in interface view to identify these commands.
2. Use their **undo** forms or follow the command reference to restore their default settings.
3. If the restoration attempt still fails, follow the error message instructions to resolve the problem.

Examples

Restore the default settings for Reth 1.

```
<Sysname> system-view
[Sysname] interface reth 1
[Sysname-Reth1] default
```

description

Use **description** to configure the description of an interface or subinterface.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

The description of a Reth interface or subinterface is *interface-name* plus **Interface** (for example, **Reth1 Interface**).

Views

Reth interface view

Reth subinterface view

Predefined user roles

network-admin

context-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 255 characters.

Examples

Configure the description of Reth 1 as **master-interface**.

```
<Sysname> system-view
[Sysname] interface reth 1
[Sysname-Reth1] description master-interface
```

display counters interface reth

Use **display counters interface reth** to display Reth interface traffic statistics.

Syntax

display counters { **inbound** | **outbound** } **interface** [**reth** [*interface-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

inbound: Displays inbound traffic statistics.

outbound: Displays outbound traffic statistics.

reth: Specifies Reth interfaces. If you do not specify this keyword, the command displays traffic statistics for all interfaces that have traffic counters.

interface-number: Specifies a Reth interface by its number. If you do not specify this argument, the command displays traffic statistics for all Reth interfaces.

Usage guidelines

This command displays traffic statistics within a statistics polling interval. You can use the **flow-interval** command to set the statistics polling interval.

To clear Reth interface traffic statistics, use the **reset counters interface reth** command.

Examples

Display inbound traffic statistics for Reth 1.

```
<Sysname> display counters inbound interface reth 1
Interface            Total (pkts)    Broadcast (pkts)    Multicast (pkts)  Err (pkts)
Reth1                         100                 100                   0           0

 Overflow: More than 14 digits (7 digits for column "Err").
       --: Not supported.
```

Table 1 Command output

Field	Description
Interface	Abbreviated interface name.
Total (pkts)	Total number of packets received or sent through the interface.
Broadcast (pkts)	Total number of broadcast packets received or sent through the interface.
Multicast (pkts)	Total number of multicast packets received or sent through the interface.
Err (pkts)	Total number of error packets received or sent through the interface.
Overflow: More than 14 digits (7 digits for column "Err").	This **Overflow** field is displayed when any of the following conditions exist: • The data length of the **Err** field exceeds 7 decimal digits. • The data length of a non-**Err** field exceeds 14 decimal digits.
--: Not supported.	If a statistical item is not supported, two hyphens (**--**) are displayed for the item.

Related commands

`flow-interval` (*Interface Command Reference*)

`reset counters interface reth`

display counters rate interface reth

Use **`display counters rate interface reth`** to display traffic rate statistics for Reth interfaces in up state during the most recent statistics polling interval.

Syntax

`display counters rate` { **`inbound`** | **`outbound`** } **`interface`** [**`reth`** [*`interface-number`*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

`inbound`: Displays inbound traffic rate statistics.

`outbound`: Displays outbound traffic rate statistics.

`reth`: Specifies Reth interfaces. If you do not specify this keyword, the command displays traffic rate statistics for all up interfaces that have traffic counters during the most recent statistics polling interval.

`interface-number`: Specifies a Reth interface by its number. If you do not specify this argument, the command displays traffic rate statistics for all up Reth interfaces during the most recent statistics polling interval.

Usage guidelines

This command displays traffic rate statistics within a statistics polling interval. You can use the **`flow-interval`** command to set the statistics polling interval.

To clear Reth interface traffic rate statistics, use the **reset counters interface reth** command.

Examples

Display inbound traffic rate statistics for Reth1.

```
<Sysname> display counters rate inbound interface reth 1
Usage: Bandwidth utilization in percentage
Interface            Usage (%)   Total (pps)   Broadcast (pps)   Multicast (pps)
Reth1                        3           200               100               100

 Overflow: More than 14 digits.
       --: Not supported.
```

Table 2 Command output

Field	Description
Interface	Abbreviated interface name.
Usage (%)	Bandwidth usage (in percentage) of the interface during the most recent statistics polling interval.
Total (pps)	Average receiving or sending rate (in pps) for all packets during the most recent statistics polling interval.
Broadcast (pps)	Average receiving or sending rate (in pps) for broadcast packets during the most recent statistics polling interval.
Multicast (pps)	Average receiving or sending rate (in pps) for multicast packets during the most recent statistics polling interval.
Overflow: More than 14 digits.	The **Overflow** field is displayed if the data length of a statistical item exceeds 14 decimal digits.
--: Not supported.	If a statistical item is not supported, two hyphens (**--**) are displayed for the item.

Related commands

flow-interval (*Interface Command Reference*)

reset counters interface reth

display interface reth

Use **display interface reth** to display Reth interface or subinterface information.

Syntax

display interface [**reth** [*interface-number* | *interface-number.subnumber*]] [**brief** [**description** | **down**]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

reth: Specifies Reth interfaces or subinterfaces.

interface-number: Specifies an existing Reth interface by its number.

interface-number.subnumber: Specifies a subinterface of a Reth interface. The *interface-number* argument specifies the main interface number. The *subnumber* argument specifies the subinterface number and is separated from the main interface number by a dot (.).

brief: Displays brief interface information. If you do not specify this keyword, the command displays detailed interface information.

down: Displays information about interfaces in down state and the causes for the down state. If you do not specify this keyword, the command displays information about interfaces in all states.

description: Displays complete interface descriptions. If you do not specify this keyword, the command displays only the first 27 characters of each interface description.

Usage guidelines

If you do not specify the **reth** keyword, the command displays information about all interfaces except for VA interfaces. For more information about VA interfaces, see PPPoE configuration in *Layer 2—WAN Access Configuration Guide*.

If you specify the **reth** keyword but do not specify an interface or subinterface, the command displays information about all Reth interfaces and subinterfaces.

If you specify the **reth** *interface-number* option or the **reth** *interface-number.subnumber* option, the command displays information about the specified Reth interface or subinterface.

Examples

Display detailed information about Reth 1.

```
<Sysname> display interface reth 1
Reth1
Current state: UP
Line protocol state: UP
Description: Reth1 Interface
Bandwidth: 10000kbps
Maximum transmission unit: 1500
Internet protocol processing: Disabled
IP packet frame type: Ethernet II, hardware address: 0cda-41b5-cf30
IPv6 packet frame type: Ethernet II, hardware address: 0cda-41b5-cf30
Physical: Reth, baudrate: 10000000 bps
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

Table 3 Command output

Field	Description
Current state	Physical link state of the interface: • **Administratively DOWN**—The interface has been shut down by using the **shutdown** command. • **DOWN**—The interface is administratively up, but its physical state is

Field	Description
	down (possibly because no physical link exists or the link has failed). • **UP**—The interface is both administratively and physically up. A Reth interface is both administratively and physically up when a minimum of one member interface is administratively and physically up.
Line protocol state	Data link layer state of the interface. The state is determined through automatic parameter negotiation at the data link layer. • **UP**—The data link layer protocol is up. • **DOWN**—The data link layer protocol is down.
Description	Description of the interface.
Bandwidth	Expected bandwidth of the interface.
Maximum transmission unit	MTU of the interface.
Internet protocol processing: Disabled	The interface is not assigned an IP address and cannot process IP packets.
Internet address: *ip-address*/*mask-length* (*Type*)	IP address of the interface and type of the address in parentheses. Possible IP address types include: • **Primary**—Manually configured primary IP address. • **Sub**—Manually configured secondary IP address. If the interface has both primary and secondary IP addresses, the primary IP address is displayed. If the interface has only secondary IP addresses, the lowest secondary IP address is displayed. • **DHCP-allocated**—DHCP allocated IP address. For more information, see DHCP client configuration in *Layer 3—IP Services Configuration Guide*. • **BOOTP-allocated**—BOOTP allocated IP address. For more information, see BOOTP client configuration in *Layer 3—IP Services Configuration Guide*. • **PPP-negotiated**—IP address assigned by a PPP server during PPP negotiation. For more information, see PPP configuration in *Layer 2—WAN Access Configuration Guide*. • **Unnumbered**—IP address borrowed from another interface. • **Cellular-allocated**—IP address allocated through the modem-manufacturer's proprietary protocol. For more information, see mobile communication modem management in *Layer 2—WAN Access Configuration Guide*. • **MAD**—IP address assigned to an IRF member device for MAD on the interface. For more information, see IRF configuration in *Virtual Technologies Configuration Guide*.
IP packet frame type	IPv4 packet framing format.
hardware address	MAC address of the interface.
IPv6 packet frame type	IPv6 packet framing format.
Physical	Interface type.
Last clearing of counters	Last time when the **`reset counters interface`** command was used to clear the interface statistics. If the **`reset counters interface`** command has never been used on the interface since the device startup, this field displays **Never**.
Last 300 seconds input rate	Average input rate (in Bps and pps) over the last 300 seconds. This field is displayed for a Reth subinterface only after you execute the **`sub-interface rate-statistic`** command.
Last 300 seconds output	Average output rate (in Bps and pps) over the last 300 seconds. This field is displayed for a Reth subinterface only after you execute the

Field	Description
rate	**sub-interface rate-statistic** command. Support for the **sub-interface rate-statistic** command depends on the device model.
Input	Incoming traffic statistics on the interface: • Number of packets. • Number of bytes. • Number of dropped packets. (A Reth interface directly drops packets received by an inactive member interface. An interface also drops packets due to insufficient receive buffer.)
Output	Outgoing traffic statistics on the interface: • Number of packets. • Number of bytes. • Number of dropped packets due to insufficient send buffer.
Brief information on interfaces in route mode	Brief information about Layer 3 interfaces.
Interface	Abbreviated interface name.
Link	Physical link state of the interface: • **UP**—The interface is physically up. • **DOWN**—The interface is physically down. • **ADM**—The interface has been shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command. • **Stby**—The interface is a backup interface in standby state. To see the primary interface, use the **display interface-backup state** command.
Protocol	Data link layer protocol state of the interface: • **UP**—The data link layer protocol of the interface is up. • **DOWN**—The data link layer protocol of the interface is down. • **UP(s)**—The data link layer protocol of the interface is up, but the link is an on-demand link or does not exist. The **(s)** attribute represents the spoofing flag.
Primary IP	Primary IP address of the interface. This field displays two hyphens (**--**) if the interface does not have an IP address.
Description	Partial or complete interface description configured by using the **description** command: • If you specify the **description** keyword in the **display interface brief** command, this field displays only the first 27 characters of the interface description. • If you do not specify the **description** keyword in the **display interface brief** command, this field displays the complete interface description.

Display brief information about Reth 1.

```
<Sysname> display interface reth 1 brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP         Description
Reth1                DOWN DOWN     --
```

Display the causes for the down state of Reth 1.

```
<Sysname> display interface reth 1 brief down
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Interface            Link Cause
Reth1                DOWN Not connected
```

Table 4 Command output

Field	Description
Brief information on interfaces in route mode:	Brief information about Layer 3 interfaces.
Interface	Interface name.
Link	Physical link state of the interface: • **UP**—The interface is physically up. • **DOWN**—The interface is physically down. • **ADM**—The interface has been shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command. • **Stby**—The interface is a backup interface in standby state. To see the primary interface, use the **display interface-backup state** command.
Protocol	Data link layer protocol state of the interface: • **UP**—The data link layer protocol of the interface is up. • **DOWN**—The data link layer protocol of the interface is down. • **UP(s)**—The data link layer protocol of the interface is up, but the link is an on-demand link or does not exist. The **(s)** attribute represents the spoofing flag. This value is typical of null interfaces and loopback interfaces.
Primary IP	Primary IP address of the interface. This field displays two hyphens (**--**) if the interface does not have an IP address.
Description	Description of the interface.
Cause	Cause for the physical link state of an interface to be **DOWN**: • **Administratively**—The interface has been manually shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command. • **Not connected**—No physical connection exists (possibly because the network cable is disconnected or faulty).

display reth interface

Use **display reth interface** to display information about the member interfaces of a Reth interface.

Syntax

display reth interface reth *interface-number*

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

reth *interface-number*: Specifies a Reth interface by its number. The Reth interface must exist.

Examples

Display information about the member interfaces of Reth 1.

```
<Sysname> display reth interface reth 1
Reth1 :
  Redundancy group  : aaa
  Member          Physical status       Forwarding status      Presence status
  GE1/0/1         UP                    Active                 Normal
  GE1/0/2         UP                    Inactive               Normal
```

Table 5 Command output

Field	Description
Redundancy group	The redundancy group to which the Reth interface belongs. If the Reth interface is not in any redundancy group, this field displays **N/A**.
Member	Name of the member interface.
Physical status	Physical status of the member interface: • **Down (redundancy down)**—The interface has been shut down by the Reth module. • **Down**—The interface is administratively up but physically down possibly because no physical link is present or the link has failed. • **UP**—The interface is both administratively and physically up.
Forwarding status	Forwarding status of the member interface: • **Active**—The member interface can forward packets. • **Inactive**—The member interface cannot forward packets.
Presence status	Status of the member interface: • **Normal**—The member interface exists. • **Absent**—The member interface does not exist.

fast-switch enable

Use **fast-switch enable** to enable fast switchover on a Reth interface.

Use **undo interface reth** to disable fast switchover on a Reth interface.

Syntax

fast-switch enable

undo fast-switch enable

The following matrixes show the hardware and command compatibility:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080	Yes
NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	No

Default

Fast traffic switchover is disabled.

Views

Reth interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

IMPORTANT:

This feature introduces low possibility of forwarding traffic on the inactive member interface while the system is operating correctly. Make sure you understand this impact on your services when you use this feature.

This feature enables faster traffic switchover between Reth member interfaces than the standard switchover mechanism of Reth when the master device is powered off or reboots unexpectedly.

This feature implements fast switchover by allowing the inactive member interface to forward packets. In rare cases, the neighbor device might learn MAC address entries on the link connected to the inactive interface and sends traffic to the inactive interface.

For this feature to take effect and operate effectively, follow these restrictions and guidelines:

- Make sure the Reth member interfaces are physical interfaces.
- Enable fast switchover on both the Reth interface for uplink traffic and the Reth interface for downlink traffic.
- Assign the downlink and uplink Reth interfaces to a redundancy group.
- Make sure the high-priority Reth member interfaces are on the master device (high-priority redundancy group node).
- To minimize the chance of receiving traffic on the inactive interface, use the **`arp timer aging`** command on the neighbor device to shorten the ARP entry aging timer.

Examples

Enable fast traffic switchover on Reth 1.

```
<Sysname> system-view
[Sysname] interface reth 1
[Sysname-Reth1] fast-switch enable
```

Related commands

`arp timer aging` (*Layer 3—IP Services Command Reference*)

interface reth

Use **interface reth** to create a Reth interface or subinterface and enter its view, or enter the view of an existing Reth interface or subinterface.

Use **undo interface reth** to delete a Reth interface or subinterface.

Syntax

interface reth { *interface-number* | *interface-number.subnumber* }

undo interface reth { *interface-number* | *interface-number.subnumber* }

Default

No Reth interfaces or subinterfaces exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interface-number: Specifies a Reth interface by its number. The value range for this argument is 1 to 255.

interface-number.subnumber: Specifies a subinterface of a Reth interface. The *interface-number* argument specifies the main interface number. The *subnumber* argument specifies the subinterface number and is separated from the main interface number by a dot (.). The value range for the *subnumber* argument is 1 to 4094.

Usage guidelines

A Reth interface is a virtual Layer 3 interface that uses two member interfaces to ensure link availability.

To create a Reth subinterface, create the Reth interface first.

You cannot create subinterfaces for a Reth interface in any of the following situations:

- The members of the Reth interface are Layer 3 Ethernet subinterfaces or Layer 3 aggregate subinterfaces.
- A minimum of one subinterface is created on the member interfaces of the Reth interface.

You cannot delete a Reth interface if it has member interfaces.

Examples

Create Reth 1 and enter its view.

```
<Sysname> system-view
[Sysname] interface reth 1
[Sysname-Reth1]
```

Create Reth 1.1 and enter its view.

```
<Sysname> system-view
[Sysname] interface reth 1.1
[Sysname-Reth1.1]
```

member interface

Use **member interface** to assign a member interface to a Reth interface.

Use **undo member interface** to remove a member interface from a Reth interface.

Syntax

member interface *interface-type interface-number* **priority** *priority*

undo member interface *interface-type interface-number*

Default

A Reth interface does not have member interfaces.

Views

Reth interface view

Predefined user roles

network-admin

context-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

The interface can be any of the following interfaces and their subinterfaces:

- Layer 3 Ethernet interfaces.
- Layer 3 aggregate interfaces.

priority: Specifies an interface priority in the range of 1 to 255. The higher the value, the higher the interface priority.

Usage guidelines

You can assign a maximum of two member interfaces to a Reth interface. An interface can belong to only one Reth interface.

As a best practice, assign interfaces of the same type and same speed to a Reth interface.

If a Layer 3 Ethernet interface is marked as a bypass interface on the panel or has the bypass feature enabled, do not use that interface as a member interface of a Reth interface. If you do so, communication errors will occur. For more information about the bypass feature, see bridge forwarding in *Layer 2—LAN Switching Configuration Guide*.

If both member interfaces of a Reth interface are subinterfaces, make sure they are on different main interfaces and terminate the same VLAN ID. For more information about VLAN termination, see *Layer 2—LAN Switching Configuration Guide*.

When the two member interfaces of a Reth interface are up, the system chooses the interface with the higher priority as the active interface to forward packet. The interface with the lower priority is inactive and cannot forward packets.

You cannot assign subinterfaces or interfaces that have subinterfaces to a Reth interface if the Reth interface has Reth subinterfaces.

Do not specify a Reth interface as the outgoing interface in IPv6 static neighbor entries if its member interfaces contain subinterfaces. For more information about IPv6 static neighbor entries, see *Layer 3—IP Services Configuration Guide*.

Examples

Assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to Reth 1, and set their priority to 100 and 50, respectively.

```
<Sysname> system-view
[Sysname] interface reth 1
[Sysname-Reth1] member interface gigabitethernet 1/0/1 priority 100
[Sysname-Reth1] member interface gigabitethernet 1/0/2 priority 50
```

mtu

Use **mtu** to set the MTU of a Reth interface or subinterface.

Use **undo mtu** to restore the default.

Syntax

mtu *size*

undo mtu

Default

The MTU is 1500 bytes for a Reth interface or subinterface.

Views

Reth interface view

Reth subinterface view

Predefined user roles

network-admin

context-admin

Parameters

size: Specifies the MTU in bytes. The value range for this argument is 46 to 8192.

Usage guidelines

The MTU size of a Reth interface or subinterface affects the fragmentation and reassembly of IP packets on the interface or subinterface.

For the configured MTU size to take effect, execute the **shutdown** command, and then the **undo shutdown** command on the interface.

Examples

Set the MTU to 200 bytes for Reth 1.

```
<Sysname> system-view
[Sysname] interface reth 1
[Sysname-Reth1] mtu 200
```

reset counters interface reth

Use **reset counters interface reth** to clear statistics for Reth interfaces or subinterfaces.

Syntax

reset counters interface [**reth** [*interface-number* | *interface-number.subnumber*]]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

interface-number: Specifies a Reth interface by its number.

interface-number.subnumber: Specifies a subinterface of a Reth interface. The *interface-number* argument specifies the main interface number. The *subnumber* argument specifies the subinterface number and is separated from the main interface number by a dot (.).

Usage guidelines

Use this command to clear history statistics before you collect traffic statistics for a time period.

If you do not specify the **reth** keyword, the command clears statistics for all interfaces except for VA interfaces.

If you specify the **reth** keyword but do not specify an interface or subinterface, the command clears statistics for all Reth interfaces and subinterfaces.

If you specify the **reth** *interface-number* option or the **reth** *interface-number.subnumber* option, the command clears statistics for the specified Reth interface or subinterface.

Examples

Clear statistics for Reth 1.

```
<Sysname> reset counters interface reth 1
```

Related commands

display counters interface reth

display counters rate interface reth

display interface reth

reth advertise retransmit

Use **reth advertise retransmit** to set the parameters for retransmitting advertisement messages to neighbors after a Reth member interface switchover.

Use **undo reth advertise retransmit** to restore the default.

Syntax

reth advertise retransmit *times* **interval** *seconds*

undo reth advertise retransmit

Default

After a Reth member interface switchover, a Reth interface retransmits advertisement messages to neighbors five times at an interval of 1 second.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

times: Specifies the number of retransmissions, in the range of 5 to 30.

seconds: Specifies the interval for retransmitting the advertisement messages, in the range of 1 to 10 seconds.

Usage guidelines

After you configure this command, a Reth interface performs the following operations when a Reth member interface switchover occurs on it:

1. Sends advertisement messages (including gratuitous ARP messages and NA messages) to neighbors immediately.
2. Retransmits the advertisement messages according to the number of retransmissions and the retransmission interval you have configured.

If a Reth interface has subinterfaces, the subinterfaces also send advertisement messages upon a Reth member interface switchover. To save CPU resources, this command takes effect only on Reth interfaces. Reth subinterfaces are not controlled by this command.

Examples

Configure Reth interfaces to retransmit advertisement messages to neighbors ten times at an interval of 5 seconds after a Reth member interface switchover.

```
<Sysname> system-view
[Sysname] reth advertise retransmit 10 interval 5
```

shutdown

Use **shutdown** to shut down a Reth interface or subinterface.

Use **undo shutdown** to bring up a Reth interface or subinterface.

Syntax

shutdown

undo shutdown

Default

A Reth interface or subinterface is not manually shut down.

Views

Reth interface view

Reth subinterface view

Predefined user roles

network-admin

context-admin

Usage guidelines

CAUTION:

This command disconnects all links set up on a Reth interface. Make sure you are fully aware of its impacts when you use it on a live network.

Examples

Shut down Reth 1.

```
<Sysname> system-view
```

```
[Sysname] interface reth 1
[Sysname-Reth1] shutdown
```

sub-interface rate-statistic

Use **sub-interface rate-statistic** to enable subinterface rate statistics collection on a Reth interface.

Use **undo sub-interface rate-statistic** to disable subinterface rate statistics collection on a Reth interface.

Syntax

sub-interface rate-statistic

undo sub-interface rate-statistic

Default

Subinterface rate statistics collection is disabled on a Reth interface.

Views

Reth interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

CAUTION:

This command is resource intensive. When you use this command, make sure you fully understand its impact on system performance.

After you execute this command, the device periodically refreshes subinterface rate statistics for the Reth interface. The statistics is displayed in the **Last 300 seconds input rate** and **Last 300 seconds output rate** fields of the command output from the **display interface reth** command.

Examples

Enable subinterface rate statistics collection on Reth 1.

```
<Sysname> system-view
[Sysname] interface reth 1
[Sysname-Reth1] sub-interface rate-statistic
```

Related commands

display interface reth

Redundancy group commands

The following matrixes show the compatibility of hardware and the redundancy group feature:

Models	Redundancy group compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	Yes
NFNX3-HDB680, NFNX3-HDB1080	No

bind slot

Use **bind slot** to bind a redundancy group node to an IRF member device.

Use **undo bind slot** to remove the binding between a redundancy group node and an IRF member device.

Syntax

bind slot *slot-number*

undo bind slot

Default

A redundancy group node is not bound to an IRF member device.

Views

Redundancy group node view

Predefined user roles

network-admin

context-admin

Parameters

slot-number: Specifies an IRF member device by its member ID.

Usage guidelines

You can create only one-to-one bindings between redundancy group nodes and IRF member devices.

The node in a binding can use interfaces of the bound IRF member device as members. Member interfaces on one node of a redundancy group back up the member interfaces on the other node.

You cannot change the binding for a node if the node has member interfaces.

Examples

Bind node 1 in redundancy group **aaa** to IRF member device 1.

```
<Sysname> system-view
[Sysname] redundancy group aaa
[Sysname-redundancy-group-aaa] node 1
[Sysname-redundancy-group-aaa-node1] bind slot 1
```

display redundancy group

Use **display redundancy group** to display redundancy group information.

Syntax

display redundancy group [*group-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

group-name: Specifies a redundancy group by its name, a case-sensitive string of 1 to 15 characters. If you do not specify a redundancy group, this command displays information about all redundancy groups.

Examples

Display information about redundancy group **aaa**.

```
<Sysname> display redundancy group aaa
Redundancy group aaa (ID 1):
  Node ID      Slot        Priority   Status           Track weight
  1            Slot1       100        Secondary        -255
  2            Slot2       99         Primary          255

Preempt delay time remained   : 0    min
Preempt delay timer setting   : 1    min
Remaining hold-down time      : 0    sec
Hold-down timer setting       : 300  sec
Manual switchover request     : No

Member interfaces:
    Reth1          Reth2

Node 1:
  Node member     Physical status
    GE1/0/2       DOWN
    GE1/0/4       DOWN(redundancy down)
  Track info:
    Track    Status               Reduced weight     Interface
    1        Negative(Faulty)     255                GE1/0/2
    2        Negative             255                GE1/0/4
Node 2:
  Node member    Physical status
    GE2/0/2      UP
    GE2/0/4      UP
```

```
Track info:
  Track    Status       Reduced weight     Interface
  3        Positive     55                 GE2/0/2
  4        Positive     55                 GE2/0/4
```

Table 6 Command output

Field	Description
Priority	Priority of the node.
Status	Node status: • **Primary**—The primary node. It can forward packets. • **Secondary**—The secondary node. When the high-priority node acts as the secondary node, all its member interfaces are shut down by the Reth module and cannot forward packets. When the low-priority node acts as the secondary node, all its member interfaces can forward packets.
Track weight	Weight of the node.
Preempt delay time remained	Remaining preemption delay time in minutes.
Preempt delay timer setting	Configured preemption delay timer in minutes.
Remaining hold-down time	Remaining hold-down time in seconds.
Hold-down timer setting	Configured hold-down timer in seconds.
Manual switchover request	Manual switchover request: • **Yes**—A request is issued. • **No**—No request is issued.
Member interfaces	Reth interfaces in the redundancy group.
Node 1	Detailed information about the redundancy group node.
Node member	Member interfaces on the redundancy group node.
Physical status	Physical status of the member interfaces on the node: • **Down (redundancy down)**—The interface is shut down by the Reth module. • **Down**—The interface is administratively up but physically down possibly because no physical link is present or the link has failed. • **UP**—The interface is both administratively and physically up.
Track info	Information about the track entries associated with the node.
Track	Track entry number.
Status	Track entry status. For the high-priority node, the first track entry that changed to **NotReady** or **Negative** state is identified as **Faulty**.
Reduced weight	Weight decrement rate of the node.
Interface	The interface excluded from the shutdown action by the Reth module. **Absent** indicates that the interface does not exist.

hold-down-interval

Use **`hold-down-interval`** to set the hold-down timer for a redundancy group.

Use **undo hold-down-interval** to restore the default.

Syntax

hold-down-interval *second*

undo hold-down-interval

Default

The hold-down timer is 1 second for a redundancy group.

Views

Redundancy group view

Predefined user roles

network-admin

context-admin

Parameters

second: Specifies the hold-down timer in the range of 0 to 1800 seconds.

Usage guidelines

Set the hold-down timer to prevent frequent switchovers. The hold-down timer specifies the minimum interval between two switchovers. This timer starts when a switchover is finished. The redundancy group can perform another switchover only after the hold-down timer expires.

Examples

Set the hold-down timer to 300 seconds for redundancy group **aaa**.

```
<Sysname> system-view
[Sysname] redundancy group aaa
[Sysname-redundancy-group-aaa] hold-down-interval 300
```

member interface

Use **member interface** to assign a Reth interface to a redundancy group.

Use **undo member interface** to remove a Reth interface from a redundancy group.

Syntax

member interface reth *interface-number* [**quick-fallback**]

undo member interface reth *interface-number*

Default

A redundancy group does not contain Reth interfaces.

Views

Redundancy group view

Predefined user roles

network-admin

context-admin

Parameters

reth *interface-number*: Specifies a Reth interface by its number. The Reth interface must exist.

quick-fallback: Enables quick fallback for the Reth interface. If quick fallback is enabled on a Reth interface, the physical state and protocol state of the higher-priority member interface are not set to down when it becomes inactive. When this feature is disabled on a Reth interface, both the physical state and protocol state of the inactive member interface are set to down. As a best practice, enable this feature if the preemption delay timer is set in seconds.

Usage guidelines

You can assign a Reth interface to only one redundancy group.

A redundancy group can contain a maximum of 32 Reth interfaces.

Examples

Assign Reth 1 to redundancy group **aaa**.

```
<Sysname> system-view
[Sysname] redundancy group aaa
[Sysname-redundancy-group-aaa] member interface reth 1
```

node

Use **node** to create a redundancy group node and enter its view, or enter the view of an existing redundancy group node.

Use **undo node** to remove a redundancy group node.

Syntax

node *node-id*

undo node *node-id*

Default

No redundancy group nodes exist.

Views

Redundancy group view

Predefined user roles

network-admin

context-admin

Parameters

node-id: Specifies a redundancy group node ID in the range of 1 to 2.

Usage guidelines

You can create a maximum of two nodes for a redundancy group. One is the primary node, and the other is the secondary node.

Before you delete a redundancy group node, you must remove the binding between the node and its IRF member device.

Examples

Create node 1 for redundancy group **aaa**.

```
<Sysname> system-view
[Sysname] redundancy group aaa
[Sysname-redundancy-group-aaa] node 1
```

Related commands

bind slot

node-member interface

Use **node-member interface** to assign a physical Ethernet interface to a redundancy group node.

Use **undo node-member interface** to remove a physical Ethernet interface from a redundancy group node.

Syntax

node-member interface *interface-type interface-number*

undo node-member interface *interface-type interface-number*

Default

A redundancy group node does not have member interfaces.

Views

Redundancy group node view

Predefined user roles

network-admin

context-admin

Parameters

interface-type interface-number: Specifies a physical interface by its type and number. The interface must belong to the IRF member device that is bound to the node.

Usage guidelines

Before you assign physical Ethernet interfaces to a redundancy group node, you must use the **bind slot** command to bind the node to an IRF member device.

The physical Ethernet interfaces cannot be members of Reth interfaces.

An interface can be assigned to only one redundancy group node.

Examples

Assign GigabitEthernet 1/0/1 to node 1 of redundancy group **aaa**.

```
<Sysname> system-view
[Sysname] redundancy group aaa
[Sysname-redundancy-group-aaa] node 1
[Sysname-redundancy-group-aaa-node1]node-member interface gigabitethernet 1/0/1
```

Related commands

bind slot

preempt-delay

Use **preempt-delay** to set the preemption delay timer for a redundancy group.

Use **undo preempt-delay** to restore the default.

Syntax

preempt-delay seconds *sec*

undo preempt-delay

Default

The preemption delay timer is 1 minute (60 seconds) for a redundancy group.

Views

Redundancy group view

Predefined user roles

network-admin

context-admin

Parameters

seconds *sec*: Specifies the preemption delay timer in the range of 0 to 720 seconds.

Usage guidelines

The preemption delay timer specifies the delay before a switchover to the high-priority node occurs after the switchover is triggered. The delay allows the system to process events (such as interface state changes) required for the switchover.

If you set the preemption delay timer to 0, automatic switchover to the high-priority node is disabled. You can perform only manual switchover.

Examples

Set the preemption delay timer to 120 seconds for redundancy group **aaa**.

```
<Sysname> system-view
[Sysname] redundancy group aaa
[Sysname-redundancy-group-aaa] preempt-delay seconds 120
```

priority

Use **priority** to set the priority of a redundancy group node.

Use **undo priority** to restore the default.

Syntax

priority *priority*

undo priority

Default

The priority of a redundancy group node is 1.

Views

Redundancy group node view

Predefined user roles

network-admin

context-admin

Parameters

priority: Specifies the priority in the range of 1 to 255. The higher the value, the higher the priority.

Usage guidelines

By default, the high-priority node is the primary node, and the low-priority node is the secondary node. If both nodes have the same priority, the lower-numbered node is the primary node.

Examples

Set the priority to 3 for node 1 of redundancy group **aaa**.

```
<Sysname> system-view
[Sysname] redundancy group aaa
[Sysname-redundancy-group-aaa] node 1
[Sysname-redundancy-group-aaa-node1] priority 3
```

redundancy group

Use **redundancy group** to create a redundancy group and enter its view, or enter the view of an existing redundancy group.

Use **undo redundancy group** to remove a redundancy group.

Syntax

redundancy group *group-name*

undo redundancy group *group-name*

Default

No redundancy groups exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a redundancy group name, a case-sensitive string of 1 to 15 characters.

Usage guidelines

Before you delete a redundancy group, make sure all its Reth interfaces and nodes are removed.

Examples

Create redundancy group **aaa** and enter its view.

```
<Sysname> system-view
[Sysname] redundancy group aaa
```

snmp-agent trap enable rddc

Use **snmp-agent trap enable rddc** to enable SNMP notifications for redundancy groups.

Use **undo snmp-agent trap enable rddc** to disable SNMP notifications for redundancy groups.

Syntax

snmp-agent trap enable rddc

undo snmp-agent trap enable rddc

Default

SNMP notifications are enabled for redundancy groups.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command enables SNMP notifications for the following events:

- A manual switchover is performed.
- An interface goes down.
- A faulty interface is recovered.

For redundancy group event notifications to be sent correctly, you must also configure SNMP on the device. For more information about SNMP configuration, see the network management and monitoring configuration guide for the device.

Examples

Enable SNMP notifications for redundancy groups.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable rddc
```

switchover request

Use **switchover request** to request a switchover to the low-priority node.

Syntax

switchover request

Views

Redundancy group view

Predefined user roles

network-admin

context-admin

Usage guidelines

Use this command to request a switchover to the low-priority node when both of the redundancy group nodes are operating correctly. This command can be used in scenarios where component replacement is required for the high-priority node.

Examples

Request a switchover to the low-priority node for redundancy group **aaa**.

```
<Sysname> system-view
[Sysname] redundancy group aaa
[Sysname-redundancy-group-aaa] switchover request
```

Related commands

switchover reset

switchover reset

Use **switchover reset** to request a switchover to the high-priority node.

Syntax

switchover reset

Views

Redundancy group view

Predefined user roles

network-admin

context-admin

Usage guidelines

Use this command to request a switchover to the high-priority node when both of the redundancy group nodes are operating correctly.

Examples

Request a switchover to the high-priority node for redundancy group **aaa**.

```
<Sysname> system-view
[Sysname] redundancy group aaa
[Sysname-redundancy-group-aaa] switchover reset
```

Related commands

preempt-delay

switchover request

track

Use **track** to associate a track entry with a redundancy group node.

Use **undo track** to remove the association between a track entry and a redundancy group node.

Syntax

track *track-entry-number* [**reduced** *weight-reduced*] [**interface** *interface-type interface-number*]

undo track *track-entry-number*

Default

A redundancy group node is not associated with track entries.

Views

Redundancy group node view

Predefined user roles

network-admin

context-admin

Parameters

track-entry-number: Specifies a track entry by its number in the range of 1 to 1024.

reduced *weight-reduced*: Specifies the weight decrement rate in the range of 1 to 255. The default is 255.

interface *interface-type interface-number*: Specifies an interface by its type and number. The interface will be excluded from the shutdown action by the Reth module. If you do not specify this option, no interface is excluded from the shutdown action by the Reth module. You must specify the tracked interface for this option if the interface has one of the following roles:

- Member of the redundancy group.
- Member of a Reth interface in the redundancy group.

Usage guidelines

You can associate a maximum of 64 track entries with a redundancy group node.

As a best practice, associate a redundancy group node with an existing track entry. If the track entry does not exist, a switchover might occur.

Do not exclude a subinterface from the shutdown action if both the subinterface and its main interface have one of the following roles on the high-priority node:

- Member of the redundancy group.
- Member of a Reth interface in the redundancy group.

When the Reth module shuts down the main interface, the subinterface is also shut down. The shutdown subinterface cannot recover automatically to trigger an automatic switchover.

Examples

Associate track entries 1 and 2 with redundancy group node 1. Exclude GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 from the shutdown action by the Reth module.

```
<Sysname> system-view
[Sysname] track 1 interface gigabitethernet 1/0/1
[Sysname] track 2 interface gigabitethernet 1/0/2
[Sysname] redundancy group aaa
[Sysname-redundancy-group-aaa] node 1
[Sysname-redundancy-group-aaa-node1] track 1 reduced 50 interface gigabitethernet 1/0/1
[Sysname-redundancy-group-aaa-node1] track 2 reduced 50 interface gigabitethernet 1/0/2
```

NSFOCUS Firewall Series

NF Security Command Reference

NSFOCUS Technologies, Inc.

Document version: 6W600-20230221

Preface

This command reference describes the commands for configuring security features, including:

This preface includes the following topics about the documentation:

- Audience.
- Conventions.

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators.

Conventions

The following information describes the conventions used in the documentation.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select a minimum of one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
CAUTION:	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Contents

Security zone commands

display security-zone

Use **display security-zone** to display security zone information.

Syntax

display security-zone [**name** *zone-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

name *zone-name*: Specifies the security zone name, a case-insensitive string of 1 to 31 characters. If you do not specify this option, the command displays all security zones, including system-defined and user-defined security zones.

Usage guidelines

When displaying all security zones, the command uses the following order:

1. System-defined security zones.
2. User-defined security zones in alphabetical order of security zone names.

Examples

Display information about security zone **myZone**.

```
<Sysname> display security-zone name myZone
Name: myZone
Members:
  GigabitEthernet1/0/1
  GigabitEthernet1/0/2 in VLAN 3
  VLAN 150-200
  192.168.1.0 255.255.255.0
  192.168.0.0 255.255.0.0 vpn-instance abc
  1001:1002::0 32
```

Table 1 Command output

Field	Description
Name	Security zone name.

Field	Description
Members	Members in the security zone: • Type and number of a Layer 3 interface. • Type and number of a Layer 2 Ethernet interface, and IDs of the VLANs to which the interface belongs. • VLAN IDs. • Address and mask (or mask length) of an IPv4 subnet on the public network. • Address and prefix length of an IPv6 subnet on the public network. • Address, mask (or mask length), and VPN instance name of an IPv4 subnet on a VPN. • Address, prefix length, and VPN instance name of an IPv6 subnet on a VPN. If a security zone does not have members, this field displays **None**.

display zone-pair security

Use **display zone-pair security** to display all zone pairs.

Syntax

display zone-pair security

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display all zone pairs.

```
<Sysname> display zone-pair security
Source zone   Destination zone
DMZ           Local
Trust         Local
```

import interface

Use **import interface** to add a Layer 3 interfaces to a security zone.

Use **undo import interface** to remove Layer 3 interfaces from a security zone.

Syntax

import interface *layer3-interface-type layer3-interface-number*

undo import interface *layer3-interface-type layer3-interface-number*

Default

A security zone does not have Layer 3 interface members.

Views

Security zone view

Predefined user roles

network-admin

context-admin

Parameters

interface *layer3-interface-type layer3-interface-number*: Specifies a Layer 3 interface by its type and number. Layer 3 interfaces include Layer 3 Ethernet interfaces, Layer 3 Ethernet subinterfaces, and other types of Layer 3 logical interfaces.

Usage guidelines

You cannot add a member to the system-defined security zone **Local**. You can add members to the other system-defined security zones.

To add multiple Layer 3 interfaces to a security zone, execute this command multiple times.

A Layer 3 interface can belong to only one security zone. To move a Layer 3 interface from one security zone to another security zone, perform the following tasks:

1. Use the **undo import interface** command to remove the interface from the current security zone.
2. Use the **import interface** command to add the interface to the new security zone.

Examples

Add Layer 3 Ethernet interface GigabitEthernet 1/0/1 to security zone **Trust**.

```
<Sysname> system-view
[Sysname] security-zone name trust
[Sysname-security-zone-Trust] import interface gigabitethernet 1/0/1
```

import interface vlan

Use **import interface vlan** to add Layer 2 interface-VLAN combinations to a security zone.

Use **undo import interface vlan** to remove Layer 2 interface-VLAN combinations from a security zone .

Syntax

import interface *layer2-interface-type layer2-interface-number* **vlan** *vlan-list*

undo import interface *layer2-interface-type layer2-interface-number* **vlan** *vlan-list*

Default

A security zone does not have Layer 2 interface-VLAN combination members.

Views

Security zone view

Predefined user roles

network-admin

context-admin

Parameters

interface *layer2-interface-type layer2-interface-number*: Specifies a Layer 2 interface by its type and number.

vlan *vlan-list*: Specifies a list of VLANs. The *vlan-list* argument must be a space-separated list of up to 10 VLAN items that meet the following requirements:

- Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-VLAN-ID* **to** *end-VLAN-ID*. The *end-VLAN-ID* is greater than the *start-VLAN-ID*.
- The VLAN IDs are in the range of 1 to 4094.
- The VLANs already exist.

Usage guidelines

You cannot add a member to the system-defined security zone **Local**. You can add members to the other system-defined security zones.

To add multiple Layer 2 Ethernet interface-VLAN combinations to a security zone, execute this command multiple times.

A Layer 2 interface-VLAN combination can belong to only one security zone. To move a Layer 2 interface-VLAN combination from one security zone to another security zone, perform the following tasks:

1. Use the **undo import interface vlan** command to remove the combination from the current security zone.
2. Use the **import interface vlan** command to add the combination to the new security zone.

Examples

Add the combination of Layer 2 Ethernet interface GigabitEthernet 1/0/1 and VLAN 10 to security zone **Untrust**.

```
<Sysname> system-view
[Sysname] security-zone name untrust
[Sysname-security-zone-Untrust] import interface gigabitethernet 1/0/1 vlan 10
```

import ip

Use **import ip** to add an IPv4 subnet to a security zone.

Use **undo import ip** to remove an IPv4 subnet from a security zone.

Syntax

import ip *ip-address* { *mask-length* | *mask* } [**vpn-instance** *vpn-instance-name*]

undo import ip *ip-address* { *mask-length* | *mask* } [**vpn-instance** *vpn-instance-name*]

Default

A security zone does not have IPv4 subnet members.

Views

Security zone view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies an IPv4 subnet by its subnet address or a host address on the subnet.

mask-length: Specifies the mask length in the range of 0 to 32.

mask: Specifies the subnet mask in dotted decimal notation.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN to which the subnet belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the subnet resides on the public network, do not specify this option. As a best practice, specify an existing VPN instance. If you specify a non-existent VPN instance, this command will be successfully executed but will not take effect. Additionally, this command will get lost after the device restarts.

Usage guidelines

You cannot add a member to the system-defined security zone **Local**. You can add members to the other system-defined security zones.

To add multiple IPv4 subnets to a security zone, execute this command multiple times.

A subnet can be added to only one security zone.

If one subnet includes another subnet, the system identifies them as different subnets. You can add them to the same security zone or different security zones. If you add them to different security zones, packets that match both subnets are identified as packets of the security zone to which the smaller subnet belongs. For example, you can assign 1.1.1.1/24 and 1.1.2.2/16 to different security zones. A packet with the IP address 1.1.1.3 is identified as a packet of the security zone to which 1.1.1.1/24 belongs.

For a dynamic routing protocol to operate correctly, add the multicast and broadcast addresses used by the protocol to security zones as needed.

Examples

Add the 192.168.1.0/24 subnet to security zone **a**.

```
<Sysname> system-view
[Sysname] security-zone name a
[Sysname-security-zone-a] import ip 192.168.1.0 24
```

Add the subnet that is identified by the address 192.168.2.1 and mask 255.255.255.0 to security zone **a**.

```
<Sysname> system-view
[Sysname] security-zone name a
[Sysname-security-zone-a] import ip 192.168.2.1 255.255.255.0
```

Add the subnet that is identified by the address 192.168.2.1 and mask 255.255.255.0 on VPN **abc** to the security zone **a**.

```
<Sysname> system-view
[Sysname] security-zone name a
[Sysname-security-zone-a] import ip 192.168.2.1 255.255.255.0 vpn-instance abc
```

import ipv6

Use **import ipv6** to add an IPv6 subnet to a security zone.

Use **undo import ipv6** to remove an IPv6 subnet from a security zone.

Syntax

import ipv6 *ipv6-address prefix-length* [**vpn-instance** *vpn-instance-name*]

undo import ipv6 *ipv6-address prefix-length* [**vpn-instance** *vpn-instance-name*]

Default

A security zone does not have IPv6 subnet members.

Views

Security zone view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies an IPv6 subnet by its subnet address or a host address on the subnet.

prefix-length: Specifies the prefix length in the range of 1 to 128.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN to which the subnet belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the subnet resides on the public network, do not specify this option. As a best practice, specify an existing VPN instance. If you specify a non-existent VPN instance, this command will be successfully executed but will not take effect. Additionally, this command will get lost after the device restarts.

Usage guidelines

You cannot add a member to the system-defined security zone **Local**. You can add members to the other system-defined security zones.

To add multiple IPv6 subnets to a security zone, execute this command multiple times.

A subnet can be added to only one security zone.

If one subnet includes another subnet, the system identifies them as different subnets. You can add them to the same security zone or different security zones. If you add them to different security zones, packets that match both subnets are identified as packets of the security zone to which the smaller subnet belongs. For example, you can assign 1:1:1::0/48 and 1:1:1::0/32 to different security zones. A packet with the address 1:1:1::2 is identified as a packet of the security zone to which 1:1:1::0/48 belongs.

Examples

Add IPv6 subnet 1001:1002::0/32 (on the public network) to security zone **a**.

```
<Sysname> system-view
[Sysname] security-zone name a
[Sysname-security-zone-a] import ipv6 1001:1002::1 32
```

Add IPv6 subnet 1001:1002::0/32 (on VPN **abc**) to security zone **a**.

```
<Sysname> system-view
[Sysname] security-zone name a
[Sysname-security-zone-a] import ipv6 1001:1002::1 32 vpn-instance abc
```

import vlan

Use **import vlan** to add VLANs to a security zone.

Use **undo import vlan** to remove VLANs from a security zone.

Syntax

import vlan *vlan-list*

undo import vlan *vlan-list*

Default

A security zone does not have VLAN members.

Views

Security zone view

Predefined user roles

network-admin

context-admin

Parameters

vlan *vlan-list*: Specifies a list of VLANs. The *vlan-list* argument must be a space-separated list of up to 10 VLAN items that meet the following requirements:

- Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-VLAN-ID* **to** *end-VLAN-ID*. The *end-VLAN-ID* is greater than the *start-VLAN-ID*.
- The VLAN IDs are in the range of 1 to 4094.
- The VLANs already exist.

Usage guidelines

You cannot add a member to system-defined security zone **Local**. You can add members to the other system-defined security zones.

To add multiple VLANs to a security zone, specify multiple VLANs for this command or execute this command multiple times.

A VLAN can belong to only one security zone. To move a VLAN from one security zone to another security zone, perform the following tasks:

1. Use the **undo import vlan** command to remove the VLAN from the current security zone.
2. Use the **import vlan** command to add the VLAN to the new security zone.

This command requires the cooperation of inter-VLAN bridge forwarding. After adding VLANs to a security zone, you must create an inter-VLAN bridge instance and add the VLANs to the bridge instance. For more information, see Layer 2 forwarding configuration in *Layer 2—LAN Switching Configuration Guide*.

Examples

Add VLAN 3, and VLAN 5 through VLAN 7 to security zone **trust**.

```
<Sysname> system-view
[Sysname] security-zone name trust
[Sysname-security-zone-Trust] import vlan 3 5 to 7
```

manage

Use **manage** to specify a permitted protocol on an interface.

Use **undo manage** to remove a permitted protocol.

Syntax

manage { { **http** | **https** | **ping** | **ssh** | **telnet** } { **inbound** | **outbound** } | { **netconf-http** | **netconf-https** | **netconf-ssh** | **snmp** } **inbound** }

undo manage { { **http** | **https** | **ping** | **ssh** | **telnet** } { **inbound** | **outbound** } | { **netconf-http** | **netconf-https** | **netconf-ssh** | **snmp** } **inbound** }

Default

The device permits packets only from other devices that are connected through interfaces in security zone **Management**.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

`http`: Specifies the HTTP protocol.

`https`: Specifies the HTTPS protocol.

`netconf-http`: Specifies the NETCONF over SOAP over HTTP protocol.

`netconf-https`: Specifies the NETCONF over SOAP over HTTPS protocol.

`netconf-ssh`: Specifies the NETCONF over SSH protocol.

`ping`: Specifies the Ping protocol.

`snmp`: Specifies the SNMP protocol.

`ssh`: Specifies the SSH protocol.

`telnet`: Specifies the Telnet protocol.

`inbound`: Permits incoming packets of the specified protocol.

`outbound`: Permits outgoing packets of the specified protocol.

Usage guidelines

After you specify a permitted protocol on an interface, the device will permit packets of the specified protocol from the device that is connected to the interface. The packets will not be limited based on security policies or traffic policies.

You can configure this command multiple times to specify multiple permitted protocols.

Examples

Specify HTTP and HTTPS as permitted protocols on GigabitEthernet1/0/1.

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] manage http inbound
[Sysname-GigabitEthernet1/0/1] manage https inbound
```

security-zone

Use **`security-zone`** to create a security zone and enter its view, or enter the view of an existing security zone.

Use **`undo security-zone`** to delete a security zone.

Syntax

`security-zone name` *`zone-name`*

`undo security-zone name` *`zone-name`*

Default

By default, the device has the following security zones: Local, Trust, DMZ, Management, and Untrust.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

name *zone-name*: Specifies the security zone name, a case-insensitive string of 1 to 31 characters. It cannot be **any**. To include a backward slash (\) or quotation mark (") in the security zone name, you must use the escape character (\).

Usage guidelines

The device provides the following system-defined security zones: **Local**, **Trust**, **DMZ**, **Management**, and **Untrust**. The system creates these security zones automatically when one of following events occurs:

- The first command for creating a security zone is executed.
- The first command related to creating an interzone policy is executed.

System-defined security zones cannot be deleted.

You can use this command multiple times to create multiple security zones.

Deleting a security zone also deletes the following items:

- All zone pairs that use the security zone as the source or destination security zone.
- All interzone policy applications on the zone pairs.

Examples

Create a security zone named **zonetest** and enter security zone view.

```
<Sysname> system-view
[Sysname] security-zone name zonetest
[Sysname-security-zone-zonetest]
```

Related commands

display security-zone

security-zone intra-zone default permit

Use **security-zone intra-zone default permit** to set the default action to **permit** for packets exchanged between interfaces in the same security zone.

Use **undo security-zone intra-zone default permit** to set the default action to **deny** for packets exchanged between interfaces in the same security zone.

Syntax

security-zone intra-zone default permit

undo security-zone intra-zone default permit

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	No

Default

The default action is **deny** for packets exchanged between interfaces in the same security zone.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

The system uses the default action for packets that are exchanged between interfaces in the same security zone in the following situations:

- A zone pair from the security zone to the security zone itself is not configured.
- A zone pair from the security zone to the security zone itself is configured, but no interzone policy is applied to the zone pair.

Examples

Set the default action to **permit** for packets exchanged between interfaces in the same security zone.

```
<Sysname> system-view
[Sysname] security-zone intra-zone default permit
```

zone-pair security

Use **zone-pair security** to create a zone pair and enter its view, or enter the view of an existing zone pair.

Use **undo zone-pair security** to delete a zone pair.

Syntax

zone-pair security source { *source-zone-name* | **any** } **destination** { *destination-zone-name* | **any** }

undo zone-pair security source { *source-zone-name* | **any** } **destination** { *destination-zone-name* | **any** }

Default

No zone pair exists.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

source *source-zone-name*: Specifies the name of the source security zone, a case-insensitive string of 1 to 31 characters. This security zone must already exist.

destination *destination-zone-name*: Specifies the name of the destination security zone, a case-insensitive string of 1 to 31 characters. This security zone must already exist.

any: Specifies any security zone.

Usage guidelines

A zone pair has a source security zone and a destination security zone. The device examines received first data packets and uses zone pairs to identify data flows. You can apply interzone policies to zone pairs so the device processes data flows based on interzone policies.

You can use the **zone-pair security source any destination any** command to define the any-to-any zone pair. This zone pair matches all packets from one security zone to another security zone.

A zone pair between specific security zones has a higher priority than the any-to-any zone pair.

A packet between the **Management** and **Local** zones matches only zone pairs of the two zones. It does not match the any-to-any zone pair.

Deleting a zone pair deletes all interzone policy applications on the zone pair.

Examples

Create a zone pair with the source security zone **Trust** and destination zone **Untrust**.

```
<Sysname> system-view
[Sysname] zone-pair security source trust destination untrust
[Sysname-zone-pair-security-Trust-Untrust]
```

Related commands

display zone-pair security

zone-pair vsip-filter enable

Use **zone-pair vsip-filter enable** to enable filtering based on virtual service IP address for zone pairs.

Use **undo zone-pair vsip-filter enable** to restore the default.

Syntax

zone-pair vsip-filter enable

undo zone-pair vsip-filter enable

Default

Filtering based on virtual service IP address is disabled for zone pairs.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

In scenarios where server load balancing is deployed, configure this command to enable the device to filter packets from external networks to internal servers by virtual service IP address. By default, filtering based on virtual service IP address is disabled. Before matching each of the packets against ACLs, the device translates the destination IP address (the virtual service IP address) to the real server IP address. For more information about packet filtering, see ACL configuration in *ACL and QoS Configuration Guide*.

Examples

Configure an IPv4 advanced ACL to permit packets destined for virtual server IP address 10.10.10.10. Configure a zone pair from **Untrust** to **DMZ**, apply the ACL to the zone pair, and enable filtering based on virtual service IP address.

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule permit ip source any destination 10.10.10.10 0
[Sysname-acl-ipv4-adv-3000] quit
[Sysname] zone-pair security source untrust destination dmz
[Sysname-zone-pair-security-Untrust-DMZ] packet-filter 3000
[Sysname-zone-pair-security-Untrust-DMZ] quit
[Sysname] zone-pair vsip-filter enable
```

Contents

Security policy commands

accelerate enhanced enable

Use **accelerate enhanced enable** to manually activate rule matching acceleration.

Syntax

accelerate enhanced enable

Views

IPv4 security policy view

IPv6 security policy view

Predefined user roles

network-admin

context-admin

Usage guidelines

Rule matching acceleration enhances connection establishment and packet forwarding performance, especially for a device using multiple rules to match packets from multiple users.

Rule matching acceleration does not take effect on newly added, modified, and moved rules unless the feature is activated for the rules. By default, the system automatically activates rule matching acceleration for such rules at specific intervals. The interval is 2 seconds if 100 or fewer rules exist and 20 seconds if over 100 rules exist.

To activate rule matching acceleration immediately after a rule change, you can execute this command.

If no rule change is detected, the system does not perform an activation operation.

Insufficient memory can cause rule matching acceleration failures. Unaccelerated rules do not take effect, and rules that have been accelerated are not affected.

Examples

Activate rule matching acceleration.

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] accelerate enhanced enable
```

action

Use **action** to set the action for a security policy rule.

Use **undo action** to restore the default.

Syntax

action { **drop** | **pass** }

undo action pass

Default

The action for a security policy rule is **drop**.

Views

Security policy rule view

Predefined user roles

network-admin

context-admin

Parameters

drop: Discards matched packets.

pass: Allows matched packets to pass.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the action for security policy rule **rule1** to **drop**.

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1] action drop
```

Related commands

display security-policy

app-group

Use **app-group** to specify an application group as a filtering criterion of a security policy rule.

Use **undo app-group** to remove the specified application group filtering criterion from a security policy rule.

Syntax

app-group *app-group-name*

undo app-group [*app-group-name*]

Default

No application group is specified as a filtering criterion for a security policy rule.

Views

Security policy rule view

Predefined user roles

network-admin

context-admin

Parameters

app-group-name: Specifies the name of an application policy, a case-insensitive string of 1 to 63 characters. The name cannot be **invalid** or **other**. If you do not specify this argument when executing the **undo app-group** command, the command removes all application groups from the rule. For more information about application groups, see APR in *Security Configuration Guide*.

Usage guidelines

You can execute the command multiple times to specify multiple application groups as the filtering criteria.

Examples

Specify application groups **app1** and **app2** as the filtering criteria of security policy rule **rule1**.

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1] app-group app1
[Sysname-security-policy-ip-0-rule1] app-group app2
```

Related commands

app-group

display security-policy

application

Use **application** to specify an application as a filtering criterion of a security policy rule.

Use **undo application** to remove the specified application filtering criterion from a security policy rule.

Syntax

application *application-name*

undo application [*application-name*]

Default

No application is specified as a filtering criterion for a security policy rule.

Views

Security policy rule view

Predefined user roles

network-admin

context-admin

Parameters

application-name: Specifies the name of an application, a case-insensitive string of 1 to 63 characters. The name cannot be **invalid** or **other**. If you do not specify this argument when executing the **undo application** command, the command removes all applications from the rule. For more information about applications, see APR in *Security Configuration Guide*.

Usage guidelines

You can execute the command multiple times to specify multiple applications as the filtering criteria.

For the application filtering criteria to be identified, you must permit the packets of the protocols on which the applications depend to pass through. If port-based packet filtering is configured and a dependent protocol uses a non-default port, you must permit the packets from the port to pass.

Examples

Specify applications **139Mail** and **51job** as the filtering criteria of security policy rule **rule1**.

```
<Sysname> system-view
[Sysname] security-policy ip
```

```
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1] application 139Mail
[Sysname-security-policy-ip-0-rule1] application 51job
```

Related commands

display security-policy

nbar application

port-mapping

counting enable

Use **counting enable** to enable statistics collection for matched packets.

Use **undo counting enable** to disable statistics collection for matched packets.

Syntax

counting enable [**period** *value*]

undo counting enable

Default

Statistics collection for matched packets is disabled.

Views

Security policy rule view

Predefined user roles

network-admin

context-admin

Parameters

period *value*: Specifies the period during which the statistics collection feature is enabled, in the range of 1 to 4294967295 minutes. If you do not specify this option, the command enables statistics collection permanently.

Usage guidelines

This feature enables the device to collect statistics about matched packets. The collected statistics can be viewed by executing the **display security-policy statistics** command.

If an enabling period is specified, the system disables the statistics collection feature and removes the configuration at period expiration. If no enabling period is specified, you must execute the **undo** command to disable the statistics collection feature.

Examples

Enable matched packet statistics collection for security policy rule **rule1** and set the enabling period to 20 minutes.

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1] counting enable period 20
```

Related commands

display security-policy

display security-policy statistics

description (security policy rule view)

Use **description** to configure a description for a security policy rule.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

No description is configured for a security policy rule.

Views

Security policy rule view

Predefined user roles

network-admin

context-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 127 characters.

Examples

Configure the description as **This rule is used for source-ip ip1** for security policy rule **rule1**.

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1] description This rule is used for source-ip ip1
```

Related commands

display object-policy ip

display object-policy ipv6

description (security policy view)

Use **description** to configure a description for the IPv4 or IPv6 security policy.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

No description is configured for the IPv4 or IPv6 security policy.

Views

IPv4 security policy view

IPv6 security policy view

Predefined user roles

network-admin

context-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 127 characters.

Examples

Configure the description as **zone-pair security office to library** for the IPv4 security policy.

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] description zone-pair security office to library
```

Related commands

display security-policy

destination-ip

Use **destination-ip** to specify a destination IP address object group as a filtering criterion of a security policy rule.

Use **undo destination-ip** to remove the specified destination IP address object group from a security policy rule.

Syntax

destination-ip *object-group-name*

undo destination-ip [*object-group-name*]

Default

No destination IP address object group is specified as a filtering criterion for a security policy rule.

Views

Security policy rule view

Predefined user roles

network-admin

context-admin

Parameters

object-group-name: Specifies the name of a destination IP address object group, a case-insensitive string of 1 to 63 characters. The name cannot be **any**. If you do not specify this argument when executing the **undo destination-ip** command, the command removes all destination IP address object groups from the rule. For more information about object groups, see *Security Configuration Guide*.

Usage guidelines

You can execute the command multiple times to specify multiple destination IP address object groups as the filtering criteria.

If you specify a nonexistent object group, the device automatically creates the specified object group with empty configuration. A rule that contains an object group with empty configuration does not match any packets.

For a security policy rule, the number of configured destination IP addresses cannot exceed 1024. If the limit has been reached, any command execution to add such a filtering criterion fails and the system prompts an error.

Examples

Specify destination IP address object groups **client1** and **client2** as the filtering criteria of security policy rule **rule1**.

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1] destination-ip client1
[Sysname-security-policy-ip-0-rule1] destination-ip client2
```

Related commands

display security-policy

object-group

destination-ip-host (IPv4 security policy view)

Use **destination-ip-host** to specify a destination IPv4 host address as a filtering criterion of a security policy rule.

Use **undo destination-ip-host** to remove the specified destination IPv4 host address from a security policy rule.

Syntax

destination-ip-host *ip-address*

undo destination-ip-host [*ip-address*]

Default

No destination IPv4 host address is specified as a filtering criterion for a security policy rule.

Views

IPv4 security policy rule view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the IPv4 address of a host. If you do not specify this argument when executing the **undo** command, the command removes all destination IPv4 host addresses from the rule.

Usage guidelines

You can execute the command multiple times to specify multiple destination IPv4 host addresses as the filtering criteria.

If you specify an IP address that has been configured as a destination host filtering criterion, the command execution fails and the system prompts an error.

For a security policy rule, the sum of configured destination host addresses, destination subnets, and destination address ranges cannot exceed 1024. If the limit has been reached, any command execution to add such a filtering criterion fails and the system prompts an error.

Examples

Specify destination IPv4 host address **192.167.0.1** as the filtering criteria of IPv4 security policy rule **rule1**.

```
<Sysname> system-view
```

```
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1] destination-ip-host 192.167.0.1
```

Related commands

display security-policy

destination-ip-host (IPv6 security policy view)

Use **destination-ip-host** to specify a destination IPv6 host address as a filtering criterion of a security policy rule.

Use **undo destination-ip-host** to remove the specified destination IPv6 host address from a security policy rule.

Syntax

destination-ip-host *ipv6-address*

undo destination-ip-host [*ipv6-address*]

Default

No destination IPv6 host address is specified as a filtering criterion for a security policy rule.

Views

IPv6 security policy rule view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address: Specifies the IPv6 address of a host. If you do not specify this argument when executing the **undo** command, the command removes all destination IPv6 host addresses from the rule.

Usage guidelines

You can execute the command multiple times to specify multiple destination IPv6 host addresses as the filtering criteria.

If you specify an IP address that has been configured as a destination host filtering criterion, the command execution fails and the system prompts an error.

For a security policy rule, the sum of configured destination host addresses, destination subnets, and destination address ranges cannot exceed 1024. If the limit has been reached, any command execution to add such a filtering criterion fails and the system prompts an error.

Examples

Specify destination IPv6 host address **192::167:1** as the filtering criteria of IPv6 security policy rule **rule1**.

```
<Sysname> system-view
[Sysname] security-policy ipv6
[Sysname-security-policy-ipv6] rule 0 name rule1
[Sysname-security-policy-ipv6-0-rule1] destination-ip-host 192::167:1
```

Related commands

display security-policy

destination-ip-range (IPv4 security policy view)

Use **destination-ip-range** to specify a destination IPv4 address range as a filtering criterion of a security policy rule.

Use **undo destination-ip-range** to remove the specified destination IPv4 address range from a security policy rule.

Syntax

destination-ip-range *ip-address1 ip-address2*

undo destination-ip-range [*ip-address1 ip-address2*]

Default

No destination IPv4 address range is specified as a filtering criterion for a security policy rule.

Views

IPv4 security policy rule view

Predefined user roles

network-admin

context-admin

Parameters

ip-address1 ip-address2: Specifies an IPv4 address range. The *ip-address1* argument represents the start IP address and the *ip-address2* argument represents the end IP address. If you do not specify the arguments when executing the **undo** command, the command removes all destination IPv4 address ranges from the rule.

Usage guidelines

You can execute the command multiple times to specify multiple destination IPv4 address ranges as the filtering criteria.

If you specify an IP address range that has been configured as a destination IP range filtering criterion, the command execution fails and the system prompts an error.

For a security policy rule, the sum of configured destination host addresses, destination subnets, and destination address ranges cannot exceed 1024. If the limit has been reached, any command execution to add such a filtering criterion fails and the system prompts an error.

When you specify an IP address range, follow these restrictions and guidelines:

- If the start IP address is the same as the end IP address, the command creates a host address filtering criteria.
- If the start IP address and the end IP address define a subnet, the command creates a subnet filtering criteria.
- If *ip-address1* is greater than *ip-address2*, the system automatically adjusts the range to [*ip-address2*, *ip-address1*].

Examples

Specify destination IPv4 address range 192.165.0.100 to 192.165.0.200 as the filtering criteria of IPv4 security policy rule **rule1**.

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1] destination-ip-range 192.165.0.100 192.165.0.200
```

Related commands

display security-policy

destination-ip-range (IPv6 security policy view)

Use **destination-ip-range** to specify a destination IPv6 address range as a filtering criterion of a security policy rule.

Use **undo destination-ip-range** to remove the specified destination IPv6 address range from a security policy rule.

Syntax

destination-ip-range *ipv6-address1 ipv6-address2*

undo destination-ip-range [*ipv6-address1 ipv6-address2*]

Default

No destination IPv6 address range is specified as a filtering criterion for a security policy rule.

Views

IPv6 security policy rule view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address1 ipv6-address2: Specifies an IPv6 address range. The *ipv6-address1* argument represents the start IP address and the *ipv6-address2* argument represents the end IP address. If you do not specify the arguments when executing the **undo** command, the command removes all destination IPv6 address ranges from the rule.

Usage guidelines

You can execute the command multiple times to specify multiple destination IPv6 address ranges as the filtering criteria.

If you specify an IP address range that has been configured as a destination IP range filtering criterion, the command execution fails and the system prompts an error.

For a security policy rule, the sum of configured destination host addresses, destination subnets, and destination address ranges cannot exceed 1024. If the limit has been reached, any command execution to add such a filtering criterion fails and the system prompts an error.

When you specify an IP address range, follow these restrictions and guidelines:

- If the start IP address is the same as the end IP address, the command creates a host address filtering criteria.
- If the start IP address and the end IP address define a subnet, the command creates a subnet filtering criteria.
- If *ipv6-address1* is greater than *ipv6-address2*, the system automatically adjusts the range to [*ipv6-address2*, *ipv6-address1*].

Examples

Specify destination IPv6 address range 192:165::100 to 192:165::200 as the filtering criteria of IPv6 security policy rule **rule1**.

```
<Sysname> system-view
[Sysname] security-policy ipv6
```

```
[Sysname-security-policy-ipv6] rule 0 name rule1
[Sysname-security-policy-ipv6-0-rule1] destination-ip-range 192:165::100 192:165::200
```

Related commands

display security-policy

destination-ip-subnet (IPv4 security policy view)

Use **destination-ip-subnet** to specify a destination IPv4 subnet as a filtering criterion of a security policy rule.

Use **undo destination-ip-subnet** to remove the specified destination IPv4 subnet from a security policy rule.

Syntax

destination-ip-subnet *ip-address* { *mask-length* | *mask* }

undo destination-ip-subnet [*ip-address* { *mask-length* | *mask* }]

Default

No destination IPv4 subnet is specified as a filtering criterion for a security policy rule.

Views

IPv4 security policy rule view

Predefined user roles

network-admin

context-admin

Parameters

ip-address { *mask-length* | *mask* }: Specifies an IPv4 subnet. You can specify the mask length or the mask in dotted decimal notation. The mask length is in the range of 0 to 32. If you set the mask length to 32 or the mask to 255.255.255.255, the command creates a host address filtering criterion. If you do not specify the arguments when executing the **undo** command, the command removes all destination IPv4 subnets from the rule.

Usage guidelines

You can execute the command multiple times to specify multiple destination IPv4 subnets as the filtering criteria.

If you specify a subnet that has been configured as a destination subnet filtering criterion, the command execution fails and the system prompts an error.

For a security policy rule, the sum of configured destination host addresses, destination subnets, and destination address ranges cannot exceed 1024. If the limit has been reached, any command execution to add such a filtering criterion fails and the system prompts an error.

Examples

Specify the destination subnet with IP address 192.167.0.0 and mask length 24 as a filtering criteria of IPv4 security policy rule **rule1**.

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1] destination-ip-subnet 192.167.0.0 24
```

Specify the destination subnet with IP address 192.166.0.0 and mask 255.255.0.0 as a filtering criteria of IPv4 security policy rule **rule1**.

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1] destination-ip-subnet 192.166.0.0 255.255.0.0
```

Related commands

display security-policy

destination-ip-subnet (IPv6 security policy view)

Use **destination-ip-subnet** to specify a destination IPv6 subnet as a filtering criterion of a security policy rule.

Use **undo destination-ip-subnet** to remove the specified destination IPv6 subnet from a security policy rule.

Syntax

destination-ip-subnet *ipv6-address prefix-length*

undo destination-ip-subnet [*ipv6-address prefix-length*]

Default

No destination IPv6 subnet is specified as a filtering criterion for a security policy rule.

Views

IPv6 security policy rule view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address prefix-length: Specifies an IPv6 subnet. The prefix length is in the range of 1 to 128. If you set the prefix length to 128, the command creates a host address filtering criterion. If you do not specify the arguments when executing the **undo** command, the command removes all destination IPv4 subnets from the rule.

Usage guidelines

You can execute the command multiple times to specify multiple destination IPv6 subnets as the filtering criteria.

If you specify a subnet that has been configured as a destination subnet filtering criterion, the command execution fails and the system prompts an error.

For a security policy rule, the sum of configured destination host addresses, destination subnets, and destination address ranges cannot exceed 1024. If the limit has been reached, any command execution to add such a filtering criterion fails and the system prompts an error.

Examples

Specify the destination subnet with IP address 192::167:0 and prefix length 64 as a filtering criteria of IPv6 security policy rule **rule1**.

```
<Sysname> system-view
[Sysname] security-policy ipv6
[Sysname-security-policy-ipv6] rule 0 name rule1
[Sysname-security-policy-ipv6-0-rule1] destination-ip-subnet 192::167:0 64
```

Related commands

display security-policy

destination-zone

Use **destination-zone** to specify a destination security zone as a filtering criterion of a security policy rule.

Use **undo destination-zone** to remove the specified destination security zone from a security policy rule.

Syntax

destination-zone *destination-zone-name*

undo destination-zone [*destination-zone-name*]

Default

No destination security zone is specified as a filtering criterion for a security policy rule.

Views

Security policy rule view

Predefined user roles

network-admin

context-admin

Parameters

object-group-name: Specifies the name of a destination security zone, a case-insensitive string of 1 to 31 characters. If you do not specify this argument when executing the **undo destination-zone** command, the command removes all destination security zones from the rule. For more information about security zones, see *Security Configuration Guide*.

Usage guidelines

You can execute the command multiple times to specify multiple destination security zones as the filtering criteria.

Examples

Specify destination security zones **trust** and **server** as the filtering criteria of security policy rule **rule1**.

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1] destination-zone trust
[Sysname-security-policy-ip-0-rule1] destination-zone server
```

Related commands

display security-policy

security-zone

disable

Use **disable** to disable a security policy rule.

Use **undo disable** to enable a security policy rule.

Syntax

disable

undo disable

Default

A security policy rule is enabled.

Views

Security policy rule view

Predefined user roles

network-admin

context-admin

Examples

Disable security policy rule **rule1**.

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1] disable
```

Related commands

display security-policy

display security-policy

Use **display security-policy** to display information about the specified security policy.

Syntax

display security-policy { **ip** | **ipv6** }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ip: Specifies the IPv4 security policy.

ipv6: Specifies the IPv6 security policy.

Examples

Display information about the IPv4 security policy.

```
<Sysname> display security-policy ip
Security-policy ip

 rule 0 name der (Inactive)
  action pass
```

```
profile er
vrf re
logging enable
counting enable period 20
counting enable TTL 1200
time-range dere
track positive 23
session aging-time 5000
session persistent aging-time 2400
source-zone trust
destination-zone trust
source-ip erer
source-ip-host 1.1.1.4
source-ip-subnet 1.1.1.0 255.255.255.0
source-ip-range 2.2.1.1 3.3.3.3
destination-ip client1
destination-ip-host 5.5.1.2
destination-ip-subnet 5.5.1.0 255.255.255.0
destination-ip-range 2.2.1.1 3.3.3.3
service ftp
service-port tcp
service-port tcp source lt 100 destination eq 104
service-port tcp source eq 100 destination range 104 2000
service-port udp
service-port udp source gt 100 destination eq 104
service-port udp destination eq 100
service-port icmp 100 122
service-port icmp
app-group ere
application 110Wang
user der
user-group ere
```

Table 1 Command output

Field	Description
rule *id* name *rule-name*	Rule ID and rule name.
action pass	Rule action: • **pass**—Allows matched packets to pass. • **drop**—Drops matched packets.
profile *app-profile-name*	DPI application profile applied to the rule.
vrf *vrf-name*	MPLS L3VPN instance whose packets can be filtered by the rule.
logging enable	Indicates that logging for matched packets is enabled.
counting enable period *value*	Indicates that statistics collection for matched packets is enabled. The *value* argument represents the enabling period in minutes.
counting enable TTL *time-value*	Indicates that statistics collection for matched packets is

Field	Description
	enabled. The *time-value* argument represents the remaining enabling period in seconds.
time-range *time-range-name*	Time range during which the rule is in effect.
track negative 1 (Active)	Track entry and track entry state associated with the security policy rule.
session aging-time *time-value*	Session aging time.
session persistent aging-time *time-value*	Persistent session aging time.
source-zone *zone-name*	Source security zone that acts as a filtering criterion.
destination-zone *zone-name*	Destination security zone that acts as a filtering criterion.
source-ip *object-group-name*	Source IP address object group that acts as a filtering criterion.
source-ip-host *ip-address*	Source IP host address that acts as a filtering criterion.
source-ip-subnet *ip-address*	Source IP subnet that acts as a filtering criterion.
source-ip-range *ip-address1 ip-address2*	Source IP address range that acts as a filtering criterion.
destination-ip *object-group-name*	Destination IP address object group that acts as a filtering criterion.
destination-ip-host ip-address	Destination IP host address that acts as a filtering criterion.
destination-ip-subnet ip-address	Destination IP subnet that acts as a filtering criterion.
destination-ip-range *ip-address1 ip-address2*	Destination IP address range that acts as a filtering criterion.
service *object-group-name*	Service object group that acts as a filtering criterion.
service-port *protocol*	Service port that acts as a filtering criterion.
app-group *app-group-name*	Application group that acts as a filtering criterion.
application *application-name*	Application that acts as a filtering criterion.
user *user-name*	User that acts as a filtering criterion.
user-group *user-group-name*	User group that acts as a filtering criterion.

Related commands

security-policy ip

security-policy ipv6

display security-policy statistics

Use **display security-policy statistics** to display security policy statistics.

Syntax

display security-policy statistics { **ip** | **ipv6** } [**rule** *rule-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ip: Specifies the IPv4 security policy.

ipv6: Specifies the IPv6 security policy.

rule *rule-name*: Specifies a security policy rule by its name, a case-insensitive string of 1 to 127 characters. If you do not specify this option, the command displays statistics about all security policy rules of the specified IP version.

Examples

Display statistics about IPv4 security policy rule **abc**.

```
<Sysname> display security-policy statistics ip rule abc
rule 0 name abc
 action: pass (5 packets, 1000 bytes)
```

Table 2 Command output

Field	Description
rule *id* name *rule-name*	Rule ID and rule name.
action	Rule action: • **pass**—Allows matched packets to pass. • **drop**—Drops matched packets.
x packets, y bytes	The rule has matched x packets, a total of y bytes. This field is displayed only if the **counting enable** or the **logging enable** command has been executed for the rule.

Related commands

reset security-policy statistics

group move

Use **group move** to move a security policy rule group to change the match order of security policy rules.

Syntax

group move *group-name1* { **after** | **before** } { **group** *group-name2* | **rule** *rule-name* }

Views

Security policy view

Predefined user roles

network-admin

context-admin

Parameters

group-name1: Specifies the name of the security policy rule group to be moved, a case-insensitive string of 1 to 63 characters.

after: Moves the security policy rule group to the place after the target security policy rule group or the target security policy rule.

before: Moves the security policy rule group to the place before the target security policy rule group or the target security policy rule.

group *group-name2*: Specifies the name of the target security policy rule group, a case-insensitive string of 1 to 63 characters.

rule *rule-name*: Specifies the name of the target security policy rule, a case-insensitive string of 1 to 127 characters.

Usage guidelines

If you specify a target security policy rule that belongs to a security policy rule group, follow these restrictions and guidelines:

- If the target rule is neither the start nor end rule of the group, you cannot move a security policy rule group to the place before or after the rule.
- If the target rule is the start rule of the group, you can only move a security policy rule group to the place before the rule.
- If the target rule is the end rule of the group, you can only move a security policy rule group to the place after the rule.

Examples

Move security policy rule group **group1** to the place before security policy rule group **group2**.

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] group move group1 before group group2
```

group name

Use **group name** to create a security policy rule group and add security policy rules to the group, or add security policy rules to an existing security policy rule group.

Use **undo group name** to delete a security policy rule group.

Syntax

group name *group-name* [**from** *rule-name1* **to** *rule-name2*] [**description** *description-text*] [**disable** | **enable**]

undo group name *group-name* [**description** | **include-member**]

Default

No security policy rule group exists.

Views

Security policy view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a security policy rule group name, a case-insensitive string of 1 to 63 characters.

from *rule-name1*: Specifies the start rule of a rule list. The *rule-name1* argument represents the security policy rule name, a case-insensitive string of 1 to 127 characters.

to *rule-name2*: Specifies the end rule of the rule list. The *rule-name2* argument represents the security policy rule name, a case-insensitive string of 1 to 127 characters.

description *description-text*: Specifies the security policy description, a case-sensitive string of 1 to 127 characters. By default, no description is specified for a security policy rule group.

disable: Disables the security policy rule group.

enable: Enables the security policy rule group. By default, a security policy rule group is enabled.

include-member: Specifies security policy rules in the security policy rule group.

Usage guidelines

Security policy rule grouping allows users to enable, disable, delete, and move security policy rules in batches.

A security policy rule in a security policy rule group takes effect only when both the rule and the group are enabled.

To add a list of security policy rules, make sure the end rule is listed behind the start rule and the specified rules do not belong to any other security policy rule group.

When you execute the **undo** command, follow these restrictions and guidelines:

- The **undo group name** *group-name* command deletes only the specified security policy rule group.
- The **undo group name** *group-name* **description** command deletes only the description for the specified security policy rule group.
- The **undo group name** *group-name* **include-member** command deletes both the specified security policy rule group and all the security policy rules in the group.

Examples

Create security policy rule group **group1**, add security policy rules **rule-name1** through **rule-name10** to the group, and specify the group description as **marketing**.

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] group name group1 from rule-name1 to rule-name10 enable
description marketing
```

group rename

Use **group rename** to rename a security policy rule group.

Syntax

group rename *old-name new-name*

Views

Security policy view

Predefined user roles

network-admin

context-admin

Parameters

old-name: Specifies the name of a security policy rule group, a case-insensitive string of 1 to 63 characters.

new-name: Specifies a new name for the security policy rule group, a case-insensitive string of 1 to 63 characters.

Examples

Rename security policy rule group **group1** to **group2**.

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] group rename group1 group2
```

logging enable

Use **logging enable** to enable logging for matched packets.

Use **undo logging enable** to disable logging for matched packets.

Syntax

logging enable

undo logging enable

Default

Logging for matched packets is disabled.

Views

Security policy rule view

Predefined user roles

network-admin

context-admin

Usage guidelines

This feature enables the security policy module to send log messages to the information center or to fast output log messages when packets match a security policy.

With the information center or fast log output, you can set log message filtering and output rules, including output destinations.

The information center can output packet matching logs to any destinations except the console and the monitor terminal. If you configure the console or monitor terminal as an output destination, the output destination setting will not take effect.

To view packet matching logs stored on the device, use the **display logbuffer** command or open the security policy log page from the Web interface of the device. Make sure you do not disable log output to the log buffer, which is enabled by default.

For more information about configuring the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Enable matched packet logging for security policy rule **rule1**.

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1] logging enable
```

Related commands

display security-policy

move rule

Use **move rule** to move a security policy rule by rule ID.

Syntax

move rule *rule-id1* { { **after** | **before** } *rule-id2* | **bottom** | **down** | **top** | **up** }

Views

IPv4 security policy view

IPv6 security policy view

Predefined user roles

network-admin

context-admin

Parameters

rule-id1: Specifies the ID of a rule to be moved, in the range of 0 to 4294967290.

after: Moves the rule to the position after the target rule.

before: Moves the rule to the position before the target rule.

rule-id2: Specifies the ID of the target rule. The target rule ID is in the range of 0 to 4294967295. If you specify 4294967295 as the target rule ID, the rule is moved to the end of the list.

bottom: Moves the rule to the end of the list.

down: Moves the rule one position down.

top: Moves the rule to the beginning of the list.

up: Moves the rule one position up.

Usage guidelines

The system does not execute the command in the following situations:

- You specify the same value for the *rule-id1* and *rule-id2* arguments.
- You specify a nonexistent rule.

Examples

Insert rule 5 before rule 2 for the IPv4 security policy.

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] move rule 5 before 2
```

Related commands

rule

security-policy ip

security-policy ipv6

move rule name

Use **move rule name** to move a security policy rule by rule name.

Syntax

move rule name *rule-name1* { { **after** | **before** } **name** *rule-name2* | **bottom** | **down** | **top** | **up** }

Views

Security policy view

Predefined user roles

network-admin

context-admin

Parameters

rule-name1: Specifies the name of the rule to move, a case-insensitive string of 1 to 127 characters.

after: Move the rule to the place after the destination rule.

before: Move the rule to the place before the destination rule.

name *rule-name2*: Specify the name of the destination rule, a case-insensitive string of 1 to 127 characters.

bottom: Move the rule to the end of the security policy.

down: Move the rule down one place.

top: Move the rule to the beginning of the security policy.

up: Move the rule up one place.

Usage guidelines

You can move a rule to change its packet matching priority.

Examples

Move rule **rule1** to the place before rule **rule2**.

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] move rule name rule1 before name rule2
```

Related commands

rule

security-policy ip

security-policy ipv6

parent-group

Use **parent-group** to specify a security policy rule group for a security policy rule.

Use **undo parent-group** to restore the default.

Syntax

parent-group *group-name*

undo parent-group

Default

A security policy rule does not belong to any security policy rule group.

Views

Security policy rule view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies the name of a security policy rule group, a case-insensitive string of 1 to 63 characters.

Examples

Assign security policy rule **rule1** to security policy rule group **group1**.

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 1 name rule1
[Sysname-security-policy-ip-1-rule1] parent-group group1
```

profile

Use **profile** to apply a DPI application profile to a security policy rule.

Use **undo profile** to remove the DPI application profile applied to a security policy rule.

Syntax

profile *app-profile-name*

undo profile

Default

No DPI application profile is applied to a security policy rule.

Views

Security policy rule view

Predefined user roles

network-admin

context-admin

Parameters

app-profile-name: Specifies the name of a DPI application profile, a case-insensitive string of 1 to 63 characters. For more information about DPI application profiles, see DPI engine in *DPI Configuration Guide*.

Usage guidelines

This feature enables the device to perform DPI on packets matching the specified rule. For more information about DPI, see *DPI Configuration Guide*.

This feature takes effect only when the rule action is **pass**.

Examples

Apply DPI application profile **p1** to IPv4 security policy rule **rule1**.

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
```

```
[Sysname-security-policy-ip-0-rule1] action pass
[Sysname-security-policy-ip-0-rule1] profile p1
```

Related commands

action pass

app-profile (*DPI Command Reference*)

display security-policy ip

reset security-policy statistics

Use **reset security-policy statistics** to clear security policy statistics.

Syntax

reset security-policy statistics [**ip** | **ipv6**] [**rule** *rule-name*]

Views

Any view

Predefined user roles

network-admin

context-admin

Parameters

ip: Specifies the IPv4 security policy.

ipv6: Specifies the IPv6 security policy.

rule *rule-name*: Specifies a security policy rule by its name, a case-insensitive string of 1 to 127 characters.

Usage guidelines

If you do not specify any keyword or option, the command clears all security policy statistics.

Examples

Clear the security policy statistics about IPv4 security policy rule **abc**.

```
<Sysname> reset security-policy statistics ip rule abc
```

Related commands

display security-policy statistics

rule

Use **rule** to create a security policy rule and enter its view, or enter the view of an existing security policy rule.

Use **undo rule** to delete the specified security policy rule.

Syntax

rule { *rule-id* | [*rule-id*] **name** *rule-name* }

undo rule { *rule-id* | **name** *rule-name* } *

Default

No security policy rules exist.

Views

IPv4 security policy view

IPv6 security policy view

Predefined user roles

network-admin

context-admin

Parameters

rule-id: Specifies a rule ID in the range of 0 to 4294967290. If you do not specify an ID for the rule, the system automatically assigns the rule the integer next to the greatest ID being used. If the greatest ID is 4294967290, the system assigns the rule the smallest unused number in the range.

rule-name: Specifies a globally unique rule name, a case-insensitive string of 1 to 127 characters. The name cannot be **default**. You must specify a rule name when creating a rule.

Examples

Create an IPv4 security policy rule with rule ID **0** and rule name **rule1**.

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1]
```

Related commands

display security-policy ip

display security-policy ipv6

rule rename

Use **rule rename** to rename a security policy rule.

Syntax

rule rename *old-name new-name*

Views

Security policy view

Predefined user roles

network-admin

context-admin

Parameters

old-name: Specifies the current name, a case-insensitive string of 1 to 127 characters.

new-name: Specifies the new name, a case-insensitive string of 1 to 127 characters. The name must be globally unique and cannot be **default**.

Examples

Change the name of security policy rule **rule1** to **rule2**.

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule rename rule1 rule2
```

Related commands

rule

security-policy ip

security-policy ipv6

security-policy

Use **security-policy** to enter security policy view.

Use **undo security-policy** to delete all configurations in security policy view.

Syntax

security-policy { **ip** | **ipv6** }

undo security-policy { **ip** | **ipv6** }

Default

No configurations exist in security policy view.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ip: Specifies the IPv4 security policy.

ipv6: Specifies the IPv6 security policy.

Usage guidelines

CAUTION:

- The **undo security-policy** { **ip** | **ipv6** } command directly deletes all security policy configurations and might cause network interruptions.
- If the security policy feature is enabled, object policy settings lose effect the first time you enter the security policy view. Make sure policy settings have been switched to security policy settings before you enter the security policy view.

Examples

Enter IPv4 security policy view.

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip]
```

Delete all IPv4 security policy configurations.

```
<Sysname> system-view
[Sysname] undo security-policy ip
This command willdelete all rules from the current policy. Continue anyway? [Y/N]:
```

Related commands

display security-policy

security-policy config-logging send-time

Use **security-policy config-logging send-time** to set the time at which the device fast outputs security policy settings as logs every day.

Use **undo security-policy config-logging send-time** to restore the default.

Syntax

security-policy config-logging send-time *time*

undo security-policy config-logging send-time

Default

The device fast outputs security policy settings as logs every day at 0 o'clock.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

time: Specify the time at which the device fast outputs security policy settings as logs, in the format of *hh*:*mm*. The value range for the *hh* argument is 00 to 23 and the value range for the *mm* argument is 00 to 59.

Usage guidelines

After the **customlog format security-policy sgcc** command is executed, the device fast outputs settings of enabled security policies as logs in SGCC format every day at the specified time. For more information about fast log output, see *Network Management and Monitoring Configuration Guide*.

Examples

Configure the device to fast output security policy settings as logs every day at 13:15.

```
<Sysname>system-view
[Sysname] security-policy config-loggging send-time 13:15
```

Related commands

customlog format security-policy sgcc (*Network Management and Monitoring Command Reference*)

customlog host export security-policy (*Network Management and Monitoring Command Reference*)

security-policy disable

Use **security-policy disable** to disable the security policy feature.

Use **undo security-policy disable** to enable the security policy feature.

Syntax

security-policy disable

undo security-policy disable

Default

The security policy feature is enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

CAUTION:

The **security-policy disable** command disables the security policy feature and might cause traffic interruption.

Security policy settings take effect only when the security policy feature is enabled.

Examples

Disable the security policy feature.

```
<Sysname> system-view
[Sysname] security-policy disable
```

service

Use **service** to specify a service object group as a filtering criterion of a security policy rule.

Use **undo service** to remove the specified service object group from a security policy rule.

Syntax

service { *object-group-name* | **any** }

undo service [*object-group-name* | **any**]

Default

No service object group is specified as a filtering criterion for a security policy rule.

Views

Security policy rule view

Predefined user roles

network-admin

context-admin

Parameters

object-group-name: Specifies the name of a service object group, a case-insensitive string of 1 to 63 characters.

any: Specifies all service object groups.

Usage guidelines

You can execute the command multiple times to specify multiple service object groups as the filtering criteria.

If you specify a nonexistent object group, the device automatically creates the specified object group with empty configuration. A rule that contains an object group with empty configuration does not match any packets.

If you specify neither an object group nor the **any** keyword when executing the **undo service** command, the command removes all service object groups from the security policy rule.

For a security policy rule, the number of configured service object groups cannot exceed 1024. If the limit has been reached, any command execution to add such a filtering criterion fails and the system prompts an error.

Examples

Specify service object groups **http** and **ftp** as the filtering criteria of security policy rule **rule1**.

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1] service http
[Sysname-security-policy-ip-0-rule1] service ftp
```

Related commands

display security-policy

object-group

service-port

Use **service-port** to specify a service port as a filtering criterion of a security policy rule.

Use **undo service-port** to remove the specified service port range from a security policy rule.

Syntax

service-port *protocol* [{ **destination** { { **eq** | **lt** | **gt** } *port* | **range** *port1 port2* } | **source** { { **eq** | **lt** | **gt** } *port* | **range** *port1 port2* } } * | *icmp-type icmp-code* | *icmpv6-type icmpv6-code*]

undo service-port [*protocol* [{ **destination** { { **eq** | **lt** | **gt** } *port* | **range** *port1 port2* } | **source** { { **eq** | **lt** | **gt** } *port* | **range** *port1 port2* } } * | *icmp-type icmp-code* | *icmpv6-type icmpv6-code*]]

Default

No service port is specified as a filtering criterion for a security policy rule.

Views

IPv4 security policy rule view

IPv6 security policy rule view

Predefined user roles

network-admin

context-admin

Parameters

protocol: Specify the number or name of a protocol. The protocol number value ranges and available protocol names vary by command execution view.

- In IPv4 security policy view, the value range for protocol numbers is 0 to 57 and 59 to 255. Available protocol names include **tcp**, **udp**, and **icmp**, whose protocol numbers are 6, 17, and 1, respectively.
- In IPv6 security policy view, the value range for protocol numbers is 0 and 2 to 255. Available protocol names include **tcp**, **udp**, and **icmp**, whose protocol numbers are 6, 17, and 58, respectively.

destination: Specifies the destination port. This configuration takes effect only when the protocol is TCP or UDP.

source: Specifies the source port. This configuration takes effect only when the protocol is TCP or UDP.

eq: Specifies the specified port.

lt: Specifies all ports whose port numbers are smaller than the specified port. If you specify this keyword, the specified port number cannot be 0.

gt: Specifies all ports whose port numbers are larger than the specified port. If you specify this keyword, the specified port number cannot be 65535.

port: Specifies a port number in the range of 0 to 65535.

range *port1 port2*: Specifies a range of port numbers. The *port1* argument represents the start port and the *port2* argument represents the end port. Each port number is in the range of 0 to 65535.

icmp-type: Specifies an ICMP message type in the range of 0 to 255. This configuration takes effect only when the protocol is ICMP.

icmp-code: Specifies the ICMP message code in the range of 0 to 255.

icmpv6-type: Specifies an ICMPv6 message type in the range of 0 to 255. This configuration takes effect only when the protocol is ICMPv6.

icmpv6-code: Specifies the ICMPv6 message code in the range of 0 to 255.

Usage guidelines

You can execute this command multiple times to specify multiple service ports as the filtering criteria.

If you specify a service port that has been configured as a service port filtering criterion, the command execution fails.

For a security policy rule, the number of configured service ports cannot exceed 1024. If the limit has been reached, any command execution to add such a filtering criterion fails and the system prompts an error.

When you specify the **range** keyword, following these restrictions and guidelines:

- If *port1* is the same as *port2*, the command takes effect as if you specified the **eq** keyword.
- If *port1* is 0, the command takes effect as if you specified the **lt** keyword with *port2* as the specified port.
- If *port2* is 65535, the command takes effect as if you specified the **gt** keyword with *port1* as the specified port.
- If *port1* is larger than *port2*, the system automatically changes the port range to [*port2*, *port1*].

If you do not specify any keyword or argument when executing the **undo** command, the command removes all service ports from the security policy rule.

Examples

Specify TCP destination and source ports as the filtering criteria of security policy rule **rule1**.

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1] service-port tcp destination range 100 200 source eq 100
```

Specify ICMP destination and source ports as the filtering criteria of security policy rule **rule1**.

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1] service-port icmp 100 150
```

Related commands

display security-policy

session aging-time

Use **session aging-time** to set the session aging time for a security policy rule.

Use **undo session aging-time** to restore the default.

Syntax

session aging-time *time-value*

undo session aging-time

Default

The session aging time is not configured for a security policy rule.

Views

Security policy rule view

Predefined user roles

network-admin

context-admin

Parameters

time-value: Specifies the aging time in the range of 1 to 2000000 seconds.

Usage guidelines

CAUTION:

Setting too long an aging time might cause persistent sessions to increase rapidly and therefore cause the CPU usage to be high.

This command sets the aging time for stable sessions created for packets matching the specified security policy rule, and takes effect only on newly created sessions.

If the aging time is not configured for a rule, the stable sessions use the aging time set by using the **session aging-time application** or the **session aging-time state** command. For more information about session management, see *Security Configuration Guide*.

Unstable sessions age based on the default session aging time configured.

Examples

Set the session aging time to 5000 seconds for security policy rule **rule1**.

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1] action pass
[Sysname-security-policy-ip-0-rule1] session aging-time 5000
```

Related commands

display security-policy

session aging-time application

session aging-time state

session persistent acl

session persistent aging-time

Use **session persistent aging-time** to set the aging time for persistent sessions.

Use **undo session persistent aging-time** to restore the default.

Syntax

session persistent aging-time *time-value*

undo session persistent aging-time

Default

The persistent session aging time is not configured for a security policy rule.

Views

Security policy rule view

Predefined user roles

network-admin

context-admin

Parameters

time-value: Specifies the aging time in the range of 0 to 24000 hours. If you set the aging time to 0, persistent sessions do not age out.

Usage guidelines

This command is effective only on TCP sessions in ESTABLISHED state.

It sets the aging time for persistent sessions created for packets matching the specified security policy rule, and takes effect only on newly created sessions.

The aging time configured by using this command takes precedence over the aging times configured by using the **session aging-time** and **session persistent acl** commands.

Examples

Set the persistent session aging time to one hour for security policy rule **rule1**.

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1] action pass
[Sysname-security-policy-ip-0-rule1] session persistent aging-time 1
```

Related commands

display security-policy

session persistent acl

source-ip

Use **source-ip** to specify a source IP address object group as a filtering criterion of a security policy rule.

Use **undo source-ip** to remove the specified source IP address object group from a security policy rule.

Syntax

source-ip *object-group-name*

undo source-ip [*object-group-name*]

Default

No source IP address object group is specified as a filtering criterion for a security policy rule.

Views

Security policy rule view

Predefined user roles

network-admin

context-admin

Parameters

object-group-name: Specifies the name of a source IP address object group, a case-insensitive string of 1 to 63 characters. The name cannot be **any**. If you do not specify this argument when executing the **undo source-ip** command, the command removes all source IP address object groups from the rule. For more information about object groups, see *Security Configuration Guide*.

Usage guidelines

You can execute the command multiple times to specify multiple source IP address object groups as the filtering criteria.

If you specify a nonexistent object group, the device automatically creates the specified object group with empty configuration. A rule that contains an object group with empty configuration does not match any packets.

For a security policy, the number of configured source IP addresses cannot exceed 1024. If the limit has been reached, any command execution to add such a filtering criterion fails and the system prompts an error.

Examples

Specify source IP address object groups **server1** and **server2** as the filtering criteria of security policy rule **rule1**.

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1] source-ip server1
[Sysname-security-policy-ip-0-rule1] source-ip server2
```

Related commands

display security-policy

object-group

source-ip-host (IPv4 security policy view)

Use **source-ip-host** to specify a source IPv4 host address as a filtering criterion of a security policy rule.

Use **undo source-ip-host** to remove the specified source IPv4 host address from a security policy rule.

Syntax

source-ip-host *ip-address*

undo source-ip-host [*ip-address*]

Default

No source IPv4 host address is specified as a filtering criterion for a security policy rule.

Views

IPv4 security policy rule view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the IPv4 address of a host. If you do not specify this argument when executing the **undo** command, the command removes all source IPv4 host addresses from the security policy rule.

Usage guidelines

You can execute the command multiple times to specify multiple source IPv4 host addresses as the filtering criteria.

If you specify an IP address that has been configured as a source host filtering criterion, the command execution fails and the system prompts an error.

For a security policy rule, the sum of configured source host addresses, source subnets, and source address ranges cannot exceed 1024. If the limit has been reached, any command execution to add such a filtering criterion fails and the system prompts an error.

Examples

Specify source IPv4 host address **192.167.0.1** as the filtering criteria of IPv4 security policy rule **rule1**.

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1] source-ip-host 192.167.0.1
```

Related commands

display security-policy

source-ip-host (IPv6 security policy view)

Use **source-ip-host** to specify a source IPv6 host address as a filtering criterion of a security policy rule.

Use **undo source-ip-host** to remove the specified source IPv6 host address from a security policy rule.

Syntax

source-ip-host *ipv6-address*

undo source-ip-host [*ipv6-address*]

Default

No source IPv6 host address is specified as a filtering criterion for a security policy rule.

Views

IPv6 security policy rule view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address: Specifies the IPv6 address of a host. If you do not specify this argument when executing the **undo** command, the command removes all source IPv6 host addresses from the security policy rule.

Usage guidelines

You can execute the command multiple times to specify multiple source IPv6 host addresses as the filtering criteria.

If you specify an IP address that has been configured as a source host filtering criterion, the command execution fails and the system prompts an error.

For a security policy rule, the sum of configured source host addresses, source subnets, and source address ranges cannot exceed 1024. If the limit has been reached, any command execution to add such a filtering criterion fails and the system prompts an error.

Examples

Specify source IPv6 host address **192::167:1** as the filtering criteria of IPv6 security policy rule **rule1**.

```
<Sysname> system-view
[Sysname] security-policy ipv6
[Sysname-security-policy-ipv6] rule 0 name rule1
[Sysname-security-policy-ipv6-0-rule1] source-ip-host 192::167:1
```

Related commands

display security-policy

source-ip-range (IPv4 security policy view)

Use **source-ip-range** to specify a source IPv4 address range as a filtering criterion of a security policy rule.

Use **undo source-ip-range** to remove the specified source IPv4 address range from a security policy rule.

Syntax

source-ip-range *ip-address1 ip-address2*

undo source-ip-range [*ip-address1 ip-address2*]

Default

No source IPv4 address range is specified as a filtering criterion for a security policy rule.

Views

IPv4 security policy rule view

Predefined user roles

network-admin

context-admin

Parameters

ip-address1 ip-address2: Specifies an IPv4 address range. The *ip-address1* argument represents the start IP address and the *ip-address2* argument represents the end IP address. If you do not specify the arguments when executing the **undo** command, the command removes all source IPv4 address ranges from the security policy rule.

Usage guidelines

You can execute the command multiple times to specify multiple source IPv4 address ranges as the filtering criteria.

If you specify an IP address range that has been configured as a source IP range filtering criterion, the command execution fails and the system prompts an error.

For a security policy rule, the sum of configured source host addresses, source subnets, and source address ranges cannot exceed 1024. If the limit has been reached, any command execution to add such a filtering criterion fails and the system prompts an error.

When you specify an IP address range, follow these restrictions and guidelines:

- If the start IP address is the same as the end IP address, the command creates a host address filtering criteria.
- If the start IP address and the end IP address define a subnet, the command creates a subnet filtering criteria.
- If *ip-address1* is greater than *ip-address2*, the system automatically adjusts the range to [*ip-address2*, *ip-address1*].

Examples

Specify source IPv4 address range 192.165.0.100 to 192.165.0.200 as the filtering criteria of IPv4 security policy rule **rule1**.

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1] source-ip-range 192.165.0.100 192.165.0.200
```

Related commands

display security-policy

source-ip-range (IPv6 security policy view)

Use **source-ip-range** to specify a source IPv6 address range as a filtering criterion of a security policy rule.

Use **undo source-ip-range** to remove the specified source IPv6 address range from a security policy rule.

Syntax

source-ip-range *ipv6-address1 ipv6-address2*

undo source-ip-range [*ipv6-address1 ipv6-address2*]

Default

No source IPv6 address range is specified as a filtering criterion for a security policy rule.

Views

IPv6 security policy rule view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address1 ipv6-address2: Specifies an IPv6 address range. The *ipv6-address1* argument represents the start IP address and the *ipv6-address2* argument represents the end IP address. If you do not specify the arguments when executing the **undo** command, the command removes all source IPv6 address ranges from the security policy rule.

Usage guidelines

You can execute the command multiple times to specify multiple source IPv6 address ranges as the filtering criteria.

If you specify an IP address range that has been configured as a source IP range filtering criterion, the command execution fails and the system prompts an error.

For a security policy rule, the sum of configured source host addresses, source subnets, and source address ranges cannot exceed 1024. If the limit has been reached, any command execution to add such a filtering criterion fails and the system prompts an error.

When you specify an IP address range, follow these restrictions and guidelines:

- If the start IP address is the same as the end IP address, the command creates a host address filtering criteria.
- If the start IP address and the end IP address define a subnet, the command creates a subnet filtering criteria.
- If *ipv6-address1* is greater than *ipv6-address2*, the system automatically adjusts the range to [*ipv6-address2*, *ipv6-address1*].

Examples

Specify source IPv6 address range 192::165:100 to 192::165:200 as the filtering criteria of IPv6 security policy rule **rule1**.

```
<Sysname> system-view
[Sysname] security-policy ipv6
[Sysname-security-policy-ipv6] rule 0 name rule1
[Sysname-security-policy-ipv6-0-rule1] source-ip-range 192::165:100 192::165:200
```

Related commands

display security-policy

source-ip-subnet (IPv4 security policy view)

Use **source-ip-subnet** to specify a source IPv4 subnet as a filtering criterion of a security policy rule.

Use **undo source-ip-subnet** to remove the specified source IPv4 subnet from a security policy rule.

Syntax

source-ip-subnet *ip-address* { *mask-length* | *mask* }

undo source-ip-subnet [*ip-address* { *mask-length* | *mask* }]

Default

No source IPv4 subnet is specified as a filtering criterion for a security policy rule.

Views

IPv4 security policy rule view

Predefined user roles

network-admin

context-admin

Parameters

ip-address { *mask-length* | *mask* }: Specifies an IPv4 subnet. You can specify the mask length or the mask in dotted decimal notation. The mask length is in the range of 0 to 32. If you set the mask length to 32 or the mask to 255.255.255.255, the command creates a host address filtering criterion. If you do not specify the arguments when executing the **undo** command, the command removes all source IPv4 subnets from the security policy rule.

Usage guidelines

You can execute the command multiple times to specify multiple source IPv4 subnets as the filtering criteria.

If you specify a subnet that has been configured as a source subnet filtering criterion, the command execution fails and the system prompts an error.

For a security policy rule, the sum of configured source host addresses, source subnets, and source address ranges cannot exceed 1024. If the limit has been reached, any command execution to add such a filtering criterion fails and the system prompts an error.

Examples

Specify the source subnet with IP address 192.167.0.0 and mask length 24 as a filtering criteria of IPv4 security policy rule **rule1**.

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1] source-ip-subnet 192.167.0.0 24
```

Specify the source subnet with IP address 192.166.0.0 and mask 255.255.0.0 as a filtering criteria of IPv4 security policy rule **rule1**.

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1] source-ip-subnet 192.166.0.0 255.255.0.0
```

Related commands

display security-policy

source-ip-subnet (IPv6 security policy view)

Use **source-ip-subnet** to specify a source IPv6 subnet as a filtering criterion of a security policy rule.

Use **undo source-ip-subnet** to remove the specified source IPv6 subnet from a security policy rule.

Syntax

source-ip-subnet *ipv6-address prefix-length*

undo source-ip-subnet [*ipv6-address prefix-length*]

Default

No source IPv6 subnet is specified as a filtering criterion for a security policy rule.

Views

IPv6 security policy rule view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address prefix-length: Specifies an IPv6 subnet. The prefix length is in the range of 1 to 128. If you set the prefix length to 128, the command creates a host address filtering criterion. If you do not specify the arguments when executing the **undo** command, the command removes all source IPv6 subnets from the security policy rule.

Usage guidelines

You can execute the command multiple times to specify multiple source IPv6 subnets as the filtering criteria.

If you specify a subnet that has been configured as a source subnet filtering criterion, the command execution fails and the system prompts an error.

For a security policy rule, the sum of configured source host addresses, source subnets, and source address ranges cannot exceed 1024. If the limit has been reached, any command execution to add such a filtering criterion fails and the system prompts an error.

Examples

Specify the source subnet with IPv6 address 192: 167::0 and prefix length 64 as a filtering criteria of IPv6 security policy rule **rule1**.

```
<Sysname> system-view
[Sysname] security-policy ipv6
[Sysname-security-policy-ipv6] rule 0 name rule1
[Sysname-security-policy-ipv6-0-rule1] source-ip-subnet 192:167::0 64
```

Related commands

display security-policy

source-mac

Use **source-mac** to specify a source MAC address object group as a filtering criterion of a security policy rule.

Use **undo source-mac** to remove the specified source MAC address object group from a security policy rule.

Syntax

source-mac *object-group-name*

undo source-mac [*object-group-name*]

Default

No source MAC address object group is specified as a filtering criterion for a security policy rule.

Views

IPv4 security policy rule view

Predefined user roles

network-admin

context-admin

Parameters

object-group-name: Specifies the name of a source MAC address object group, a case-insensitive string of 1 to 63 characters. The name cannot be **any**. If you do not specify this argument when executing the **undo source-mac** command, the command removes all source MAC address object groups from the rule. For more information about MAC address object groups, see *Security Configuration Guide*.

Usage guidelines

You can execute the command multiple times to specify multiple source MAC address object groups as the filtering criteria.

If you specify a nonexistent object group, the device automatically creates the specified object group with empty configuration. A rule that contains an object group with empty configuration does not match any packets.

Examples

Specify source MAC address object groups **mac1** and **mac2** as the filtering criteria of security policy rule **rule1**.

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1] source-mac mac1
[Sysname-security-policy-ip-0-rule1] source-mac mac2
```

Related commands

display security-policy

object-group

source-zone

Use **source-zone** to specify a source security zone as a filtering criterion of a security policy rule.

Use **undo source-zone** to remove the specified source security zone from a security policy rule.

Syntax

source-zone *source-zone-name*

undo source-zone [*source-zone-name*]

Default

No source security zone is specified as a filtering criterion for a security policy rule.

Views

Security policy rule view

Predefined user roles

network-admin

context-admin

Parameters

source-zone-name: Specifies the name of a source security zone, a case-insensitive string of 1 to 63 characters. If you do not specify this argument when executing the **undo source-zone** command, the command removes all source security zones from the rule. For more information about security zones, see *Security Configuration Guide*.

Usage guidelines

You can execute the command multiple times to specify multiple source security zones as the filtering criteria.

Examples

Specify source security zones **trust** and **dmz** as the filtering criteria of security policy rule **rule1**.

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1] source-zone trust
[Sysname-security-policy-ip-0-rule1] source-zone dmz
```

Related commands

display security-policy

security-zone

time-range

Use **time-range** to specify the time range during which a security policy rule is in effect.

Use **undo time-range** to restore the default.

Syntax

time-range *time-range-name*

undo time-range [*time-range-name*]

Default

A security policy rule is in effect at any time.

Views

Security policy rule view

Predefined user roles

network-admin

context-admin

Parameters

time-range-name: Specifies the name of a time range, a case-insensitive string of 1 to 32 characters. If you do not specify this parameter for an undo operation, the command deletes the time range during which the rule takes effect. For more information about time ranges, see *ACL and QoS Configuration Guide*.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Enable security policy rule **rule1** to be in effect during time range **work**.

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1] time-range work
```

Related commands

display security-policy

time-range (*ACL and QoS Command Reference*)

track

Use **track** to associate a security policy rule with a track entry.

Use **undo track** to disassociate a security policy rule from the track entry.

Syntax

track { **negative** | **positive** } *track-entry-number*

undo track

Default

No track entry is associated with a security policy rule.

Views

Security policy rule view

Predefined user roles

network-admin

context-admin

Parameters

negative: Specifies the Negative state of a track entry.

positive: Specifies the Positive state of a track entry.

track-entry-number: Specifies the number of a track entry, in the range of 1 to 1024. For more information about Track, see *Network Management and Monitoring Configuration Guide*.

Usage guidelines

Use this command to enable the collaboration between the track module and a security policy rule. The collaboration operates as follows:

- If a rule is associated with the Negative state of a track entry, the device:
  - Sets the rule state to Active if the track entry is in Negative state.
  - Sets the rule state to Inactive if the track entry is in Positive state.
- If a rule is associated with the Positive state of a track entry, the device:
  - Sets the rule state to Active if the track entry is in Positive state.
  - Sets the rule state to Inactive if the track entry is in Negative state.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Associate security policy rule **rule1** with the Positive state of track entry 10.

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1] track positive 10
```

Related commands

display security-policy

track bfd (*Network Management and Monitoring Command Reference*)

track interface (*Network Management and Monitoring Command Reference*)

track ip route reachability (*Network Management and Monitoring Command Reference*)

track nqa (*Network Management and Monitoring Command Reference*)

user

Use **user** to specify a user as a filtering criterion of a security policy rule.

Use **undo user** to remove the specified user filtering criterion from a security policy rule.

Syntax

user *username* [**domain** *domain-name*]

undo user [*username* [**domain** *domain-name*]]

Default

No user is specified as a filtering criterion for a security policy rule.

Views

Security policy rule view

Predefined user roles

network-admin

context-admin

Parameters

username: Specifies a username, a case-sensitive string of 1 to 55 characters. The name cannot be **a**, **al**, or **all** and cannot contain at signs (@). If you do not specify this argument when executing the **undo user** command, the command removes all users from the rule. For more information about users and identity domains, see user identification in *Security Configuration Guide*.

domain *domain-name*: Matches the user in an identity domain. The *domain-name* argument represents the identity domain name, a case-insensitive string of 1 to 255 characters. The string cannot contain forward slashes (/), backslashes (\), vertical bars (|), colons (:), asterisks (*), question marks (?), left angle brackets (<), right angle brackets (>), or at signs (@). If you do not specify this option, the command matches the user among users that do not belong to any identity domain.

Usage guidelines

You can execute the command multiple times to specify multiple users as the filtering criteria.

Examples

Specify users **usera** and **userb** in identity domain **test** as the filtering criteria of security policy rule **rule1**.

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1] user usera domain test
[Sysname-security-policy-ip-0-rule1] user userb domain test
```

Related commands

display security-policy

user-identity enable

user-identity static-user

user-group

Use **user-group** to specify a user group as a filtering criterion of a security policy rule.

Use **undo user-group** to remove the specified user group filtering criterion from a security policy rule.

Syntax

user-group *user-group-name* [**domain** *domain-name*]

undo user-group [*user-group-name* [**domain** *domain-name*]]

Default

No user group is specified as a filtering criterion for a security policy rule.

Views

Security policy rule view

Predefined user roles

network-admin

context-admin

Parameters

user-group-name: Specifies the name of a user group, a case-insensitive string of 1 to 200 characters. If you do not specify this argument when executing the **undo user-group** command, the command removes all user groups from the rule. For more information about user groups and identity domains, see user identification in *Security Configuration Guide*.

domain *domain-name*: Matches the user group in an identity domain. The *domain-name* argument represents the identity domain name, a case-insensitive string of 1 to 255 characters. The string cannot contain forward slashes (/), backslashes (\), vertical bars (|), colons (:), asterisks (*), question marks (?), left angle brackets (<), right angle brackets (>), or at signs (@). If you do not specify this option, the command matches the user group among user groups that do not belong to any identity domain.

Usage guidelines

You can execute the command multiple times to specify multiple user groups as the filtering criteria.

Examples

Specify user groups **groupa** and **groupb** in identity domain **test** as the filtering criteria of security policy rule **rule1**.

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
```

```
[Sysname-security-policy-ip-0-rule1] user-group groupa domain test
[Sysname-security-policy-ip-0-rule1] user-group groupb domain test
```

Related commands

display security-policy

user-group

vrf

Use **vrf** to configure a security policy rule to take effect on received packets of the specified MPLS L3VPN instance.

Use **undo vrf** to restore the default.

Syntax

vrf *vrf-name*

undo vrf

Default

A security policy rule takes effect on received packets of the public network.

Views

Security policy rule view

Predefined user roles

network-admin

context-admin

Parameters

vrf-name: Specifies the name of an MPLS L3VPN instance, a case-sensitive string of 1 to 31 characters.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure security policy rule **rule1** to take effect on received packets of MPLS L3VPN instance **vpn1**.

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1] user-group groupa
[Sysname-security-policy-ip-0-rule1] user-group groupb
```

Related commands

display security-policy

Contents

ASPF commands

aspf apply policy

Use **aspf apply policy** to apply an ASPF policy to a zone pair.

Use **undo aspf apply policy** to remove an ASPF policy application from a zone pair.

Syntax

aspf apply policy *aspf-policy-number*

undo aspf apply policy *aspf-policy-number*

Default

The system applies the predefined ASPF policy to a zone pair when the zone pair is created.

Views

Zone pair view

Predefined user roles

network-admin

context-admin

Parameters

aspf-policy-number: Specifies an ASPF policy number. The value range for this argument is 1 to 256.

Usage guidelines

With the predefined policy, ASPF inspects FTP packets and packets of all transport layer protocols, but it does not perform ICMP error message check or the TCP SYN packet check.

The predefined ASPF policy cannot be modified. To change the ASPF policy application, define an ASPF policy and apply it to the zone pair.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Apply an ASPF policy to a zone pair.

```
<Sysname> system-view
[Sysname] security-zone name trust
[Sysname-security-zone-Trust] import interface gigabitethernet 1/0/1
[Sysname-security-zone-Trust] quit
[Sysname] security-zone name untrust
[Sysname-security-zone-Untrust] import interface gigabitethernet 1/0/2
[Sysname-security-zone-Untrust] quit
[Sysname] zone-pair security source trust destination untrust
[Sysname-zone-pair-security-Trust-Untrust] aspf apply policy 1
```

Related commands

aspf policy

display aspf all

zone-pair security

aspf icmp-error reply

Use **aspf icmp-error reply** to enable the device to send ICMP error messages upon packet dropping by interzone policies applied to zone pairs.

Use **undo aspf icmp-error reply** to restore the default.

Syntax

aspf icmp-error reply

undo aspf icmp-error reply

Default

The device does not send ICMP error messages when the device drops packets that do not match interzone policies applied to zone pairs.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

Typically, to reduce useless packets transmitted over the network and save bandwidth, do not use this command.

However, you must use this command when you use traceroute because ICMP error messages in this situation are required.

Examples

Enable ICMP error message sending upon packet dropping by interzone policies applied to zone pairs.

```
<Sysname> system-view
[Sysname] aspf icmp-error reply
```

aspf policy

Use **aspf policy** to create an ASPF policy and enter its view, or enter the view of an existing ASPF policy.

Use **undo aspf policy** to remove an ASPF policy.

Syntax

aspf policy *aspf-policy-number*

undo aspf policy *aspf-policy-number*

Default

No ASPF policies exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

aspf-policy-number: Assigns a number to the ASPF policy. The value range for this argument is 1 to 256.

Examples

Create ASPF policy 1 and enter its view.

```
<Sysname> system-view
[Sysname] aspf policy 1
[Sysname-aspf-policy-1]
```

Related commands

display aspf all

display aspf policy

detect

Use **detect** to configure ASPF inspection for an application layer protocol.

Use **undo detect** to restore the default.

Syntax

detect { **dns** [**action** { **drop** | **logging** } *] | { **ftp** | **h323** | **http** | **sccp** | **sip** | **smtp** } [**action drop**] | **gtp** | **ils** | **mgcp** | **nbt** | **pptp** | **rsh** | **rtsp** | **sqlnet** | **tftp** | **xdmcp** }

undo detect { **dns** | **ftp** | **gtp** | **h323** | **http** | **ils** | **mgcp** | **nbt** | **pptp** | **rsh** | **rtsp** | **sccp** | **sip** | **smtp** | **sqlnet** | **tftp** | **xdmcp** }

Default

ASPF inspects only transport layer protocols and application protocol FTP.

Views

ASPF policy view

Predefined user roles

network-admin

context-admin

Parameters

dns: Specifies DNS, an application layer protocol.

ftp: Specifies FTP, an application layer protocol.

gtp: Specifies GPRS Tunneling Protocol (GTP), an application layer protocol.

h323: Specifies H.323 protocol stack, application layer protocols.

http: Specifies HTTP, an application layer protocol.

ils: Specifies Internet Locator Service (ILS), an application layer protocol.

mgcp: Specifies Media Gateway Control Protocol (MGCP), an application layer protocol.

nbt: Specifies NetBIOS over TCP/IP (NBT), an application layer protocol.

pptp: Specifies Point-to-Point Tunneling Protocol (PPTP), an application layer protocol.

rsh: Specifies Remote Shell (RSH), an application layer protocol.

rtsp: Specifies Real Time Streaming Protocol (RTSP), an application layer protocol.

sccp: Specifies Skinny Client Control Protocol (SCCP), an application layer protocol.

sip: Specifies Session Initiation Protocol (SIP), an application layer protocol.

smtp: Specifies SMTP, an application layer protocol.

sqlnet: Specifies SQLNET, an application layer protocol.

tftp: Specifies TFTP, an application layer protocol.

xdmcp: Specifies X Display Manager Control Protocol (XDMCP), an application layer protocol.

action: Specifies an action on the packets that do not pass the protocol status validity check. If you do not specify an action, ASPF does not perform the protocol status validity check, and it only maintains connection status information.

drop: Drops the packets that do not pass the protocol status validity check.

logging: Generates log messages for packets that do not pass the protocol status validity check.

Usage guidelines

This command is required to ensure successful data connections for multichannel protocols when either of the following conditions exists:

- The ALG feature is disabled in other service modules (such as NAT).
- Other service modules with the ALG feature (such as DPI) are not configured.

This command is optional for multichannel protocols if ALG is enabled in other service modules (such as NAT) or if other service modules with the ALG feature are configured.

Application protocols supported by this command (except HTTP, SMTP, and TFTP) are multichannel protocols.

Repeat the **detect** command to configure ASPF inspection for multiple application protocols.

ASPF inspection for transport layer protocols is always enabled and is not configurable. The supported transport layer protocols include TCP, UDP, UDP-Lite, SCTP, Raw IP, ICMP, ICMPv6, and DCCP.

This command configures ASPF inspection for application protocols. ASPF inspection supports protocol status validity check for application protocols of DNS, FTP, H323, HTTP, SCCP, SIP, and SMTP. The device deals with packets with invalid protocol status according to the actions you have specified. To configure protocol status validity check for an application protocol, you must specify the **action** keyword.

Examples

Configure ASPF inspection for FTP packets.

```
<Sysname> system-view
[Sysname] aspf policy 1
[Sysname-aspf-policy-1] detect ftp
```

Configure ASPF inspection for DNS packets, drop packets that fail protocol status validity check and generate log messages for these packets.

```
<Sysname> system-view
[Sysname] aspf policy 1
[Sysname-aspf-policy-1] detect dns action drop logging
```

Related commands

display aspf policy

display aspf all

Use **display aspf all** to display the configuration of all ASPF policies and their applications.

Syntax

display aspf all

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display the configuration of all ASPF policies and their applications.

```
<Sysname> display aspf all
ASPF policy configuration:
  Policy default:
    ICMP error message check: Disabled
    Inspected protocol    Action
      FTP                  None
  Policy number: 1
    ICMP error message check: Disabled
    TCP SYN packet check: Disabled
    Inspected protocol    Action
      FTP                  None


Zone-pair security application:
  Source Trust destination Untrust
    Apply ASPF policy: default
```

Table 1 Command output

Field	Description
Policy default	Predefined ASPF policy.
ICMP error message check	Whether ICMP error message check is enabled.
TCP SYN packet check	Whether TCP SYN check is enabled.
Inspected protocol	Protocols to be inspected by ASPF.
Action	Actions on the detected illegal packets: • **Drop**—Drops illegal packets. • **Log**—Generates log messages for illegal packets. • **None**—Allows illegal packets to pass. If the protocol does not support the action configuration, this field displays a hyphen (-).
Zone-pair security application	Information about zone-pair security application.

Field	Description
Source *XXX* destination *XXX*	Source zone and destination zone.
Apply ASPF policy	Number of ASPF policy applied to the zone pair.

Related commands

aspf apply policy

aspf policy

display aspf policy

display aspf policy

Use **display aspf policy** to display the configuration of an ASPF policy.

Syntax

display aspf policy { *aspf-policy-number* | **default** }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

aspf-policy-number: Specifies the number of an ASPF policy. The value range for this argument is 1 to 256.

default: Specifies the predefined ASPF policy.

Examples

Display the configuration of ASPF policy 1.

```
<Sysname> display aspf policy 1
ASPF policy configuration:
  Policy number: 1
    ICMP error message check: Disabled
    TCP SYN packet check: Enabled
    Inspected protocol   Action
     FTP                  Drop
     HTTP                 None
     RSH                  -
```

Table 2 Command output

Field	Description
ICMP error message check	Whether ICMP error message check is enabled.
TCP SYN packet check	Whether TCP SYN check is enabled.
Inspected protocol	Protocols to be inspected by ASPF.

Field	Description
Action	Actions on the detected illegal packets: • **Drop**—Drops illegal packets. • **Log**—Generates log messages for illegal packets. • **None**—Allows illegal packets to pass. If the protocol does not support the action configuration, this field displays a hyphen (-).

Related commands

aspf policy

display aspf session

Use **display aspf session** to display ASPF sessions.

Syntax

display aspf session [**ipv4** | **ipv6**] [**slot** *slot-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ipv4: Displays IPv4 ASPF sessions.

ipv6: Displays IPv6 ASPF sessions.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays ASPF sessions for all member devices.

verbose: Displays detailed information about ASPF sessions. If you do not specify this keyword, the command displays the brief information about ASPF sessions.

Usage guidelines

If you do not specify the **ipv4** keyword or the **ipv6** keyword, this command displays all ASPF sessions on the device.

Examples

Display brief information about IPv4 ASPF sessions.

```
<Sysname> display aspf session ipv4
Slot 1:
Initiator:
  Source      IP/port: 192.168.1.18/1877
  Destination IP/port: 192.168.1.55/22
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
```

```
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: SrcZone
Initiator:
  Source      IP/port: 192.168.1.18/1792
  Destination IP/port: 192.168.1.55/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: SrcZone

Total sessions found: 2
```

Display detailed information about IPv4 ASPF sessions.

```
<Sysname> display aspf session ipv4 verbose
```

Slot 1:

```
Initiator:
  Source      IP/port: 192.168.1.18/1877
  Destination IP/port: 192.168.1.55/22
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: SrcZone
Responder:
  Source      IP/port: 192.168.1.55/22
  Destination IP/port: 192.168.1.18/1877
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: DestZone
State: TCP_SYN_SENT
Application: SSH
Start time: 2011-07-29 19:12:36  TTL: 28s
Initiator->Responder:         1 packets         48 bytes
Responder->Initiator:         0 packets          0 bytes

Initiator:
  Source      IP/port: 192.168.1.18/1792
  Destination IP/port: 192.168.1.55/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: SrcZone
Responder:
  Source      IP/port: 192.168.1.55/1792
  Destination IP/port: 192.168.1.18/0
```

```
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: DestZone
State: ICMP_REQUEST
Application: OTHER
Start time: 2011-07-29 19:12:33  TTL: 55s
Initiator->Responder:         1 packets         6048 bytes
Responder->Initiator:         0 packets          0 bytes

Total sessions found: 2
```

Table 3 Command output

Field	Description
Initiator	Session information from initiator to responder.
Responder	Session information from responder to initiator.
Source IP/port	Source IP address and port number.
Destination IP/port	Destination IP address and port number.
DS-Lite tunnel peer	IP address of the DS-Lite tunnel peer. If the session is not tunneled by DS-Lite, this field displays a hyphen (-).
VPN-instance/VLAN ID/Inline ID	• **VPN-instance**—MPLS L3VPN instance where the session is initiated. • **VLAN ID**—VLAN to which the session belongs during Layer 2 forwarding. • **Inline ID**—Inline to which the session belongs during Layer 2 forwarding. If no MPLS L3VPN instance, VLAN ID, or Inline ID is specified, a hyphen (-) is displayed for each field.
Protocol	Transport layer protocols, including DCCP, ICMP, ICMPv6, Raw IP, SCTP, TCP, UDP, and UDP-Lite. Number in parentheses represents the protocol number.
Source security zone	Security zone to which the inbound interface belongs. If the inbound interface does not belong to any security zone, this field displays a hyphen (-).
State	Protocol status of the session.
Application	Application layer protocol, including FTP and DNS. If it is an unknown protocol identified by an unknown port, this field displays **OTHER**.
Start time	Establishment time of the session.
TTL	Remaining lifetime of the session, in seconds.
Initiator->Responder	Number of packets and bytes from initiator to responder.
Responder->Initiator	Number of packets and bytes from responder to initiator.

Related commands

reset aspf session

icmp-error drop

Use **icmp-error drop** to enable ICMP error message dropping.

Use **undo icmp-error drop** to disable ICMP error message dropping.

Syntax

icmp-error drop

undo icmp-error drop

Default

ICMP error message dropping is disabled.

Views

ASPF policy view

Predefined user roles

network-admin

context-admin

Usage guidelines

An ICMP error message carries information about the corresponding connection. ICMP error message dropping verifies the information. If the information does not match the connection, ASPF drops the message.

Examples

Enable ICMP error message dropping for ASPF policy 1.

```
<Sysname> system-view
[Sysname] aspf policy 1
[Sysname-aspf-policy-1] icmp-error drop
```

Related commands

aspf policy

display aspf policy

reset aspf session

Use **reset aspf session** to clear ASPF session statistics.

Syntax

reset aspf session [**ipv4** | **ipv6**] [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

ipv4: Clears IPv4 ASPF session statistics.

ipv6: Clears IPv6 ASPF session statistics.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears ASPF session statistics for all member devices.

Usage guidelines

If you do not specify the **ipv4** keyword or the **ipv6** keyword, this command clears all ASPF session statistics.

Examples

Clear all ASPF session statistics.

```
<Sysname> reset aspf session
```

Related commands

display aspf session

tcp syn-check

Use **tcp syn-check** to enable TCP SYN check.

Use **undo tcp syn-check** to disable TCP SYN check.

Syntax

tcp syn-check

undo tcp syn-check

Default

TCP SYN check is disabled.

Views

ASPF policy view

Predefined user roles

network-admin

context-admin

Usage guidelines

TCP SYN check checks the first packet to establish a TCP connection whether it is a SYN packet. If the first packet is not a SYN packet, ASPF drops the packet.

When a router attached to the network is started up, it can receive a non-SYN packet of an existing TCP connection for the first time. If you do not want to interrupt the existing TCP connection, you can disable the TCP SYN check. Then, the router allows the non-SYN packet that is the first packet to establish a TCP connection to pass. After the network topology becomes steady, you can enable TCP SYN check again.

Examples

Enable TCP SYN check for ASPF policy 1.

```
<Sysname> system-view
[Sysname] aspf policy 1
[Sysname-aspf-policy-1] tcp syn-check
```

Related commands

`aspf policy`

Contents

Session management commands

display session aging-time application

Use **display session aging-time application** to display the aging time for sessions of different application layer protocols or applications.

Syntax

display session aging-time application

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display the aging time for sessions of different application layer protocols and applications.

```
<Sysname> display session aging-time application
Application                                                     Aging time(s)
bootpc                                                          120
bootps                                                          120
dns                                                             30
ftp                                                             3600
ftp-data                                                        240
gprs-data                                                       60
gprs-sig                                                        60
gtp-control                                                     60
gtp-user                                                        60
h225                                                            3600
h245                                                            3600
https                                                           600
ils                                                             3600
l2tp                                                            120
mgcp-callagent                                                  60
mgcp-gateway                                                    60
netbios-dgm                                                     3600
netbios-ns                                                      3600
netbios-ssn                                                     3600
ntp                                                             120
pptp                                                            3600
qq                                                              120
ras                                                             300
rip                                                             120
rsh                                                             60
```

```
rtsp                                    3600
sccp                                    3600
sip                                     300
snmp                                    120
snmptrap                                120
sqlnet                                  600
stun                                    600
syslog                                  120
tacacs-ds                               120
tftp                                    60
who                                     120
xdmcp                                   3600
others:                                 1200
```

Table 1 Command output

Field	Description
Application	Name of an application layer protocol or an application.
Aging time(s)	Aging time in seconds.
others:1200	All application layer protocols and applications whose aging time is 1200 seconds is displayed as **others**.

Related commands

`session aging-time application`

display session aging-time state

Use **`display session aging-time stat`** to display the aging time for sessions in different protocol states.

Syntax

`display session aging-time state`

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display the aging time for sessions in different protocol states.

```
<Sysname> display session aging-time state
State                   Aging Time(s)
SYN                     10
TCP-EST                 3600
FIN                     10
UDP-OPEN                10
```

```
UDP-READY                30
ICMP-REQUEST             30
ICMP-REPLY               10
RAWIP-OPEN               30
RAWIP-READY              60
UDPLITE-OPEN             30
UDPLITE-READY            60
DCCP-REQUEST             30
DCCP-EST                 3600
DCCP-CLOSEREQ            30
SCTP-INIT                30
SCTP-EST                 3600
SCTP-SHUTDOWN            30
ICMPV6-REQUEST           60
ICMPV6-REPLY             30
TCP-TIME-WAIT            2
TCP-CLOSE                2
```

Table 2 Command output

Field	Description
State	Protocol state.
Aging Time(s)	Aging time in seconds.

Related commands

session aging-time state

display session dual-active transparent statistics

Use **display session dual-active transparent statistics** to display statistics about transparently transmitted packets in session dual-active mode.

Syntax

display session dual-active transparent statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays packet statistics for all member devices.

Examples

Display statistics about transparently transmitted packets in session dual-active mode.

```
<Sysname> display session dual-active transparent statistics
Slot 1:
          UDP relay packets :                   0
         Hash relay packets :                   0
      Sent relay packets :                      0
    Received relay packets :                    0
```

Table 3 Command output

Field	Description
UDP relay packets	Number of transparently transmitted UDP packets.
Hash relay packets	Number of packets for which sessions are created according to the result of source IP-based hashing.
Sent relay packets	Number of sent packets that are transparently transmitted.
Received relay packets	Number of received packets that are transparently transmitted.

Related commands

session dual-active enable

session statistics enable

display session fast-drop statistics

Use **display session fast-drop statistics** to display unicast deny session statistics.

Syntax

display session fast-drop statistics [**summary**] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

summary: Displays summary information about unicast deny session statistics. If you do not specify this keyword, the command displays detailed information about unicast deny session statistics.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information on all member devices.

Examples

Display detailed information about unicast deny session statistics.

```
<Sysname> display session fast-drop statistics
Slot 1:
Current : 1
  Session type             Est count
```

```
            TCP :                    0
            UDP :                    0
           ICMP :                    1
         ICMPv6 :                    0
       UDP-Lite :                    0
           SCTP :                    0
           DCCP :                    0
          RAWIP :                    0
            DNS :                    0
            FTP :                    0
            GTP :                    0
           H323 :                    0
           HTTP :                    0
            ILS :                    0
           MGCP :                    0
            NBT :                    0
           PPTP :                    0
            RSH :                    0
           RTSP :                    0
           SCCP :                    0
            SIP :                    0
           SMTP :                    0
         SQLNET :                    0
            SSH :                    0
         TELNET :                    0
           TFTP :                    0
          XDMCP :                    0
Deny session establishment rate: 0/s
 Session type               Est count
            TCP :                  0/s
            UDP :                  0/s
           ICMP :                  0/s
         ICMPv6 :                  0/s
       UDP-Lite :                  0/s
           SCTP :                  0/s
           DCCP :                  0/s
          RAWIP :                  0/s
```

Table 4 Command output

Field	Description
Current	Total number of unicast deny sessions.
Session type	Deny session type: • TCP. • UDP. • ICMP. • ICMPv6. • UDP-Lite. • SCTP.

Field	Description
	• DCCP. • RAWIP. • DNS. • FTP. • GTP. • H323. • HTTP. • ILS. • MGCP. • NBT. • PPTP. • RSH. • RTSP. • SCCP. • SIP. • SMTP. • SQLNET. • SSH. • TELNET. • TFTP. • XDMCP.
Est count	Number of deny sessions created for each protocol.
Deny session establishment rate	Rate of deny session establishment.
Session type	Deny session type: • TCP. • UDP. • ICMP. • ICMPv6. • UDP-Lite. • SCTP. • DCCP. • RAWIP.
Est count	Number of deny sessions created per second for each protocol.

Display summary information about unicast deny session statistics.

```
<Sysname> display session fast-drop statistics summary
Slot 1:
type      Sessions  TCP sessions  UDP sessions  Rate      TCP rate  UDP rate
Est       1         0             0             1/s       0/s       0/s
Try       47        0             0             1/s       0/s       0/s
```

Table 5 Command output

Field	Description
type	Deny session type: • **Est**—Successfully created deny session. • **Try**—Deny session that the system attempted to create.

Field	Description
Sessions	Total number of unicast deny sessions.
TCP sessions	Number of TCP unicast deny sessions.
UDP sessions	Number of UDP unicast deny sessions.
Rate	Rate of unicast deny session creation.
TCP rate	Rate of TCP unicast deny session creation.
UDP rate	Rate of UDP unicast deny session creation.

display session fast-drop table ipv4

Use **display session fast-drop table ipv4** to display IPv4 unicast deny session entries.

Syntax

display session fast-drop table ipv4 [**slot** *slot-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information on all member devices.

verbose: Displays detailed information about IPv4 unicast deny session entries. If you do not specify this keyword, the command displays brief information about IPv4 unicast deny session entries.

Examples

Display brief information about all IPv4 unicast deny session entries.

```
<Sysname> display session fast-drop table ipv4
Slot 1:
Initiator:
  Source      IP/port: 192.168.1.18/1877
  Destination IP/port: 192.168.1.55/22
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: Trust
Total deny session found: 1
```

Display detailed information about all IPv4 unicast deny session entries.

```
<Sysname> display session fast-drop table ipv4 verbose
Slot 1:
```

```
Initiator:
  Source      IP/port: 192.168.1.18/1877
  Destination IP/port: 192.168.1.55/22
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: Trust
Responder:
  Source      IP/port: 192.168.1.55/22
  Destination IP/port: 192.168.1.18/1877
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Local
State: TCP_SYN_SENT
Application: SSH
Rule ID: 1
Rule name: test
Start time: 2011-07-29 19:12:36  TTL: 28s
Initiator->Responder:         1 packets         48 bytes
Responder->Initiator:         0 packets          0 bytes
Total deny session found: 1
```

Table 6 Command output

Field	Description
Initiator	Information about the unicast deny session from the initiator to the responder.
Responder	Information about the unicast deny session from the responder to the initiator.
DS-Lite tunnel peer	Address of the DS-Lite tunnel peer. When the unicast deny session is not tunneled by DS-Lite, this field displays a hyphen (**-**).
VPN instance/VLAN ID/Inline ID	MPLS L3VPN instance to which the unicast deny session belongs. VLAN and inline to which the deny session belongs during Layer 2 forwarding. If a parameter is not specified, a hyphens (-) is displayed for the proper field.
Protocol	Transport layer protocol: • DCCP. • ICMP. • ICMPv6. • Raw IP. • SCTP. • TCP. • UDP. • UDP-Lite. The number in the brackets indicates the protocol number.
Inbound interface	Interface on which packets are received.

Field	Description
Source security zone	Security zone to which the inbound interface belongs. If the inbound interface does not belong to any security zone, this field displays a hyphen (**-**).
State	Unicast deny session state.
Application	Application layer protocol, FTP or DNS. If it is an unknown protocol identified by an unknown port, this field displays **OTHER**.
Rule ID	ID of the security policy rule.
Rule name	Name of the security policy rule.
Start time	Unicast deny session establishment time.
TTL	Remaining lifetime of the unicast deny session, in seconds.
Initiator->Responder	Number of packets and bytes from the initiator to the responder.
Responder->Initiator	Number of packets and bytes from the responder to the initiator.
Total deny session found	Total number of found unicast deny session entries.

display session fast-drop table ipv6

Use **display session fast-drop table ipv6** to display IPv6 unicast deny session entries.

Syntax

display session fast-drop table ipv6 [**slot** *slot-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information on all member devices.

verbose: Displays detailed information about IPv6 unicast deny session entries. If you do not specify this keyword, the command displays brief information about IPv6 unicast deny session entries.

Examples

Display brief information about all IPv6 unicast deny session entries.

```
<Sysname> display session fast-drop table ipv6
Slot 1:
Initiator:
  Source      IP/port: 2011::2/58473
  Destination IP/port: 2011::8/32768
  DS-Lite tunnel peer: -
```

```
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: Trust
Total deny session found: 1
```

Display detailed information about all IPv6 unicast deny session entries.

```
<Sysname> display session fast-drop table ipv6 verbose
Slot 1:
Initiator:
  Source      IP/port: 2011::2/58473
  Destination IP/port: 2011::8/32768
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: Trust
Responder:
  Source      IP/port: 192.168.1.55/22
  Destination IP/port: 192.168.1.18/1877
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Local
State: TCP_SYN_SENT
Application: SSH
Rule ID: 1
Rule name: test
Start time: 2011-07-29 19:12:36  TTL: 28s
Initiator->Responder:         1 packets         48 bytes
Responder->Initiator:         0 packets          0 bytes
Total deny session found: 1
```

Table 7 Command output

Field	Description
Initiator	Information about the unicast deny session from the initiator to the responder.
Responder	Information about the unicast deny session from the responder to the initiator.
DS-Lite tunnel peer	Address of the DS-Lite tunnel peer. When the unicast deny session is not tunneled by DS-Lite, this field displays a hyphen (**-**).
VPN instance/VLAN ID/Inline ID	MPLS L3VPN instance to which the unicast deny session belongs. VLAN and inline to which the unicast deny session belongs during Layer 2 forwarding. If a parameter is not specified, a hyphens (**-**) is displayed for the proper field.
Protocol	Transport layer protocol: • DCCP.

Field	Description
	• ICMP. • ICMPv6. • Raw IP. • SCTP. • TCP. • UDP. • UDP-Lite. The number in the brackets indicates the protocol number.
Inbound interface	Interface on which packets are received.
Source security zone	Security zone to which the inbound interface belongs. If the inbound interface does not belong to any security zone, this field displays a hyphen (-).
State	Unicast deny session state.
Application	Application layer protocol, FTP or DNS. If it is an unknown protocol identified by an unknown port, this field displays **OTHER**.
Rule ID	ID of the security policy rule.
Rule name	Name of the security policy rule.
Start time	Unicast deny session establishment time.
TTL	Remaining lifetime of the unicast deny session, in seconds.
Initiator->Responder	Number of packets and bytes from the initiator to the responder.
Responder->Initiator	Number of packets and bytes from the responder to the initiator.
Total deny session found	Total number of found unicast deny session entries.

display session fast-drop top-statistics

Use **display session fast-drop top-statistics** to display top deny session statistics.

Syntax

display session fast-drop top-statistics { last-1-hour | last-24-hours | last-30-days }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

last-1-hour: Displays top deny session statistics in last hour.

last-24-hours: Displays top deny session statistics in last 24 hours.

last-30-days: Displays top deny session statistics in last 30 days.

Usage guidelines

This command displays nothing if the top deny session statistics feature is disabled. A maximum of 10 session items can be displayed.

Examples

Display top deny session statistics in last hour.

```
<Sysname> display session fast-drop top-statistics last-1-hour
Counting by source addresses:
No.      Source address          Sessions
1        8.1.1.1                 6085
2        111.15.111.16           10
3        6::2                    2

Counting by destination addresses:
No.      Destination address     Sessions
1        8.1.1.2                 6085
2        6::3                    2
3        30.1.1.8                1
4        30.1.1.4                1
5        30.1.1.11               1
6        30.1.1.9                1
7        30.1.1.6                1
8        30.1.1.5                1
9        30.1.1.7                1
10       30.1.1.3                1
```

Table 8 Command output

Field	Description
Counting by source addresses	Top deny session statistics based on source addresses.
Counting by destination addresses	Top deny session statistics based on destination addresses.
No.	Ranking number.
Source address	Source IP address of the deny sessions.
Destination address	Destination IP address of the deny sessions.
Sessions	Total number of deny sessions.

Related commands

session fast-drop enable

session fast-drop top-statistics enable

display session relation-table

Use **display session relation-table** to display relation entries.

Syntax

display session relation-table { **ipv4** | **ipv6** } [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ipv4: Specifies IPv4 relation entries.

ipv6: Specifies IPv6 relation entries.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays relation entries for all member devices.

Examples

Display all IPv4 relation entries.

```
<Sysname> display session relation-table ipv4
Slot 1:
Source IP/port:      192.168.1.100/-
Destination IP/port: 192.168.2.100/99
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: 1/-/-
Protocol: TCP(6)    TTL: 1234s    App: FTP-DATA

Source IP/port:      -/-
Destination IP/port: 192.168.2.200/1212
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: 1/-/-
Protocol: TCP(6)    TTL: 3100s    App: H225

Total entries found:  2
```

Display all IPv6 relation entries.

```
<Sysname> display session relation-table ipv6
Slot 1:
Source IP:             2011::0002
Destination IP/port: 2011::0008/1212
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: TCP(6)    TTL: 567s    App: FTP-DATA

Total entries found:  1
```

Table 9 Command output

Field	Description
Source IP/port	Source IP address and port number of the session. If the IP or port number is not specified, this field displays a hyphen (-). For an IPv6 relation entry, the source port number is not displayed.
Destination IP/port	Destination IP address and port number of the session.

Field	Description
DS-Lite tunnel peer	Peer tunnel interface address of the DS-Lite tunnel to which the session belongs. If no peer tunnel interface address is specified, a hyphen (-) is displayed.
VPN instance/VLAN ID/ Inline ID	MPLS L3VPN instance to which the relation entry belongs. VLAN and inline to which the relation entry belongs during Layer 2 forwarding. If a parameter is not specified, a hyphen (-) is displayed for the proper field.
Protocol	Transport layer protocol.
TTL	Remaining lifetime of the relation entry, in seconds.
App	Application layer protocol.
Total entries found	Total number of found relation entries.

display session statistics

Use **display session statistics** to display unicast session statistics.

Syntax

display session statistics [**history-max** | **summary**] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

history-max: Displays history statistics of the maximum unicast sessions and the maximum unicast session establishment rates. If you do not specify this keyword, the command displays all unicast session statistics.

summary: Displays summary information about unicast session statistics. If you do not specify this keyword, the command displays detailed information about unicast session statistics.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays unicast session statistics for all member devices.

Usage guidelines

If you do not specify any parameters, this command displays detailed information about the current unicast session statistics.

Examples

Display detailed information about unicast session statistics.

```
<Sysname> display session statistics
Slot 1:
Current sessions: 3
```

```
          TCP sessions:                   0
          UDP sessions:                   0
         ICMP sessions:                   3
       ICMPv6 sessions:                   0
     UDP-Lite sessions:                   0
         SCTP sessions:                   0
         DCCP sessions:                   0
        RAWIP sessions:                   0
          DNS sessions:                   0
          FTP sessions:                   0
          GTP sessions:                   0
         H323 sessions:                   0
         HTTP sessions:                   0
          ILS sessions:                   0
         MGCP sessions:                   0
          NBT sessions:                   0
         PPTP sessions:                   0
          RSH sessions:                   0
         RTSP sessions:                   0
         SCCP sessions:                   0
          SIP sessions:                   0
         SMTP sessions:                   0
       SQLNET sessions:                   0
          SSH sessions:                   0
       TELNET sessions:                   0
         TFTP sessions:                   0
        XDMCP sessions:                   0
History average sessions per second:
      Past hour: 1
      Past 24 hours: 0
      Past 30 days: 0
History average session establishment rate:
      Past hour: 0/s
      Past 24 hours: 0/s
      Past 30 days: 0/s
Current relation-table entries: 0
Relation table establishment rate: 0/s
Session establishment rate: 0/s
          TCP:                  0/s
          UDP:                  0/s
         ICMP:                  0/s
       ICMPv6:                  0/s
     UDP-Lite:                  0/s
         SCTP:                  0/s
         DCCP:                  0/s
        RAWIP:                  0/s
Received TCP      :                  0 packets                  0 bytes
Received UDP      :                118 packets              13568 bytes
```

```
Received ICMP     :                105 packets                 8652 bytes
Received ICMPv6   :                  0 packets                    0 bytes
Received UDP-Lite :                  0 packets                    0 bytes
Received SCTP     :                  0 packets                    0 bytes
Received DCCP     :                  0 packets                    0 bytes
Received RAWIP    :                  0 packets                    0 bytes
```

Table 10 Command output

Field	Description
Current sessions	Total number of unicast sessions.
TCP sessions	Number of TCP sessions.
UDP sessions	Number of UDP sessions.
ICMP sessions	Number of ICMP sessions.
ICMPv6 sessions	Number of ICMPv6 sessions.
UDP-Lite sessions	Number of UDP-Lite sessions.
SCTP sessions	Number of SCTP sessions.
DCCP sessions	Number of DCCP sessions.
RAWIP sessions	Number of Raw IP sessions.
DNS sessions	Number of DNS unicast sessions.
FTP sessions	Number of FTP unicast sessions.
GTP sessions	Number of GTP unicast sessions.
H323 sessions	Number of H.323 unicast sessions.
HTTP sessions	Number of HTTP unicast sessions.
ILS sessions	Number of ILS unicast sessions.
MGCP sessions	Number of MGCP unicast sessions.
NBT sessions	Number of NBT unicast sessions.
PPTP sessions	Number of PPTP unicast sessions.
RSH sessions	Number of RSH unicast sessions.
RTSP sessions	Number of RTSP unicast sessions.
SCCP sessions	Number of SCCP unicast sessions.
SIP sessions	Number of SIP unicast sessions.
SMTP sessions	Number of SMTP unicast sessions.
SQLNET sessions	Number of SQLNET unicast sessions.
SSH sessions	Number of SSH unicast sessions.
TELNET sessions	Number of Telnet unicast sessions.

Field	Description
TFTP sessions	Number of TFTP unicast sessions.
XDMCP sessions	Number of XDMCP unicast sessions.
History average sessions per second	History statistics of average sessions per second.
Past hour	The average number of sessions per second in the most recent hour.
Past 24 hours	The average number of sessions per second in the most recent 24 hours.
Past 30 days	The average number of sessions per second in the most recent 30 days.
History average session establishment rate	History statistics of average session establishment rates.
Past hour	The average session establishment rate in the most recent hour.
Past 24 hours	The average session establishment rate in the most recent 24 hours.
Past 30 days	The average session establishment rate in the most recent 30 days.
Current relation-table entries	Total number of relation entries.
Relation table establishment rate	Rate of relation table establishment.
Session establishment rate	Unicast session establishment rate, and rates for establishing unicast sessions of different protocols.
Received TCP	Number of received TCP packets and bytes.
Received UDP	Number of received UDP packets and bytes.
Received ICMP	Number of received ICMP packets and bytes.
Received ICMPv6	Number of received ICMPv6 packets and bytes.
Received UDP-Lite	Number of received UDP-Lite packets and bytes.
Received SCTP	Number of received SCTP packets and bytes.
Received DCCP	Number of received DCCP packets and bytes.
Received RAWIP	Number of received Raw IP packets and bytes.

Display summary information about unicast session statistics.

```
<Sysname> display session statistics summary
Slot Sessions  TCP       UDP       Rate      TCP rate  UDP rate
1    3         0         0         0/s       0/s       0/s
```

Table 11 Command output

Field	Description
Sessions	Total number of unicast sessions.
TCP	Number of TCP unicast sessions.

Field	Description
UDP	Number of UDP unicast sessions.
Rate	Rate of unicast session creation.
TCP rate	Rate of TCP unicast session creation.
UDP rate	Rate of UDP unicast session creation.

Display history statistics of the maximum unicast sessions and maximum unicast session establishment rates.

```
<Sysname> display session statistics history-max
Slot 1
Max sessions: 20084                           Time: 2017-03-04 12:03:53
Max session establishment rate: 9080/s        Time: 2017-03-04 12:03:53
Max TCP sessions: 20084                       Time: 2017-03-04 12:03:53
Max TCP session establishment rate: 9080/s    Time: 2017-03-04 12:03:53
Max UDP sessions: 0                           Time: 2017-03-04 12:03:53
Max UDP session establishment rate: 0         Time: 2017-03-04 12:03:53
```

Table 12 Command output

Field	Description
Max sessions	History statistics of the maximum unicast sessions.
Max session establishment rate	History statistics of the maximum rate at which unicast sessions were created.
Max TCP sessions	History statistics of the maximum TCP unicast sessions.
Max TCP session establishment rate	History statistics of the maximum rate at which TCP unicast sessions were created.
Max UDP sessions	History statistics of the maximum UDP unicast sessions.
Max UDP session establishment rate	History statistics of the maximum rate at which UDP unicast sessions were created.

display session statistics ipv4

Use **display session statistics ipv4** to display IPv4 unicast session statistics.

Syntax

display session statistics ipv4 [[**responder**] { **application** *application-name* | **destination-ip** *destination-ip* | **destination-port** *destination-port* | **destination-zone** *destination-zone-name* | **interface** *interface-type interface-number* | **protocol** { **dccp** | **dns** | **ftp** | **gtp** | **h323** | **http** | **icmp** | **ils** | **mgcp** | **nbt** | **pptp** | **raw-ip** | **rsh** | **rtsp** | **sccp** | **sctp** | **sip** | **smtp** | **sqlnet** | **ssh** | **tcp** | **telnet** | **tftp** | **udp** | **udp-lite** | **xdmcp** } | **security-policy-rule** *rule-name* | **source-ip** *source-ip* | **source-port** *source-port* | **source-zone** *source-zone-name* | **state** { **dccp-closereq** | **dccp-closing** | **dccp-open** | **dccp-partopen** | **dccp-request** | **dccp-respond** | **dccp-timewait** | **icmp-reply** | **icmp-request** | **rawip-open** | **rawip-ready** | **sctp-closed** | **sctp-cookie-echoed** | **sctp-cookie-wait** | **sctp-established** | **sctp-shutdown-ack-sent** | **sctp-shutdown-recd** | **sctp-shutdown-sent** |

tcp-close | **tcp-close-wait** | **tcp-est** | **tcp-fin-wait** | **tcp-last-ack** | **tcp-syn-recv** | **tcp-syn-sent** | **tcp-syn-sent2** | **tcp-time-wait** | **udp-open** | **udp-ready** | **udplite-open** | **udplite-ready** } | **vpn-instance** *vpn-instance-name* } *] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

responder: Displays statistics about IPv4 unicast sessions from the responder to the initiator. If you do not specify this keyword, the command displays statistics about IPv4 unicast sessions from the initiator to the responder.

application *application-name*: Specifies an application protocol by its name. The *application-name* argument is a case-insensitive string of 1 to 63 characters. The names **invalid** and **other** are not allowed.

destination-ip *destination-ip*: Specifies a destination IPv4 address for a unicast session.

destination-port *destination-port*: Specifies a destination port by its number. The *destination-port* argument specifies the destination port of an IPv6 unicast session. The value range for the *destination-port* argument is 0 to 65535.

destination-zone *destination-zone-name*: Specifies a destination security zone by its name, a case-insensitive string of 1 to 31 characters.

interface *interface-type interface-num*: Specifies an interface by its type and number.

protocol { **dccp** | **dns** | **ftp** | **gtp** | **h323** | **http** | **icmp** | **ils** | **mgcp** | **nbt** | **pptp** | **raw-ip** | **rsh** | **rtsp** | **sccp** | **sctp** | **sip** | **smtp** | **sqlnet** | **ssh** | **tcp** | **telnet** | **tftp** | **udp** | **udp-lite** | **xdmcp** }: Specifies an IPv4 protocol.

security-policy-rule *rule-name*: Specifies a security policy rule by its name for session filtering. The *rule-name* argument represents the name of the security policy rule, a case-sensitive string of 1 to 127 characters.

source-ip *source-ip*: Specifies a source IPv4 address for a unicast session.

source-port *source-port*: Specifies a source port by its number. The *source-port* argument specifies the source port of an IPv4 unicast session. The value range for the *source-port* argument is 0 to 65535.

source-zone *source-zone-name*: Specifies a source security zone by its name, a case-insensitive string of 1 to 31 characters.

state { **dccp-closereq** | **dccp-closing** | **dccp-open** | **dccp-partopen** | **dccp-request** | **dccp-respond** | **dccp-timewait** | **icmp-reply** | **icmp-request** | **rawip-open** | **rawip-ready** | **sctp-closed** | **sctp-cookie-echoed** | **sctp-cookie-wait** | **sctp-established** | **sctp-shutdown-ack-sent** | **sctp-shutdown-recd** | **sctp-shutdown-sent** | **tcp-close** | **tcp-close-wait** | **tcp-est** | **tcp-fin-wait** | **tcp-last-ack** | **tcp-syn-recv** | **tcp-syn-sent** | **tcp-syn-sent2** | **tcp-time-wait** | **udp-open** | **udp-ready** | **udplite-open** | **udplite-ready** }: Specifies a protocol state.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command displays IPv4 unicast session statistics in the public network.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv4 unicast session statistics for all member devices.

Usage guidelines

If you do not specify any parameters, this command displays all IPv4 unicast session statistics.

Examples

Display statistics for unicast sessions from IP address 111.15.111.66.

```
<Sysname> display session statistics ipv4 source-ip 111.15.111.66
Slot 1:
Current sessions: 3
          TCP sessions:                   0
          UDP sessions:                   0
         ICMP sessions:                   3
     UDP-Lite sessions:                   0
         SCTP sessions:                   0
         DCCP sessions:                   0
        RAWIP sessions:                   0

          DNS sessions:                   0
          FTP sessions:                   0
          GTP sessions:                   0
         H323 sessions:                   0
         HTTP sessions:                   0
          ILS sessions:                   0
         MGCP sessions:                   0
          NBT sessions:                   0
         PPTP sessions:                   0
          RSH sessions:                   0
         RTSP sessions:                   0
         SCCP sessions:                   0
          SIP sessions:                   0
         SMTP sessions:                   0
       SQLNET sessions:                   0
          SSH sessions:                   0
       TELNET sessions:                   0
         TFTP sessions:                   0
        XDMCP sessions:                   0
```

Display statistics for IPv4 unicast TCP sessions.

```
<Sysname> display session statistics ipv4 protocol tcp
Slot 1:
Current sessions: 3
          TCP sessions:                   3
```

Table 13 Command output

Field	Description
Current sessions	Total number of unicast sessions.
TCP sessions	Number of TCP unicast sessions.
UDP sessions	Number of UDP unicast sessions.
ICMP sessions	Number of ICMP unicast sessions.
UDP-Lite sessions	Number of UDP-Lite unicast sessions.
SCTP sessions	Number of SCTP unicast sessions.
DCCP sessions	Number of DCCP unicast sessions.
RAWIP sessions	Number of Raw IP unicast sessions.
DNS sessions	Number of DNS unicast sessions.
FTP sessions	Number of FTP unicast sessions.
GTP sessions	Number of GTP unicast sessions.
H323 sessions	Number of H.323 unicast sessions.
HTTP sessions	Number of HTTP unicast sessions.
ILS sessions	Number of ILS unicast sessions.
MGCP sessions	Number of MGCP unicast sessions.
NBT sessions	Number of NBT unicast sessions.
PPTP sessions	Number of PPTP unicast sessions.
RSH sessions	Number of RSH unicast sessions.
RTSP sessions	Number of RTSP unicast sessions.
SCCP sessions	Number of SCCP unicast sessions.
SIP sessions	Number of SIP unicast sessions.
SMTP sessions	Number of SMTP unicast sessions.
SQLNET sessions	Number of SQLNET unicast sessions.
SSH sessions	Number of SSH unicast sessions.
TELNET sessions	Number of Telnet unicast sessions.
TFTP sessions	Number of TFTP unicast sessions.
XDMCP sessions	Number of XDMCP unicast sessions.

display session statistics ipv6

Use **`display session statistics ipv6`** to display IPv6 unicast session statistics.

Syntax

display session statistics ipv6 [[**responder**] { **application** *application-name* | **destination-ip** *destination-ip* | **destination-port** *destination-port* | **destination-zone** *destination-zone-name* | **interface** *interface-type interface-number* | **protocol** { **dccp** | **dns** | **ftp** | **gtp** | **h323** | **http** | **icmpv6** | **ils** | **mgcp** | **nbt** | **pptp** | **raw-ip** | **rsh** | **rtsp** | **sccp** | **sctp** | **sip** | **smtp** | **sqlnet** | **ssh** | **tcp** | **telnet** | **tftp** | **udp** | **udp-lite** | **xdmcp** } | **security-policy-rule** *rule-name* | **source-ip** *source-ip* | **source-port** *source-port* | **source-zone** *source-zone-name* | **state** { **dccp-closereq** | **dccp-closing** | **dccp-open** | **dccp-partopen** | **dccp-request** | **dccp-respond** | **dccp-timewait** | **icmpv6-reply** | **icmpv6-request** | **rawip-open** | **rawip-ready** | **sctp-closed** | **sctp-cookie-echoed** | **sctp-cookie-wait** | **sctp-established** | **sctp-shutdown-ack-sent** | **sctp-shutdown-recd** | **sctp-shutdown-sent** | **tcp-close** | **tcp-close-wait** | **tcp-est** | **tcp-fin-wait** | **tcp-last-ack** | **tcp-syn-recv** | **tcp-syn-sent** | **tcp-syn-sent2** | **tcp-time-wait** | **udp-open** | **udp-ready** | **udplite-open** | **udplite-ready** } | **vpn-instance** *vpn-instance-name* } *] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

responder: Displays statistics about IPv6 unicast sessions from the responder to the initiator. If you do not specify this keyword, the command displays statistics about IPv6 unicast sessions from the initiator to the responder.

application *application-name*: Specifies an application protocol by its name. The *application-name* argument is a case-insensitive string of 1 to 63 characters. The names **invalid** and **other** are not allowed.

destination-ip *destination-ip*: Specifies a destination IPv6 address for a unicast session.

destination-port *destination-port*: Specifies a destination port by its number. The *destination-port* argument specifies the destination port of an IPv6 unicast session. The value range for the *destination-port* argument is 0 to 65535.

destination-zone *destination-zone-name*: Specifies a destination security zone by its name, a case-insensitive string of 1 to 31 characters.

interface *interface-type interface-num*: Specifies an interface by its type and number.

protocol { **dccp** | **dns** | **ftp** | **gtp** | **h323** | **http** | **icmpv6** | **ils** | **mgcp** | **nbt** | **pptp** | **raw-ip** | **rsh** | **rtsp** | **sccp** | **sctp** | **sip** | **smtp** | **sqlnet** | **ssh** | **tcp** | **telnet** | **tftp** | **udp** | **udp-lite** | **xdmcp** }: Specifies an IPv6 protocol.

security-policy-rule *rule-name*: Specifies a security policy rule by its name for session filtering. The *rule-name* argument represents the name of the security policy rule, a case-sensitive string of 1 to 127 characters.

source-ip *source-ip*: Specifies a source IPv6 address for a unicast session.

source-port *source-port*: Specifies a source port by its number. The *source-port* argument specifies the source port of an IPv6 unicast session. The value range for the *source-port* argument is 0 to 65535.

source-zone *source-zone-name*: Specifies a source security zone by its name, a case-insensitive string of 1 to 31 characters.

state { **dccp-closereq** | **dccp-closing** | **dccp-open** | **dccp-partopen** | **dccp-request** | **dccp-respond** | **dccp-timewait** | **icmpv6-reply** | **icmpv6-request** | **rawip-open** | **rawip-ready** | **sctp-closed** | **sctp-cookie-echoed** | **sctp-cookie-wait** | **sctp-established** | **sctp-shutdown-ack-sent** | **sctp-shutdown-recd** | **sctp-shutdown-sent** | **tcp-close** | **tcp-close-wait** | **tcp-est** | **tcp-fin-wait** | **tcp-last-ack** | **tcp-syn-recv** | **tcp-syn-sent** | **tcp-syn-sent2** | **tcp-time-wait** | **udp-open** | **udp-ready** | **udplite-open** | **udplite-ready** }: Specifies a protocol state.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command displays IPv6 unicast session statistics in the public network.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv6 unicast session statistics for all member devices.

Examples

Display statistics for unicast sessions from IPv6 address 100::2.

```
<Sysname> display session statistics ipv6 source-ip 100::2
Slot 1:
Current sessions: 3
          TCP sessions:                  0
          UDP sessions:                  0
       ICMPv6 sessions:                  3
     UDP-Lite sessions:                  0
         SCTP sessions:                  0
         DCCP sessions:                  0
        RAWIP sessions:                  0

          DNS sessions:                  0
          FTP sessions:                  0
          GTP sessions:                  0
         H323 sessions:                  0
         HTTP sessions:                  0
          ILS sessions:                  0
         MGCP sessions:                  0
          NBT sessions:                  0
         PPTP sessions:                  0
          RSH sessions:                  0
         RTSP sessions:                  0
         SCCP sessions:                  0
          SIP sessions:                  0
         SMTP sessions:                  0
       SQLNET sessions:                  0
          SSH sessions:                  0
       TELNET sessions:                  0
         TFTP sessions:                  0
```

```
        XDMCP sessions:                    0
```

Display statistics for IPv6 unicast TCP sessions.

```
<Sysname> display session statistics ipv6 protocol tcp
Slot 1:
Current sessions: 3
          TCP sessions:                    3
```

Table 14 Command output

Field	Description
Current sessions	Total number of unicast sessions.
TCP sessions	Number of TCP unicast sessions.
UDP sessions	Number of UDP unicast sessions.
ICMPv6 sessions	Number of ICMPv6 unicast sessions.
UDP-Lite sessions	Number of UDP-Lite unicast sessions.
SCTP sessions	Number of SCTP unicast sessions.
DCCP sessions	Number of DCCP unicast sessions.
RAWIP sessions	Number of Raw IP unicast sessions.
DNS sessions	Number of DNS unicast sessions.
FTP sessions	Number of FTP unicast sessions.
GTP sessions	Number of GTP unicast sessions.
H323 sessions	Number of H.323 unicast sessions.
HTTP sessions	Number of HTTP unicast sessions.
ILS sessions	Number of ILS unicast sessions.
MGCP sessions	Number of MGCP unicast sessions.
NBT sessions	Number of NBT unicast sessions.
PPTP sessions	Number of PPTP unicast sessions.
RSH sessions	Number of RSH unicast sessions.
RTSP sessions	Number of RTSP unicast sessions.
SCCP sessions	Number of SCCP unicast sessions.
SIP sessions	Number of SIP unicast sessions.
SMTP sessions	Number of SMTP unicast sessions.
SQLNET sessions	Number of SQLNET unicast sessions.
SSH sessions	Number of SSH unicast sessions.
TELNET sessions	Number of Telnet unicast sessions.
TFTP sessions	Number of TFTP unicast sessions.

Field	Description
XDMCP sessions	Number of XDMCP unicast sessions.

display session statistics multicast

Use **display session statistic multicast** to display multicast session statistics.

Syntax

display session statistics multicast [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays multicast session statistics for all member devices.

Examples

Display information about multicast session statistics.

```
<Sysname> display session statistics multicast
Slot 1:
Current sessions: 0
Session establishment rate: 0/s
History max sessions: 0                                Time: 2017-04-25 11:28:00
History max session establishment rate: 0/s            Time: 2017-04-25 11:28:00
Received:                   0 packets                    0 bytes
Sent    :                   0 packets                    0 bytes
```

Table 15 Command output

Field	Description
Current sessions	Total number of multicast sessions.
Session establishment rate	Rate of multicast session creation.
History max sessions	History statistics of the maximum multicast sessions.
History max session establishment rate	History statistics of the maximum rate at which multicast sessions were created.
Received	Number of received multicast packets and bytes.
Sent	Number of sent multicast packets and bytes.

display session table ipv4

Use **display session table ipv4** to display information about IPv4 unicast session entries that match specific criteria.

Syntax

display session table ipv4 [**slot** *slot-number*] [[**responder**] { **application** *application-name* | **destination-ip** *start-destination-ip* [*end-destination-ip*] | **destination-port** *destination-port* | **destination-zone** *destination-zone-name* | **interface** *interface-type interface-number* | **protocol** { **dccp** | **icmp** | **raw-ip** | **sctp** | **tcp** | **udp** | **udp-lite** } | **security-policy-rule** *rule-name* | **source-ip** *start-source-ip* [*end-source-ip*] | **source-port** *source-port* | **source-zone** *source-zone-name* | **state** { **dccp-closereq** | **dccp-closing** | **dccp-open** | **dccp-partopen** | **dccp-request** | **dccp-respond** | **dccp-timewait** | **icmp-reply** | **icmp-request** | **rawip-open** | **rawip-ready** | **sctp-closed** | **sctp-cookie-echoed** | **sctp-cookie-wait** | **sctp-established** | **sctp-shutdown-ack-sent** | **sctp-shutdown-recd** | **sctp-shutdown-sent** | **tcp-close** | **tcp-close-wait** | **tcp-est** | **tcp-fin-wait** | **tcp-last-ack** | **tcp-syn-recv** | **tcp-syn-sent** | **tcp-syn-sent2** | **tcp-time-wait** | **udp-open** | **udp-ready** | **udplite-open** | **udplite-ready** } | **vpn-instance** *vpn-instance-name* } *] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all member devices.

responder: Displays entries of IPv4 unicast sessions from the responder to the initiator. If you do not specify this keyword, the command displays entries of IPv4 unicast sessions from the initiator to the responder.

application *application-name*: Specifies an application protocol by its name. The *application-name* argument is a case-insensitive string of 1 to 63 characters. The names **invalid** and **other** are not allowed.

destination-ip *start-destination-ip* [*end-destination-ip*]: Specifies a destination IPv4 address or IPv4 address range for a unicast session. The *start destination-ip* argument specifies the start destination IPv4 address. The *end destination-ip* argument specifies the end destination IPv4 address.

destination-port *destination-port*: Specifies a destination port by its number. The *destination-port* argument specifies the destination port of a unicast session. The value range for the *destination-port* argument is 0 to 65535.

destination-zone *destination-zone-name*: Specifies a destination security zone by its name, a case-insensitive string of 1 to 31 characters.

interface *interface-type interface-num*: Specifies an interface by its type and number.

protocol { **dccp** | **icmp** | **raw-ip** | **sctp** | **tcp** | **udp** | **udp-lite** }: Specifies an IPv4 transport layer protocol, including DCCP, ICMP, Raw IP, SCTP, TCP, UDP, and UDP-Lite.

security-policy-rule *rule-name*: Specifies a security policy rule by its name for session filtering. The *rule-name* argument represents the name of the security policy rule, a case-sensitive string of 1 to 127 characters.

source-ip *start-source-ip* [*end-source-ip*]: Specifies a source IPv4 address or IPv4 address range for a unicast session. The *start source-ip* argument specifies the start source IPv4 address. The *end source-ip* argument specifies the end source IPv4 address.

source-port *source-port*: Specifies a source port by its number. The *source-port* argument specifies the source port of a unicast session. The value range for the *source-port* argument is 0 to 65535.

source-zone *source-zone-name*: Specifies a source security zone by its name, a case-insensitive string of 1 to 31 characters.

state { **dccp-closereq** | **dccp-closing** | **dccp-open** | **dccp-partopen** | **dccp-request** | **dccp-respond** | **dccp-timewait** | **icmp-reply** | **icmp-request** | **rawip-open** | **rawip-ready** | **sctp-closed** | **sctp-cookie-echoed** | **sctp-cookie-wait** | **sctp-established** | **sctp-shutdown-ack-sent** | **sctp-shutdown-recd** | **sctp-shutdown-sent** | **tcp-close** | **tcp-close-wait** | **tcp-est** | **tcp-fin-wait** | **tcp-last-ack** | **tcp-syn-recv** | **tcp-syn-sent** | **tcp-syn-sent2** | **tcp-time-wait** | **udp-open** | **udp-ready** | **udplite-open** | **udplite-ready** }: Specifies a protocol state.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command displays IPv4 unicast session entries in the public network.

verbose: Displays detailed information about IPv4 unicast session entries. If you do not specify this keyword, the command displays brief information about IPv4 unicast session entries.

Usage guidelines

If you do not specify any parameters, this command displays all IPv4 unicast session entries.

Examples

Display brief information about all IPv4 unicast session entries.

```
<Sysname> display session table ipv4
Slot 1:
Initiator:
  Source      IP/port: 192.168.1.18/1877
  Destination IP/port: 192.168.1.55/22
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: Trust


Total sessions found: 1
```

Display detailed information about all IPv4 unicast session entries.

```
<Sysname> display session table ipv4 verbose
Slot 1:
Initiator:
  Source      IP/port: 192.168.1.18/1877
  Destination IP/port: 192.168.1.55/22
```

```
  DS-Lite tunnel peer:-
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: Trust
Responder:
  Source      IP/port: 192.168.1.55/22
  Destination IP/port: 192.168.1.18/1877
  DS-Lite tunnel peer:-
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Local
State: TCP_SYN_SENT
Application: SSH
Rule ID: 1
Rule name: test
Start time: 2011-07-29 19:12:36  TTL: 28s
Initiator->Responder:         1 packets         48 bytes
Responder->Initiator:         0 packets          0 bytes

Total sessions found: 1
```

Table 16 Command output

Field	Description
Initiator	Information about the unicast session from the initiator to the responder.
Responder	Information about the unicast session from the responder to the initiator.
DS-Lite tunnel peer	Address of the DS-Lite tunnel peer. When the unicast session does not belong to any DS-Lite tunnel, this field displays a hyphen (-).
VPN instance/VLAN ID/Inline ID	MPLS L3VPN instance to which the unicast session belongs. VLAN and inline to which the session belongs during Layer 2 forwarding. If a parameter is not specified, a hyphens (-) is displayed for the proper field.
Protocol	Transport layer protocol: • DCCP. • ICMP. • ICMPv6. • Raw IP. • SCTP. • TCP. • UDP. • UDP-Lite. The number in the brackets indicates the protocol number.
Inbound interface	Interface on which packets are received.
Source security zone	Security zone to which the inbound interface belongs. If the inbound interface does not belong to any security zone, this field displays a hyphen

Field	Description
	(-).
State	Unicast session state.
Application	Application layer protocol, FTP or DNS. If it is an unknown protocol identified by an unknown port, this field displays **OTHER**.
Rule ID	ID of the security policy rule.
Rule name	Name of the security policy rule.
Start time	Unicast session establishment time.
TTL	Remaining lifetime of the unicast session, in seconds.
Initiator->Responder	Number of packets and bytes from the initiator to the responder.
Responder->Initiator	Number of packets and bytes from the responder to the initiator.
Total sessions found	Total number of found unicast session entries.

display session table ipv6

Use **display session table ipv6** to display information about IPv6 unicast session entries that match specific criteria.

Syntax

display session table ipv6 [**slot** *slot-number*] [[**responder**] { **application** *application-name* | **destination-ip** *start-destination-ip* [*end-destination-ip*] | **destination-port** *destination-port* | **destination-zone** *destination-zone-name* | **interface** *interface-type interface-number* | **protocol** { **dccp** | **icmpv6** | **raw-ip** | **sctp** | **tcp** | **udp** | **udp-lite** } | **security-policy-rule** *rule-name* | **source-ip** *start-source-ip* [*end-source-ip*] | **source-port** *source-port* | **source-zone** *source-zone-name* | **state** { **dccp-closereq** | **dccp-closing** | **dccp-open** | **dccp-partopen** | **dccp-request** | **dccp-respond** | **dccp-timewait** | **icmpv6-reply** | **icmpv6-request** | **rawip-open** | **rawip-ready** | **sctp-closed** | **sctp-cookie-echoed** | **sctp-cookie-wait** | **sctp-established** | **sctp-shutdown-ack-sent** | **sctp-shutdown-recd** | **sctp-shutdown-sent** | **tcp-close** | **tcp-close-wait** | **tcp-est** | **tcp-fin-wait** | **tcp-last-ack** | **tcp-syn-recv** | **tcp-syn-sent** | **tcp-syn-sent2** | **tcp-time-wait** | **udp-open** | **udp-ready** | **udplite-open** | **udplite-ready** } | **vpn-instance** *vpn-instance-name* } *] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all member devices.

responder: Displays entries of IPv6 unicast sessions from the responder to the initiator. If you do not specify this keyword, the command displays entries of IPv6 unicast sessions from the initiator to the responder.

application *application-name*: Specifies an application protocol by its name. The *application-name* argument is a case-insensitive string of 1 to 63 characters. The names **invalid** and **other** are not allowed.

destination-ip *start-destination-ip* [*end-destination-ip*]: Specifies a destination IPv6 address or IPv6 address range for a unicast session. The *start destination-ip* argument specifies the start destination IPv6 address. The *end destination-ip* argument specifies the end destination IPv6 address.

destination-port *destination-port*: Specifies a destination port by its number. The *destination-port* argument specifies the destination port of a unicast session. The value range for the *destination-port* argument is 0 to 65535.

destination-zone *destination-zone-name*: Specifies a destination security zone by its name, a case-insensitive string of 1 to 31 characters.

interface *interface-type interface-num*: Specifies an interface by its type and number.

protocol { **dccp** | **icmpv6** | **raw-ip** | **sctp** | **tcp** | **udp** | **udp-lite** }: Specifies an IPv6 transport layer protocol, including DCCP, ICMPv6, Raw IP, SCTP, TCP, UDP, and UDP-Lite.

security-policy-rule *rule-name*: Specifies a security policy rule by its name for session filtering. The *rule-name* argument represents the name of the security policy rule, a case-sensitive string of 1 to 127 characters.

source-ip *start-source-ip* [*end-source-ip*]: Specifies a source IPv6 address or IPv6 address range for a unicast session. The *start source-ip* argument specifies the start source IPv6 address. The *end source-ip* argument specifies the end source IPv6 address.

source-port *source-port*: Specifies a source port by its number. The *source-port* argument specifies the source port of a unicast session. The value range for the *source-port* argument is 0 to 65535.

source-zone *source-zone-name*: Specifies a source security zone by its name, a case-insensitive string of 1 to 31 characters.

state { **dccp-closereq** | **dccp-closing** | **dccp-open** | **dccp-partopen** | **dccp-request** | **dccp-respond** | **dccp-timewait** | **icmpv6-reply** | **icmpv6-request** | **rawip-open** | **rawip-ready** | **sctp-closed** | **sctp-cookie-echoed** | **sctp-cookie-wait** | **sctp-established** | **sctp-shutdown-ack-sent** | **sctp-shutdown-recd** | **sctp-shutdown-sent** | **tcp-close** | **tcp-close-wait** | **tcp-est** | **tcp-fin-wait** | **tcp-last-ack** | **tcp-syn-recv** | **tcp-syn-sent** | **tcp-syn-sent2** | **tcp-time-wait** | **udp-open** | **udp-ready** | **udplite-open** | **udplite-ready** }: Specifies a protocol state.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command displays IPv6 unicast session entries in the public network.

verbose: Displays detailed information about IPv6 unicast session entries. If you do not specify this keyword, the command displays brief information about IPv6 unicast session entries.

Usage guidelines

If you do not specify any parameters, this command displays all IPv6 unicast session entries.

Examples

Display brief information about all IPv6 unicast session entries.

```
<Sysname> display session table ipv6
Slot 1:
Initiator:
  Source      IP/port: 2011::2/58473
  Destination IP/port: 2011::8/32768
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: IPV6-ICMP(58)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: Trust

Total sessions found: 1
```

Display detailed information about all IPv6 unicast session entries.

```
<Sysname> display session table ipv6 verbose
Slot 1:
Initiator:
  Source      IP/port: 2011::2/58473
  Destination IP/port: 2011::8/32768
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: IPV6-ICMP(58)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: Trust
Responder:
  Source      IP/port: 2011::8/58473
  Destination IP/port: 2011::2/33024
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: IPV6-ICMP(58)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Local
State: ICMPV6_REQUEST
Application: OTHER
Rule ID: 1
Rule name: test
Start time: 2011-07-29 19:23:41  TTL: 55s
Initiator->Responder:         1 packets         104 bytes
Responder->Initiator:         0 packets          0 bytes

Total sessions found: 1
```

Table 17 Command output

Field	Description
Initiator	Information about the unicast session from the initiator to the responder.
Responder	Information about the unicast session from the responder to the initiator.

Field	Description
DS-Lite tunnel peer	Address of the DS-Lite tunnel peer. When the unicast session is not tunneled by DS-Lite, this field displays a hyphen (-).
VPN instance/VLAN ID/Inline ID	MPLS L3VPN instance to which the unicast session belongs. VLAN and inline to which the unicast session belongs during Layer 2 forwarding. If a parameter is not specified, a hyphens (-) is displayed for the proper field.
Protocol	Transport layer protocol: • DCCP. • ICMP. • ICMPv6. • Raw IP. • SCTP. • TCP. • UDP. • UDP-Lite. The number in the brackets indicates the protocol number.
Inbound interface	Interface on which packets are received.
Source security zone	Security zone to which the inbound interface belongs. If the inbound interface does not belong to any security zone, this field displays a hyphen (-).
State	Unicast session state.
Application	Application layer protocol, FTP or DNS. If it is an unknown protocol identified by an unknown port, this field displays **OTHER**.
Rule ID	ID of the security policy rule.
Rule name	Name of the security policy rule.
Start time	Unicast session establishment time.
TTL	Remaining lifetime of the unicast session, in seconds.
Initiator->Responder	Number of packets and bytes from the initiator to the responder.
Responder->Initiator	Number of packets and bytes from the responder to the initiator.
Total sessions found	Total number of found unicast session entries.

display session table multicast ipv4

Use **display session table multicast ipv4** to display information about IPv4 multicast session entries that match specific criteria.

Syntax

display session table multicast ipv4 [**slot** *slot-number*] [[**responder**] { **destination-ip** *start-destination-ip* [*end-destination-ip*] | **destination-port** *destination-port* | **protocol** { **dccp** | **icmp** | **raw-ip** | **sctp** |

tcp | **udp** | **udp-lite** } | **source-ip** *start-source-ip* [*end-source-ip*] | **source-port** *source-port* } *] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all member devices.

responder: Displays entries of IPv4 multicast sessions from the responder to the initiator. If you do not specify this keyword, the command displays entries of IPv4 multicast sessions from the initiator to the responder.

destination-ip *start-destination-ip* [*end-destination-ip*]: Specifies a destination IPv4 address or IPv4 address range for a multicast session. The *start destination-ip* argument specifies the start destination IPv4 address. The *end destination-ip* argument specifies the end destination IPv4 address.

destination-port *destination-port*: Specifies a destination port by its number. The *destination-port* argument specifies the destination port of a multicast session. The value range for the *destination-port* argument is 0 to 65535.

protocol { **dccp** | **icmp** | **raw-ip** | **sctp** | **tcp** | **udp** | **udp-lite** }: Specifies an IPv4 transport layer protocol.

source-ip *start-source-ip* [*end-source-ip*]: Specifies a source IPv4 address or IPv4 address range for a multicast session. The *start source-ip* argument specifies the start source IPv4 address. The *end source-ip* argument specifies the end source IPv4 address.

source-port *source-port*: Specifies a source port by its number. The *source-port* argument specifies the source port of a multicast session. The value range for the *source-port* argument is 0 to 65535.

verbose: Displays detailed information about IPv4 multicast session entries. If you do not specify this keyword, the command displays brief information about IPv4 multicast session entries.

Usage guidelines

If you do not specify any parameters, this command displays all IPv4 multicast session entries.

Examples

Display brief information about all IPv4 multicast session entries.

```
<Sysname> display session table multicast ipv4
Slot 1:
Inbound initiator:
  Source      IP/port: 3.3.3.4/1609
  Destination IP/port: 232.0.0.1/1025
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: UDP(17)
Inbound interface: GigabitEthernet1/0/1
```

```
Outbound interface list:
    GigabitEthernet1/0/2
    GigabitEthernet1/0/3

Total sessions found: 3
```

Display detailed information about all IPv4 multicast session entries.

```
<Sysname> display session table multicast ipv4 verbose
Slot 1:
Total sessions found: 0

CPU 1 on slot 2:
Inbound initiator:
  Source      IP/port: 3.3.3.4/1609
  Destination IP/port: 232.0.0.1/1025
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: UDP(17)
Inbound responder:
  Source      IP/port: 232.0.0.1/1025
  Destination IP/port: 3.3.3.4/1609
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: UDP(17)
Inbound interface: GigabitEthernet1/0/1
Source security zone: Trust
State: UDP_OPEN
Application: OTHER
Start time: 2014-03-03 15:59:22  TTL: 18s
Initiator->Responder:            1 packets         84 bytes

Outbound initiator:
  Source      IP/port: 3.3.3.4/1609
  Destination IP/port: 232.0.0.1/1025
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: UDP(17)
Outbound responder:
  Source      IP/port: 232.0.0.1/1025
  Destination IP/port: 3.3.3.4/1609
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: UDP(17)
Outbound interface: GigabitEthernet1/0/2
Destination security zone: aaa
State: UDP_OPEN
Application: OTHER
Start time: 2014-03-03 15:59:22  TTL: 18s
Initiator->Responder:            1 packets         84 bytes
```

```
Outbound initiator:
  Source      IP/port: 3.3.3.4/1609
  Destination IP/port: 232.0.0.1/1025
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: UDP(17)
Outbound responder:
  Source      IP/port: 232.0.0.1/1025
  Destination IP/port: 3.3.3.4/1609
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: UDP(17)
Outbound interface: GigabitEthernet1/0/3
Destination security zone: bbb
State: UDP_OPEN
Application: OTHER
Start time: 2014-03-03 15:59:22  TTL: 18s
Initiator->Responder:            1 packets         84 bytes

Total sessions found: 3
```

Table 18 Command output

Field	Description
Inbound initiator	Information about the multicast session from the initiator to the responder on the inbound interface.
Inbound responder	Information about the multicast session from the responder to the initiator on the inbound interface.
Outbound initiator	Information about the multicast session from the initiator to the responder on the outbound interface.
Outbound responder	Information about the multicast session from the responder to the initiator on the outbound interface.
DS-Lite tunnel peer	Address of the DS-Lite tunnel peer. If the multicast session is not tunneled by DS-Lite, this field displays a hyphen (-).
VPN instance/VLAN ID/Inline ID	MPLS L3VPN instance to which the multicast session belongs. VLAN and inline to which the multicast session belongs during Layer 2 forwarding. If a parameter is not specified, a hyphens (-) is displayed for the proper field.
Protocol	Transport layer protocol: • DCCP. • ICMP. • Raw IP. • SCTP. • TCP. • UDP. • UDP-Lite. The number in the brackets indicates the protocol number.

Field	Description
State	Multicast session state.
Application	Application layer protocol, FTP or DNS. If it is an unknown protocol identified by an unknown port, this field displays **OTHER**.
Start time	Time when the multicast session was created.
TTL	Remaining lifetime of the multicast session, in seconds.
Inbound interface	Inbound interface of the first packet from the initiator to responder.
Outbound interface	Outbound interface of the first packet from the initiator to responder.
Outbound interface list	Outbound interfaces of the first packet from the initiator to responder.
Source security zone	Security zone to which the inbound interface belongs. If the inbound interface does not belong to any security zone, this field displays a hyphen (-).
Destination security zone	Security zone to which the outbound interface belongs. If the outbound interface does not belong to any security zone, this field displays a hyphen (-).
Initiator->Responder	Number of packets and bytes from the initiator to the responder.
Total sessions found	Total number of found multicast session entries.

display session table multicast ipv6

Use **display session table multicast ipv6** to display information about IPv6 multicast session entries that match specific criteria.

Syntax

display session table multicast ipv6 [**slot** *slot-number*] [[**responder**] { **destination-ip** *start-destination-ip* [*end-destination-ip*] | **destination-port** *destination-port* | **protocol** { **dccp** | **icmpv6** | **raw-ip** | **sctp** | **tcp** | **udp** | **udp-lite** } | **source-ip** *start-source-ip* [*end-source-ip*] | **source-port** *source-port* } *] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all member devices.

responder: Displays entries of IPv6 multicast sessions from the responder to the initiator. If you do not specify this keyword, the command displays entries of IPv4 multicast sessions from the initiator to the responder.

destination-ip *start-destination-ip* [*end-destination-ip*]: Specifies a destination IPv6 address or IPv6 address range for a multicast session. The *start destination-ip* argument specifies the start destination IPv6 address. The *end destination-ip* argument specifies the end destination IPv6 address.

destination-port *destination-port*: Specifies a destination port by its number. The *destination-port* argument specifies the destination port of a multicast session. The value range for the *destination-port* argument is 0 to 65535.

protocol { **dccp** | **icmpv6** | **raw-ip** | **sctp** | **tcp** | **udp** | **udp-lite** }: Specifies an IPv6 transport layer protocol.

source-ip *start-source-ip* [*end-source-ip*]: Specifies a source IPv6 address or IPv6 address range for a multicast session. The *start source-ip* argument specifies the start source IPv6 address. The *end source-ip* argument specifies the end source IPv6 address.

source-port *source-port*: Specifies a source port by its number. The *source-port* argument specifies the source port of a multicast session. The value range for the *source-port* argument is 0 to 65535.

verbose: Displays detailed information about IPv6 multicast session entries. If you do not specify this keyword, the command displays brief information about IPv6 multicast session entries.

Usage guidelines

If you do not specify any parameters, this command displays all IPv6 multicast session entries.

Examples

Display brief information about all IPv6 multicast session entries.

```
<Sysname> display session table multicast ipv6
Slot 1:
Inbound initiator:
  Source      IP/port: 3::4/1617
  Destination IP/port: FF0E::1/1025
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: UDP(17)
Inbound interface: GigabitEthernet1/0/1
Outbound interface list:
    GigabitEthernet1/0/2
    GigabitEthernet1/0/3

Total sessions found: 3
```

Display detailed information about all IPv6 multicast session entries.

```
<Sysname> display session table multicast ipv6 verbose
Slot 1:
Inbound initiator:
  Source      IP/port: 3::4/1617
  Destination IP/port: FF0E::1/1025
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: UDP(17)
Inbound responder:
  Source      IP/port: FF0E::1/1025
  Destination IP/port: 3::4/1617
```

```
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: UDP(17)
Inbound interface: GigabitEthernet1/0/1
Source security zone: Trust
State: UDP_OPEN
Application: OTHER
Start time: 2014-03-03 16:10:58  TTL: 23s
Initiator->Responder:            5 packets        520 bytes

Outbound initiator:
  Source      IP/port: 3::4/1617
  Destination IP/port: FF0E::1/1025
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: UDP(17)
Outbound responder:
  Source      IP/port: FF0E::1/1025
  Destination IP/port: 3::4/1617
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: UDP(17)
Outbound interface: GigabitEthernet1/0/2
Destination security zone: bbb
State: UDP_OPEN
Application: OTHER
Start time: 2014-03-03 16:10:58  TTL: 23s
Initiator->Responder:            5 packets        520 bytes

Outbound initiator:
  Source      IP/port: 3::4/1617
  Destination IP/port: FF0E::1/1025
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: UDP(17)
Outbound responder:
  Source      IP/port: FF0E::1/1025
  Destination IP/port: 3::4/1617
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: UDP(17)
Outbound interface: GigabitEthernet1/0/3
Destination security zone: ccc
State: UDP_OPEN
Application: OTHER
Start time: 2014-03-03 16:10:58  TTL: 23s
Initiator->Responder:            5 packets        520 bytes
```

```
Total sessions found: 3
```

Table 19 Command output

Field	Description
Inbound initiator	Information about the multicast session from the initiator to the responder on the inbound interface.
Inbound responder	Information about the multicast session from the responder to the initiator on the inbound interface.
Outbound initiator	Information about the multicast session from the initiator to the responder on the outbound interface.
Outbound responder	Information about the multicast session from the responder to the initiator on the outbound interface.
DS-Lite tunnel peer	Address of the DS-Lite tunnel peer. If the multicast session is not tunneled by DS-Lite, this field displays a hyphen (-).
VPN instance/VLAN ID/Inline ID	MPLS L3VPN instance to which the multicast session belongs. VLAN and inline to which the multicast session belongs during Layer 2 forwarding. If a parameter is not specified, a hyphens (-) is displayed for the proper field.
Protocol	Transport layer protocol: • DCCP. • ICMPv6. • Raw IP. • SCTP. • TCP. • UDP. • UDP-Lite. The number in the brackets indicates the protocol number.
State	Multicast session state.
Application	Application layer protocol, FTP or DNS. If it is an unknown protocol identified by an unknown port, this field displays **OTHER**.
Start time	Time when the multicast session was created.
TTL	Remaining lifetime of the multicast session, in seconds.
Inbound interface	Inbound interface of the first packet from the initiator to responder.
Outbound interface	Outbound interface of the first packet from the initiator to responder.
Outbound interface list	Outbound interfaces of the first packet from the initiator to responder.
Source security zone	Security zone to which the inbound interface belongs. If the inbound interface does not belong to any security zone, this field displays a hyphen (-).
Destination security zone	Security zone to which the outbound interface belongs. If the outbound interface does not belong to any security zone, this field displays a hyphen (-).
Initiator->Responder	Number of packets and bytes from the initiator to the responder.

Field	Description
Total sessions found	Total number of found multicast session entries.

display session top-statistics

Use **display session top-statistics** to display top session statistics.

Syntax

display session top-statistics { last-1-hour | last-24-hours | last-30-days }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

last-1-hour: Displays top session statistics in last hour.

last-24-hours: Displays top session statistics in last 24 hours.

last-30-days: Displays top session statistics in last 30 days.

Usage guidelines

This command displays nothing if the top session statistics feature is not enabled. A maximum of ten session items can be displayed.

Examples

Display top session statistics in last hour.

```
<Sysname> display session top-statistics last-1-hour

Counting by source addresses:
No.      Source address               Sessions
1        10.1.2.3                     50004302
2        10.1.2.2                     40123255
3        10.2.2.10                    26664302
4        10.1.2.11                    7123255
5        10.1.2.12                    424302
6        10.1.2.13                    253255
7        10.1.2.14                    55302
8        10.1.2.15                    50025
9        10.1.2.16                    3555
10       10.1.2.1                     995

Counting by destination addresses:
No.      Destination address          Sessions
```

```
1        20.1.2.3                  50004302
2        20.1.2.2                  40123255
3        20.2.2.10                 26664302
4        20.1.2.11                 7123255
5        20.1.2.12                 424302
6        20.1.2.13                 325325
7        20.1.2.14                 55530
8        20.1.2.15                 50025
9        20.1.2.16                 3555
10       20.1.2.1                  995
```

Table 20 Command output

Field	Description
Counting by source addresses	Top session statistics based on source addresses.
Counting by destination addresses	Top session statistics based on destination addresses.
No.	Ranking number.
Source address	Source IP address of the sessions.
Destination address	Destination IP address of the sessions.
Sessions	Total number of sessions.

Related commands

session top-statistics enable

reset session relation-table

Use **reset session relation-table** to clear relation entries.

Syntax

reset session relation-table [**ipv4** | **ipv6**] [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

ipv4: Specifies IPv4 relation entries.

ipv6: Specifies IPv6 relation entries.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears relation entries for all member devices.

Usage guidelines

If you do not specify any parameters, this command clears all relation entries.

Examples

Clear all IPv4 relation entries.

```
<Sysname> reset session relation-table ipv4
```

Related commands

display session relation-table

reset session statistics

Use **reset session statistics** to clear unicast session statistics.

Syntax

reset session statistics [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears unicast session statistics for all member devices.

Examples

Clear all unicast session statistics.

```
<Sysname> reset session statistics
```

Related commands

display session statistics

reset session statistics multicast

Use **reset session statistics multicast** to clear multicast session statistics.

Syntax

reset session statistics multicast [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears multicast session statistics for all member devices.

Examples

Clear all multicast session statistics.

```
<Sysname> reset session statistics multicast
```

Related commands

display session statistics multicast

reset session table

Use **reset session table** to clear IP unicast session entries.

Syntax

reset session table [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears unicast session entries for all member devices.

Examples

Clear all unicast session entries.

```
<Sysname> reset session table
```

Related commands

display session table ipv4

display session table ipv6

reset session table ipv4

Use **reset session table ipv4** to clear information about IPv4 unicast session entries that match specific criteria.

Syntax

reset session table ipv4 [**slot** *slot-number*] [**source-ip** *source-ip*] [**destination-ip** *destination-ip*] [**protocol** { **dccp** | **icmp** | **raw-ip** | **sctp** | **tcp** | **udp** | **udp-lite** }] [**source-port** *source-port*] [**destination-port** *destination-port*] [**vpn-instance** *vpn-instance-name*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears information for all member devices.

source-ip *source-ip*: Specifies a source IPv4 address. The *source-ip* argument specifies the source IPv4 address of a unicast session from the initiator to the responder.

destination-ip *destination-ip*: Specifies a destination IPv4 address. The *destination-ip* argument specifies the destination IPv4 address of a unicast session from the initiator to the responder.

protocol { **dccp** | **icmp** | **raw-ip** | **sctp** | **tcp** | **udp** | **udp-lite** }: Specifies an IPv4 transport layer protocol, including DCCP, ICMP, Raw IP, SCTP, TCP, UDP, and UDP-Lite.

source-port *source-port*: Specifies a source port by its number. The *source-port* argument specifies the source port of a unicast session from the initiator to the responder. The value range for the *source-port* argument is 0 to 65535.

destination-port *destination-port*: Specifies a destination port by its number. The *destination-port* argument specifies the destination port of a unicast session from the initiator to the responder. The value range for the *destination-port* argument is 0 to 65535.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you want to clear IPv4 unicast session entries on the public network, do not specify this option.

Usage guidelines

If you do not specify any parameters, this command clears all IPv4 unicast session entries on the public network.

Examples

Clear all IPv4 unicast session entries.

```
<Sysname> reset session table ipv4
```

Clear the IPv4 unicast session entries with the source IP address of 10.10.10.10.

```
<Sysname> reset session table ipv4 source-ip 10.10.10.10
```

Related commands

display session table ipv4

reset session table ipv6

Use **reset session table ipv6** to clear information about IPv6 unicast session entries that match the specified criteria.

Syntax

reset session table ipv6 [**slot** *slot-number*] [**source-ip** *source-ip*] [**destination-ip** *destination-ip*] [**protocol** { **dccp** | **icmpv6** | **raw-ip** | **sctp** | **tcp** | **udp** | **udp-lite** }] [**source-port** *source-port*] [**destination-port** *destination-port*] [**vpn-instance** *vpn-instance-name*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears information for all member devices.

source-ip *source-ip*: Specifies a source IPv6 address. The *source-ip* argument specifies the source IPv6 address of a unicast session from the initiator to the responder.

destination-ip *destination-ip*: Specifies a destination IPv6 address. The *destination-ip* argument specifies the destination IPv6 address of a unicast session from the initiator to the responder.

protocol { **dccp** | **icmpv6** | **raw-ip** | **sctp** | **tcp** | **udp** | **udp-lite** }: Specifies an IPv6 transport layer protocol, including DCCP, ICMPv6, Raw IP, SCTP, TCP, UDP, and UDP-Lite.

source-port *source-port*: Specifies a source port by its number. The *source-port* argument specifies the source port of a unicast session from the initiator to the responder. The value range for the *source-port* argument is 0 to 65535.

destination-port *destination-port*: Specifies a destination port by its number. The *destination-port* argument specifies the destination port of a unicast session from the initiator to the responder. The value range for the *destination-port* argument is 0 to 65535.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you want to clear IPv6 unicast session entries on the public network, do not specify this option.

Usage guidelines

If you do not specify any parameters, this command clears all IPv6 unicast session entries on the public network.

Examples

Clear all IPv6 unicast session entries.

```
<Sysname> reset session table ipv6
```

Clear the IPv6 unicast session entries with the source IP address of 2011::0002.

```
<Sysname> reset session table ipv6 source-ip 2011::0002
```

Related commands

display session table ipv6

reset session table multicast

Use **reset session table multicast** to clear IP multicast session entries.

Syntax

reset session table multicast [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears multicast session entries for all member devices.

Examples

Clear all multicast session entries.

```
<Sysname> reset session table multicast
```

Related commands

display session table multicast ipv4

display session table multicast ipv6

reset session table multicast ipv4

Use **reset session table multicast ipv4** to clear information about IPv4 multicast session entries that match specific criteria.

Syntax

reset session table multicast ipv4 [**slot** *slot-number*] [**source-ip** *source-ip*] [**destination-ip** *destination-ip*] [**protocol** { **dccp** | **icmp** | **raw-ip** | **sctp** | **tcp** | **udp** | **udp-lite** }] [**source-port** *source-port*] [**destination-port** *destination-port*] [**vpn-instance** *vpn-instance-name*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears information for all member devices.

source-ip *source-ip*: Specifies a source IPv4 address. The *source-ip* argument specifies the source IPv4 address of a multicast session from the initiator to the responder.

destination-ip *destination-ip*: Specifies a destination IPv4 address. The *destination-ip* argument specifies the destination IPv4 address of a multicast session from the initiator to the responder.

protocol { **dccp** | **icmp** | **raw-ip** | **sctp** | **tcp** | **udp** | **udp-lite** }: Specifies an IPv4 transport layer protocol, including DCCP, ICMP, Raw IP, SCTP, TCP, UDP, and UDP-Lite.

source-port *source-port*: Specifies a source port by its number. The *source-port* argument specifies the source port of a multicast session from the initiator to the responder. The value range for the *source-port* argument is 0 to 65535.

destination-port *destination-port*: Specifies a destination port by its number. The *destination-port* argument specifies the destination port of a multicast session from the initiator to the responder. The value range for the *destination-port* argument is 0 to 65535.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you want to clear IPv4 multicast session entries on the public network, do not specify this option.

Usage guidelines

If you do not specify any parameters, this command clears all IPv4 multicast session entries on the public network.

Examples

Clear all IPv4 multicast session entries.

```
<Sysname> reset session table multicast ipv4
```

Clear the IPv4 multicast session entries with the source IP address of 10.10.10.10.

```
<Sysname> reset session table multicast ipv4 source-ip 10.10.10.10
```

Related commands

display session table multicast ipv4

reset session table multicast ipv6

Use **reset session table multicast ipv6** to clear information about IPv6 multicast session entries that match specific criteria.

Syntax

reset session table multicast ipv6 [**slot** *slot-number*] [**source-ip** *source-ip*] [**destination-ip** *destination-ip*] [**protocol** { **dccp** | **icmpv6** | **raw-ip** | **sctp** | **tcp** | **udp** | **udp-lite** }] [**source-port** *source-port*] [**destination-port** *destination-port*] [**vpn-instance** *vpn-instance-name*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears information for all member devices.

source-ip *source-ip*: Specifies a source IPv6 address. The *source-ip* argument specifies the source IPv6 address of a multicast session from the initiator to the responder.

destination-ip *destination-ip*: Specifies a destination IPv6 address. The *destination-ip* argument specifies the destination IPv6 address of a multicast session from the initiator to the responder.

protocol { **dccp** | **icmpv6** | **raw-ip** | **sctp** | **tcp** | **udp** | **udp-lite** }: Specifies an IPv6 transport layer protocol, including DCCP, ICMPv6, Raw IP, SCTP, TCP, UDP, and UDP-Lite.

source-port *source-port*: Specifies a source port by its number. The *source-port* argument specifies the source port of a multicast session from the initiator to the responder. The value range for the *source-port* argument is 0 to 65535.

destination-port *destination-port*: Specifies a destination port by its number. The *destination-port* argument specifies the destination port of a multicast session from the initiator to the responder. The value range for the *destination-port* argument is 0 to 65535.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you want to clear IPv6 multicast session entries on the public network, do not specify this option.

Usage guidelines

If you do not specify any parameters, this command clears all IPv6 multicast session entries on the public network.

Examples

Clear all IPv6 multicast session entries.

```
<Sysname> reset session table multicast ipv6
```

Clear the IPv6 multicast session entries with the source IP address of 2011::0002.

```
<Sysname> reset session table multicast ipv6 source-ip 2011::0002
```

Related commands

display session table multicast ipv6

session aging-time application

Use **session aging-time application** to set the aging time for sessions of an application layer protocol or an application.

Use **undo session aging-time application** to restore the default. If you do not specify an application layer protocol or an application, this command restores the default aging time for all sessions of the supported application layer protocols and applications.

Syntax

session aging-time application *application-name time-value*

undo session aging-time application [*application-name*]

Default

The aging time is 1200 seconds for sessions of application layer protocols or applications except for the following sessions:

- BOOTPC sessions: 120 seconds.
- BOOTPS sessions: 120 seconds.
- DNS sessions: 30 seconds.
- FTP sessions: 3600 seconds.
- FTP-DATA sessions: 240 seconds.
- GPRS-DATA sessions: 60 seconds.
- GPRS-SIG sessions: 60 seconds.
- GTP-CONTROL sessions: 60 seconds.
- GTP-USER sessions: 60 seconds.
- H.225 sessions: 3600 seconds.
- H.245 sessions: 3600 seconds.
- HTTPS sessions: 600 seconds.
- ILS sessions: 3600 seconds.
- L2TP sessions: 120 seconds.
- MGCP-CALLAGENT sessions: 60 seconds.
- MGCP-GATEWAY sessions: 60 seconds.
- NETBIOS-DGM sessions: 3600 seconds.
- NETBIOS-NS sessions: 3600 seconds.
- NETBIOS-SSN sessions: 3600 seconds.
- NTP sessions: 120 seconds.
- PPTP sessions: 3600 seconds.
- QQ sessions: 120 seconds.
- RAS sessions: 300 seconds.
- RIP sessions: 120 seconds.
- RSH sessions: 60 seconds.
- RTSP session: 3600 seconds.
- SCCP sessions: 3600 seconds.
- SIP sessions: 300 seconds.
- SNMP sessions: 120 seconds.

- SNMPTRAP sessions: 120 seconds.
- SQLNET sessions: 600 seconds.
- STUN sessions: 600 seconds.
- SYSLOG sessions: 120 seconds.
- TACACS-DS sessions: 120 seconds.
- TFTP sessions: 60 seconds.
- WHO sessions: 120 seconds.
- XDMCP sessions: 3600 seconds.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

application-name: Specifies an application layer protocol or an application by its name, a case-insensitive string of 1 to 63 characters. Valid characters can be digits, letters, hyphens (-), and underscores (_). The names **invalid** and **other** are not allowed. The application layer protocol or application must exist on the device.

time-value: Specifies the aging time in seconds. The value range 1 to 100000.

Usage guidelines

This command sets the aging time for stable sessions of the specified application layer protocols or applications. For TCP sessions, the stable state is ESTABLISHED. For UDP sessions, the stable state is READY.

For sessions of application layer protocols or applications that are not supported by this command, the aging time is set by the **session aging-time state** command. For persistent sessions, the aging time is set by the **session persistent acl** command.

Supported application layer protocols or applications specified in this command depend on the APR module. For information about APR, see *Security Configuration Guide*.

Examples

Set the aging time for FTP sessions to 1800 seconds.

```
<Sysname> system-view
[Sysname] session aging-time application ftp 1800
```

Set the aging time for 126WebEmail sessions to 1800 seconds.

```
<Sysname> system-view
[Sysname] session aging-time application 126WebEmail 1800
```

Related commands

display session aging-time application

nbar application

port-mapping

session aging-time state

session persistent acl

session aging-time state

Use **session aging-time state** to set the aging time for the sessions in a protocol state.

Use **undo session aging-time state** to restore the default for the sessions in a protocol state. If you do not specify a protocol state, this command restores all aging time for sessions in different protocol states to the default.

Syntax

session aging-time state { **fin** | **icmp-reply** | **icmp-request** | **icmpv6-reply** | **icmpv6-request** | **rawip-open** | **rawip-ready** | **syn** | **tcp-close** | **tcp-est** | **tcp-time-wait** | **udp-open** | **udp-ready** } *time-value*

undo session aging-time state [**fin** | **icmp-reply** | **icmp-request** | **icmpv6-reply** | **icmpv6-request** | **rawip-open** | **rawip-ready** | **syn** | **tcp-close** | **tcp-est** | **tcp-time-wait** | **udp-open** | **udp-ready**]

Default

The aging time for sessions in different protocol states is as follows:

- FIN_WAIT: 30 seconds.
- ICMP-REPLY: 30 seconds.
- ICMP-REQUEST: 60 seconds.
- ICMPv6-REPLY: 30 seconds.
- ICMPv6-REQUEST: 60 seconds.
- RAWIP-OPEN: 30 seconds.
- RAWIP-READY: 60 seconds.
- TCP SYN-SENT and SYN-RCV: 30 seconds.
- TCP-CLOSE: 2 seconds.
- TCP ESTABLISHED: 3600 seconds.
- TCP TIME-WAIT: 2 seconds.
- UDP-OPEN: 30 seconds.
- UDP-READY: 60 seconds.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

fin: Specifies the TCP FIN_WAIT state.

icmp-reply: Specifies the ICMP REPLY state.

icmp-request: Specifies the IGMP REQUEST state.

icmpv6-reply: Specifies the ICMPv6 REPLY state.

icmpv6-request: Specifies the IGMPv6 REQUEST state.

rawip-open: Specifies the RAWIP-OPEN state.

rawip-ready: Specifies the RAWIP-READY state.

syn: Specifies the TCP SYN-SENT and SYN-RCV states.

tcp-close: Specifies the TCP CLOSE state.

tcp-est: Specifies the TCP ESTABLISHED state.

tcp-time-wait: Specifies the TCP TIME-WAIT state.

udp-open: Specifies the UDP OPEN state.

udp-ready: Specifies the UDP READY state.

time-value: Specifies the aging time in seconds. For the TCP CLOSE and TCP TIME-WAIT states, the value range is 0 to 100000. For other states, the value range is 1 to 100000.

Usage guidelines

This command sets the aging time for stable sessions of the application layer protocols that are not supported by the **session aging-time application** command. For persistent sessions, the aging time is set by the **session persistent acl** command.

Examples

Set the aging time for TCP sessions in SYN-SENT and SYN-RCV states to 60 seconds.

```
<Sysname> system-view
[Sysname] session aging-time state syn 60
```

Related commands

display session aging-time state

session aging-time application

session persistent acl

session alarm rate-abrupt enable

Use **session alarm rate-abrupt enable** to enable alarms for abrupt session creation rate changes.

Use **undo session alarm rate-abrupt enable** to disable alarms for abrupt session creation rate changes.

Syntax

session alarm rate-abrupt enable

undo session alarm rate-abrupt enable

Default

Alarms are disabled for abrupt session creation rate changes.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command enables the device to generate alarms for abrupt increase or drop in the session creation rate when the alarm thresholds for abrupt session creation rate changes are crossed.

Examples

Enable alarms for abrupt session creation rate changes.

```
<Sysname> system-view
[Sysname] session alarm rate-abrupt enable
```

Related commands

session alarm rate-abrupt threshold

session alarm rate-abrupt threshold

Use **session alarm rate-abrupt threshold** to set the alarm thresholds for abrupt session creation rate changes.

Use **undo session alarm rate-abrupt threshold** to restore the default.

Syntax

session alarm rate-abrupt threshold *threshold-value* [**base-threshold** *base-value*]

undo session alarm rate-abrupt threshold

Default

The session creation rate change threshold is 20%, and the base session creation rate threshold is 10%.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

threshold-value: Sets the session creation rate change threshold in percentage. The value range for this argument is 1 to 100.

base-threshold *base-value*: Sets the base session creation rate threshold in percentage. The value range for this argument is 1 to 100. If you do not specify this option, the default setting applies.

Usage guidelines

With alarms enabled for abrupt session creation rate changes, the system collects the session creation rate at an interval of 10 seconds and checks whether the following indicators reach the corresponding alarm thresholds:

- **Session creation rate change in percentage**—Obtained by dividing the difference between the session creation rates at the beginning and end of a collection interval by the session creation rate at the beginning of the collection interval.
- **Base session creation rate in percentage**—Obtained by dividing the session creation rate at the beginning of a collection interval by 100000.

If both of the following conditions are met in a detection interval, the system generates an alarm for the abrupt change of the session creation rate:

- The session creation rate change threshold is reached.
- The base session creation rate threshold is crossed.

Examples

Set the session creation rate change threshold to 30%.

```
<Sysname> system-view
[Sysname] session alarm rate-abrupt threshold 30
```

Related commands

session alarm rate-abrupt enable

session alarm try-rate-abrupt enable

Use **session alarm try-rate-abrupt enable** to enable alarms for abrupt session attempt rate changes.

Use **undo session alarm try-rate-abrupt enable** to disable alarms for abrupt session attempt rate changes.

Syntax

session alarm try-rate-abrupt enable

undo session alarm try-rate-abrupt enable

Default

Alarms are disabled for abrupt session attempt rate changes.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command enables the device to generate alarms for abrupt increase or drop in the session creation attempt rate when the alarm thresholds for abrupt session attempt rate changes are reached.

Examples

Enable alarms for abrupt session attempt rate changes.

```
<Sysname> system-view
[Sysname] session alarm try-rate-abrupt enable
```

Related commands

session alarm try-rate-abrupt threshold

session alarm try-rate-abrupt threshold

Use **session alarm try-rate-abrupt threshold** to set the alarm thresholds for abrupt session attempt rate changes.

Use **undo session alarm try-rate-abrupt threshold** to restore the default.

Syntax

session alarm try-rate-abrupt threshold *threshold-value* [**base-threshold** *base-value*]

undo session alarm try-rate-abrupt threshold

Default

The session attempt rate change threshold is 20%, and the base session attempt rate threshold is 10%.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

threshold-value: Sets the session attempt rate change threshold in percentage. The value range for this argument is 1 to 100.

base-threshold *base-value*: Sets the base session attempt rate threshold in percentage. The value range for this argument is 1 to 100. If you do not specify this option, the default setting applies.

Usage guidelines

With alarms enabled for abrupt session attempt rate changes, the system collects the session creation attempt rate at an interval of 10 seconds and checks whether the following indicators reach the corresponding alarm thresholds:

- **Session attempt rate change in percentage**—Obtained by dividing the difference between the session creation attempt rates at the beginning and end of a collection interval by the session creation attempt rate at the beginning of the collection interval.
- **Base session attempt rate in percentage**—Obtained by dividing the session creation attempt rate at the beginning of a collection interval by 100000.

If both of the following conditions are met in a detection interval, the system generates an alarm for the abrupt change of the session creation attempt rate:

- The session attempt rate change threshold is reached.
- The base session attempt rate threshold is crossed.

Examples

Set the session attempt rate change threshold to 30%.

```
<Sysname> system-view
[Sysname] session alarm try-rate-abrupt threshold 30
```

Related commands

session alarm try-rate-abrupt enable

session alarm usage-abrupt enable

Use **session alarm usage-abrupt enable** to enable alarms for abrupt session table usage changes.

Use **undo session alarm usage-abrupt enable** to disable alarms for abrupt session table usage changes.

Syntax

session alarm usage-abrupt enable

undo session alarm usage-abrupt enable

Default

Alarms are disabled for abrupt session table usage changes.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command enables the device to generate alarms for abrupt increase or drop in the session table usage when the alarm thresholds for abrupt session table usage changes are reached.

Examples

Enable alarms for abrupt session table usage changes.

```
<Sysname> system-view
[Sysname] session alarm usage-abrupt enable
```

Related commands

session alarm usage-abrupt threshold

session alarm usage-abrupt threshold

Use **session alarm usage-abrupt threshold** to set the alarm thresholds for abrupt session table usage changes.

Use **undo session alarm usage-abrupt threshold** to restore the default.

Syntax

session alarm usage-abrupt threshold *threshold-value* [**base-threshold** *base-value*]

undo session alarm usage-abrupt threshold

Default

The session table usage change threshold is 20%, and the base session table usage threshold is 10%.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

threshold-value: Sets the session table usage change threshold in percentage. The value range for this argument is 1 to 100.

base-threshold *base-value*: Sets the base session table usage threshold in percentage. The value range for this argument is 1 to 100. If you do not specify this option, the default setting applies.

Usage guidelines

With alarms enabled for abrupt session table usage changes, the system collects the session table usage at an interval of 10 seconds and checks whether the following indicators reach the corresponding alarm thresholds:

- **Session table usage change in percentage**—Obtained by dividing the difference between the session entry counts at the beginning and end of a collection interval by the session entry count at the beginning of the collection interval.
- **Base session table usage in percentage**—Obtained by dividing the session entry count at the beginning of a collection interval by the supported maximum number of session entries.

If both of the following conditions are met in a detection interval, the system generates an alarm for the abrupt change of the session table usage:

- The session table usage change threshold is reached.
- The base session table usage threshold is crossed.

Examples

Set the session table usage change threshold to 30%.

```
<Sysname> system-view
[Sysname] session alarm usage-abrupt threshold 30
```

Related commands

session alarm usage-abrupt enable

session alg fragment

Use **session alg fragment** to enable ALG to process fragments.

Use **undo session alg fragment** to disable ALG from processing fragments.

Syntax

session alg fragment sip

undo session alg fragment sip

Default

ALG does not process fragments.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

sip: Specifies SIP fragments.

Usage guidelines

This command enables ALG to process fragments of specified protocols. In the current software version, ALG can process only SIP fragments.

Examples

Enable ALG to process SIP fragments.

```
<Sysname> system
[Sysname] session alg fragment sip
```

session dual-active create-mode

Use **session dual-active create-mode** to set the session creation mode when the device is operating in session dual-active mode.

Use **undo session dual-active create-mode** to restore the default.

Syntax

session dual-active create-mode { **hash** | **local** }

undo session dual-active create-mode

Default

Local-based session creation is used in session dual-active mode.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

hash: Specifies hash-based session creation.

local: Specifies local-based session creation.

Usage guidelines

This feature takes effect only in session dual-active mode.

In a hot backup system operating in session dual-active mode, both devices process services. To balance the service load on the devices, you can use one of the following session creation modes:

- **Hash-based session creation**—A session is created on the device to which its first packet is relayed according to the hash result. The device where a session is created might not be the device that receives the traffic. This mode applies if traffic is unevenly distributed among the devices.
- **Local-based session creation**—A session is created on the device where the first packet of the session arrives. This mode applies if traffic is evenly distributed among the devices.

Examples

Enable hash-based session creation when the device is operating in session dual-active mode.

```
<Sysname> system-view
[Sysname] session dual-active create-mode hash
```

Related commands

session dual-active enable

session dual-active enable

Use **session dual-active enable** to enable session dual-active mode.

Use **undo session dual-active enable** to disable session dual-active mode.

Syntax

session dual-active enable

undo session dual-active enable

Default

Session dual-active mode is disabled. The device is operating in session active/standby mode.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

In a hot backup system operating in session active/standby mode, only one device processes security services. Session dual-active mode increases load capacity of the system by enabling both devices to process security services.

Examples

Enable session dual-active mode.

```
<Sysname> system-view
[Sysname] session dual-active enable
```

Related commands

session synchronization enable

session dual-active transparent udp enable

Use **session dual-active transparent udp enable** to enable transparent transmission for UDP packets in session dual-active mode.

Use **undo session dual-active transparent udp enable** to disable transparent transmission for UDP packets in session dual-active mode.

Syntax

session dual-active transparent udp enable

undo session dual-active transparent udp enable

Default

Transparent transmission for UDP packets is disabled in session dual-active mode.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This feature takes effect only in session dual-active mode.

In a hot backup system operating in session dual-active mode, a device cannot identify the direction of packets in a UDP traffic flow due to UDP mechanisms. By default, if the return packets of a

session do not match any sessions, the device creates a new session. This results in the following issues:

- If the security control policy permits a UDP traffic flow in one direction, the return packets of the flow are dropped.
- If the security control policy permits a UDP traffic flow in both directions, two sessions are created for the flow. This affects traffic processing of security services.

To resolve these issues, you can enable transparent transmission for UDP packets. This feature allows a device to relay UDP packets that do not match any sessions to the other device in the hot back system. If the UDP packets also do not match any sessions on the other device, a new session is created locally.

As a best practice, enable this feature only when asymmetric UDP traffic exists in the hot backup system and sessions cannot be synchronized timely. This feature degrades forwarding performance. Make sure you are fully aware of the impact of this feature when you use it on a live network.

Transparent transmission for UDP packets takes effect only when local-based session creation is used. If hash-based session creation is used, the devices do not relay UDP packets.

Examples

Enable transparent transmission for UDP packets in session dual-active mode.

```
<Sysname> system-view
[Sysname] session dual-active transparent udp enable
```

Related commands

session dual-active enable

session fast-drop aging-time

Use **session fast-drop aging-time** to set the aging time for deny sessions.

Use **undo session fast-drop aging-time** to restore the default.

Syntax

session fast-drop aging-time *time-value*

undo session fast-drop aging-time

Default

The aging time for deny sessions is 3 seconds.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

time-value: Specifies the aging time in seconds. The value range 1 to 3.

Usage guidelines

The system deletes deny sessions based on the deny session aging time. The deny session aging time is not refreshed when packets match deny sessions.

Examples

Set the aging time for deny sessions to 1 second.

```
<Sysname> system-view
[Sysname] session fast-drop aging-time 1
```

Related commands

session fast-drop aspf enable

session fast-drop enable

Use **session fast-drop enable** to enable the deny session feature for modules.

Use **undo session fast-drop enable** to disable the deny session feature for modules.

Syntax

session fast-drop { **aspf** | **connection-limit** } * **enable**

undo session fast-drop { **aspf** | **connection-limit** } * **enable**

Default

The deny session feature is disabled.

Views

System view

Parameters

aspf: Specifies the ASPF module.

connection-limit: Specifies the connection limit module.

Predefined user roles

network-admin

context-admin

Usage guidelines

The deny session feature allows the device to create sessions for dropped packets. These sessions are called deny sessions. To improve forwarding performance, the device drops all packets that match deny sessions.

The device generates deny sessions only for the packets dropped by the ASPF or connection limit module.

Examples

Enable the deny session feature for ASPF.

```
<Sysname> system-view
[Sysname] session fast-drop aspf enable
```

Related commands

display session fast-drop table ipv4

display session fast-drop table ipv6

session fast-drop resource-ratio

Use **session fast-drop resource-ratio** to set the maximum ratio of deny sessions to all sessions.

Use **undo session fast-drop resource-ratio** to restore the default.

Syntax

session fast-drop resource-ratio *ratio*

undo session fast-drop resource-ratio

Default

The maximum ratio of deny sessions to all sessions is 20‰.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ratio: Specifies the maximum ratio of deny sessions to all sessions, in permillage. The value range for this argument is 1 to 20.

Usage guidelines

When the ratio of deny session entries reaches the maximum ratio set by using this command, the device stops generating deny sessions.

Examples

Set the maximum ratio of deny sessions to all sessions to 1‰.

```
<Sysname> system-view
[Sysname] session fast-drop resource-ratio 1
```

Related commands

session fast-drop aspf enable

session fast-drop top-statistics enable

Use **session fast-drop top-statistics enable** to enable the top deny session statistics feature.

Use **undo session fast-drop top-statistics enable** to disable the top deny session statistics feature.

Syntax

session fast-drop top-statistics enable

undo session fast-drop top-statistics enable

Default

The top deny session statistics feature is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command collects the number of deny sessions for session-based services and ranks the deny sessions by source address and by destination address.

To display the top deny session statistics, use the **display session fast-drop top-statistics** command.

Examples

Enable the top deny session statistics feature.

```
<Sysname> system-view
[Sysname] session fast-drop top-statistics enable
```

Related commands

display session fast-drop top-statistics

session fast-drop enable

session log { bytes-active | packets-active }

Use **session log** { **bytes-active** | **packets-active** } to set a threshold for traffic-based logging.

Use **undo session log** { **bytes-active** | **packets-active** } to restore the default.

Syntax

session log { **bytes-active** *bytes-value* | **packets-active** *packets-value* }

undo session log { **bytes-active** | **packets-active** }

Default

No threshold is set for traffic-based logging.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

bytes-value: Specifies the byte-based threshold in the range of 1 to 100000 MB.

packets-value: Specifies the packet-based threshold in the range of 1 to 100000 mega-packets.

Usage guidelines

For this command to take effect, make sure the session statistics collection for software fast forwarding feature is enabled.

If you set both the traffic-based and time-based logging, the device outputs a session log when whichever is reached. After outputting a session log, the device resets the traffic counter and restarts the interval for the session.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure the device to output session logs on a per-10-mega-packet basis.

```
<Sysname> system-view
[Sysname] session statistics enable
```

```
[Sysname] session log packets-active 10
```

Related commands

session log enable

session statistics enable

session log enable

Use **session log enable** to enable session logging.

Use **undo session log enable** to disable session logging.

Syntax

session log enable { **ipv4** | **ipv6** } [**acl** *acl-number*] { **inbound** | **outbound** }

undo session log enable { **ipv4** | **ipv6** } [**acl** *acl-number*] { **inbound** | **outbound** }

Default

Session logging is disabled.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ipv4: Logs IPv4 sessions.

ipv6: Logs IPv6 sessions.

acl *acl-number*: Specifies an ACL by its number in the range of 2000 to 3999. If you do not specify an ACL, this command enables session logging for all IPv4 or IPv6 sessions on the interface.

inbound: Specifies the inbound direction.

outbound: Specifies the outbound direction.

Usage guidelines

If you do not specify the **inbound** or the **outbound** keyword, this command enables session logging on both directions.

A maximum of one IPv4 ACL and one IPv6 ACL can be applied to each direction.

After session logging is enabled, the device outputs session logs as follows:

- Outputs a session log when the specified traffic threshold or interval is reached.
- Outputs a session log when a session entry is created or removed only if the logging for session creation or deletion is enabled.

The session logging feature must work with the flow log or fast log output feature to generate session logs. Session logs can be output in flow log or fast log output format. By default, they are output in flow log format. For information about flow log and fast log output, see *Network Management and Monitoring*.

Examples

Enable IPv4 session logging in the inbound direction of GigabitEthernet 1/0/1.

```
<Sysname> system-view
```

```
[Sysname] session log flow-begin
[Sysname] session log flow-end
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] session log enable ipv4 inbound
```

Enable session logging on GigabitEthernet 1/0/2 for IPv4 sessions that match ACL 2050 in the outbound direction.

```
<Sysname> system-view
[Sysname] session log flow-begin
[Sysname] session log flow-end
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] session log enable ipv4 acl 2050 outbound
```

Enable session logging on GigabitEthernet 1/0/3 for IPv6 sessions that match ACL 2050 in the outbound direction.

```
<Sysname> system-view
[Sysname] session log flow-begin
[Sysname] session log flow-end
[Sysname] interface gigabitethernet 1/0/3
[Sysname-GigabitEthernet1/0/3] session log enable ipv6 acl 2050 outbound
```

Related commands

session log bytes-active

session log flow-begin

session log flow-end

session log packets-active

session log time-active

session log flow-begin

Use **session log flow-begin** to enable logging for session creation.

Use **undo session log flow-begin** to disable logging for session creation.

Syntax

session log flow-begin

undo session log flow-begin

Default

Logging for session creation is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

For the device to output a session log when a session entry is created, make sure both session logging and logging for session creation are enabled.

Examples

Enable logging for session creation.

```
<Sysname> system-view
[Sysname] session log flow-begin
```

Related commands

session log enable

session log flow-end

Use **session log flow-end** to enable logging for session deletion.

Use **undo session log flow-end** to disable logging for session deletion.

Syntax

session log flow-end

undo session log flow-end

Default

Logging for session deletion is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

For the device to output a session log when a session entry is deleted, make sure both session logging and logging for session deletion are enabled.

Examples

Enable logging for session deletion.

```
<Sysname> system-view
[Sysname] session log flow-end
```

Related commands

session log enable

session log time-active

Use **session log time-active** to set the time-based session logging.

Use **undo session log time-active** to restore the default.

Syntax

session log time-active *time-value*

undo session log time-active

Default

The device does not output session logs.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

time-value: Specifies the interval in minutes. The value range for the *time-value* argument is 10 to 120 and the value must be integer times of 10.

Usage guidelines

If you set both time-based and traffic-based logging, the device outputs a session log when whichever is reached. After outputting a session log, the device resets the traffic counter and restarts the interval for the session.

Examples

Configure the device to output session logs every 50 minutes.

```
<Sysname> system
[Sysname] session log time-active 50
```

Related commands

session log enable

session log { **bytes-active** | **packets-active** }

session persistent acl

Use **session persistent acl** to specify persistent sessions.

Use **undo session persistent acl** to restore the default.

Syntax

session persistent acl [**ipv6**] *acl-number* [**aging-time** *time-value*]

undo session persistent acl [**ipv6**] *acl-number*

Default

No persistent sessions exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ipv6: Specifies an IPv6 ACL. To specify an IPv4 ACL, do not specify this keyword.

acl-number: Specifies an ACL by its number in the range of 2000 to 3999.

aging-time *time-value*: Specifies the aging time for persistent sessions in hours. The value range for the *time-value* argument is 0 to 360, and the default value is 24. To disable the aging for persistent sessions, set the value to 0.

Usage guidelines

This command is effective only on TCP sessions in ESTABLISHED state.

For a TCP session in ESTABLISHED state, the priority of the aging time is as follows:

- Aging time for persistent sessions.
- Aging time for sessions of application layer protocols.
- Aging time for sessions in different protocol states.

A persistent session is not removed until one of the following events occurs:

- The session entry ages out.
- The device receives a connection close request from the initiator or responder.
- You manually clear the session entries.

The configuration of persistent sessions applies only to new sessions. It has no effect on existing sessions.

Repeat this command to use multiple ACLs to specify persistent sessions.

Examples

Specify IPv4 ACL 2000 for identifying persistent sessions and set the aging time to 72 hours.

```
<Sysname> system-view
[Sysname] session persistent acl 2000 aging-time 72
```

Specify IPv6 ACL 3000 for identifying persistent sessions and set the aging time to 100 hours.

```
<Sysname> system-view
[Sysname] session persistent acl ipv6 3000 aging-time 100
```

Related commands

session aging-time application

session aging-time state

session state-machine mode

Use **session state-machine mode** to set the mode of session state machine.

Use **undo session state-machine mode** to restore the default.

Syntax

session state-machine mode { **compact** | **loose** }

undo session state-machine mode

Default

The session state machine is in strict mode.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

compact: Specifies compact mode.

loose: Specifies loose mode.

Usage guidelines

When asymmetric-path traffic exists in a hot backup system operating in session active/standby mode, set the mode of session state machine to loose to avoid abnormal traffic loss.

When asymmetric-path traffic exists in a hot backup system operating in session dual-active mode, set the mode of session state machine to compact for disconnected sessions to age out timely.

As a best practice, change the mode of session state machine only when asymmetric-path traffic exists. This feature degrades performance of session-based security check. Make sure you are fully aware of the impact of this command when you use it on a live network.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the mode of session state machine to loose.

```
<Sysname> system-view
[Sysname] session state-machine mode loose
```

session statistics enable

Use **session statistics enable** to enable session statistics collection for software fast forwarding.

Use **undo session statistics enable** to disable session statistics collection for software fast forwarding.

Syntax

session statistics enable

undo session statistics enable

Default

The following compatibility matrixes show the defaults for this command:

Models	Default
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	Session statistics collection is disabled for software fast forwarding.
NFNX3-HDB1780, NFNX3-HDB3080	Session statistics collection is enabled for software fast forwarding.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command enables the device to collect the session-based outbound and inbound packets and bytes for software fast forwarding.

To display statistics per session, use the **display session table** command. To display statistics per packet type, use the **display session statistics** command.

This command is CPU and memory intensive. Before using this command, make sure you fully understand its impact on system performance.

Examples

Enable session statistics collection for software fast forwarding.

```
<Sysname> system-view
[Sysname] session statistics enable
```

Related commands

display session statistics

display session table

session synchronization { dns | http } *

Use **session synchronization** { **dns** | **http** } * to enable session synchronization for DNS, HTTP, or both.

Use **undo session synchronization** { **dns** | **http** } * to disable session synchronization for DNS, HTTP, or both.

Syntax

session synchronization { **dns** | **http** } *

undo session synchronization { **dns** | **http** } *

Default

Session synchronization is disabled for DNS and HTTP.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

dns: Specifies the DNS protocol.

http: Specifies the HTTP protocol.

Usage guidelines

DNS or HTTP connections usually do not last long. When a DNS or HTTP connection is terminated because of an active/standby switchover, the client will immediately reinitiate a connection request. The connection exception is barely noticed.

DNS and HTTP sessions do not require session synchronization except for the following conditions:

- Users are aware that the current HTTP or DNS sessions will last for a long time.
- HTTP or DNS session backup is required.

For this command to take effect, you must also configure the **session synchronization enable** command.

This command takes effect only on sessions of the application protocols HTTP and DNS. Sessions of other application protocols will be backed up if the **session synchronization enable** command is configured.

Examples

Enable session synchronization for stateful failover, and enable session synchronization for HTTP.

```
<Sysname> system-view
[Sysname] session synchronization enable
[Sysname] session synchronization http
```

Related commands

session synchronization enable

session synchronization enable

Use **session synchronization enable** to enable session synchronization for stateful failover.

Use **undo session synchronization enable** to disable session synchronization for stateful failover.

Syntax

session synchronization enable [**asymmetric**]

undo session synchronization enable

Default

Session synchronization for stateful failover is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

asymmetric: Specifies asymmetric traffic. If you do not specify this keyword, this command supports only symmetric traffic.

Usage guidelines

This features enables the master and backup devices to synchronize sessions and dynamic entries of session-based services.

In a network that has asymmetric traffic, heavy service traffic might cause service delay or service unavailable because sessions cannot be backed up timely. For example, one device forwards the TCP SYN packets, and another device forwards its ACK packets. If the session tables of the two devices are not synchronized, the TCP packets will be dropped because of state error. To resolve this issue, use the **session synchronization enable asymmetric** command.

This command cannot be used together with the **hot-backup enable** command. For information about the **hot-backup enable** command, see RBM-based hot backup in *High Availability Command Reference*.

Examples

Enable session synchronization for stateful failover.

```
<Sysname> system-view
<Sysname> session synchronization enable
```

Enable session synchronization for both symmetric and asymmetric traffic.

```
<Sysname> system-view
```

```
<Sysname> session synchronization enable asymmetric
```

Related commands

hot-backup enable (*High Availability Command Reference*)

session top-statistics enable

Use **session top-statistics enable** to enable the top session statistics feature.

Use **undo session top-statistics enable** to disable the top session statistics feature.

Syntax

session top-statistics enable

undo session top-statistics enable

Default

The top session statistics feature is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command collects the number of sessions for session-based services and ranks the sessions by source address and by destination address.

To display the top session statistics, use the **display session top-statistics** command.

Examples

Enable the top session statistics feature.

```
<Sysname> system-view
[Sysname] session top-statistics enable
```

Related commands

display session top-statistics

Contents

Object group commands

description

Use **description** to configure a description for an object group.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

No description is configured for an object group.

Views

Object group view

Predefined user roles

network-admin

context-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 127 characters.

Examples

Configure the description as **This is an IPv4 object-group** for an IPv4 address object group.

```
<Sysname> system-view
[Sysname] object-group ip address ipgroup
[Sysname-obj-grp-ip-ipgroup] description This is an IPv4 object-group
```

display object-group

Use **display object-group** to display information about object groups.

Syntax

display object-group [{ { **ip** | **ipv6** } **address** | **mac-address** | **service** } [**default**] [**name** *object-group-name*] | **name** *object-group-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ip address: Specifies the IPv4 address object groups.

ipv6 address: Specifies the IPv6 address object groups.

mac-address: Specifies the MAC address object groups.

service: Specifies the service object groups.

default: Specifies the default object groups.

name *object-group-name*: Specifies an object group by its name, a case-insensitive string of 1 to 63 characters.

Examples

Display information about all object groups.

```
<Sysname> display object-group
IP address object group obj1: 0 object(in use)

IP address object group obj2: 6 objects(out of use)
0 network host address 1.1.1.1
object 0 description this is a description for object 0
10 network host name host
object 10 description this is a description for object 10
20 network subnet 1.1.1.1 255.255.255.0
30 network range 1.1.1.1 1.1.1.2
40 network group-object obj1
50 network user-group group1

IPv6 address object-group obj3: 0 object(in use)

IPv6 address object-group obj4: 5 objects(out of use)
0 network host address 1::1:1
10 network host name host
20 network subnet 1::1:0 112
30 network range 1::1:1 1::1:2
40 network group-object obj3

Service object-group obj5: 0 object(in use)

Service object-group obj6: 6 objects(out of use)
0 service 200
10 service tcp source lt 50 destination range 30 40
20 service udp source range 30 40 destination gt 30
30 service icmp 20 20
40 service icmpv6 20 20
50 service group-object obj5



MAC object-group obj7: 0 object(in use)

MAC object-group obj8: 2 objects(out of use)
0 MAC address 0010-dc28-11ac
10 MAC group-object obj7
```

Display information about object group **obj2**.

```
<Sysname> display object-group name obj2
IP address object-group obj2: 5 objects(out of use)
0 network host address 1.1.1.1
10 network host name host
20 network subnet 1.1.1.1 255.255.255.0
30 network range 1.1.1.1 1.1.1.2
40 network group-object obj1
```

Display information about all IPv4 address object groups.

```
<Sysname> display object-group ip address
IP address object-group obj1: 0 object(in use)

IP address object-group obj2: 5 objects(out of use)
0 network host address 1.1.1.1
10 network host name host
20 network subnet 1.1.1.1 255.255.255.0
30 network range 1.1.1.1 1.1.1.2
40 network group-object obj1
```

Display information about IPv6 address object group **obj4**.

```
<Sysname> display object-group ipv6 address name obj4
IPv6 address object-group obj4: 5 objects(out of use)
0 network host address 1::1:1
10 network host name host
20 network subnet 1::1:0 112
30 network range 1::1:1 1::1:2
40 network group-object obj3
```

Table 1 Command output

Field	Description
in use	The object group is used by an ACL or object group.
out of use	The object group is not used.

display object-group host

Use **display object-group host** to display IPv4 or IPv6 addresses for host names.

Syntax

display object-group { **ip** | **ipv6** } **host** { **object-group-name** *object-group-name* | **name** *host-name* [**vpn-instance** *vpn-instance-name*] } * [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

object-group-name *object-group-name*: Specifies an object group by its name, a case-insensitive string of 1 to 63 characters. If you do not specify this option, the command displays information about the specified host name.

name *host-name*: Specifies a host by its name, a case-insensitive string of 1 to 60 characters. If you do not specify this option, the command displays information about all the included and excluded host names in the specified object group.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN to which the host belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the host resides on the public network, do not specify this option.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify this option, this command displays information about host names of all member devices.

Examples

Display IPv4 addresses for host name **www.a.com** in object group **group1**.

```
[Sysname] display object-group ip host object-group-name group1 name www.a.com
Object group      : group1
  Object ID       : 0
    Host name     : www.a.com
    VPN instance  : -
      Updated at  : 2019-05-20 11:04:24
      IP addresses :
        169.0.0.10
        169.0.0.11
```

Display IPv6 addresses for all host names in object group **group1**.

```
<Sysname> display object-group ipv6 host object-group-name group1
Object group : group1
  Object ID       : 0
    Host name     : www.a.com
    VPN instance  : -
      Updated at  : 2019-05-20 11:04:24
      IP addresses :
        169:0::0:10
        169:0::0:11
  Object ID       : 10
    Host name     : www.b.com
    VPN instance  : -
      Updated at  : 2019-05-20 11:04:24
      IP addresses :
        169:0::0:11
        169:0::0:12
```

Related commands

object-group

mac

Use **mac** to configure a MAC address object.

Use **undo mac** to delete a MAC address object.

Syntax

[*object-id*] **mac** { *mac-address* | **group-object** *object-group-name* }

undo mac { *mac-address* | **group-object** *object-group-name* }

undo *object-id*

Default

No MAC address objects exist.

Views

MAC address object group view

Predefined user roles

network-admin

context-admin

Parameters

object-id: Specifies an object ID in the range of 0 to 4294967294. If you do not specify an object ID, the system automatically assigns the object a multiple of 10 next to the greatest ID being used. For example, if the greatest ID is 22, the system automatically assigns 30.

mac-address: Specifies a MAC address in format H-H-H.

group-object *object-group-name*: Specifies a MAC address object group by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

You can execute this command multiple times to create multiple MAC address objects for a MAC address object group.

This command creates a MAC address object if the specified object ID does not exist. Otherwise, the command overwrites the configuration of the specified object.

When you use the **group-object** *object-group-name* option, follow these guidelines:

- The object group to be used must be a MAC address object group.
- If the specified object group does not exist, the system creates a MAC address object group with the name you specified and uses the object group for the object.
- Two object groups cannot use each other at the same time.
- The system supports a maximum of five object group hierarchy layers. For example, if groups 1, 2, 3, and 4 use groups 2, 3, 4, and 5, respectively, group 5 cannot use another group and group 1 cannot be used by another group.

Examples

Configure a MAC address object with MAC address 0010-dc28-a4e9.

```
<Sysname> system-view
[Sysname] object-group mac-address groupmac
[Sysname-obj-grp-mac-groupmac] mac 0010-dc28-a4e9
```

Examples

display object-group

object-group

network (IPv4 address object group view)

Use **network** to configure an IPv4 address object.

Use **undo network** to delete an IPv4 address object.

Syntax

[*object-id*] **network** { **host** { **address** *ip-address* | **name** *host-name* [**vpn-instance** *vpn-instance-name*] } | **subnet** *ip-address* { *mask-length* | *mask* | **wildcard** *wildcard* } | **range** *ip-address1 ip-address2* | **group-object** *object-group-name* | **user** *user-name* [**domain** *domain-name*] | **user-group** *user-group-name* [**domain** *domain-name*] }

undo network { **host** { **address** *ip-address* | **name** *host-name* [**vpn-instance** *vpn-instance-name*] } | **subnet** *ip-address* { *mask-length* | *mask* | **wildcard** *wildcard* } | **range** *ip-address1 ip-address2* | **group-object** *object-group-name* | **user** *user-name* [**domain** *domain-name*] | **user-group** *user-group-name* [**domain** *domain-name*] }

undo *object-id*

Default

No IPv4 address objects exist.

Views

IPv4 address object group view

Predefined user roles

network-admin

context-admin

Parameters

object-id: Specifies an object ID in the range of 0 to 4294967294. If you do not specify an object ID, the system automatically assigns the object a multiple of 10 next to the greatest ID being used. For example, if the greatest ID is 22, the system automatically assigns 30.

host: Configures an IPv4 address object with the host address or name.

address *ip-address*: Specifies an IPv4 host address.

name *host-name*: Specifies a host name, a case-insensitive string of 1 to 60 characters. This parameter supports fuzzy matching. You can add an asterisk (*) to the front, end, or both of a string to indicate all host names that include the string. If no asterisks are attached, the system performs exact matching with the specified host name.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN to which the host belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the host resides on the public network, do not specify this option.

subnet *ip-address* { *mask-length* | *mask* | **wildcard** *wildcard* }: Configures an IPv4 address object with the subnet address followed by a mask length in the range of 0 to 32 or a mask in dotted decimal notation. The **wildcard** *wildcard* option specifies a wildcard mask in dotted decimal notation. A wildcard mask of zeros represents a host address.

range *ip-address1 ip-address2*: Configures an IPv4 address object with the address range.

group-object *object-group-name*: Specifies an IPv4 address object group by its name, a case-insensitive string of 1 to 63 characters.

user *user-name*: Specifies a user by its name, a case-sensitive string of 1 to 55 characters.

user-group *user-group-name*: Specifies a user group by its name, a case-insensitive string of 1 to 32 characters.

domain *domain-name*: Specifies the name of a domain to which the user or the user group belongs, a case-insensitive string of 1 to 255 characters. The string cannot contain question marks (?). If you do not specify this option, the command considers that the user or the user group does not belong to any domains.

Usage guidelines

This command fails if you use it to configure or change an IPv4 address object to be identical with an existing object.

This command creates an IPv4 address object if the specified object ID does not exist. Otherwise, the command overwrites the configuration of the specified object.

If you configure a subnet with the mask length of 32 or the mask of 255.255.255.255, the system configures the object with a host address.

When you use the **range** *ip-address1 ip-address2* option, follow these guidelines:

- If *ip-address1* is equal to *ip-address2,* the system configures the object with a host address.
- If *ip-address1* is not equal to *ip-address2*, the system compares the two IPv4 addresses, configures a range starting with the lower IPv4 address, and performs the following operations:
  - Configures the object with an address range if the two addresses are in different subnets.
  - Configures the object with a subnet address if the two addresses are in the same subnet.

When you use the **group-object** *object-group-name* option, follow these guidelines:

- The object group to be used must be an IPv4 address object group.
- If the specified object group does not exist, the system creates an IPv4 address object group with the name you specified and uses the object group for the object.
- Two object groups cannot use each other at the same time.
- The system supports a maximum of five object group hierarchy layers. For example, if groups 1, 2, 3, and 4 use groups 2, 3, 4, and 5, respectively, group 5 cannot use another group and group 1 cannot be used by another group.

Examples

Configure an IPv4 address object with the host address of **192.168.0.1**.

```
<Sysname> system-view
[Sysname] object-group ip address ipgroup
[Sysname-obj-grp-ip-ipgroup] network host address 192.168.0.1
```

Configure an IPv4 address object with exact-matching host name **pc3**.

```
<Sysname> system-view
[Sysname] object-group ip address ipgroup
[Sysname-obj-grp-ip-ipgroup] network host name pc3
```

Configure an IPv4 address object with fuzzy-matching host name **abc**.

```
<Sysname> system-view
[Sysname] object-group ip address ipgroup1
[Sysname-obj-grp-ip-ipgroup1] network host name *abc*
```

Configure an IPv4 address object with the IPv4 address of **192.167.0.0** and mask length of **24**.

```
<Sysname> system-view
[Sysname] object-group ip address ipgroup
[Sysname-obj-grp-ip-ipgroup] network subnet 192.167.0.0 24
```

Configure an IPv4 address object with the IPv4 address of **192.166.0.0** and mask of **255.255.0.0**.

```
<Sysname> system-view
[Sysname] object-group ip address ipgroup
[Sysname-obj-grp-ip-ipgroup] network subnet 192.166.0.0 255.255.0.0
```

Configure an IPv4 address object with the address range of **192.165.0.100** to **192.165.0.200**.

```
<Sysname> system-view
[Sysname] object-group ip address ipgroup
[Sysname-obj-grp-ip-ipgroup] network range 192.165.0.100 192.165.0.200
```

Configure an IPv4 address object using object group **ipgroup2**.

```
<Sysname> system-view
[Sysname] object-group ip address ipgroup
[Sysname-obj-grp-ip-ipgroup] network group-object ipgroup2
```

Configure an IPv4 address object with the IPv4 address of **192.168.0.1** and wildcard mask of **0.0.255.0**.

```
<Sysname> system-view
[Sysname] object-group ip address ipgroup
[Sysname-obj-grp-ip-ipgroup] network subnet 192.168.0.1 wildcard 0.0.255.0
```

Configure an IPv4 address object using user **user1** in domain **domain1**.

```
<Sysname> system-view
[Sysname] object-group ip address ipgroup
[Sysname-obj-grp-ip-ipgroup] network user user1 domain domain1
```

Configure an IPv4 address object using user group **usergroup1** in domain **domain1**.

```
<Sysname> system-view
[Sysname] object-group ip address ipgroup
[Sysname-obj-grp-ip-ipgroup] network user-group usergroup1 domain domain1
```

network (IPv6 address object group view)

Use **network** to configure an IPv6 address object.

Use **undo network** to delete an IPv6 address object.

Syntax

[*object-id*] **network** { **host** { **address** *ipv6-address* | **name** *host-name* [**vpn-instance** *vpn-instance-name*] } | **subnet** *ipv6-address prefix-length* | **range** *ipv6-address ipv6-address2* | **group-object** *object-group-name* | **user** *user-name* [**domain** *domain-name*] | **user-group** *user-group-name* [**domain** *domain-name*] }

undo network { **host** { **address** *ipv6-address* | **name** *host-name* [**vpn-instance** *vpn-instance-name*] } | **subnet** *ipv6-address prefix-length* | **range** *ipv6-address1 ipv6-address2* | **group-object** *object-group-name* | **user** *user-name* [**domain** *domain-name*] | **user-group** *user-group-name* [**domain** *domain-name*] }

undo *object-id*

Default

No IPv6 address objects exist.

Views

IPv6 address object group view

Predefined user roles

network-admin

context-admin

Parameters

object-id: Specifies an object ID in the range of 0 to 4294967294. If you do not configure an object ID, the system automatically assigns the object a multiple of 10 next to the greatest ID being used. For example, if the greatest ID is 22, the system automatically assigns 30.

host: Configures an IPv6 address object with the host address or name.

address *ipv6-address*: Specifies an IPv6 host address.

name *host-name*: Specifies a host name, a case-insensitive string of 1 to 60 characters. This parameter supports fuzzy matching. You can add an asterisk (*) to the front, end, or both of a string to indicate all host names that include the string. If no asterisks are attached, the system performs exact matching with the specified host name.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN to which the host belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the host resides on the public network, do not specify this option.

subnet *ipv6-address prefix-length*: Configures an IPv6 address object with the subnet address followed by the prefix length in the range of 1 to 128.

range *ipv6-address1 ipv6-address2*: Configures an IPv6 address object.

group-object *object-group-name*: Specifies an IPv6 address object group by its name, a case-insensitive string of 1 to 63 characters.

user *user-name*: Specifies a user by its name, a case-sensitive string of 1 to 55 characters.

user-group *user-group-name*: Specifies a user group by its name, a case-insensitive string of 1 to 32 characters.

domain *domain-name*: Specifies the name of a domain to which the user or the user group belongs, a case-insensitive string of 1 to 255 characters. The string cannot contain question marks (?). If you do not specify this option, the command considers that the user or the user group does not belong to any domains.

Usage guidelines

This command fails if you use it to configure or change an IPv6 address object to be identical with an existing object.

This command creates an IPv6 address object if the specified object ID does not exist. Otherwise, the command overwrites the configuration of the specified object.

If you configure a subnet address with the prefix length of 128, the system configures the object with a host address.

When you use the **range** *ipv6-address1 ipv6-address2* option, follow these guidelines:

- If *ipv6-address1* is equal to *ipv6-address2,* the system configures the object with a host address.
- If *ipv6-address1* is not equal to *ipv6-address2*, the system compares the two IPv6 addresses, configures a range starting with the lower IPv6 address, and performs the following operations:

- Configures the object with an address range if the two addresses are in different subnets.
- Configures the object with a subnet address if the two addresses are in the same subnet.

When you use the **group-object** *object-group-name* option, follow these guidelines:

- The object group to be used must be an IPv6 address object group.
- If the specified object group does not exist, the system creates an IPv6 address object group with the name you specified and uses the object group for the object.
- Two object groups cannot use each other at the same time.
- The system supports a maximum of five object group hierarchy layers. For example, if groups 1, 2, 3, and 4 use groups 2, 3, 4, and 5, respectively, group 5 cannot use another group and group 1 cannot be used by another group.

Examples

Configure an IPv6 address object with the host address of **1::1**.

```
<Sysname> system-view
[Sysname] object-group ipv6 address ipv6group
[Sysname-obj-grp-ipv6-ipv6group] network host address 1::1
```

Configure an IPv6 address object with exact-matching host name **pc3**.

```
<Sysname> system-view
[Sysname] object-group ipv6 address ipv6group
[Sysname-obj-grp-ipv6-ipv6group] network host name pc3
```

Configure an IPv6 address object with fuzzy-matching host name **abc**.

```
<Sysname> system-view
[Sysname] object-group ipv6 address ipv6group1
[Sysname-obj-grp-ipv6-ipv6group1] network host name *abc*
```

Configure an IPv6 address object with the IPv6 address of **1:1:1::1** and prefix length of **24**.

```
<Sysname> system-view
[Sysname] object-group ipv6 address ipv6group
[Sysname-obj-grp-ipv6-ipv6group] network subnet 1:1:1::1 24
```

Configure an IPv6 address object with the address range of **1:1:1::1** to **1:1:1::100**

```
<Sysname> system-view
[Sysname] object-group ipv6 address ipv6group
[Sysname-obj-grp-ipv6-ipv6group] network range 1:1:1::1 1:1:1::100
```

Configure an IPv6 address object using object group **ipv6group2**.

```
<Sysname> system-view
[Sysname] object-group ipv6 address ipv6group
[Sysname-obj-grp-ipv6-ipv6group] network group-object ipv6group2
```

Configure an IPv6 address object using user **user1** in domain **domain1**.

```
<Sysname> system-view
[Sysname] object-group ipv6 address ipv6group
[Sysname-obj-grp-ipv6-ipv6group] network user user1 domain domain1
```

Configure an IPv6 address object using user group **usergroup1** in domain **domain1**.

```
<Sysname> system-view
[Sysname] object-group ipv6 address ipv6group
[Sysname-obj-grp-ipv6-ipv6group] network user-group usergroup1 domain domain1
```

network exclude (IPv4 address object group view)

Use **network exclude** to exclude an IPv4 address or a subnet from an address object.

Use **undo network exclude** to restore the default.

Syntax

object-id **network exclude** { *ip-address* | **subnet** *ip-address* { *mask-length* | *mask* } }

undo *object-id* **network exclude** { *ip-address* | **subnet** *ip-address* { *mask-length* | *mask* } }

Default

No IPv4 address or subnet in an address object is excluded.

Views

IPv4 address object group view

Predefined user roles

network-admin

context-admin

Parameters

object-id: Specifies an address object by its ID in the range of 1 to 4294967294. The specified address object must have been created.

ip-address: Specifies the IPv4 address to be excluded.

subnet *ip-address* { *mask-length* | *mask* }: Specifies the IPv4 address and mask of a subnet to be excluded. You can specify the mask length or specify the mask in dotted decimal notation. The mask length is in the range of 0 to 32.

Usage guidelines

You can execute this command multiple times to exclude multiple IPv4 addresses or subnets from an address object.

The configuration fails if either of the following conditions exists:

- The specified address is the same as an existing excluded address or is contained in an existing excluded subnet.
- The specified subnet contains an existing excluded address or overlaps with an existing excluded subnet.

Examples

Configure an IPv4 address object with the IPv4 address of **192.166.0.0** and mask of **255.255.0.0**. Exclude IPv4 address **192.166.0.10** and subnet **192.166.1.0/24** from the address object.

```
<Sysname> system-view
[Sysname] object-group ip address ipgroup
[Sysname-obj-grp-ip-ipgroup] 10 network subnet 192.166.0.0 255.255.0.0
[Sysname-obj-grp-ip-ipgroup] 10 network exclude 192.166.0.10
[Sysname-obj-grp-ip-ipgroup] 10 network exclude subnet 192.166.1.0 255.255.255.0
```

network exclude (IPv6 address object group view)

Use **network exclude** to exclude an IPv6 address or a subnet from an address object.

Use **undo network exclude** to restore the default.

Syntax

object-id **network exclude** { *ipv6-address* | **subnet** *ipv6-address prefix-length* }

undo *object-id* **network exclude** { *ipv6-address* | **subnet** *ipv6-address prefix-length* }

Default

No IPv6 address or subnet in an address object is excluded.

Views

IPv6 address object group view

Predefined user roles

network-admin

context-admin

Parameters

object-id: Specifies an address object by its ID in the range of 1 to 4294967294. The specified address object must have been created.

ip-address: Specifies the IPv6 address to be excluded.

subnet *ipv6-address prefix-length*: Specifies the IPv6 subnet to be excluded. The prefix length is in the range of 1 to 128.

Usage guidelines

You can execute this command multiple times to exclude multiple IPv6 addresses or subnets from an address object.

The configuration fails if either of the following conditions exists:

- The specified address is the same as an existing excluded address or is contained in an existing excluded subnet.
- The specified subnet contains an existing excluded address or overlaps with an existing excluded subnet.

Examples

Configure an IPv6 address object with the IPv6 address of **1:1:1::1** and prefix length of **24**. Exclude IPv6 address **1:1:1::10** and subnet **1:1:1::2:0** with a prefix length of **112** from the address object.

```
<Sysname> system-view
[Sysname] object-group ipv6 address ipv6group
[Sysname-obj-grp-ipv6-ipv6group] 10 network subnet 1:1:1::1 24
[Sysname-obj-grp-ipv6-ipv6group] 10 network exclude 1:1:1::10
[Sysname-obj-grp-ipv6-ipv6group] 10 network exclude subnet 1:1:1::2:0 112
```

object description

Use **object description** to configure a description for an object.

Use **undo object description** to restore the default.

Syntax

object *object-id* **description** *text*

undo object *object-id* **description**

Default

No description is configured for an object.

Views

Object group view

Predefined user roles

network-admin

context-admin

Parameters

object-id: Specifies an object ID in the range of 0 to 4294967294. The object must already exist.

text: Specifies a description, a case-sensitive string of 1 to 127 characters.

Examples

Configure the description as **This is a description for object 0** for the object 0.

```
<Sysname> system-view
[Sysname] object-group ip address ipgroup
[Sysname-obj-grp-ip-ipgroup] 0 network host address 1.2.3.4
[Sysname-obj-grp-ip-ipgroup] object 0 description This is a description for object 0
```

Related commands

- **object-group**

object-group

Use **object-group** to create an object group and enter its view, or enter the view of an existing object group.

Use **undo object-group** to delete an object group.

Syntax

object-group { { **ip** | **ipv6** } **address** | **mac-address** | **service** } *object-group-name*

undo object-group { { **ip** | **ipv6** } **address** | **mac-address** | **service** } *object-group-name*

Default

Default object groups exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ip address: Creates an IPv4 address object group.

ipv6 address: Creates an IPv6 address object group.

mac-address: Creates a MAC object group.

service: Creates a service object group.

object-group-name: Specifies an object group name, a case-insensitive string of 1 to 63 characters. The object group name must be globally unique.

Usage guidelines

The **object-group** command execution results vary with the specified object group.

- If the specified group does not exist, the system creates a new object group and enters the object group view.
- If the specified group exists but the group type is different from that in the command, the command fails.

The **undo object-group** command execution results vary with the specified object group.

- If the specified group does not exist, the system executes the command without any system prompt.
- If the specified group exists and the group type is the same as that in the command, the system deletes the group.
- If the specified group exists but the group type is different from that in the command, the command fails.
- If the specified object group is being used by an ACL or another object group, the command fails.

Default object groups cannot be deleted.

Examples

Create an IPv4 address object group named **ipgroup**.

```
<Sysname> system-view
[Sysname] object-group ip address ipgroup
```

Create an IPv6 address object group named **ipv6group**.

```
<Sysname> system-view
[Sysname] object-group ipv6 address ipv6group
```

Create a MAC object group named **groupmac**.

```
<Sysname> system-view
[Sysname] object-group mac-address groupmac
```

Create a service object group named **servicegroup**.

```
<Sysname> system-view
[Sysname] object-group service servicegroup
```

object-group dns-aging

Use **object-group dns-aging** to enable aging of DNS-resolved IP addresses from host names.

Use **undo object-group dns-aging** to disable aging of DNS-resolved IP addresses from host names.

Syntax

object-group dns-aging [**time** *aging-time*]

undo object-group dns-aging

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	No

Default

Aging of DNS-resolved IP addresses from host names is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

time *aging-time*: Specifies the aging time in the range of 1 to 70000000 minutes. The default value is 120.

Usage guidelines

In load balancing scenarios where one host name maps to several IP addresses, DNS-resolved IP address for a host name changes between these mapping addresses. Upon every change, the object group module notifies relevant policies (such as security policy) of the change, which causes policies to submit changes frequently and consumes memory. To resolve this issue, you can enable aging of DNS-resolved IP addresses from host names.

With this feature enabled, the system maintains an IP address group for each host name. If a resolved IP address is not in the group, the system adds the address to the group and notifies relevant policies of the change. If a resolved IP address is in the group, the system does not notify relevant policies.

As a best practice, set the aging time to be longer than the TTL of resolution records on the DNS server.

Examples

Enable aging of DNS-resolved IP addresses from host names and set the aging time to 5 minutes.

```
<Sysname> system-view
[Sysname] object-group dns-aging
[Sysname] object-group dns-aging time 5
```

object-group rename

Use **object-group rename** to rename an object group.

Syntax

object-group rename *old-object-group-name new-object-group-name*

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

old-object-group-name: Specifies the name of the object group to be renamed, a case-insensitive string of 1 to 63 characters.

new-object-group-name: Specifies a new name for the object group, a case-insensitive string of 1 to 63 characters. The object group name must be globally unique.

Usage guidelines

You can only rename non-default object groups.

Examples

Rename object group **ipgroup1** to **ipgroup2**.

```
<Sysname> system-view
[Sysname] object-group rename ipgroup1 ipgroup2
```

Related commands

object-group

security-zone

Use **security-zone** to specify a security zone for an IP address object group.

Use **undo security-zone** to restore the default.

Syntax

security-zone *security-zone-name*

undo security-zone

Default

No security zone is specified for an IP address object group.

Views

IPv4 address object group view

IPv6 address object group view

Predefined user roles

network-admin

context-admin

Parameters

security-zone-name: Specifies the security zone name, a case-insensitive string of 1 to 31 characters. The string cannot contain hyphens (-) and cannot be **any**.

Usage guidelines

This feature enables fast selection of IP address object groups when you specify IP address filtering criteria for a security policy from the Web interface. If a security policy uses an IP address object group specified with a security zone, you can specify only IP address object groups from the same or no security zone for the policy.

You can specify only one security zone for an IP address object group. If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the security zone for IPv4 address object group 1 as **Local**.

```
<Sysname> system-view
[Sysname] object-group ip address 1
[Sysname-obj-grp-ip-1] security-zone Local
```

Related commands

object-group

service (service object group view)

Use **service** to configure a service object.

Use **undo service** to delete a service object.

Syntax

[*object-id*] **service** { *protocol* [{ **source** { { **eq** | **lt** | **gt** } *port* | **range** *port1 port2* } | **destination** { { **eq** | **lt** | **gt** } *port* | **range** *port1 port2* } } * | *icmp-type icmp-code* | *icmpv6-type icmpv6-code*] | **group-object** *object-group-name* }

undo service { *protocol* [{ **source** { { **eq** | **lt** | **gt** } *port* | **range** *port1 port2* } | **destination** { { **eq** | **lt** | **gt** } *port* | **range** *port1 port2* } } * | *icmp-type icmp-code* | *icmpv6-type icmpv6-code*] | **group-object** *object-group-name* }

undo *object-id*

Default

No service objects exist.

Views

Service object group view

Predefined user roles

network-admin

context-admin

Parameters

object-id: Configures an object ID in the range of 0 to 4294967294. If you do not configure an ID for the object, the system automatically assigns the object a multiple of 10 next to the greatest ID being used. For example, if the greatest ID is 22, the automatically assigned ID is 30.

protocol: Configures the protocol number in the range of 0 to 255, or the protocol name such as TCP, UDP, ICMP, and ICMPv6.

source: Configures a service object with a source port when the protocol is TCP or UDP.

destination: Configures a service object with a destination port when the protocol is TCP or UDP.

eq: Configures a port equal to the specified port.

lt: Configures a port smaller than the specified port.

gt: Configures a port greater than the specified port.

port: Specifies a port number in the range of 0 to 65535.

range *port1 port2*: Configures a service object with a port range. The value range for the *port1* and *port2* arguments is 0 to 65535.

icmp-type: Configures the ICMP message type in the range of 0 to 255.

icmp-code: Configures the ICMP message code in the range of 0 to 255.

icmpv6-type: Configures the ICMPv6 message type in the range of 0 to 255.

icmpv6-code: Configures the ICMPv6 message code in the range of 0 to 255.

group-object *object-group-name*: Specifies a service object group by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

This command fails if you use it to configure or change a service object to be identical with an existing object.

This command creates a service object if the specified object ID does not exist. Otherwise, the command overwrites the configuration of the specified object.

When you use the **lt** *port* option, follow these guidelines:

- The value of *port* cannot be 0.
- If the value of *port* is 1, the system configures the object with a port number of 0.
- If the value of *port* is in the range of 2 to 65535, the system configures the object with a port number range of [0, *port*–1].

When you use the **gt** *port* option, follow these guidelines:

- The value of *port* cannot be 65535.
- If the value of *port* is 65534, the system configures the object with a port number of 65535.
- If the value of *port* is in the range of 0 to 65533, the system configures the object with a port number range of [*port*+1, 65535].

When you use the **range** *port1 port2* option, follow these guidelines:

- If *port1* is equal to *port2*, the system configures the object with the port number *port1*.
- If *port1* is smaller than *port2*, the system configures the object with the port number range.
- If *port1* is greater than *port2*, the system changes the range to [*port2*, *port1*] and configures the object with the changed port number range.
- If *port1* is 0, the range is displayed as **lt** *port2*+1.
- If *port2* is 65535, the range is displayed as **gt** *port1*–1.

When use the **group-object** *object-group-name* option, follow these guidelines:

- The object group to be used must be a service object group.
- If the specified object group does not exist, the system creates a service object group with the name you specified and uses the object group for the object.
- Two object groups cannot use each other at the same time.
- The system supports a maximum of five object group hierarchy layers. For example, if groups 1, 2, 3, and 4 use groups 2, 3, 4, and 5, respectively, group 5 cannot use another group and group 1 cannot be used by another group.

Examples

Configure a service object with a protocol number of **100**.

```
<Sysname> system-view
[Sysname] object-group service servicegroup
[Sysname-obj-grp-service-servicegroup] service 100
```

Configure a service object with the source and destination port numbers for the TCP service.

```
<Sysname> system-view
[Sysname] object-group service servicegroup
```

```
[Sysname-obj-grp-service-servicegroup] service tcp source eq 100 destination range 10 100
```

Configure a service object with the message type and code for the ICMP service.

```
<Sysname> system-view
[Sysname] object-group service servicegroup
[Sysname-obj-grp-service-servicegroup] service icmp 100 150
```

Configure a service object using object group **servicegroup2**.

```
<Sysname> system-view
[Sysname] object-group service servicegroup
[Sysname-obj-grp-service-servicegroup] service group-object servicegroup2
```

Contents

IP source guard commands

display ip source binding

Use **display ip source binding** to display IPv4SG bindings.

Syntax

display ip source binding [**static** | [**vpn-instance** *vpn-instance-name*] [**dhcp-relay** | **dhcp-server** | **ip-mac-vlan** | **ip-mac-vpn**]] [**ip-address** *ip-address*] [**mac-address** *mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

static: Displays static IPv4SG bindings.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. To display dynamic IPv4SG bindings for the public network, do not specify a VPN instance.

dhcp-relay: Specifies the DHCP relay agent module.

dhcp-server: Specifies the DHCP server module.

ip-mac-vlan: Specifies IPv4SG IP-MAC-VLAN bindings that are generated based on the IP-MAC binding module.

ip-mac-vpn: Specifies IPv4SG IP-MAC-VPN bindings that are generated based on the IP-MAC binding module.

ip-address *ip-address*: Specifies an IPv4 address.

mac-address *mac-address*: Specifies a MAC address in H-H-H format.

vlan *vlan-id*: Specifies a VLAN ID in the range of 1 to 4094.

interface *interface-type interface-number*: Specifies an interface by its type and number.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv4SG bindings for the master device.

Examples

Display all IPSG bindings on the public network.

```
<Sysname> display ip source binding
Total entries found: 7
IP Address      MAC Address    Interface               VLAN Type
Total entries found: 7
```

```
IP Address      MAC Address    Interface                VLAN Type
10.1.0.5        040a-0000-4000 GE1/0/1                  1    Static
10.1.0.6        040a-0000-3000 GE1/0/1                  1    Static
10.1.0.7        040a-0000-2000 GE1/0/1                  1    Static
10.1.0.8        040a-0000-1000 GE1/0/2                  N/A  DHCP relay
10.1.0.9        040a-0000-2000 GE1/0/2                  N/A  Static
10.1.0.10       040a-0000-3000 N/A                      1    IP-MAC VLAN
10.1.0.11       040a-0000-4000 N/A                      N/A  IP-MAC VPN
```

Table 1 Command output

Field	Description
Total entries found	Total number of IPv4SG bindings.
IP Address	IPv4 address in the IPv4SG binding. If no IP address is bound in the binding, this field displays **N/A**.
MAC Address	MAC address in the IPv4SG binding. If no MAC address is bound in the binding, this field displays **N/A**.
Interface	Interface of the binding. This field displays **N/A** for a global IPv4SG binding.
VLAN	VLAN information in the IPv4SG binding. If the binding contains no VLAN information, this field displays **N/A**.
Type	IPSG binding type: • **Static**—Manually configured by using the **ip source binding** command. Static bindings are for packet filtering in IPSG or used by other modules to provide security services. • **DHCP relay**—Dynamically generated based on DHCP relay agent. The binding is for packet filtering in IPSG. • **DHCP server**—Dynamically generated based on DHCP server. The binding is used by other modules to provide security services. • **IP-MAC VLAN**—Dynamically generated based on IP-MAC binding module. This type of IPSG bindings binds IPv4 address, MAC address, and VLAN ID. • **IP-MAC VPN**—Dynamically generated based on IP-MAC binding module. This type of IPSG bindings binds IPv4 address, MAC address, and VPN instance.

Related commands

ip source binding

ip verify source

display ipv6 source binding

Use **display ipv6 source binding** to display IPv6SG bindings.

Syntax

display ipv6 source binding [**static** | [**vpn-instance** *vpn-instance-name*] [**ipv6-mac-vlan** | **ipv6-mac-vpn**]] [**ip-address** *ipv6-address*] [**mac-address** *mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

`static`: Displays static IPv6SG bindings.

`vpn-instance` *`vpn-instance-name`*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. To display dynamic IPv6SG bindings for the public network, do not specify a VPN instance.

`ipv6-mac-vlan`: Specifies IPv6SG IPv6-MAC-VLAN bindings that are generated based on the IP-MAC binding module.

`ipv6-mac-vpn`: Specifies IPv6SG IPv6-MAC-VPN bindings that are generated based on the IP-MAC binding module.

`ip-address` *`ipv6-address`*: Specifies an IPv6 address.

`mac-address` *`mac-address`*: Specifies a MAC address in H-H-H format.

`vlan` *`vlan-id`*: Specifies a VLAN ID in the range of 1 to 4094.

`interface` *`interface-type interface-number`*: Specifies an interface by its type and number.

`slot` *`slot-number`*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv6SG bindings for the master device.

Examples

Display all IPv6SG bindings on the public network.

```
<Sysname> display ipv6 source binding
Total entries found: 4
IPv6 Address         MAC Address    Interface              VLAN Type
Total entries found: 4
IPv6 Address         MAC Address    Interface              VLAN Type
2012:1222:2012:1222: 000f-2202-0435 GE1/0/1                1    Static
2012:1222:2012:1222
2012:1222:2012:1222: 000f-2202-0436 GE1/0/1                N/A  Static
2012:1222:2012:1223
2012:1222:2012:1222: 040a-0000-3000 N/A                    1    IPv6-MAC VLAN
2012:1222:2012:1224
2012:1222:2012:1222: 040a-0000-4000 N/A                    N/A  IPv6-MAC VPN
2012:1222:2012:1225
```

Table 2 Command output

Field	Description
Total entries found	Total number of IPv6SG bindings.
IPv6 Address	IPv6 address in the IPv6SG binding. If no IPv6 address is bound in the binding, this field displays **N/A**.
MAC Address	MAC address in the IPv6SG binding. If no MAC address is bound in the binding, this field displays **N/A**.

Field	Description
Interface	Interface of the IPv6SG binding. This field displays **N/A** for a global IPv6SG binding.
VLAN	VLAN information in the IPv6SG binding. If the binding contains no VLAN information, this field displays **N/A**.
Type	Type of the IPv6SG binding: • **Static**—Manually configured by using the **ipv6 source binding** command. Static bindings are for packet filtering in IPv6SG or used by other modules to provide security services. • **IPv6-MAC VLAN**—Dynamically generated based on IP-MAC binding module. This type of IPSG bindings binds IPv6 address, MAC address, and VLAN ID. • **IPv6-MAC VPN**—Dynamically generated based on IP-MAC binding module. This type of IPSG bindings binds IPv6 address, MAC address, and VPN instance.

Related commands

ipv6 source binding

ipv6 verify source

ip source binding (interface view)

Use **ip source binding** to configure a static IPv4SG binding on an interface.

Use **undo ip source binding** to delete the static IPv4SG bindings configured on an interface.

Syntax

ip source binding { **ip-address** *ip-address* | **ip-address** *ip-address* **mac-address** *mac-address* | **mac-address** *mac-address* } [**vlan** *vlan-id*]

undo ip source binding { **all** | **ip-address** *ip-address* | **ip-address** *ip-address* **mac-address** *mac-address* | **mac-address** *mac-address* } [**vlan** *vlan-id*]

Default

No static IPv4SG bindings are configured on an interface.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Layer 3 Ethernet subinterface view

VLAN interface view

Reth interface view

Reth subinterface view

Predefined user roles

network-admin

context-admin

Parameters

all: Removes all static IPv4SG bindings on the interface.

ip-address *ip-address*: Specifies an IPv4 address for the static binding. The IPv4 address must be a class A, B, or C address, and cannot be 127.x.x.x or 0.0.0.0.

mac-address *mac-address*: Specifies a MAC address for the static binding. The MAC address must be in H-H-H format, and cannot be all 0s, all Fs (a broadcast MAC address), or a multicast MAC address.

vlan *vlan-id*: Specifies a VLAN ID for the static binding. The value range is 1 to 4094. This option is supported only in Layer 2 Ethernet interface view.

Usage guidelines

Static IPv4SG bindings on an interface implement the following functions:

- Filter incoming IPv4 packets on the interface.
- Check user validity by cooperating with the ARP attack detection feature.

Examples

Configure a static IPv4SG binding on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip source binding ip-address 192.168.0.1 mac-address
0001-0001-0001
```

Related commands

display ip source binding

ip source binding (system view)

ip source binding (system view)

Use **ip source binding** to configure a global static IPv4SG binding.

Use **undo ip source binding** to delete one or all global static IPv4SG bindings.

Syntax

ip source binding ip-address *ip-address* **mac-address** *mac-address*

undo ip source binding { **all** | **ip-address** *ip-address* **mac-address** *mac-address* }

Default

No global static IPv4SG bindings exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ip-address *ip-address*: Specifies the IPv4 address for the static binding. The IPv4 address must be a class A, B, or C address, and cannot be 127.x.x.x or 0.0.0.0.

mac-address *mac-address*: Specifies the MAC address for the static binding. The MAC address is in the format H-H-H but cannot be all 0s, all Fs (a broadcast MAC address), or a multicast MAC address.

all: Removes all global static IPv4SG bindings.

Usage guidelines

A global static IPv4SG binding takes effect on all interfaces.

Examples

Configure a global static IPv4SG binding.

```
<Sysname> system-view
[Sysname] ip source binding ip-address 192.168.0.1 mac-address 0001-0001-0001
```

Related commands

display ip source binding

ip source binding (interface view)

ip verify source

Use **ip verify source** to enable IPv4SG on an interface.

Use **undo ip verify source** to disable IPv4SG on an interface.

Syntax

ip verify source { **ip-address** | **ip-address mac-address** | **mac-address** }

undo ip verify source

Default

The IPv4SG feature is disabled on an interface.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Layer 3 Ethernet subinterface view

Layer 3 aggregate interface view

Layer 3 aggregate subinterface view

VLAN interface view

Reth interface view

Reth subinterface view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Filters incoming packets by source IPv4 addresses.

ip-address mac-address: Filters incoming packets by source IPv4 addresses and source MAC addresses.

mac-address: Filters incoming packets by source MAC addresses.

Usage guidelines

After you enable IPv4SG on an interface, this feature uses static and dynamic IPv4SG bindings to match incoming packets on the interface. Packets that match an IPv4SG binding are forwarded and packets that do not match any IPv4SG binding are discarded.

The matching criterion specified by this command applies only to dynamic IPSG. Static IPv4SG uses static bindings configured by using the **ip source binding** command.

Examples

Enable IPv4SG on Layer 2 Ethernet interface GigabitEthernet 1/0/1 and verify the source IPv4 address and MAC address for dynamic IPSG.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip verify source ip-address mac-address
```

Enable IPv4SG on VLAN-interface 100 and verify the source IPv4 address and MAC address for dynamic IPSG.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ip verify source ip-address mac-address
```

Enable IPv4SG on Layer 3 Ethernet interface GigabitEthernet 1/0/2 and verify the source IPv4 address and MAC address for dynamic IPSG.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] ip verify source ip-address mac-address
```

Enable IPv4SG on Layer 3 Ethernet interface GigabitEthernet 1/0/2 and verify the source MAC address for dynamic IPSG.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] ip verify source mac-address
```

Related commands

display ip source binding

ipv6 source binding (interface view)

Use **ipv6 source binding** to configure a static IPv6SG binding.

Use **undo ipv6 source binding** to delete the static IPv6SG bindings configured on an interface.

Syntax

ipv6 source binding { **ip-address** *ipv6-address* | **ip-address** *ipv6-address* **mac-address** *mac-address* | **mac-address** *mac-address* } [**vlan** *vlan-id*]

undo ipv6 source binding { **all** | **ip-address** *ipv6-address* | **ip-address** *ipv6-address* **mac-address** *mac-address* | **mac-address** *mac-address* } [**vlan** *vlan-id*]

Default

No static IPv6SG bindings exist on an interface.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Layer 3 Ethernet subinterface view

VLAN interface view

Reth interface view

Reth subinterface view

Predefined user roles

network-admin

context-admin

Parameters

all: Removes all the static IPv6SG bindings on the interface.

ip-address *ipv6-address*: Specifies an IPv6 address for the static binding. The IPv6 address cannot be an all-zero address, a multicast address, or a loopback address.

mac-address *mac-address*: Specifies a MAC address for the static binding. The MAC address must be in H-H-H format, and cannot be all 0s, all Fs (a broadcast MAC address), or a multicast MAC address.

vlan *vlan-id*: Specifies a VLAN ID for the static binding. The value range is 1 to 4094. This option is supported only in Layer 2 Ethernet interface view.

Usage guidelines

Static IPv6SG bindings on an interface filter incoming IPv6 packets.

Examples

Configure a static IPv6SG binding on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 source binding ip-address 2001::1 mac-address
0002-0002-0002
```

Related commands

display ipv6 source binding

ipv6 source binding (system view)

ipv6 source binding (system view)

Use **ipv6 source binding** to configure a global static IPv6SG binding.

Use **undo ipv6 source binding** to delete one or all global static IPv6SG bindings.

Syntax

ipv6 source binding ip-address *ipv6-address* **mac-address** *mac-address*

undo ipv6 source binding { **all** | **ip-address** *ipv6-address* **mac-address** *mac-address* }

Default

No global static IPv6SG bindings exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address *ipv6-address*: Specifies the IPv6 address for the static binding. The IPv6 address cannot be an all-zero address, a multicast address, or a loopback address.

mac-address *mac-address*: Specifies the MAC address for the static binding. The MAC address must be in H-H-H format, and cannot be all 0s, all Fs (a broadcast MAC address), or a multicast MAC address.

all: Removes all global static IPv6SG bindings.

Usage guidelines

A global static IPv6SG binding takes effect on all interfaces.

Examples

Configure a global static IPv6SG binding.

```
<Sysname> system-view
[Sysname] ipv6 source binding ipv6-address 2001::1 mac-address 0002-0002-0002
```

Related commands

display ipv6 source binding

ipv6 source binding (interface view)

ipv6 verify source

Use **ipv6 verify source** to enable IPv6SG on an interface.

Use **undo ipv6 verify source** to disable IPv6SG on an interface.

Syntax

ipv6 verify source { **ip-address** | **ip-address mac-address** | **mac-address** }

undo ipv6 verify source

Default

The IPv6SG feature is disabled on an interface.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Layer 3 Ethernet subinterface view

Layer 3 aggregate interface view

Layer 3 aggregate subinterface view

VLAN interface view

Reth interface view

Reth subinterface view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Filters incoming packets by source IPv6 addresses.

ip-address mac-address

mac-address: Filters incoming packets by source MAC addresses.

Usage guidelines

After you enable IPv6SG on an interface, this feature uses static and dynamic IPv6SG bindings to match incoming packets on the interface. Packets that match an IPv6SG binding are forwarded and packets that do not match any IPv6SG binding are discarded.

The matching criterion specified by this command applies only to dynamic IPv6SG. Static IPv6SG uses static bindings configured by using the **ipv6 source binding** command.

Examples

Enable IPv6SG on Layer 2 Ethernet interface GigabitEthernet 1/0/1 and verify the source IPv6 address and MAC address for dynamic IPv6SG.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 verify source ip-address mac-address
```

Related commands

display ipv6 source binding

Contents

AAA commands

General AAA commands

aaa nas-id profile

Use **aaa nas-id profile** to create a NAS-ID profile and enter its view, or enter the view of an existing NAS-ID profile.

Use **undo aaa nas-id profile** to delete a NAS-ID profile.

Syntax

aaa nas-id profile *profile-name*

undo aaa nas-id profile *profile-name*

Default

No NAS-ID profiles exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

profile-name: Specifies the NAS-ID profile name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

Configure a NAS-ID profile to maintain NAS-ID and VLAN bindings on the device.

During RADIUS authentication, the device uses a NAS-ID to set the NAS-Identifier attribute of RADIUS packets so that the RADIUS server can identify the access location of users.

The device selects the NAS-ID for the NAS-Identifier attribute in the following order:

1. NAS-ID bound with VLANs in a NAS-ID profile.
2. NAS-ID in an ISP domain.

By default, the device uses the device name as the NAS-ID.

Examples

Create a NAS-ID profile named **aaa** and enter its view.

```
<Sysname> system-view
[Sysname] aaa nas-id profile aaa
[Sysname-nas-id-prof-aaa]
```

Related commands

nas-id

nas-id bind vlan

portal nas-id-profile

aaa session-id mode

Use **aaa session-id mode** to specify the format for attribute Acct-Session-Id.

Use **undo aaa session-id mode** to restore the default.

Syntax

aaa session-id mode { **common** | **simplified** }

undo session-id mode

Default

The device uses the common mode for attribute Acct-Session-Id.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

common: Specifies the common format for attribute Acct-Session-Id. In this format, the Acct-Session-Id attribute is a string with a minimum length of 38 characters. This string contains the prefix (indicating the access type), date and time, sequence number, LIP address of the access node, device ID, and job ID of the access process.

simplified: Specifies the simple format for attribute Acct-Session-Id. In this format, the Acct-Session-Id attribute is a string of 16 characters. This string contains the prefix (indicating the access type), month, sequence number, device ID, and LIP address of the access node.

Usage guidelines

Configure the format for attribute Acct-Session-Id to meet the requirements of the RADIUS servers.

Examples

Specify the simple format for attribute Acct-Session-Id.

```
<Sysname> system-view
[Sysname] aaa session-id mode simplified
```

aaa session-limit

Use **aaa session-limit** to set the maximum number of concurrent users that can log on to the device through the specified method.

Use **undo aaa session-limit** to restore the default maximum number of concurrent users for the specified login method.

Syntax

aaa session-limit { **ftp** | **http** | **https** | **ssh** | **telnet** } *max-sessions*

undo aaa session-limit { **ftp** | **http** | **https** | **ssh** | **telnet** }

Default

The maximum number of concurrent users is 32 for each user type.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ftp: FTP users.

http: HTTP users.

https: HTTPS users.

ssh: SSH users.

telnet: Telnet users.

max-sessions: Specifies the maximum number of concurrent login users. The value range is 1 to 64 for HTTP and HTTPS services, is 1 to 32 for SSH and Telnet services, and is 1 to 64 for FTP service.

Usage guidelines

After the maximum number of concurrent login users for a user type exceeds the upper limit, the system denies the subsequent users of this type.

For HTTP and HTTPS services, the number of concurrent users of an application is separately limited. For example, if the maximum number of concurrent HTTP users is 20, a maximum of 20 concurrent users are allowed for each HTTP-based application, such as RESTful, Web, and NETCONF.

Examples

Set the maximum number of concurrent FTP users to 4.

```
<Sysname> system-view
[Sysname] aaa session-limit ftp 4
```

accounting advpn

Use **accounting advpn** to specify accounting methods for ADVPN users.

Use **undo accounting advpn** to restore the default.

Syntax

accounting advpn { **local** [**radius-scheme** *radius-scheme-name*] [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo accounting advpn

Default

The default accounting methods of the ISP domain are used for ADVPN users.

Views

ISP domain view

Predefined user roles

network-admin

context-admin

Parameters

local: Performs local accounting.

none: Does not perform accounting.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

You can specify one primary accounting method and multiple backup accounting methods.

When the primary method is invalid, the device attempts to use the backup methods in sequence. For example, the **accounting advpn radius-scheme** *radius-scheme-name* **local none** command specifies a primary RADIUS accounting method and two backup methods (local accounting and no accounting). The device performs RADIUS accounting by default and performs local accounting when the RADIUS server is invalid. The device does not perform accounting when both of the previous methods are invalid.

The remote accounting method is invalid in the following situations:

- The specified accounting scheme does not exist.
- Accounting packet sending fails.
- The device does not receive any accounting response packets from an accounting server.

The local accounting method is invalid if the device fails to find the matching local user configuration.

When the primary accounting method is local, the following rules apply to the accounting of a user:

- The device uses the backup accounting methods in sequence only if local accounting is invalid for one of the following reasons:
  - An exception occurs in the local accounting process.
  - The user account is not configured on the device or the user is not allowed to use the ADVPN service.
- The device does not turn to the backup accounting methods if local accounting is invalid because of any other reason. Accounting fails for the user.

Examples

In ISP domain **test**, perform local accounting for ADVPN users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting advpn local
```

In ISP domain **test**, perform RADIUS accounting for ADVPN users based on scheme **rd** and use local accounting as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting advpn radius-scheme rd local
```

Related commands

accounting default

local-user

radius scheme

accounting command

Use **accounting command** to specify the command line accounting method.

Use **undo accounting command** to restore the default.

Syntax

accounting command hwtacacs-scheme *hwtacacs-scheme-name*

undo accounting command

Default

The default accounting methods of the ISP domain are used for command line accounting.

Views

ISP domain view

Predefined user roles

network-admin

context-admin

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

The command line accounting feature works with the accounting server to record valid commands that have been successfully executed on the device.

- When the command line authorization feature is disabled, the accounting server records all valid commands that have been successfully executed.
- When the command line authorization feature is enabled, the accounting server records only authorized commands that have been successfully executed.

Command line accounting can use only a remote HWTACACS server.

Examples

In ISP domain **test**, perform command line accounting based on HWTACACS scheme **hwtac**.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting command hwtacacs-scheme hwtac
```

Related commands

accounting default

command accounting (*Fundamentals Command Reference*)

hwtacacs scheme

accounting default

Use **accounting default** to specify default accounting methods for an ISP domain.

Use **undo accounting default** to restore the default.

Syntax

accounting default { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] [**none**] | **local** [**radius-scheme** *radius-scheme-name* | **hwtacacs-scheme** *hwtacacs-scheme-name*] * [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] [**none**] }

undo accounting default

Default

The default accounting method of an ISP domain is local.

Views

ISP domain view

Predefined user roles

network-admin

context-admin

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters.

local: Performs local accounting.

none: Does not perform accounting.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

The default accounting method is used for all users that support this method and do not have an accounting method configured.

Local accounting is only used for monitoring and controlling the number of local user connections. It does not provide the statistics function that the accounting feature generally provides.

You can specify one primary default accounting method and multiple backup default accounting methods.

When the primary method is invalid, the device attempts to use the backup methods in sequence. For example, the **accounting default radius-scheme** *radius-scheme-name* **local none** command specifies the primary default RADIUS accounting method and two backup methods (local accounting and no accounting). The device performs RADIUS accounting by default and performs local accounting when the RADIUS server is invalid. The device does not perform accounting when both of the previous methods are invalid.

The remote accounting method is invalid in the following situations:

- The specified accounting scheme does not exist.
- Accounting packet sending fails.
- The device does not receive any accounting response packets from an accounting server.

The local accounting method is invalid if the device fails to find the matching local user configuration.

When the primary accounting method is local, the following rules apply to the accounting of a user:

- The device uses the backup accounting methods in sequence only if local accounting is invalid for one of the following reasons:
  - An exception occurs in the local accounting process.
  - The user account is not configured on the device or the user is not allowed to use the access service.
- The device does not turn to the backup accounting methods if local accounting is invalid because of any other reason. Accounting fails for the user.

Examples

In ISP domain **test**, use RADIUS scheme **rd** as the primary default accounting method and use local accounting as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting default radius-scheme rd local
```

Related commands

hwtacacs scheme

local-user

radius scheme

accounting ipoe

Use **accounting ipoe** to specify accounting methods for IPoE users.

Use **undo accounting ipoe** to restore the default.

Syntax

accounting ipoe { **broadcast radius-scheme** *radius-scheme-name1* **radius-scheme** *radius-scheme-name2* [**local**] [**none**] | **local** [**radius-scheme** *radius-scheme-name*] [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo accounting ipoe

Default

The default accounting methods of the ISP domain are used for IPoE users.

Views

ISP domain view

Predefined user roles

network-admin

context-admin

Parameters

broadcast: Broadcasts accounting requests to servers in RADIUS schemes.

radius-scheme *radius-scheme-name1*: Specifies the primary broadcast RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

radius-scheme *radius-scheme-name2*: Specifies the backup broadcast RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

local: Performs local accounting.

none: Does not perform accounting.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

You can specify one primary accounting method and multiple backup accounting methods.

When the primary method is invalid, the device attempts to use the backup methods in sequence. For example, the **accounting ipoe radius-scheme** *radius-scheme-name* **local none** command specifies a primary RADIUS accounting method and two backup methods (local accounting and no accounting). The device performs RADIUS accounting by default and performs local accounting when the RADIUS server is invalid. The device does not perform accounting when both of the previous methods are invalid.

The remote accounting method is invalid in the following situations:

- The specified accounting scheme does not exist.
- Accounting packet sending fails.

- The device does not receive any accounting response packets from an accounting server.

The local accounting method is invalid if the device fails to find the matching local user configuration.

The following guidelines apply to broadcast accounting:

- The device sends accounting requests to the primary accounting servers in the specified broadcast RADIUS schemes at the real-time accounting interval set in the primary broadcast RADIUS scheme. If the primary server is unavailable in a scheme, the device sends accounting requests to the secondary servers of the scheme in the order the servers are configured.
- The accounting result is determined by the primary broadcast RADIUS scheme. The accounting result from the backup scheme is used as reference only. If the primary scheme does not return any result, the device considers the accounting as a failure.

When the primary accounting method is local, the following rules apply to the accounting of a user:

- The device uses the backup accounting methods in sequence only if local accounting is invalid for one of the following reasons:
  - An exception occurs in the local accounting process.
  - The user account is not configured on the device or the user is not allowed to use the IPoE service.
- The device does not turn to the backup accounting methods if local accounting is invalid because of any other reason. Accounting fails for the user.

Examples

In ISP domain **test**, perform local accounting for IPoE users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting ipoe local
```

In ISP domain **test**, perform RADIUS accounting for IPoE users based on scheme **rd** and use local accounting as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting ipoe radius-scheme rd local
```

In ISP domain **test**, broadcast accounting requests of IPoE users to RADIUS servers in schemes **rd1** and **rd2**, and use local accounting as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting ipoe broadcast radius-scheme rd1 radius-scheme rd2 local
```

Related commands

accounting default

local-user

radius scheme

timer realtime-accounting

accounting lan-access

Use **accounting lan-access** to specify accounting methods for LAN users.

Use **undo accounting lan-access** to restore the default.

Syntax

accounting lan-access { **broadcast radius-scheme** *radius-scheme-name1* **radius-scheme** *radius-scheme-name2* [**local**] [**none**] | **local** [**radius-scheme** *radius-scheme-name*] [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo accounting lan-access

Default

The default accounting methods of the ISP domain are used for LAN users.

Views

ISP domain view

Predefined user roles

network-admin

context-admin

Parameters

broadcast: Broadcasts accounting requests to servers in RADIUS schemes.

radius-scheme *radius-scheme-name1*: Specifies the primary broadcast RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

radius-scheme *radius-scheme-name2*: Specifies the backup broadcast RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

local: Performs local accounting.

none: Does not perform accounting.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

You can specify one primary accounting method and multiple backup accounting methods.

When the primary method is invalid, the device attempts to use the backup methods in sequence. For example, the **accounting lan-access radius-scheme** *radius-scheme-name* **local none** command specifies a primary RADIUS accounting method and two backup methods (local accounting and no accounting). The device performs RADIUS accounting by default and performs local accounting when the RADIUS server is invalid. The device does not perform accounting when both of the previous methods are invalid.

The remote accounting method is invalid in the following situations:

- The specified accounting scheme does not exist.
- Accounting packet sending fails.
- The device does not receive any accounting response packets from an accounting server.

The local accounting method is invalid if the device fails to find the matching local user configuration.

The following guidelines apply to broadcast accounting:

- The device sends accounting requests to the primary accounting servers in the specified broadcast RADIUS schemes at the real-time accounting interval set in the primary broadcast RADIUS scheme. If the primary server is unavailable in a scheme, the device sends accounting requests to the secondary servers of the scheme in the order the servers are configured.
- The accounting result is determined by the primary broadcast RADIUS scheme. The accounting result from the backup scheme is used as reference only. If the primary scheme does not return any result, the device considers the accounting as a failure.

When the primary accounting method is local, the following rules apply to the accounting of a user:

- The device uses the backup accounting methods in sequence only if local accounting is invalid for one of the following reasons:
  - An exception occurs in the local accounting process.
  - The user account is not configured on the device or the user is not allowed to use the LAN access service.
- The device does not turn to the backup accounting methods if local accounting is invalid because of any other reason. Accounting fails for the user.

Examples

In ISP domain **test**, perform local accounting for LAN users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting lan-access local
```

In ISP domain **test**, perform RADIUS accounting for LAN users based on scheme **rd** and use local accounting as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting lan-access radius-scheme rd local
```

In ISP domain **test**, broadcast accounting requests of LAN users to RADIUS servers in schemes **rd1** and **rd2**, and use local accounting as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting lan-access broadcast radius-scheme rd1 radius-scheme rd2
local
```

Related commands

accounting default

local-user

radius scheme

timer realtime-accounting

accounting login

Use **accounting login** to specify accounting methods for login users.

Use **undo accounting login** to restore the default.

Syntax

accounting login { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] [**none**] | **local** [**radius-scheme** *radius-scheme-name* | **hwtacacs-scheme** *hwtacacs-scheme-name*] * [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] [**none**] }

undo accounting login

Default

The default accounting methods of the ISP domain are used for login users.

Views

ISP domain view

Predefined user roles

network-admin

context-admin

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters.

local: Performs local accounting.

none: Does not perform accounting.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

Accounting is not supported for FTP, SFTP, and SCP users.

You can specify one primary accounting method and multiple backup accounting methods.

When the primary method is invalid, the device attempts to use the backup methods in sequence. For example, the **accounting login radius-scheme** *radius-scheme-name* **local none** command specifies a primary default RADIUS accounting method and two backup methods (local accounting and no accounting). The device performs RADIUS accounting by default and performs local accounting when the RADIUS server is invalid. The device does not perform accounting when both of the previous methods are invalid.

The remote accounting method is invalid in the following situations:

- The specified accounting scheme does not exist.
- Accounting packet sending fails.
- The device does not receive any accounting response packets from an accounting server.

The local accounting method is invalid if the device fails to find the matching local user configuration.

When the primary accounting method is local, the following rules apply to the accounting of a user:

- The device uses the backup accounting methods in sequence only if local accounting is invalid for one of the following reasons:
  - An exception occurs in the local accounting process.
  - The user account is not configured on the device.
- The device does not turn to the backup accounting methods if local accounting is invalid because of any other reason. Accounting fails for the user.

Examples

In ISP domain **test**, perform local accounting for login users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting login local
```

In ISP domain **test**, perform RADIUS accounting for login users based on scheme **rd** and use local accounting as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting login radius-scheme rd local
```

Related commands

accounting default

hwtacacs scheme

local-user

radius scheme

accounting portal

Use **accounting portal** to specify accounting methods for portal users.

Use **undo accounting portal** to restore the default.

Syntax

accounting portal { **broadcast radius-scheme** *radius-scheme-name1* **radius-scheme** *radius-scheme-name2* [**local**] [**none**] | **local** [**radius-scheme** *radius-scheme-name*] [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo accounting portal

Default

The default accounting methods of the ISP domain are used for portal users.

Views

ISP domain view

Predefined user roles

network-admin

context-admin

Parameters

broadcast: Broadcasts accounting requests to servers in RADIUS schemes.

radius-scheme *radius-scheme-name1*: Specifies the primary broadcast RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

radius-scheme *radius-scheme-name2*: Specifies the backup broadcast RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

local: Performs local accounting.

none: Does not perform accounting.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

You can specify one primary accounting method and multiple backup accounting methods.

When the primary method is invalid, the device attempts to use the backup methods in sequence. For example, the **accounting portal radius-scheme** *radius-scheme-name* **local none** command specifies a primary default RADIUS accounting method and two backup methods (local accounting and no accounting). The device performs RADIUS accounting by default and performs local accounting when the RADIUS server is invalid. The device does not perform accounting when both of the previous methods are invalid.

The remote accounting method is invalid in the following situations:

- The specified accounting scheme does not exist.
- Accounting packet sending fails.
- The device does not receive any accounting response packets from an accounting server.

The local accounting method is invalid if the device fails to find the matching local user configuration.

The following guidelines apply to broadcast accounting:

- The device sends accounting requests to the primary accounting servers in the specified broadcast RADIUS schemes at the real-time accounting interval set in the primary broadcast RADIUS scheme. If the primary server is unavailable in a scheme, the device sends accounting requests to the secondary servers of the scheme in the order the servers are configured.
- The accounting result is determined by the primary broadcast RADIUS scheme. The accounting result from the backup scheme is used as reference only. If the primary scheme does not return any result, the device considers the accounting as a failure.

When the primary accounting method is local, the following rules apply to the accounting of a user:

- The device uses the backup accounting methods in sequence only if local accounting is invalid for one of the following reasons:
  - An exception occurs in the local accounting process.
  - The user account is not configured on the device or the user is not allowed to use the portal service.
- The device does not turn to the backup accounting methods if local accounting is invalid because of any other reason. Accounting fails for the user.

Examples

In ISP domain **test**, perform local accounting for portal users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting portal local
```

In ISP domain **test**, perform RADIUS accounting for portal users based on scheme **rd** and use local accounting as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting portal radius-scheme rd local
```

In ISP domain **test**, broadcast accounting requests of portal users to RADIUS servers in schemes **rd1** and **rd2**, and use local accounting as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting portal broadcast radius-scheme rd1 radius-scheme rd2 local
```

Related commands

accounting default

local-user

radius scheme

timer realtime-accounting

accounting ppp

Use **accounting ppp** to specify accounting methods for PPP users.

Use **undo accounting ppp** to restore the default.

Syntax

accounting ppp { **broadcast radius-scheme** *radius-scheme-name1* **radius-scheme** *radius-scheme-name2* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] [**none**] | **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] [**none**]

| **local** [**radius-scheme** *radius-scheme-name* | **hwtacacs-scheme** *hwtacacs-scheme-name*] * [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] [**none**] }

undo accounting ppp

Default

The default accounting methods of the ISP domain are used for PPP users.

Views

ISP domain view

Predefined user roles

network-admin

context-admin

Parameters

broadcast: Broadcasts accounting requests to servers in RADIUS schemes.

radius-scheme *radius-scheme-name1*: Specifies the primary broadcast RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

radius-scheme *radius-scheme-name2*: Specifies the backup broadcast RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters.

local: Performs local accounting.

none: Does not perform accounting.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

You can specify one primary accounting method and multiple backup accounting methods.

When the primary method is invalid, the device attempts to use the backup methods in sequence. For example, the **accounting ppp radius-scheme** *radius-scheme-name* **local none** command specifies a primary RADIUS accounting method and two backup methods (local accounting and no accounting). The device performs RADIUS accounting by default and performs local accounting when the RADIUS server is invalid. The device does not perform accounting when both of the previous methods are invalid.

The remote accounting method is invalid in the following situations:

- The specified accounting scheme does not exist.
- Accounting packet sending fails.
- The device does not receive any accounting response packets from an accounting server.

The local accounting method is invalid if the device fails to find the matching local user configuration.

The following guidelines apply to broadcast accounting:

- The device sends accounting requests to the primary accounting servers in the specified broadcast RADIUS schemes at the real-time accounting interval set in the primary broadcast RADIUS scheme. If the primary server is unavailable for a scheme, the device sends accounting requests to the secondary servers of the scheme in the order the servers are configured.

- The accounting result is determined by the primary broadcast RADIUS scheme. The accounting result from the backup scheme is used as reference only. If the primary scheme does not return any result, the device considers the accounting as a failure.

When the primary accounting method is local, the following rules apply to the accounting of a user:

- The device uses the backup accounting methods in sequence only if local accounting is invalid for one of the following reasons:
  - An exception occurs in the local accounting process.
  - The user account is not configured on the device or the user is not allowed to use the PPP service.
- The device does not turn to the backup accounting methods if local accounting is invalid because of any other reason. Accounting fails for the user.

Examples

In ISP domain **test**, perform local accounting for PPP users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting ppp local
```

In ISP domain **test**, perform RADIUS accounting for PPP users based on scheme **rd** and use local accounting as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting ppp radius-scheme rd local
```

In ISP domain **test**, broadcast accounting requests of PPP users to RADIUS servers in schemes **rd1** and **rd2**, and use local accounting as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting ppp broadcast radius-scheme rd1 radius-scheme rd2 local
```

Related commands

accounting default

hwtacacs scheme

local-user

radius scheme

timer realtime-accounting

accounting quota-out

Use **accounting quota-out** to configure access control for users that have used up their data or time accounting quotas.

Use **undo accounting quota-out** to restore the default.

Syntax

accounting quota-out { **offline** | **online** }

undo accounting quota-out

Default

The device logs off users that have used up their accounting quotas.

Views

ISP domain view

Predefined user roles

network-admin

context-admin

Parameters

offline: Logs off users that have used up their accounting quotas.

online: Allows users that have used up their accounting quotas to stay online.

Examples

In ISP domain **test**, configure the device to allow users that have used up their accounting quotas to stay online.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting quota-out online
```

accounting sslvpn

Use **accounting sslvpn** to specify accounting methods for SSL VPN users.

Use **undo accounting sslvpn** to restore the default.

Syntax

accounting sslvpn { **local** [**radius-scheme** *radius-scheme-name*] [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo accounting sslvpn

Default

The default accounting methods of the ISP domain are used for SSL VPN users.

Views

ISP domain view

Predefined user roles

network-admin

context-admin

Parameters

local: Performs local accounting.

none: Does not perform accounting.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

You can specify one primary accounting method and multiple backup accounting methods.

When the primary method is invalid, the device attempts to use the backup methods in sequence. For example, the **accounting sslvpn radius-scheme** *radius-scheme-name* **local none** command specifies a primary RADIUS accounting method and two backup methods (local accounting and no accounting). The device performs RADIUS accounting by default and performs

local accounting when the RADIUS server is invalid. The device does not perform accounting when both of the previous methods are invalid.

The remote accounting method is invalid in the following situations:

- The specified accounting scheme does not exist.
- Accounting packet sending fails.
- The device does not receive any accounting response packets from an accounting server.

The local accounting method is invalid if the device fails to find the matching local user configuration.

When the primary accounting method is local, the following rules apply to the accounting of a user:

- The device uses the backup accounting methods in sequence only if local accounting is invalid for one of the following reasons:
  - An exception occurs in the local accounting process.
  - The user account is not configured on the device or the user is not allowed to use the SSL VPN service.
- The device does not turn to the backup accounting methods if local accounting is invalid because of any other reason. Accounting fails for the user.

Examples

In ISP domain **test**, perform local accounting for SSL VPN users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting sslvpn local
```

In ISP domain **test**, perform RADIUS accounting for SSL VPN users based on scheme **rd** and use local accounting as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting sslvpn radius-scheme rd local
```

Related commands

accounting default

local-user

radius scheme

accounting start-fail

Use **accounting start-fail** to configure access control for users that encounter accounting-start failures.

Use **undo accounting start-fail** to restore the default.

Syntax

accounting start-fail { **offline** | **online** }

undo accounting start-fail

Default

The device allows users that encounter accounting-start failures to stay online.

Views

ISP domain view

Predefined user roles

network-admin

context-admin

Parameters

offline: Logs off users that encounter accounting-start failures.

online: Allows users that encounter accounting-start failures to stay online.

Examples

In ISP domain **test**, configure the device to allow users that encounter accounting-start failures to stay online.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting start-fail online
```

accounting update-fail

Use **accounting update-fail** to configure access control for users that have failed all their accounting-update attempts.

Use **undo accounting update-fail** to restore the default.

Syntax

accounting update-fail { [**max-times** *max-times*] **offline** | **online** }

undo accounting update-fail

Default

The device allows users that have failed all their accounting-update attempts to stay online.

Views

ISP domain view

Predefined user roles

network-admin

context-admin

Parameters

max-times *max-times*: Specifies the maximum number of consecutive accounting-update failures allowed by the device for each user. The value range for the *times* argument is 1 to 255, and the default value is 1.

offline: Logs off users that have failed all their accounting-update attempts.

online: Allows users that have failed all their accounting-update attempts to stay online.

Examples

In ISP domain **test**, configure the device to allow users that have failed all their accounting-update attempts to stay online.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting update-fail online
```

authentication advpn

Use **authentication advpn** to specify authentication methods for ADVPN users.

Use **undo authentication advpn** to restore the default.

Syntax

authentication advpn { **local** [**radius-scheme** *radius-scheme-name*] [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authentication advpn

Default

The default authentication methods of the ISP domain are used for ADVPN users.

Views

ISP domain view

Predefined user roles

network-admin

context-admin

Parameters

local: Performs local authentication.

none: Does not perform authentication.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

You can specify one primary authentication method and multiple backup authentication methods.

When the primary method is invalid, the device attempts to use the backup methods in sequence. For example, the **authentication advpn radius-scheme** *radius-scheme-name* **local none** command specifies a primary RADIUS authentication method and two backup methods (local authentication and no authentication). The device performs RADIUS authentication by default and performs local authentication when the RADIUS server is invalid. The device does not perform authentication when both of the previous methods are invalid.

The remote authentication method is invalid in the following situations:

- The specified authentication scheme does not exist.
- Authentication packet sending fails.
- The device does not receive any authentication response packets from an authentication server.

The local authentication method is invalid if the device fails to find the matching local user configuration.

When the primary authentication method is local, the following rules apply to the authentication of a user:

- The device uses the backup authentication methods in sequence only if local authentication is invalid for one of the following reasons:
  - An exception occurs in the local authentication process.
  - The user account is not configured on the device or the user is not allowed to use the ADVPN service.

- The device does not turn to the backup authentication methods if local authentication is invalid because of any other reason. Authentication fails for the user.

Examples

In ISP domain **test**, perform local authentication for ADVPN users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication advpn local
```

In ISP domain **test**, perform RADIUS authentication for ADVPN users based on scheme **rd** and use local authentication as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication advpn radius-scheme rd local
```

Related commands

authentication default

local-user

radius scheme

authentication default

Use **authentication default** to specify default authentication methods for an ISP domain.

Use **undo authentication default** to restore the default.

Syntax

authentication default { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] [**none**] | **ldap-scheme** *ldap-scheme-name* [**local**] [**none**] | **local** [**radius-scheme** *radius-scheme-name* | **hwtacacs-scheme** *hwtacacs-scheme-name*] * [**none**] | **local** [**ldap-scheme** *ldap-scheme-name*] [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] [**none**] }

undo authentication default

Default

The default authentication method of an ISP domain is local.

Views

ISP domain view

Predefined user roles

network-admin

context-admin

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters.

ldap-scheme *ldap-scheme-name*: Specifies an LDAP scheme by its name, a case-insensitive string of 1 to 32 characters.

local: Performs local authentication.

none: Does not perform authentication.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

The default authentication method is used for all users that support this method and do not have an authentication method configured.

You can specify one primary default authentication method and multiple backup default authentication methods.

When the primary method is invalid, the device attempts to use the backup methods in sequence. For example, the **authentication default radius-scheme** *radius-scheme-name* **local none** command specifies a primary default RADIUS authentication method and two backup methods (local authentication and no authentication). The device performs RADIUS authentication by default and performs local authentication when the RADIUS server is invalid. The device does not perform authentication when both of the previous methods are invalid.

The remote authentication method is invalid in the following situations:

- The specified authentication scheme does not exist.
- Authentication packet sending fails.
- The device does not receive any authentication response packets from an authentication server.

The local authentication method is invalid if the device fails to find the matching local user configuration.

When the primary authentication method is local, the following rules apply to the authentication of a user:

- The device uses the backup authentication methods in sequence only if local authentication is invalid for one of the following reasons:
  - An exception occurs in the local authentication process.
  - The user account is not configured on the device or the user is not allowed to use the access service.
- The device does not turn to the backup authentication methods if local authentication is invalid because of any other reason. Authentication fails for the user.

Examples

In ISP domain **test**, use RADIUS scheme **rd** as the primary default authentication method and use local authentication as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication default radius-scheme rd local
```

Related commands

hwtacacs scheme

ldap scheme

local-user

radius scheme

authentication ike

Use **authentication ike** to specify extended authentication methods for IKE users.

Use **undo authentication ike** to restore the default.

Syntax

authentication ike { **local** [**radius-scheme** *radius-scheme-name*] [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authentication ike

Default

The default authentication methods of the ISP domain are used for IKE extended authentication.

Views

ISP domain view

Predefined user roles

network-admin

context-admin

Parameters

local: Performs local authentication.

none: Does not perform authentication.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

You can specify one primary authentication method and multiple backup authentication methods.

When the primary method is invalid, the device attempts to use the backup methods in sequence. For example, the **authentication ike radius-scheme** *radius-scheme-name* **local none** command specifies a primary RADIUS authentication method and two backup methods (local authentication and no authentication). The device performs RADIUS authentication by default and performs local authentication when the RADIUS server is invalid. The device does not perform authentication when both of the previous methods are invalid.

The remote authentication method is invalid in the following situations:

- The specified authentication scheme does not exist.
- Authentication packet sending fails.
- The device does not receive any authentication response packets from an authentication server.

The local authentication method is invalid if the device fails to find the matching local user configuration.

When the primary authentication method is local, the following rules apply to the authentication of a user:

- The device uses the backup authentication methods in sequence only if local authentication is invalid for one of the following reasons:
  - An exception occurs in the local authentication process.
  - The user account is not configured on the device or the user is not allowed to use the IKE service.
- The device does not turn to the backup authentication methods if local authentication is invalid because of any other reason. Authentication fails for the user.

Examples

In ISP domain **test**, configure the device to perform local authentication through IKE extended authentication.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication ike local
```

In ISP domain **test**, perform IKE extended authentication based on RADIUS scheme **rd** and use local authentication as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication ike radius-scheme rd local
```

Related commands

authentication default

local-user

radius scheme

authentication ipoe

Use **authentication ipoe** to specify authentication methods for IPoE users.

Use **undo authentication ipoe** to restore the default.

Syntax

authentication ipoe { **local** [**radius-scheme** *radius-scheme-name*] [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authentication ipoe

Default

The default authentication methods of the ISP domain are used for IPoE users.

Views

ISP domain view

Predefined user roles

network-admin

context-admin

Parameters

local: Performs local authentication.

none: Does not perform authentication.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

You can specify one primary authentication method and multiple backup authentication methods.

When the primary method is invalid, the device attempts to use the backup methods in sequence. For example, the **authentication ipoe radius-scheme** *radius-scheme-name* **local none** command specifies a primary RADIUS authentication method and two backup methods (local authentication and no authentication). The device performs RADIUS authentication by default and performs local authentication when the RADIUS server is invalid. The device does not perform authentication when both of the previous methods are invalid.

The remote authentication method is invalid in the following situations:

- The specified authentication scheme does not exist.

- Authentication packet sending fails.
- The device does not receive any authentication response packets from an authentication server.

The local authentication method is invalid if the device fails to find the matching local user configuration.

When the primary authentication method is local, the following rules apply to the authentication of a user:

- The device uses the backup authentication methods in sequence only if local authentication is invalid for one of the following reasons:
  - An exception occurs in the local authentication process.
  - The user account is not configured on the device or the user is not allowed to use the IPoE service.
- The device does not turn to the backup authentication methods if local authentication is invalid because of any other reason. Authentication fails for the user.

Examples

In ISP domain **test**, perform local authentication for IPoE users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication ipoe local
```

In ISP domain **test**, perform RADIUS authentication for IPoE users based on scheme **rd** and use local authentication as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication ipoe radius-scheme rd local
```

Related commands

authentication default

local-user

radius scheme

authentication lan-access

Use **authentication lan-access** to specify authentication methods for LAN users.

Use **undo authentication lan-access** to restore the default.

Syntax

authentication lan-access { **ldap-scheme** *ldap-scheme-name* [**local**] [**none**] | **local** [**ldap-scheme** *ldap-scheme-name* | **radius-scheme** *radius-scheme-name*] [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authentication lan-access

Default

The default authentication methods of the ISP domain are used for LAN users.

Views

ISP domain view

Predefined user roles

network-admin

context-admin

Parameters

ldap-scheme *ldap-scheme-name*: Specifies an LDAP scheme by its name, a case-insensitive string of 1 to 32 characters.

local: Performs local authentication.

none: Does not perform authentication.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

You can specify one primary authentication method and multiple backup authentication methods.

When the primary method is invalid, the device attempts to use the backup methods in sequence. For example, the **authentication lan-access radius-scheme** *radius-scheme-name* **local none** command specifies a primary RADIUS authentication method and two backup methods (local authentication and no authentication). The device performs RADIUS authentication by default and performs local authentication when the RADIUS server is invalid. The device does not perform authentication when both of the previous methods are invalid.

The remote authentication method is invalid in the following situations:

- The specified authentication scheme does not exist.
- Authentication packet sending fails.
- The device does not receive any authentication response packets from an authentication server.

The local authentication method is invalid if the device fails to find the matching local user configuration.

When the primary authentication method is local, the following rules apply to the authentication of a user:

- The device uses the backup authentication methods in sequence only if local authentication is invalid for one of the following reasons:
  - An exception occurs in the local authentication process.
  - The user account is not configured on the device or the user is not allowed to use the LAN access service.
- The device does not turn to the backup authentication methods if local authentication is invalid because of any other reason. Authentication fails for the user.

Examples

In ISP domain **test**, perform local authentication for LAN users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication lan-access local
```

In ISP domain **test**, perform RADIUS authentication for LAN users based on scheme **rd** and use local authentication as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication lan-access radius-scheme rd local
```

Related commands

authentication default

ldap scheme

local-user

radius scheme

authentication login

Use **authentication login** to specify authentication methods for login users.

Use **undo authentication login** to restore the default.

Syntax

authentication login { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] [**none**] | **ldap-scheme** *ldap-scheme-name* [**local**] [**none**] | **local** [**radius-scheme** *radius-scheme-name* | **hwtacacs-scheme** *hwtacacs-scheme-name*] * [**none**] | **local** [**ldap-scheme** *ldap-scheme-name*] [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] [**none**] }

undo authentication login

Default

The default authentication methods of the ISP domain are used for login users.

Views

ISP domain view

Predefined user roles

network-admin

context-admin

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters.

ldap-scheme *ldap-scheme-name*: Specifies an LDAP scheme by its name, a case-insensitive string of 1 to 32 characters.

local: Performs local authentication.

none: Does not perform authentication.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

You can specify one primary authentication method and multiple backup authentication methods.

When the primary method is invalid, the device attempts to use the backup methods in sequence. For example, the **authentication login radius-scheme** *radius-scheme-name* **local none** command specifies the default primary RADIUS authentication method and two backup methods (local authentication and no authentication). The device performs RADIUS authentication by default and performs local authentication when the RADIUS server is invalid. The device does not perform authentication when both of the previous methods are invalid.

The remote authentication method is invalid in the following situations:

- The specified authentication scheme does not exist.
- Authentication packet sending fails.
- The device does not receive any authentication response packets from an authentication server.

The local authentication method is invalid if the device fails to find the matching local user configuration.

When the primary authentication method is local, the following rules apply to the authentication of a user:

- The device uses the backup authentication methods in sequence only if local authentication is invalid for one of the following reasons:
  - An exception occurs in the local authentication process.
  - The user account is not configured on the device or the user is not allowed to use the service for accessing the device.
- The device does not turn to the backup authentication methods if local authentication is invalid because of any other reason. Authentication fails for the user.

Examples

In ISP domain **test**, perform local authentication for login users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication login local
```

In ISP domain **test**, perform RADIUS authentication for login users based on scheme **rd** and use local authentication as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication login radius-scheme rd local
```

Related commands

authentication default

hwtacacs scheme

ldap scheme

local-user

radius scheme

authentication portal

Use **authentication portal** to specify authentication methods for portal users.

Use **undo authentication portal** to restore the default.

Syntax

authentication portal { **ldap-scheme** *ldap-scheme-name* [**local**] [**none**] | **local** [**ldap-scheme** *ldap-scheme-name* | **radius-scheme** *radius-scheme-name*] [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authentication portal

Default

The default authentication methods of the ISP domain are used for portal users.

Views

ISP domain view

Predefined user roles

network-admin

context-admin

Parameters

ldap-scheme *ldap-scheme-name*: Specifies an LDAP scheme by its name, a case-insensitive string of 1 to 32 characters.

local: Performs local authentication.

none: Does not perform authentication.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

You can specify one primary authentication method and multiple backup authentication methods.

When the primary method is invalid, the device attempts to use the backup methods in sequence. For example, the **authentication portal radius-scheme** *radius-scheme-name* **local none** command specifies the default primary RADIUS authentication method and two backup methods (local authentication and no authentication). The device performs RADIUS authentication by default and performs local authentication when the RADIUS server is invalid. The device does not perform authentication when both of the previous methods are invalid.

The remote authentication method is invalid in the following situations:

- The specified authentication scheme does not exist.
- Authentication packet sending fails.
- The device does not receive any authentication response packets from an authentication server.

The local authentication method is invalid if the device fails to find the matching local user configuration.

When the primary authentication method is local, the following rules apply to the authentication of a user:

- The device uses the backup authentication methods in sequence only if local authentication is invalid for one of the following reasons:
  - An exception occurs in the local authentication process.
  - The user account is not configured on the device or the user is not allowed to use the portal service.
- The device does not turn to the backup authentication methods if local authentication is invalid because of any other reason. Authentication fails for the user.

Examples

In ISP domain **test**, perform local authentication for portal users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication portal local
```

In ISP domain **test**, perform RADIUS authentication for portal users based on scheme **rd** and use local authentication as the backup.

```
<Sysname> system-view
[Sysname] domain test
```

```
[Sysname-isp-test] authentication portal radius-scheme rd local
```

Related commands

authentication default

ldap scheme

local-user

radius scheme

authentication ppp

Use **authentication ppp** to specify authentication methods for PPP users.

Use **undo authentication ppp** to restore the default.

Syntax

authentication ppp { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] [**none**] | **ldap-scheme** *ldap-scheme-name* [**local**] [**none**] | **local** [**radius-scheme** *radius-scheme-name* | **hwtacacs-scheme** *hwtacacs-scheme-name*] * [**none**] | **local** [**ldap-scheme** *ldap-scheme-name*] [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] [**none**] }

undo authentication ppp

Default

The default authentication methods of the ISP domain are used for PPP users.

Views

ISP domain view

Predefined user roles

network-admin

context-admin

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters.

ldap-scheme *ldap-scheme-name*: Specifies an LDAP scheme by its name, a case-insensitive string of 1 to 32 characters.

local: Performs local authentication.

none: Does not perform authentication.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

You can specify one primary authentication method and multiple backup authentication methods.

When the primary method is invalid, the device attempts to use the backup methods in sequence. For example, the **authentication ppp radius-scheme** *radius-scheme-name* **local none** command specifies a primary RADIUS authentication method and two backup methods (local authentication and no authentication). The device performs RADIUS authentication by default and performs local authentication when the RADIUS server is invalid. The device does not perform authentication when both of the previous methods are invalid.

The remote authentication method is invalid in the following situations:

- The specified authentication scheme does not exist.
- Authentication packet sending fails.
- The device does not receive any authentication response packets from an authentication server.

The local authentication method is invalid if the device fails to find the matching local user configuration.

When the primary authentication method is local, the following rules apply to the authentication of a user:

- The device uses the backup authentication methods in sequence only if local authentication is invalid for one of the following reasons:
  - An exception occurs in the local authentication process.
  - The user account is not configured on the device or the user is not allowed to use the PPP service.
- The device does not turn to the backup authentication methods if local authentication is invalid because of any other reason. Authentication fails for the user.

Examples

In ISP domain **test**, perform local authentication for PPP users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication ppp local
```

In ISP domain **test**, perform RADIUS authentication for PPP users based on scheme **rd** and use local authentication as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication ppp radius-scheme rd local
```

Related commands

authentication default

hwtacacs scheme

ldap scheme

local-user

radius scheme

authentication sslvpn

Use **authentication sslvpn** to specify authentication methods for SSL VPN users.

Use **undo authentication sslvpn** to restore the default.

Syntax

authentication sslvpn { **ldap-scheme** *ldap-scheme-name* [**local**] [**none**] | **local** [**ldap-scheme** *ldap-scheme-name* | **radius-scheme** *radius-scheme-name*] [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authentication sslvpn

Default

The default authentication methods of the ISP domain are used for SSL VPN users.

Views

ISP domain view

Predefined user roles

network-admin

context-admin

Parameters

ldap-scheme *ldap-scheme-name*: Specifies an LDAP scheme by its name, a case-insensitive string of 1 to 32 characters.

local: Performs local authentication.

none: Does not perform authentication.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

You can specify one primary authentication method and multiple backup authentication methods.

When the primary method is invalid, the device attempts to use the backup methods in sequence. For example, the **authentication sslvpn radius-scheme** *radius-scheme-name* **local none** command specifies a primary RADIUS authentication method and two backup methods (local authentication and no authentication). The device performs RADIUS authentication by default and performs local authentication when the RADIUS server is invalid. The device does not perform authentication when both of the previous methods are invalid.

The remote authentication method is invalid in the following situations:

- The specified authentication scheme does not exist.
- Authentication packet sending fails.
- The device does not receive any authentication response packets from an authentication server.

The local authentication method is invalid if the device fails to find the matching local user configuration.

When the primary authentication method is local, the following rules apply to the authentication of a user:

- The device uses the backup authentication methods in sequence only if local authentication is invalid for one of the following reasons:
  - An exception occurs in the local authentication process.
  - The user account is not configured on the device or the user is not allowed to use the SSL VPN service.
- The device does not turn to the backup authentication methods if local authentication is invalid because of any other reason. Authentication fails for the user.

If you specify multiple authentication methods for SSL VPN users in an ISP domain, the device does not support the online user password change feature for the SSL VPN users.

If you specify an LDAP scheme for SSL VPN users in an ISP domain, the device does not support the online user password change feature for the SSL VPN users.

Examples

In ISP domain **test**, perform local authentication for SSL VPN users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication sslvpn local
```

In ISP domain **test**, perform LDAP authentication for SSL VPN users based on scheme **ldp** and use local authentication as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication sslvpn ldap-scheme ldp local
```

Related commands

authentication default

ldap scheme

local-user

radius scheme

authentication super

Use **authentication super** to specify a method for user role authentication.

Use **undo authentication super** to restore the default.

Syntax

authentication super { **hwtacacs-scheme** *hwtacacs-scheme-name* | **radius-scheme** *radius-scheme-name* } *

undo authentication super

Default

The default authentication methods of the ISP domain are used for user role authentication.

Views

ISP domain view

Predefined user roles

network-admin

context-admin

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

To enable a user to obtain another user role without reconnecting to the device, you must configure user role authentication. The device supports local and remote methods for user role authentication. For more information about user role authentication, see RBAC configuration in *Fundamentals Configuration Guide*.

You can specify one authentication method and one backup authentication method to use in case that the previous authentication method is invalid.

Examples

In ISP domain **test**, perform user role authentication based on HWTACACS scheme **tac**.

```
<Sysname> system-view
[Sysname] super authentication-mode scheme
[Sysname] domain test
```

```
[Sysname-isp-test] authentication super hwtacacs-scheme tac
```

Related commands

authentication default

hwtacacs scheme

radius scheme

authorization advpn

Use **authorization advpn** to specify authorization methods for ADVPN users.

Use **undo authorization advpn** to restore the default.

Syntax

authorization advpn { **local** [**radius-scheme** *radius-scheme-name*] [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authorization advpn

Default

The default authorization methods of the ISP domain are used for ADVPN users.

Views

ISP domain view

Predefined user roles

network-admin

context-admin

Parameters

local: Performs local authorization.

none: Does not perform authorization.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

The RADIUS authorization configuration takes effect only when authentication and authorization methods of the ISP domain use the same RADIUS scheme.

You can specify one primary authorization method and multiple backup authorization methods.

When the primary method is invalid, the device attempts to use the backup methods in sequence. For example, the **authorization advpn radius-scheme** *radius-scheme-name* **local none** command specifies a primary RADIUS authorization method and two backup methods (local authorization and no authorization). The device performs RADIUS authorization by default and performs local authorization when the RADIUS server is invalid. The device does not perform authorization when both of the previous methods are invalid.

The remote authorization method is invalid in the following situations:

- The specified authorization scheme does not exist.
- Authorization packet sending fails.
- The device does not receive any authorization response packets from an authorization server.

The local authorization method is invalid if the device fails to find the matching local user configuration.

When the primary authorization method is local, the following rules apply to the authorization of a user:

- The device uses the backup authorization methods in sequence only if local authorization is invalid for one of the following reasons:
  - An exception occurs in the local authorization process.
  - The user account is not configured on the device or the user is not allowed to use the ADVPN service.
- The device does not turn to the backup authorization methods if local authorization is invalid because of any other reason. Authorization fails for the user.

Examples

In ISP domain **test**, perform local authorization for ADVPN users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization advpn local
```

In ISP domain **test**, perform RADIUS authorization for ADVPN users based on scheme **rd** and use local authorization as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization advpn radius-scheme rd local
```

Related commands

authorization default

local-user

radius scheme

authorization command

Use **authorization command** to specify command authorization methods.

Use **undo authorization command** to restore the default.

Syntax

authorization command { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] [**none**] | **local** [**none**] | **none** }

undo authorization command

Default

The default authorization methods of the ISP domain are used for command authorization.

Views

ISP domain view

Predefined user roles

network-admin

context-admin

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters.

local: Performs local authorization.

none: Does not perform authorization. The authorization server does not verify whether the entered commands are permitted by the user role. The commands are executed successfully if the user role has permission to the commands.

Usage guidelines

Command authorization restricts login users to execute only authorized commands by employing an authorization server to verify whether each entered command is permitted.

When local command authorization is configured, the device compares each entered command with the user's configuration on the device. The command is executed only when it is permitted by the user's authorized user roles.

The commands that can be executed are controlled by both the access permission of user roles and command authorization of the authorization server. Access permission only controls whether the authorized user roles have access to the entered commands, but it does not control whether the user roles have obtained authorization to these commands. If a command is permitted by the access permission but denied by command authorization, this command cannot be executed.

You can specify one primary command authorization method and multiple backup command authorization methods.

When the default authorization method is invalid, the device attempts to use the backup authorization methods in sequence. For example, the **authorization command hwtacacs-scheme** *hwtacacs-scheme-name* **local none** command specifies the default HWTACACS authorization method and two backup methods (local authorization and no authorization). The device performs HWTACACS authorization by default and performs local authorization when the HWTACACS server is invalid. The device does not perform command authorization when both of the previous methods are invalid.

The remote authorization method is invalid in the following situations:

- The specified authorization scheme does not exist.
- Authorization packet sending fails.
- The device does not receive any authorization response packets from an authorization server.

The local authorization method is invalid if the device fails to find the matching local user configuration.

Examples

In ISP domain **test**, configure the device to perform local command authorization.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization command local
```

In ISP domain **test**, perform command authorization based on HWTACACS scheme **hwtac** and use local authorization as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization command hwtacacs-scheme hwtac local
```

Related commands

command authorization (*Fundamentals Command Reference*)

hwtacacs scheme

local-user

authorization default

Use **authorization default** to specify default authorization methods for an ISP domain.

Use **undo authorization default** to restore the default.

Syntax

authorization default { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] [**none**] | **local** [**radius-scheme** *radius-scheme-name* | **hwtacacs-scheme** *hwtacacs-scheme-name*] * [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] [**none**] }

undo authorization default

Default

The default authorization method of an ISP domain is local.

Views

ISP domain view

Predefined user roles

network-admin

context-admin

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters.

local: Performs local authorization.

none: Does not perform authorization. The following default authorization information applies after users pass authentication:

- Login users obtain the level-0 user role. Login users include the Telnet, FTP, SFTP, SCP, and terminal users. Terminal users can access the device through the console port. For more information about the level-0 user role, see RBAC configuration in *Fundamentals Configuration Guide*.
- The working directory for FTP, SFTP, and SCP login users is the root directory of the NAS. However, the users do not have permission to access the root directory.
- Non-login users can access the network.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

The default authorization method is used for all users that support this method and do not have an authorization method configured.

The RADIUS authorization configuration takes effect only when the authentication method and authorization method of the ISP domain use the same RADIUS scheme.

You can specify one primary authorization method and multiple backup authorization methods.

When the default authorization method is invalid, the device attempts to use the backup authorization methods in sequence. For example, the **authorization default radius-scheme** *radius-scheme-name* **local none** command specifies the default RADIUS authorization method and two backup methods (local authorization and no authorization). The device performs RADIUS authorization by default and performs local authorization when the RADIUS server is invalid. The device does not perform authorization when both of the previous methods are invalid.

The remote authorization method is invalid in the following situations:

- The specified authorization scheme does not exist.

- Authorization packet sending fails.
- The device does not receive any authorization response packets from an authorization server.

The local authorization method is invalid if the device fails to find the matching local user configuration.

When the primary authorization method is local, the following rules apply to the authorization of a user:

- The device uses the backup authorization methods in sequence only if local authorization is invalid for one of the following reasons:
  - An exception occurs in the local authorization process.
  - The user account is not configured on the device or the user is not allowed to use the access service.
- The device does not turn to the backup authorization methods if local authorization is invalid because of any other reason. Authorization fails for the user.

Examples

In ISP domain **test**, use RADIUS scheme **rd** as the primary default authorization method and use local authorization as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization default radius-scheme rd local
```

Related commands

hwtacacs scheme

local-user

radius scheme

authorization ike

Use **authorization ike** to specify authorization methods for IKE extended authentication.

Use **undo authorization ike** to restore the default.

Syntax

authorization ike { **local** [**radius-scheme** *radius-scheme-name*] [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authorization ike

Default

The default authorization methods of the ISP domain are used for IKE extended authentication.

Views

ISP domain view

Predefined user roles

network-admin

context-admin

Parameters

local: Performs local authorization.

none: Does not perform authorization.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

You can specify one primary authorization method and multiple backup authorization methods.

When the default authorization method is invalid, the device attempts to use the backup authorization methods in sequence. For example, the **authorization ike radius-scheme** *radius-scheme-name* **local none** command specifies the default RADIUS authorization method and two backup methods (local authorization and no authorization). The device performs RADIUS authorization by default and performs local authorization when the RADIUS server is invalid. The device does not perform authorization when both of the previous methods are invalid.

The remote authorization method is invalid in the following situations:

- The specified authorization scheme does not exist.
- Authorization packet sending fails.
- The device does not receive any authorization response packets from an authorization server.

The local authorization method is invalid if the device fails to find the matching local user configuration.

When the primary authorization method is local, the following rules apply to the authorization of a user:

- The device uses the backup authorization methods in sequence only if local authorization is invalid for one of the following reasons:
  - An exception occurs in the local authorization process.
  - The user account is not configured on the device or the user is not allowed to use the IKE service.
- The device does not turn to the backup authorization methods if local authorization is invalid because of any other reason. Authorization fails for the user.

Examples

In ISP domain **test**, perform local authorization for IKE extended authentication.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization ike local
```

Related commands

authorization default

local-user

authorization ipoe

Use **authorization ipoe** to specify authorization methods for IPoE users.

Use **undo authorization ipoe** to restore the default.

Syntax

authorization ipoe { **local** [**radius-scheme** *radius-scheme-name*] [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authorization ipoe

Default

The default authorization methods of the ISP domain are used for IPoE users.

Views

ISP domain view

Predefined user roles

network-admin

context-admin

Parameters

`local`: Performs local authorization.

none: Does not perform authorization.

`radius-scheme` *`radius-scheme-name`*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

The RADIUS authorization configuration takes effect only when authentication and authorization methods of the ISP domain use the same RADIUS scheme.

You can specify one primary authorization method and multiple backup authorization methods.

When the primary method is invalid, the device attempts to use the backup methods in sequence. For example, the **`authorization ipoe radius-scheme`** *`radius-scheme-name`* **`local`** **none** command specifies a primary RADIUS authorization method and two backup methods (local authorization and no authorization). The device performs RADIUS authorization by default and performs local authorization when the RADIUS server is invalid. The device does not perform authorization when both of the previous methods are invalid.

The remote authorization method is invalid in the following situations:

- The specified authorization scheme does not exist.
- Authorization packet sending fails.
- The device does not receive any authorization response packets from an authorization server.

The local authorization method is invalid if the device fails to find the matching local user configuration.

When the primary authorization method is local, the following rules apply to the authorization of a user:

- The device uses the backup authorization methods in sequence only if local authorization is invalid for one of the following reasons:
  - An exception occurs in the local authorization process.
  - The user account is not configured on the device or the user is not allowed to use the IPoE service.
- The device does not turn to the backup authorization methods if local authorization is invalid because of any other reason. Authorization fails for the user.

Examples

In ISP domain **test**, perform local authorization for IPoE users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization ipoe local
```

In ISP domain **test**, perform RADIUS authorization for IPoE users based on scheme **rd** and use local authorization as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization ipoe radius-scheme rd local
```

Related commands

authorization default

local-user

radius scheme

authorization lan-access

Use **authorization lan-access** to specify authorization methods for LAN users.

Use **undo authorization lan-access** to restore the default.

Syntax

authorization lan-access { **local** [**radius-scheme** *radius-scheme-name*] [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authorization lan-access

Default

The default authorization methods of the ISP domain are used for LAN users.

Views

ISP domain view

Predefined user roles

network-admin

context-admin

Parameters

local: Performs local authorization.

none: Does not perform authorization. An authenticated LAN user directly accesses the network.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

The RADIUS authorization configuration takes effect only when authentication and authorization methods of the ISP domain use the same RADIUS scheme.

You can specify one primary authorization method and multiple backup authorization methods.

When the primary method is invalid, the device attempts to use the backup methods in sequence. For example, the **authorization lan-access radius-scheme** *radius-scheme-name* **local none** command specifies a primary RADIUS authorization method and two backup methods (local authorization and no authorization). The device performs RADIUS authorization by default and performs local authorization when the RADIUS server is invalid. The device does not perform authorization when both of the previous methods are invalid.

The remote authorization method is invalid in the following situations:

- The specified authorization scheme does not exist.
- Authorization packet sending fails.
- The device does not receive any authorization response packets from an authorization server.

The local authorization method is invalid if the device fails to find the matching local user configuration.

When the primary authorization method is local, the following rules apply to the authorization of a user:

- The device uses the backup authorization methods in sequence only if local authorization is invalid for one of the following reasons:
  - An exception occurs in the local authorization process.
  - The user account is not configured on the device or the user is not allowed to use the LAN access service.
- The device does not turn to the backup authorization methods if local authorization is invalid because of any other reason. Authorization fails for the user.

Examples

In ISP domain **test**, perform local authorization for LAN users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization lan-access local
```

In ISP domain **test**, perform RADIUS authorization for LAN users based on scheme **rd** and use local authorization as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization lan-access radius-scheme rd local
```

Related commands

authorization default

local-user

radius scheme

authorization login

Use **authorization login** to specify authorization methods for login users.

Use **undo authorization login** to restore the default.

Syntax

authorization login { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] [**none**] | **local** [**radius-scheme** *radius-scheme-name* | **hwtacacs-scheme** *hwtacacs-scheme-name*] * [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] [**none**] }

undo authorization login

Default

The default authorization methods of the ISP domain are used for login users.

Views

ISP domain view

Predefined user roles

network-admin

context-admin

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters.

local: Performs local authorization.

none: Does not perform authorization. The following default authorization information applies after users pass authentication:

- Login users obtain the level-0 user role. Login users include the Telnet, FTP, SFTP, SCP, and terminal users. Terminal users can access the device through the console port. For more information about the level-0 user role, see RBAC configuration in *Fundamentals Configuration Guide*.
- The working directory for FTP, SFTP, and SCP login users is the root directory of the NAS. However, the users do not have permission to access the root directory.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

The RADIUS authorization configuration takes effect only when the authentication method and authorization method of the ISP domain use the same RADIUS scheme.

You can specify one primary authorization method and multiple backup authorization methods.

When the default authorization method is invalid, the device attempts to use the backup authorization methods in sequence. For example, the **authorization login radius-scheme** *radius-scheme-name* **local none** command specifies the default RADIUS authorization method and two backup methods (local authorization and no authorization). The device performs RADIUS authorization by default and performs local authorization when the RADIUS server is invalid. The device does not perform authorization when both of the previous methods are invalid.

The remote authorization method is invalid in the following situations:

- The specified authorization scheme does not exist.
- Authorization packet sending fails.
- The device does not receive any authorization response packets from an authorization server.

The local authorization method is invalid if the device fails to find the matching local user configuration.

When the primary authorization method is local, the following rules apply to the authorization of a user:

- The device uses the backup authorization methods in sequence only if local authorization is invalid for one of the following reasons:
  - An exception occurs in the local authorization process.
  - The user account is not configured on the device or the user is not allowed to use the service for accessing the device.
- The device does not turn to the backup authorization methods if local authorization is invalid because of any other reason. Authorization fails for the user.

Examples

In ISP domain **test**, perform local authorization for login users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization login local
```

In ISP domain **test**, perform RADIUS authorization for login users based on scheme **rd** and use local authorization as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization login radius-scheme rd local
```

Related commands

authorization default

hwtacacs scheme

local-user

radius scheme

authorization portal

Use **authorization portal** to specify authorization methods for portal users.

Use **undo authorization portal** to restore the default.

Syntax

authorization portal { **local** [**radius-scheme** *radius-scheme-name*] [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authorization portal

Default

The default authorization methods of the ISP domain are used for portal users.

Views

ISP domain view

Predefined user roles

network-admin

context-admin

Parameters

local: Performs local authorization.

none: Does not perform authorization. An authenticated portal user directly accesses the network.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

The RADIUS authorization configuration takes effect only when the authentication method and authorization method of the ISP domain use the same RADIUS scheme.

You can specify one primary authorization method and multiple backup authorization methods.

When the default authorization method is invalid, the device attempts to use the backup authorization methods in sequence. For example, the **authorization portal radius-scheme** *radius-scheme-name* **local none** command specifies the default RADIUS authorization method and two backup methods (local authorization and no authorization). The device performs RADIUS authorization by default and performs local authorization when the RADIUS server is invalid. The device does not perform authorization when both of the previous methods are invalid.

The remote authorization method is invalid in the following situations:

- The specified authorization scheme does not exist.
- Authorization packet sending fails.
- The device does not receive any authorization response packets from an authorization server.

The local authorization method is invalid if the device fails to find the matching local user configuration.

When the primary authorization method is local, the following rules apply to the authorization of a user:

- The device uses the backup authorization methods in sequence only if local authorization is invalid for one of the following reasons:
  - An exception occurs in the local authorization process.
  - The user account is not configured on the device or the user is not allowed to use the portal service.
- The device does not turn to the backup authorization methods if local authorization is invalid because of any other reason. Authorization fails for the user.

Examples

In ISP domain **test**, perform local authorization for portal users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization portal local
```

In ISP domain **test**, perform RADIUS authorization for portal users based on scheme **rd** and use local authorization as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization portal radius-scheme rd local
```

Related commands

authorization default

local-user

radius scheme

authorization ppp

Use **authorization ppp** to specify authorization methods for PPP users.

Use **undo authorization ppp** to restore the default.

Syntax

authorization ppp { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] [**none**] | **ldap-scheme** *ldap-scheme-name* [**local**] [**none**] | **local** [**radius-scheme** *radius-scheme-name* | **hwtacacs-scheme** *hwtacacs-scheme-name*] * [**none**] | **local** [**ldap-scheme** *ldap-scheme-name*] [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] [**none**] }

undo authorization ppp

Default

The default authorization methods of the ISP domain are used for PPP users.

Views

ISP domain view

Predefined user roles

network-admin

context-admin

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters.

ldap-scheme *ldap-scheme-name*: Specifies an LDAP scheme by its name, a case-insensitive string of 1 to 32 characters.

local: Performs local authorization.

none: Does not perform authorization.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

The RADIUS authorization configuration takes effect only when the authentication method and authorization method of the ISP domain use the same RADIUS scheme.

You can specify one primary authorization method and multiple backup authorization methods.

When the primary method is invalid, the device attempts to use the backup methods in sequence. For example, the **authorization ppp radius-scheme** *radius-scheme-name* **local none** command specifies a primary RADIUS authorization method and two backup methods (local authorization and no authorization). The device performs RADIUS authorization by default and performs local authorization when the RADIUS server is invalid. The device does not perform authorization when both of the previous methods are invalid.

The remote authorization method is invalid in the following situations:

- The specified authorization scheme does not exist.
- Authorization packet sending fails.
- The device does not receive any authorization response packets from an authorization server.

The local authorization method is invalid if the device fails to find the matching local user configuration.

When the primary authorization method is local, the following rules apply to the authorization of a user:

- The device uses the backup authorization methods in sequence only if local authorization is invalid for one of the following reasons:
  - An exception occurs in the local authorization process.
  - The user account is not configured on the device or the user is not allowed to use the PPP service.
- The device does not turn to the backup authorization methods if local authorization is invalid because of any other reason. Authorization fails for the user.

Examples

In ISP domain **test**, perform local authorization for PPP users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization ppp local
```

In ISP domain **test**, perform RADIUS authorization for PPP users based on scheme **rd** and use local authorization as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization ppp radius-scheme rd local
```

Related commands

authorization default

hwtacacs scheme

ldap scheme

local-user

radius scheme

authorization sslvpn

Use **authorization sslvpn** to specify authorization methods for SSL VPN users.

Use **undo authorization sslvpn** to restore the default.

Syntax

authorization sslvpn { **ldap-scheme** *ldap-scheme-name* [**local**] [**none**] | **local** [**ldap-scheme** *ldap-scheme-name* | **radius-scheme** *radius-scheme-name*] [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authorization sslvpn

Default

The default authorization methods of the ISP domain are used for SSL VPN users.

Views

ISP domain view

Predefined user roles

network-admin

context-admin

Parameters

ldap-scheme *ldap-scheme-name*: Specifies an LDAP scheme by its name, a case-insensitive string of 1 to 32 characters.

local: Performs local authorization.

none: Does not perform authorization. Authenticated SSL VPN users can access the network directly.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

The RADIUS authorization configuration takes effect only when the authentication method and authorization method of the ISP domain use the same RADIUS scheme.

You can specify one primary authorization method and multiple backup authorization methods.

When the primary method is invalid, the device attempts to use the backup methods in sequence. For example, the **authorization sslvpn radius-scheme** *radius-scheme-name* **local none** command specifies a primary RADIUS authorization method and two backup methods (local authorization and no authorization). The device performs RADIUS authorization by default and performs local authorization when the RADIUS server is invalid. The device does not perform authorization when both of the previous methods are invalid.

The remote authorization method is invalid in the following situations:

- The specified authorization scheme does not exist.
- Authorization packet sending fails.
- The device does not receive any authorization response packets from an authorization server.

The local authorization method is invalid if the device fails to find the matching local user configuration.

When the primary authorization method is local, the following rules apply to the authorization of a user:

- The device uses the backup authorization methods in sequence only if local authorization is invalid for one of the following reasons:
  - An exception occurs in the local authorization process.
  - The user account is not configured on the device or the user is not allowed to use the SSL VPN service.
- The device does not turn to the backup authorization methods if local authorization is invalid because of any other reason. Authorization fails for the user.

Examples

In ISP domain **test**, perform local authorization for SSL VPN users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization sslvpn local
```

In ISP domain **test**, perform LDAP authorization for SSL VPN users based on scheme **ldp** and use local authorization as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization sslvpn ldap-scheme ldp local
```

Related commands

authorization default

ldap scheme

local-user

radius scheme

authorization-attribute (ISP domain view)

Use **authorization-attribute** to configure authorization attributes for users in an ISP domain.

Use **undo authorization-attribute** to restore the default of an authorization attribute.

Syntax

authorization-attribute { **acl** *acl-number* | **car inbound cir** *committed-information-rate* [**pir** *peak-information-rate*] **outbound cir** *committed-information-rate* [**pir** *peak-information-rate*] | **idle-cut** *minutes* [*flow*] | **igmp max-access-number** *max-access-number* | **ip-pool** *ipv4-pool-name* | **ipv6-pool** *ipv6-pool-name* | **ipv6-prefix** *ipv6-prefix prefix-length* | { **primary-dns** | **secondary-dns** } { **ip** *ipv4-address* | **ipv6** *ipv6-address* } | **session-timeout** *minutes* | **url** *url-string* | **user-group** *user-group-name* | **vpn-instance** *vpn-instance-name* }

undo authorization-attribute { **acl** | **car** | **idle-cut** | **igmp** | **ip-pool** | **ipv6-pool** | **ipv6-prefix** | **primary-dns** | **secondary-dns** | **session-timeout** | **url** | **user-group** | **vpn-instance** }

Default

The idle cut feature is disabled.

An IPv4 user can concurrently join a maximum of four IGMP multicast groups.

An IPv6 user can concurrently join a maximum of four MLD multicast groups.

No other authorization attributes exist.

Views

ISP domain view

Predefined user roles

network-admin

context-admin

Parameters

acl *acl-number*: Specifies an ACL to filter traffic for users. The value range for the *acl-number* argument is 2000 to 5999. This option is applicable only to portal and LAN users. The device processes the traffic that matches the rules in the authorization ACL based on the permit or deny statement in the rules.

car: Specifies a CAR action for users. Typically, the attribute applies to authenticated users. If you configure the attribute in a portal preauthentication domain, the CAR action applies before portal authentication. This keyword is applicable only to IPoE, portal, and PPP users.

inbound: Specifies the upload rate of users.

outbound: Specifies the download rate of users.

cir *committed-information-rate*: Specifies the committed information rate in kbps, in the range of 1 to 4194303.

pir *peak-information-rate*: Specifies the peak information rate in kbps, in the range of 1 to 4194303. The peak information rate cannot be smaller than the committed information rate. If you do not specify this option, the CAR action does not restrict users by peak information rate.

idle-cut *minutes*: Specifies an idle timeout period in minutes. The value range for the *minutes* argument is 1 to 600. This option is applicable only to IPoE, portal, and PPP users.

flow: Specifies the minimum traffic that must be generated in the idle timeout period in bytes. The value range is 1 to 10240000, and the default value is 10240.

igmp max-access-number *max-access-number*: Specifies the maximum number of IGMP groups that an IPv4 user can join concurrently. The value range for the *max-access-number* argument is 1 to 64. This option is applicable only to IPoE, portal, and PPP users.

ip-pool *ipv4-pool-name*: Specifies an IPv4 address pool for users. The *ipv4-pool-name* argument is a case-insensitive string of 1 to 63 characters. This option is applicable only to PPP, IKE, IPoE, and portal users.

ipv6-pool *ipv6-pool-name*: Specifies an IPv6 address pool for users. The *ipv6-pool-name* argument is a case-insensitive string of 1 to 63 characters. This option is applicable only to IPoE, portal, and PPP users.

ipv6-prefix *ipv6-prefix prefix-length*: Specifies an IPv6 prefix for users. The value range for the *prefix-length* argument is 1 to 128. The IPv6 prefix cannot be ::/128, ::1/128, or an IPv6 multicast prefix. This option is applicable only to IPoE and PPP users.

primary-dns ip *ipv4-address*: Specifies the IPv4 address of the primary DNS server for users. This option is applicable only to IPoE and PPP users.

primary-dns ipv6 *ipv6-address*: Specifies the IPv6 address of the primary DNS server for users. This option is applicable only to IPoE and PPP users.

secondary-dns ip *ipv4-address*: Specifies the IPv4 address of the secondary DNS server for users. This option is applicable only to IPoE and PPP users.

secondary-dns ipv6 *ipv6-address*: Specifies the IPv6 address of the secondary DNS server for users. This option is applicable only to IPoE and PPP users.

session-timeout *minutes*: Specifies the session timeout timer for users, in minutes. The value range for the *minutes* argument is 1 to 4294967295. The device logs off a user when the user's session timeout timer expires. This option is applicable only to PPP, portal, IPoE, and LAN users.

url *url-string*: Specifies a redirect URL for users. The *url-string* argument is a case-sensitive string of 1 to 255 characters. The URL must start with **http://** or **https://**. You can configure the redirect URL attribute to push advertisements or notifications to users after the users pass authentication or push bill overdue notifications to users. This option is applicable only to PPPoE users. For IPoE users, you must specify a URL with port number 80 or 443.

user-group *user-group-name*: Specifies a user group for users. The *user-group-name* argument is a case-insensitive string of 1 to 32 characters. Authenticated users obtain all attributes of the user group.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance to which the users belong. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. When a user passes authentication, it has permission to access the network resources in the specified VPN. This option is applicable only to PPP and IPoE users.

Usage guidelines

When the idle cut feature is configured, the device periodically detects the traffic of each online user. The device logs out users that do not meet the minimum traffic requirement in the idle timeout period. When the idle cut feature is disabled on the device, the idle cut feature of the server takes effect. The server considers a user idle if the user's traffic is less than 10240 bytes in a configurable idle timeout period.

If the server or NAS does not authorize a type of attribute to an authenticated user, the device authorizes the attribute in the ISP domain to the user.

You can configure multiple authorization attributes for users in an ISP domain. If you execute the command multiple times with the same attribute specified, the most recent configuration takes effect.

When you specify an authorized ACL, follow these restrictions and guidelines:

- If the specified ACL does not exist or the ACL does not contain any rules, the system considers that no ACL is specified. If the strict check method is enabled for portal authorized ACLs, the system logs off portal users.
- For portal users to come online after passing authentication, make sure ACLs assigned to portal users do not have rules specified with a source IP or MAC address.

Examples

Specify user group **abc** as the authorization user group for users in ISP domain **test**.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization-attribute user-group abc
```

Related commands

display domain

basic-service-ip-type

Use **basic-service-ip-type** to specify the types of IP addresses that L2TP users must rely on to use the basic services.

Use **undo basic-service-ip-type** to restore the default.

Syntax

basic-service-ip-type { **ipv4** | **ipv6** | **ipv6-pd** } *

undo basic-service-ip-type

Default

L2TP users do not rely on any types of IP addresses to use the basic services.

Views

ISP domain view

Predefined user roles

network-admin

context-admin

Parameters

ipv4: Specifies the IPv4 address type.

ipv6: Specifies the IPv6 address type.

ipv6-pd: Specifies the IPv6-PD address type. This type of IPv6 addresses are generated based on the DHCPv6 server-assigned prefix.

Usage guidelines

This command takes effect only when the device acts as an L2TP LNS and only on L2TP users.

A user might request multiple services of different IP address types. By default, the device logs off the user if the user does not obtain an IP address. This command enables the device to allow the user to come online if the user has obtained IP addresses of all the specified types for the basic services.

The device does not allow a user to come online if the user does not obtain IP addresses of all the specified types for the basic services. For example, if you execute the **basic-service-ip-type ipv6** command, the device does not allow a user to come online if the user does not obtain an IPv6 address.

If you specify both the **ipv6** and **ipv6-pd** keywords, the device does not allow a user that fails IPv6 address negotiation or PD negotiation to come online.

Examples

In ISP domain **test**, specify L2TP users to rely on IPv4 addresses to use the basic services.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] basic-service-ip-type ipv4
```

dhcpv6-follow-ipv6cp

Use **dhcpv6-follow-ipv6cp** to set the IPv6 address wait timer for L2TP users.

Use **undo dhcpv6-follow-ipv6cp** to restore the default.

Syntax

dhcpv6-follow-ipv6cp timeout *delay-time*

undo dhcpv6-follow-ipv6cp

Default

The IPv6 address wait timer for L2TP users is 60 seconds.

Views

ISP domain view

Predefined user roles

network-admin

context-admin

Parameters

timeout *delay-time*: Sets the IPv6 address wait timer, in the range of 30 to 120 seconds.

Usage guidelines

This command takes effect only when the device acts as an L2TP LNS and only on L2TP users.

The IPv6 address wait timer defines the maximum amount of time that a user can wait before the device determines that the user fails to obtain an IPv6 address or PD prefix.

The device starts an IPv6 address wait timer for a user after it finishes IPv6CP negotiation with the user. If the user's basic service relies on an IPv6 address or PD prefix but it fails to obtain any IPv6 address or PD prefix when the timer expires, the user cannot come online.

As a best practice, increase the IPv6 address wait timer in the following situations:

- The network communication is unstable.
- The device uses DHCPv6 to assign IPv6 addresses to users.
- The ISP domain serves a large number of users.

Examples

In ISP domain **test**, set the IPv6 address wait timer to 90 seconds for L2TP users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] dhcpv6-follow-ipv6cp timeout 90
```

Related commands

basic-service-ip-type

display domain

Use **display domain** to display ISP domain configuration.

Syntax

display domain [*isp-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

isp-name: Specifies an ISP domain by its name, a case-insensitive string of 1 to 255 characters. If you do not specify an ISP domain, this command displays the configuration of all ISP domains.

Examples

Display the configuration of all ISP domains.

```
<Sysname> display domain
```

```
Total 2 domains

Domain: system
  State: Active
  Default authentication scheme:  Local
  Default authorization  scheme:  Local
  Default accounting     scheme:  Local
  Accounting start failure action: Online
  Accounting update failure action: Online
  Accounting quota out action: Offline
  Service type: HSI
  Session time: Exclude idle time
  NAS-ID: N/A
  DHCPv6-follow-IPv6CP timeout: 60 seconds
  Authorization attributes:
    Idle cut: Disabled
    Session timeout: Disabled
    IGMP access limit: 4
    MLD access limit: 4

Domain: dm
  State: Active
  Login   authentication scheme:  RADIUS=rad
  Login   authorization  scheme:  HWTACACS=hw
  Super   authentication scheme:  RADIUS=rad
  Command authorization  scheme:  HWTACACS=hw
  LAN access authentication scheme:  RADIUS=r4
  Default authentication scheme:  RADIUS=rad, Local, None
  Default authorization  scheme:  Local
  Default accounting     scheme:  None
  Accounting start failure action: Online
  Accounting update failure action: Online
  Accounting quota out action: Offline
  Service type: HSI
  Session time: Include idle time
  User address type: ipv4
  NAS-ID: test
  Authorization attributes:
    Idle cut : Enabled
      Idle timeout: 2 minutes
      Flow: 10240 bytes
    Session timeout: 34 minutes
    IP pool: appy
    Inbound CAR: CIR 64000 bps PIR 640000 bps
    Outbound CAR: CIR 64000 bps PIR 640000 bps
    ACL number: 3000
    User group: ugg
    IPv6 prefix: 1::1/34
```

```
    IPv6 pool: ipv6pool
    Primary DNS server: 6.6.6.6
    Secondary DNS server: 3.6.2.3
    URL: http://test
    VPN instance: vpn1
    IGMP access limit: 4
    MLD access limit: 4

Default domain name: system
```

Table 1 Command output

Field	Description
Domain	ISP domain name.
State	Status of the ISP domain.
Default authentication scheme	Default authentication methods.
Default authorization scheme	Default authorization methods.
Default accounting scheme	Default accounting methods.
ADVPN authentication scheme	Authentication methods for ADVPN users.
ADVPN authorization scheme	Authorization methods for ADVPN users.
ADVPN accounting scheme	Accounting methods for ADVPN users.
Login authentication scheme	Authentication methods for login users.
Login authorization scheme	Authorization methods for login users.
Login accounting scheme	Accounting methods for login users.
Super authentication scheme	Authentication methods for obtaining another user role without reconnecting to the device.
PPP authentication scheme	Authentication methods for PPP users.
PPP authorization scheme	Authorization methods for PPP users.
PPP accounting scheme	Accounting methods for PPP users.
Command authorization scheme	Command line authorization methods.
Command accounting scheme	Command line accounting method.
LAN access authentication scheme	Authentication methods for LAN users.
LAN access authorization scheme	Authorization methods for LAN users.
LAN access accounting scheme	Accounting methods for LAN users.
Portal authentication scheme	Authentication methods for portal users.
Portal authorization scheme	Authorization methods for portal users.
Portal accounting scheme	Accounting methods for portal users.
IKE authentication scheme	IKE extended authentication methods.
IKE authorization scheme	Authorization methods for IKE extended authentication.
IPoE authentication scheme	Authentication methods for IPoE users.
IPoE authorization scheme	Authorization methods for IPoE users.
IPoE accounting scheme	Accounting methods for IPoE users.

Field	Description
SSL VPN authentication scheme	Authentication methods for SSL VPN users.
SSL VPN authorization scheme	Authorization methods for SSL VPN users.
SSL VPN accounting scheme	Accounting methods for SSL VPN users.
RADIUS	RADIUS scheme.
HWTACACS	HWTACACS scheme.
LDAP	LDAP scheme.
Local	Local scheme.
None	No authentication, no authorization, or no accounting.
Accounting start failure action	Access control for users that encounter accounting-start failures: • **Online**—Allows the users to stay online. • **Offline**—Logs off the users.
Accounting update failure max-times	Maximum number of consecutive accounting-update failures allowed by the device for each user in the domain.
Accounting update failure action	Access control for users that have failed all their accounting-update attempts: • **Online**—Allows the users to stay online. • **Offline**—Logs off the users.
Accounting quota out action	Access control for users that have used up their accounting quotas: • **Online**—Allows the users to stay online. • **Offline**—Logs off the users.
Service type	Service type of the ISP domain, including HSI, STB, and VoIP.
Session time	Online duration sent to the server for users that went offline due to connection failure or malfunction: • **Include idle time**—The online duration includes the idle timeout period. • **Exclude idle time**—The online duration does not include the idle timeout period.
User address type	Type of IP addresses for users in the ISP domain. This field is not available if no user address type is specified in the ISP domain.
NAS-ID	NAS-ID of the device. This field displays **N/A** if no NAS-ID is set in the ISP domain.
User basic service IP type	Types of IP addresses that PPPoE and L2TP users rely on to use the basic services: • **IPv4**. • **IPv6**. • **IPv6-PD**.
DHCPv6-follow-IPv6CP timeout	IPv6 address wait timer (in seconds) that starts after IPv6CP negotiation for PPPoE and L2TP users.
Authorization attributes	Authorization attributes for users in the ISP domain.
Idle cut	Idle cut feature status: • **Enabled**—The feature is enabled. The device logs off users that do not meet the minimum traffic requirements in an idle timeout period.

Field	Description
	• **Disabled**—The feature is disabled. It is the default idle cut state.
Idle timeout	Idle timeout period, in minutes.
Flow	Minimum traffic that a login user must generate in an idle timeout period, in bytes.
Session timeout	Session timeout time for users in the ISP domain, in minutes.
IP pool	Name of the authorization IPv4 address pool.
Inbound CAR	Authorization inbound CAR: • **CIR**—Committed information rate in bps. • **PIR**—Peak information rate in bps.
Outbound CAR	Authorization outbound CAR: • **CIR**—Committed information rate in bps. • **PIR**—Peak information rate in bps.
ACL number	Authorization ACL for users.
User group	Authorization user group for users.
IPv6 prefix	Authorization IPv6 prefix for users.
IPv6 pool	Name of the authorization IPv6 address pool for users.
Primary DNS server	IPv4 address of the authorization primary DNS server for users.
Secondary DNS server	IPv4 address of the authorization secondary DNS server for users.
Primary DNSV6 server	IPv6 address of the authorization primary DNS server for users.
Secondary DNSV6 server	IPv6 address of the authorization secondary DNS server for users.
URL	Authorization redirect URL for users.
VPN instance	Name of the authorization VPN instance for users.
IGMP access limit	Maximum number of IGMP groups that an IPv4 user is authorized to join concurrently.
MLD access limit	This field is not supported in the current software version. Maximum number of MLD groups that an IPv6 user is authorized to join concurrently.

domain

Use **domain** to create an ISP domain and enter its view, or enter the view of an existing ISP domain.

Use **undo domain** to delete an ISP domain.

Syntax

domain *isp-name*

undo domain *isp-name*

Default

A system-defined ISP domain exists. The domain name is **system**.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

isp-name: Specifies the ISP domain name, a case-insensitive string of 1 to 255 characters. The name must meet the following requirements:

- The name cannot contain a forward slash (/), backslash (\), vertical bar (|), quotation marks ("), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or at sign (@).
- The name cannot be **d**, **de**, **def**, **defa**, **defau**, **defaul**, **default**, **i**, **if**, **if-**, **if-u**, **if-un**, **if-unk**, **if-unkn**, **if-unkno**, **if-unknow**, or **if-unknown**.

Usage guidelines

All ISP domains are in active state when they are created.

You can modify settings for the system-defined ISP domain **system**, but you cannot delete this domain.

An ISP domain cannot be deleted when it is the default ISP domain. Before you use the **undo domain** command, change the domain to a non-default ISP domain by using the **undo domain default enable** command.

Use short domain names to ensure that user names containing a domain name do not exceed the maximum name length required by different types of users.

Examples

Create an ISP domain named **test** and enter ISP domain view.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test]
```

Related commands

display domain

domain default enable

domain if-unknown

state (ISP domain view)

domain default enable

Use **domain default enable** to specify the default ISP domain. Users without any domain name included in the usernames are considered in the default domain.

Use **undo domain default enable** to restore the default.

Syntax

domain default enable *isp-name*

undo domain default enable

Default

The default ISP domain is the system-defined ISP domain **system**.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

isp-name: Specifies the ISP domain name, a case-insensitive string of 1 to 255 characters. The ISP domain must already exist.

Usage guidelines

The system has only one default ISP domain.

An ISP domain cannot be deleted when it is the default ISP domain. Before you use the **undo domain** command, change the domain to a non-default ISP domain by using the **undo domain default enable** command.

Examples

Create an ISP domain named **test**, and configure the domain as the default ISP domain.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] quit
[Sysname] domain default enable test
```

Related commands

display domain

domain

domain if-unknown

Use **domain if-unknown** to specify an ISP domain to accommodate users that are assigned to nonexistent domains.

Use **undo domain if-unknown** to restore the default.

Syntax

domain if-unknown *isp-name*

undo domain if-unknown

Default

No ISP domain is specified to accommodate users that are assigned to nonexistent domains.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

isp-name: Specifies the ISP domain name, a case-insensitive string of 1 to 255 characters. The name must meet the following requirements:

- The name cannot contain a forward slash (/), backslash (\), vertical bar (|), quotation marks ("), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or at sign (@).
- The name cannot be **d**, **de**, **def**, **defa**, **defau**, **defaul**, **default**, **i**, **if**, **if-**, **if-u**, **if-un**, **if-unk**, **if-unkn**, **if-unkno**, **if-unknow**, or **if-unknown**.

Usage guidelines

The device chooses an authentication domain for each user in the following order:

1. The authentication domain specified for the access module.
2. The ISP domain in the username.
3. The default ISP domain of the device.

If the chosen domain does not exist on the device, the device searches for the ISP domain that accommodates users assigned to nonexistent domains. If no such ISP domain is configured, user authentication fails.

NOTE:

Support for the authentication domain configuration depends on the access module.

Examples

Specify ISP domain **test** to accommodate users that are assigned to nonexistent domains.

```
<Sysname> system-view
[Sysname] domain if-unknown test
```

Related commands

display domain

domain-delimiter

Use **domain-delimiter** to configure global domain name delimiters.

Use **undo domain-delimiter** to restore the default.

Syntax

domain-delimiter [**advpn** | **ike** | **ipoe** | **lanaccess** | **login** | **portal** | **ppp** | **sslvpn** | **super**] *string*

undo domain-delimiter [**advpn** | **ike** | **ipoe** | **lanaccess** | **login** | **portal** | **ppp** | **sslvpn** | **super**]

Default

Global domain name delimiters include at sign (@), slash (/), and backslash (\).

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

advpn: Specifies ADVPN tunnel users.

ike: Specifies IKE users that access the network through IKE extended authentication.

ipoe: Specifies IPoE users.

lanaccess: Specifies LAN access users.

login: Specifies users that log in to the device.

portal: Specifies portal users.

ppp: Specifies PPP users.

ssh: Specifies SSH users.

sslvpn: Specifies SSL VPN users.

super: Specifies users that obtain temporary user role authorization.

string: Specifies a string of 1 to 16 global domain name delimiters. Valid delimiters include at sign (@), dot (.), slash (/), and backslash (\). To specify a backslash (\), you must precede the backslash with an escape character (\).

Usage guidelines

A domain name delimiter separates the username part from the domain name part in a username. For the device to correctly extract the username and domain name parts in usernames, you can configure domain name delimiters. Table 2 shows the way that the device interprets a username based on different domain name delimiters.

Table 2 Domain name delimiters and username formats

Domain name delimiter	Username format
At sign (@)	*username@domain-name*
Backslash (\)	*domain-name\username*
Slash (/)	*username/domain-name*
Dot (.)	*username.domain-name*

If a username includes multiple domain name delimiters, the device selects the first delimiter in the search direction specified by using the **domain-delimiter search-from** command.

If you do not specify a user type, the configured domain name delimiters take effect on all types of users.

The access module-specific domain name delimiters have higher priority than global domain name delimiters.

Modification of global domain name delimiters takes effect only on users that come online after the modification.

Examples

Configure global domain name delimiters as at sign (@) and slash (/).

```
<Sysname> system-view
[Sysname] domain-delimiter login @/
```

Related commands

domain-delimiter search-from

domain-delimiter search-direction

Use **domain-delimiter search-direction** to specify the search direction for the domain name delimiter.

Use **undo domain-delimiter search-direction** to restore the default.

Syntax

domain-delimiter search-direction { **backward** | **forward** }

undo domain-delimiter search-direction

Default

The device searches for a domain name delimiter in usernames from right to left.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

backward: Specifies the right-to-left search direction.

forward: Specifies the left-to-right search direction.

Usage guidelines

In authentication, it is very import for the device to correctly extract the username and domain name parts in a username. If a username includes multiple domain name delimiters, the search direction for the domain name delimiter determines how the device interprets a username. For example, if a username is 1234@456@789 and the domain name delimiter is at sign (@), the device can interpret the username in the following ways:

- If the search direction is left-to-right, the device uses the first at sign (@) as the delimiter. The username part is 1234 and the domain name part is 456@789.
- If the search direction is right-to-left, the device uses the second at sign (@) as the delimiter. The username part is 1234@789 and the domain name part is 789.

Use this command to specify the direction in which the device search for a domain name delimiter in usernames.

If you execute this command multiple times, the most recent configuration takes effect.

Modification of the search direction takes effect only on users that come online after the modification.

Examples

Specify the left-to-right direction for the device to search for a domain name delimiter in usernames.

```
<Sysname> system-view
[Sysname] domain-delimiter search-direction forward
```

Related commands

domain-delimiter

local-server log change-password-prompt

Use **local-server log change-password-prompt** to enable password change prompt logging.

Use **undo local-server log change-password-prompt** to disable password change prompt logging.

Syntax

local-server log change-password-prompt

undo local-server log change-password-prompt

Default

Password change prompt logging is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Non-default vSystems do not support this command.

Use this feature to enhance the protection of passwords for Telnet, SSH, HTTP, HTTPS, NETCONF over SSH, and NETCONF over SOAP users and improve the system security.

This feature enables the device to generate logs to prompt users to change their weak passwords at an interval of 24 hours and at the users' login.

A password is a weak password if it does not meet the following requirements:

- Password composition restriction configured by using the **password-control composition** command.
- Minimum password length restriction set by using the **password-control length** command.
- Password complexity checking policy configured by using the **password-control complexity** command.

For a NETCONF over SSH or NETCONF over SOAP user, the device also generates a password change prompt log if any of the following conditions exists:

- The current password of the user is the default password or has expired.
- The user logs in to the device for the first time or uses a new password to log in after global password control is enabled.

The device will no longer generate password change prompt logs for a user when one of the following conditions exists:

- The password change prompt logging feature is disabled.
- The user has changed the password and the new password meets the password control requirements.
- The enabling status of a related password control feature has changed so the current password of the user meets the password control requirements.
- The password composition policy or the minimum password length has changed.

You can use the **display password-control** command to display password control configuration. For more information about password control commands, see "Password control commands."

Examples

Enable password change prompt logging.

```
<Sysname> system-view
[Sysname] local-server log change-password-prompt
```

Related commands

display password-control

password-control composition

password-control length

local-server log change-password-prompt

Use **local-server log change-password-prompt** to enable password change prompt logging.

Use **undo local-server log change-password-prompt** to disable password change prompt logging.

Syntax

local-server log change-password-prompt

undo local-server log change-password-prompt

Default

Password change prompt logging is enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

Use this feature to enhance the protection of passwords for Telnet, SSH, HTTP, HTTPS, NETCONF over SSH, and NETCONF over SOAP users and improve the system security.

This feature enables the device to generate logs to prompt users to change their weak passwords at an interval of 24 hours and at the users' login.

A password is a weak password if it does not meet the following requirements:

- Password composition restriction configured by using the **password-control composition** command.
- Minimum password length restriction set by using the **password-control length** command.
- Password complexity checking policy configured by using the **password-control complexity** command.

For a NETCONF over SSH or NETCONF over SOAP user, the device also generates a password change prompt log if any of the following conditions exists:

- The current password of the user is the default password or has expired.
- The user logs in to the device for the first time or uses a new password to log in after global password control is enabled.

The device will no longer generate password change prompt logs for a user when one of the following conditions exists:

- The password change prompt logging feature is disabled.
- The user has changed the password and the new password meets the password control requirements.
- The enabling status of a related password control feature has changed so the current password of the user meets the password control requirements.
- The password composition policy or the minimum password length has changed.

You can use the **display password-control** command to display password control configuration. For more information about password control commands, see "Password control commands."

Examples

Enable password change prompt logging.

```
<Sysname> system-view
[Sysname] local-server log change-password-prompt
```

Related commands

display password-control

password-control complexity

password-control composition

password-control length

nas-id

Use **nas-id** to set the NAS-ID in an ISP domain.

Use **undo nas-id** to restore the default.

Syntax

nas-id *nas-identifier*

undo nas-id

Default

No NAS-ID is set in an ISP domain.

Views

ISP domain view

Predefined user roles

network-admin

context-admin

Parameters

nas-identifier: Specifies a NAS-ID, a case-sensitive string of 1 to 31 characters.

Usage guidelines

During RADIUS authentication, the device uses a NAS-ID to set the NAS-Identifier attribute of RADIUS packets so that the RADIUS server can identify the access location of users.

You can configure a NAS-ID in VSRP instance view, in NAS-ID profile view, or in ISP domain view. The device selects the NAS-ID for the NAS-Identifier attribute in the following order:

1. NAS-ID bound with VLANs in a NAS-ID profile.
2. NAS-ID in an ISP domain.

If no NAS-ID is selected, the device uses the device name as the NAS-ID.

Examples

Set the NAS-ID to **test** for ISP domain **test**.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] nas-id test
```

Related commands

aaa nas-id profile

nas-id bind vlan

Use **nas-id bind vlan** to bind a NAS-ID with a VLAN.

Use **undo nas-id bind vlan** to remove a NAS-ID and VLAN binding.

Syntax

nas-id *nas-identifier* **bind vlan** *vlan-id*

undo nas-id *nas-identifier* **bind vlan** *vlan-id*

Default

No NAS-ID and VLAN bindings exist.

Views

NAS-ID profile view

Predefined user roles

network-admin

context-admin

Parameters

nas-identifier: Specifies a NAS-ID, a case-sensitive string of 1 to 31 characters.

vlan-id: Specifies a VLAN ID in the range of 1 to 4094.

Usage guidelines

You can configure multiple NAS-ID and VLAN bindings in a NAS-ID profile.

A NAS-ID can be bound with more than one VLAN, but a VLAN can be bound with only one NAS-ID. If you configure multiple bindings for the same VLAN, the most recent configuration takes effect.

Examples

Bind NAS-ID 222 with VLAN 2 in NAS-ID profile **aaa**.

```
<Sysname> system-view
[Sysname] aaa nas-id profile aaa
[Sysname-nas-id-prof-aaa] nas-id 222 bind vlan 2
```

Related commands

aaa nas-id profile

service-type (ISP domain view)

Use **service-type** to specify the service type for users in an ISP domain.

Use **undo service-type** to restore the default.

Syntax

service-type { **hsi** | **stb** | **voip** }

undo service-type

Default

The service type is **hsi** for users in an ISP domain.

Views

ISP domain view

Predefined user roles

network-admin

context-admin

Parameters

hsi: Specifies the High Speed Internet (HSI) service. This service is applicable to users that access the network through PPP or leased IPoE.

stb: Specifies the Set Top Box (STB) service. This service is applicable to users that access the network through STB.

voip: Specifies the Voice over IP (VoIP) service. This service is applicable to users that access the network through IP phones.

Usage guidelines

When the HSI service is specified, the multicast feature of the access module is disabled to save system resources.

When the STB service is specified, the multicast feature of the access module is enabled to improve the performance of the multicast module.

When the VoIP service is specified, the QoS module increases the priority of voice traffic to reduce the transmission delay for IP phone users.

For PPP (excluding PPPoE) users, the system uses the HSI service forcibly even if the STB or VoIP service is specified.

You can configure only one service type for an ISP domain.

Examples

Specify the STB service for users in ISP domain **test**.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] service-type stb
```

session-time include-idle-time

Use **session-time include-idle-time** to configure the device to include the idle timeout period in the user online duration sent to the server.

Use **undo session-time include-idle-time** to restore the default.

Syntax

session-time include-idle-time

undo session-time include-idle-time

Default

The device does not include the idle timeout period in the user online duration sent to the server.

Views

ISP domain view

Predefined user roles

network-admin

context-admin

Usage guidelines

Whether to configure the device to include the idle timeout period in the user online duration sent to the server, depending on the accounting policy in your network. The idle timeout period is assigned to users by the authorization server after the users pass authentication. For portal users, the device includes the idle timeout period set for the online portal user detection feature in the user online duration. For more information about online detection for portal users, see portal authentication configuration in *Security Configuration Guide*.

If the user goes offline due to connection failure or malfunction, the user online duration sent to the server is not the same as the actual online duration.

- If the **session-time include-idle-time** command is used, the user's online duration sent to the server includes the idle timeout period. The online duration that is generated on the server is longer than the actual online duration of the user.
- If the **undo session-time include-idle-time** command is used, the user's online duration sent to the server excludes the idle timeout period. The online duration that is generated on the server is shorter than the actual online duration of the user.

Examples

Configure the device to include the idle timeout period in the online duration sent to the server for users in ISP domain **test**.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] session-time include-idle-time
```

Related commands

display domain

state (ISP domain view)

Use **state** to set the status of an ISP domain.

Use **undo state** to restore the default.

Syntax

state { **active** | **block** }

undo state

Default

An ISP domain is in active state.

Views

ISP domain view

Predefined user roles

network-admin

context-admin

Parameters

active: Places the ISP domain in active state to allow the users in the ISP domain to request network services.

block: Places the ISP domain in blocked state to prevent users in the ISP domain from requesting network services.

Usage guidelines

By blocking an ISP domain, you disable offline users of the domain from requesting network services. However, the online users are not affected.

Examples

Place ISP domain **test** in blocked state.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] state block
```

Related commands

display domain

user-address-type

Use **user-address-type** to specify the user address type in the ISP domain.

Use **undo user-address-type** to restore the default.

Syntax

user-address-type { **ds-lite** | **ipv6** | **nat64** | **private-ds** | **private-ipv4** | **public-ds** | **public-ipv4** }

undo user-address-type

Default

No user address type is specified for the ISP domain.

Views

ISP domain view

Predefined user roles

network-admin

context-admin

Parameters

ds-lite: Specifies the DS-Lite address type.

ipv6: Specifies the IPv6 address type.

nat64: Specifies the NAT64 address type.

private-ds: Specifies the private-DS address type.

private-ipv4: Specifies the private IPv4 address type.

public-ds: Specifies the public-DS address type.

public-ipv4: Specifies the public IPv4 address type.

Usage guidelines

Any change to the user address type does not affect online users.

Examples

Specify the private IPv4 address type for users in ISP domain **test**.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] user-address-type private-ipv4
```

Related commands

display domain

Local user commands

access-limit

Use **access-limit** to set the maximum number of concurrent logins using the local user name.

Use **undo access-limit** to restore the default.

Syntax

access-limit *max-user-number*

undo access-limit

Default

The number of concurrent logins using the local user name is not limited.

Views

Local user view

Predefined user roles

network-admin

context-admin

Parameters

max-user-number: Specifies the maximum number of concurrent logins, in the range of 1 to 1024.

Usage guidelines

This command takes effect only when local accounting is configured for the local user.

The command does not apply to FTP, SFTP, or SCP users. These users do not support accounting.

For this command to take effect on network access users, you also need to execute the **accounting start-fail offline** command in the ISP domain view.

Examples

Set the maximum number of concurrent logins to 5 for users using the local user name **abc**.

```
<Sysname> system-view
[Sysname] local-user abc
[Sysname-luser-manage-abc] access-limit 5
```

Related commands

display local-user

access-user email authentication

Use **access-user email authentication** to specify the username and password used to log in to the SMTP server that sends email notifications to network access users.

Use **undo access-user email authentication** to restore the default.

Syntax

access-user email authentication username *user-name* **password** { **cipher** | **simple** } *string*

undo access-user email authentication

Default

No SMTP server username or password is specified.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

username *user-name*: Specifies the username, a case-sensitive string of 1 to 63 characters.

password: Specifies the password.

cipher: Specifies the password in encrypted form.

simple: Specifies the password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password string. Its plaintext form is a case-sensitive string of 1 to 63 characters. Its encrypted form is a case-sensitive string of 1 to 117 characters.

Usage guidelines

If the SMTP server requires a username and password for login, you must use this command to specify the username and password on the device.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the username to **abc** and the password to **123** for logging in to the SMTP server that sends email notifications to network access users.

```
<Sysname> system-view
[Sysname] access-user email authentication username abc password simple 123
```

Related commands

access-user email format

access-user email sender

access-user email smtp-server

access-user email format

Use **access-user email format** to configure the subject and body for the email notifications to send to network access users.

Use **undo access-user email format** to restore the default.

Syntax

access-user email format { **body** *body-string* | **subject** *sub-string* }

undo access-user email format { **body** | **subject** }

Default

The email subject is **Password reset notification**.

The email body is as follows:

```
A random password has been generated for your account.
Username: xxx
Password: yyy
Validity: YYYY/MM/DD hh:mm:ss to YYYY/MM/DD hh:mm:ss
```

The xxx string represents the username, the yyy string represents the password, and the YYYY/MM/DD hh:mm:ss to YYYY/MM/DD hh:mm:ss string represents the validity period.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

body *body-string*: Configures the body content. The *body-string* argument is a case-sensitive string of 1 to 255 characters.

subject *sub-string*: Configures the email subject. The *sub-string* argument is a case-sensitive string of 1 to 127 characters.

Usage guidelines

You can configure the device to generate a random password for a network access user on the Web interface. The random password is sent to the user by email. Use this command to configure the email subject and body content.

The email body includes the string configured by using the *body-string* argument and the following information:

```
Username: xxx
Password: yyy
Validity: YYYY/MM/DD hh:mm:ss to YYYY/MM/DD hh:mm:ss
```

The xxx string represents the username, the yyy string represents the password, and the YYYY/MM/DD hh:mm:ss to YYYY/MM/DD hh:mm:ss string represents the validity period.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure the subject and body for the email notifications to send to network access users.

```
<Sysname> system-view
[Sysname] access-user email format subject new password setting
[Sysname] access-user email format body The username, password, and validity period of
the account are given below.
```

Related commands

access-user email authentication

access-user email sender

access-user email smtp-server

access-user email sender

Use **access-user email sender** to configure the email sender address in email notifications sent by the device to network access users.

Use **undo access-user email sender** to restore the default.

Syntax

access-user email sender *email-address*

undo access-user email sender

Default

No email sender address is configured for the email notifications sent by the device to network access users.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

email-address: Specifies the email sender address, a case-sensitive string of 1 to 255 characters. The string must contain an at sign (@), and it can contain only one at sign (@). In addition, the string cannot contain only the at sign (@).

Usage guidelines

If you do not specify the email sender address, the device cannot send email notifications to any network access users.

The device supports only one email sender address for network access users. If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the email sender address as **abc@yyy.com** for email notifications of network access users.

```
<Sysname> system-view
[Sysname] access-user email sender abc@yyy.com
```

Related commands

access-user email authentication

access-user email format

access-user email smtp-server

access-user email smtp-server

Use **access-user email smtp-server** to specify an SMTP server to send email notifications of network access users.

Use **undo access-user email smtp-server** to restore the default.

Syntax

access-user email smtp-server *url-string*

undo access-user email smtp-server

Default

No SMTP server is specified to send email notifications of network access users.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

url-string: Specifies the path of the SMTP server, a case-sensitive string of 1 to 255 characters. The path must comply with the standard SMTP protocol and start with **smtp://**.

Usage guidelines

You can specify only one SMTP server to send email notifications of network access users.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the SMTP server at **smtp://www.test.com/smtp** to send email notifications of network access users.

```
<Sysname> system-view
[Sysname] access-user email smtp-server smtp://www.test.com/smtp
```

Related commands

access-user email authentication

access-user email format

access-user email sender

authorization-attribute (local user view/user group view)

Use **authorization-attribute** to configure authorization attributes for a local user or user group. After the local user or a local user in the user group passes authentication, the device assigns these attributes to the user.

Use **undo authorization-attribute** to restore the default of an authorization attribute.

Syntax

authorization-attribute { **acl** *acl-number* | **callback-number** *callback-number* | **idle-cut** *minutes* | **ip** *ipv4-address* | **ip-pool** *ipv4-pool-name* | **ipv6** *ipv6-address* | **ipv6-pool** *ipv6-pool-name* | **ipv6-prefix** *ipv6-prefix prefix-length* | { **primary-dns** | **secondary-dns** } { **ip** *ipv4-address* | **ipv6** *ipv6-address* } | **session-timeout** *minutes* | **sslvpn-policy-group** *group-name* | **url** *url-string* | **user-role** *role-name* | **vlan** *vlan-id* | **vpn-instance** *vpn-instance-name* | **work-directory** *directory-name* } *

undo authorization-attribute { **acl** | **callback-number** | **idle-cut** | **ip** | **ip-pool** | **ipv6** | **ipv6-pool** | **ipv6-prefix** | **primary-dns** | **secondary-dns**| **session-timeout** | **sslvpn-policy-group** | **url** | **user-role** *role-name* | **vlan** | **vpn-instance** | **work-directory** } *

Default

The working directory for FTP, SFTP, and SCP users is the root directory of the NAS. However, the users do not have permission to access the root directory.

The local users created by a network-admin or level-15 user on the default context are assigned the network-operator user role. The local users created by a context-admin or level-15 user on a non-default context are assigned the context-operator user role.

Views

Local user view

User group view

Predefined user roles

network-admin

context-admin

Parameters

acl *acl-number*: Specifies an authorization ACL. The value range for the *acl-number* argument is 2000 to 5999. The device processes the traffic that matches the rules in the authorization ACL based on the permit or deny statement in the rules.

callback-number *callback-number*: Specifies an authorized PPP callback number. The *callback-number* argument is a case-sensitive string of 1 to 64 characters. After a local user passes authentication, the device uses this number to call the user.

idle-cut *minutes*: Specifies an idle timeout period in minutes. The value range for the *minutes* argument is 1 to 120. An online user is logged out if its idle period exceeds the specified idle timeout period.

ip *ipv4-address*: Assigns a static IPv4 address to the user after it passes authentication. You can specify this option only in local user view. This option is not supported in user group view.

ip-pool *ipv4-pool-name*: Specifies an IPv4 address pool for the user. The *ipv4-pool-name* argument is a case-insensitive string of 1 to 63 characters.

ipv6 *ipv6-address*: Assigns a static IPv6 address to the user after it passes authentication. You can specify this option only in local user view. This option is not supported in user group view.

ipv6-pool *ipv6-pool-name*: Specifies an IPv6 address pool for the user. The *ipv6-pool-name* argument is a case-insensitive string of 1 to 63 characters.

ipv6-prefix *ipv6-prefix prefix-length*: Specifies an IPv6 prefix for the user. The value range for the *prefix-length* argument is 1 to 128. The IPv6 prefix cannot be ::/128, ::1/128, or an IPv6 multicast prefix. After passing authentication, a local user can use the IPv6 prefix.

primary-dns ip *ipv4-address*: Specifies the IPv4 address of the primary DNS server for the user.

primary-dns ipv6 *ipv6-address*: Specifies the IPv6 address of the primary DNS server for the user.

secondary-dns ip *ipv4-address*: Specifies the IPv4 address of the secondary DNS server for the user.

secondary-dns ipv6 *ipv6-address*: Specifies the IPv6 address of the secondary DNS server for the user.

session-timeout *minutes*: Specifies the session timeout timer for the user, in minutes. The value range for the *minutes* argument is 1 to 1440. The device logs off the user after the timer expires.

sslvpn-policy-group *group-name*: Specifies an SSL VPN policy group for the user. The *group-name* argument is a case-insensitive string of 1 to 31 characters. For information about SSL VPN policy groups, see *Security Configuration Guide*.

url *url-string*: Specifies a redirect URL. The *url-string* argument is a case-sensitive string of 1 to 255 characters. The URL must start with **http://** or **https://**. You can configure the redirect URL attribute to push advertisements or notifications to users after the users pass authentication or push bill overdue notifications to users. This option is applicable only to IPoE and LAN users. For IPoE users, you must specify a URL with port number 80 or 443.

user-role *role-name*: Specifies an authorized user role. The *role-name* argument is a case-sensitive string of 1 to 63 characters. A maximum of 64 user roles can be specified for a user. For user role-related commands, see *Fundamentals Command Reference* for RBAC commands. This option is available only in local user view, and is not available in user group view.

vlan *vlan-id*: Specifies an authorized VLAN. The value range for the *vlan-id* argument is 1 to 4094. After passing authentication and being authorized a VLAN, a local user can access only the resources in this VLAN.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance to which the user belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. After passing authentication, the user has permission to access the network resources in the specified VPN.

work-directory *directory-name*: Specifies the working directory for FTP, SFTP, or SCP users. The *directory-name* argument is a case-insensitive string of 1 to 255 characters. The directory must already exist.

Usage guidelines

Configure authorization attributes according to the application environments and purposes. Support for authorization attributes depends on the service types of users.

For PPP users, only the following authorization attributes take effect: **callback-number**, **idle-cut**, **ip**, **ip-pool**, **ipv6-pool**, **ipv6-prefix**, **primary-dns**, **secondary-dns**, **vpn-instance**, and **session-timeout**.

For IPoE users, only the following authorization attributes take effect: **idle-cut**, **ip-pool**, **ipv6-pool**, **ipv6-prefix**, **url**, **user-profile**, **vpn-instance**, **primary-dns**, **secondary-dns**, and **session-timeout**.

For portal users, only the following authorization attributes take effect: **idle-cut**, **acl**, **ip-pool**, **ipv6-pool**, **vpn-instance**, and **session-timeout**.

For SSH, Telnet, and terminal users, only the **user-role** authorization attribute takes effect.

For HTTP and HTTPS users, only the authorization attribute **user-role** takes effect.

For FTP users, only the authorization attributes **user-role** and **work-directory** take effect.

For SSL VPN users, only the authorization attribute **sslvpn-policy-group** takes effect.

For IKE users, only the authorization attribute **ip-pool** takes effect.

For other types of local users, no authorization attribute takes effect.

Authorization attributes configured for a user group are intended for all local users in the group. You can group local users to improve configuration and management efficiency. An authorization attribute configured in local user view takes precedence over the same attribute configured in user group view.

When you specify an authorized ACL, follow these restrictions and guidelines:

- If the specified ACL does not exist or the ACL does not contain any rules, the system considers that no ACL is specified. If the strict check method is enabled for portal authorized ACLs, the system logs off portal users.

- For portal users to come online after passing authentication, make sure ACLs assigned to them do not have rules specified with a source IP or MAC address.

To make sure FTP, SFTP, and SCP users can access the directory after an IRF master/subordinate switchover, do not specify slot information for the working directory.

To make sure the user have only the user roles authorized by using this command, use the **undo authorization-attribute user-role** command to remove the default user role.

The security-audit user role has access to the commands for managing security log files and security log file system. To display all the accessible commands of the security-audit user role, use the **display role name security-audit** command. For more information about security log management, see information center configuration in *Network Management and Monitoring Configuration Guide*. For more information about file system management, see *Fundamentals Configuration Guide*.

You cannot delete a local user if the local user is the only user that has the security-audit user role.

The security-audit user role is mutually exclusive with other user roles.

The users assigned with the system-admin, security-admin, or audit-admin user role have access to specific Web pages and the **ping** and **tracert** commands. For more information about the access permissions of these user roles, see RBAC in *Fundamentals Configuration Guide*.

The system-admin, security-admin, and audit-admin user roles are mutually exclusive in a user account. In addition, these user roles are mutually exclusive with other user roles in a user account.

When you assign user roles to a user, the system prompts you to confirm the deletion of the user roles that are mutually exclusive with the new user roles.

Examples

Configure the authorized VLAN of network access user **abc** as VLAN 2.

```
<Sysname> system-view
[Sysname] local-user abc class network
[Sysname-luser-network-abc] authorization-attribute vlan 2
```

Configure the authorized VLAN of user group **abc** as VLAN 3.

```
<Sysname> system-view
[Sysname] user-group abc
[Sysname-ugroup-abc] authorization-attribute vlan 3
```

Assign the **security-audit** user role to device management user **xyz** as the authorized user role.

```
<Sysname> system-view
[Sysname] local-user xyz class manage
[Sysname-luser-manage-xyz] authorization-attribute user-role security-audit
This operation will delete all other roles of the user. Are you sure? [Y/N]:y
```

Related commands

display local-user

display user-group

bind-attribute

Use **bind-attribute** to configure binding attributes for a local user.

Use **undo bind-attribute** to remove binding attributes of a local user.

Syntax

bind-attribute { **call-number** *call-number* [**:** *subcall-number*] | **location interface** *interface-type interface-number* | **mac** *mac-address* | **vlan** *vlan-id* } *

undo bind-attribute { **call-number** | **location** | **mac** | **vlan** } *

Default

No binding attributes are configured for a local user.

Views

Local user view

Predefined user roles

network-admin

context-admin

Parameters

call-number *call-number*: Specifies a calling number for PPP user authentication. The *call-number* argument is a string of 1 to 64 characters. This option applies only to PPP users.

subcall-number: Specifies the subcalling number. The total length of the calling number and the subcalling number cannot be more than 62 characters.

location interface *interface-type interface-number*: Specifies the interface to which the user is bound. The *interface-type* argument represents the interface type, and the *interface-number* argument represents the interface number. To pass authentication, the user must access the network through the bound interface. This option applies only to LAN, PPP, IPoE, and portal users.

mac *mac-address*: Specifies the MAC address of the user in the format H-H-H. This option applies only to SSL VPN users that log in through iNode clients, LAN users, PPP users, IPoE users, and portal users.

vlan *vlan-id*: Specifies the VLAN to which the user belongs. The *vlan-id* argument is in the range of 1 to 4094. This option applies only to LAN, PPP, IPoE, and portal users.

Usage guidelines

To perform local authentication of a user, the device matches the actual user attributes with the configured binding attributes. If the user has a non-matching attribute or lacks a required attribute, the user will fail authentication.

Binding attribute check takes effect on all access services. Configure the binding attributes for a user based on the access services and make sure the device can obtain all attributes to be checked from the user's packet.

The binding interface type must meet the requirements of the local user. Configure the binding interface based on the service type of the user. If the user is a portal user, specify the portal-enabled interface. Specify the Layer 2 Ethernet interface if portal is enabled on a VLAN interface and the **portal roaming enable** command is not configured.

Examples

Bind MAC address 11-11-11 with network access user **abc**.

```
<Sysname> system-view
[Sysname] local-user abc class network
[Sysname-luser-network-abc] bind-attribute mac 11-11-11
```

Related commands

display local-user

company

Use **company** to specify the company of a local guest.

Use **undo company** to restore the default.

Syntax

company *company-name*

undo company

Default

No company is specified for a local guest.

Views

Local guest view

Predefined user roles

network-admin

context-admin

Parameters

company-name: Specifies the company name, a case-sensitive string of 1 to 255 characters.

Examples

Specify company **yyy** for local guest **abc**.

```
<Sysname> system-view
[Sysname] local-user abc class network guest
[Sysname-luser-network(guest)-abc] company yyy
```

Related commands

display local-user

description

Use **description** to configure a description for a network access user.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

No description is configured for a network access user.

Views

Network access user view

Predefined user roles

network-admin

context-admin

Parameters

text: Configures a description, case-sensitive string of 1 to 127 characters.

Usage guidelines

To mark a network access user for special displaying or management purposes in the Web interface, configure description **#user_from_server#** for the user. The purposes depend on the implementation of the Web interface.

Examples

Configure a description for network access user **123**.

```
<Sysname> system-view
[Sysname] local-user 123 class network
[Sysname-luser-network-123] description Manager of MSC company
```

Related commands

display local-user

display local-guest waiting-approval

Use **display local-guest waiting-approval** to display pending registration requests for local guests.

Syntax

display local-guest waiting-approval [**user-name** *user-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

user-name *user-name*: Specifies a local guest by its username, a string of 1 to 55 characters. If you do not specify a guest, this command displays pending registration requests for all local guests. The username can contain a domain name or not.

- If the username does not contain an at sign (@), all characters in the username string are case sensitive. The device parses the username as a pure username. The username cannot be **a**, **al**, or **all**, and it cannot contain a forward slash (/), backslash (\), vertical bar (|), colon (:), asterisk (*), question mark (?), left angle bracket (<), or right angle bracket (>).
- If the username contains an at sign (@), it must be in the format of xxx@yyy. The at sign (@) is the delimiter between the pure username and the domain name.
  - The xxx part is case sensitive. It cannot contain a forward slash (/), backslash (\), vertical bar (|), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or at sign (@), and cannot be **a**, **al**, or **all**.
  - The yyy part is case insensitive and cannot contain an at sign (@).

Usage guidelines

On the Web registration page, users submit local guest registration requests for approval. The guest manager can add supplementary information to the guest accounts and approves the requests. The device then creates local guest accounts based on the approved requests.

Examples

Display all pending registration requests for local guests.

```
<Sysname> display local-guest waiting-approval
Total 1 guest informations matched.

Guest user Smith:
  Full name  : Smith Li
  Company    : YYY
  Email      : Smith@yyy.com
  Phone      : 139189301033
  Description: The employee of YYY company
```

Table 3 Command output

Field	Description
Total 1 guest informations matched.	Number of local guests that have pending registration requests.
Full name	Full name of the local guest.
Company	Company name of the local guest.
Email	Email address of the local guest.
Phone	Phone number of the local guest.
Description	Description of the local guest.

Related commands

reset local-guest waiting-approval

display local-user

Use **display local-user** to display the local user configuration and online user statistics.

Syntax

display local-user [**class** { **manage** | **network** [**guest**] } | **idle-cut** { **disable** | **enable** } | **service-type** { **advpn** | **ftp** | **http** | **https** | **ike** | **ipoe** | **lan-access** | **portal** | **ppp** | **ssh** | **sslvpn** | **telnet** | **terminal** } | **state** { **active** | **block** } | **user-name** *user-name* **class** { **manage** | **network** [**guest**] } | **vlan** *vlan-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

class: Specifies the local user type.

manage: Device management user.

network: Network access user.

guest: Guest user account.

idle-cut { **disable** | **enable** }: Specifies local users by the status of the idle cut feature.

service-type: Specifies the local users that use a specific type of service.

advpn: ADVPN tunnel users.

ftp: FTP users.

http: HTTP users.

https: HTTPS users.

ike: IKE users that access the network through IKE extended authentication.

ipoe: IPoE users that access the network through Layer 2 or Layer 3 leased lines or STBs.

lan-access: LAN users that typically access the LAN network.

portal: Portal users.

ppp: PPP users.

ssh: SSH users.

sslvpn: SSL VPN users.

telnet: Telnet users.

terminal: Terminal users that log in through console ports.

state { **active** | **block** }: Specifies local users in active or blocked state. A local user in active state can access network services, but a local user in blocked state cannot.

user-name *user-name*: Specifies all local users using the specified username. The username must be a string of 1 to 55 characters, which can be a pure username or a username containing a domain name.

- If the username does not contain an at sign (@), all characters in the username string are case sensitive. The device parses the username as a pure username. The username cannot be **a**, **al**, or **all**, and it cannot contain a forward slash (/), backslash (\), vertical bar (|), colon (:), asterisk (*), question mark (?), left angle bracket (<), or right angle bracket (>).
- If the username contains an at sign (@), it must be in the format of xxx@yyy. The at sign (@) is the delimiter between the pure username and the domain name.
  - The xxx part is case sensitive. It cannot contain a forward slash (/), backslash (\), vertical bar (|), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or at sign (@), and cannot be **a**, **al**, or **all**.
  - The yyy part is case insensitive and cannot contain an at sign (@).

vlan *vlan-id*: Specifies all local users in a VLAN. The *vlan-id* argument is in the range of 1 to 4094.

Usage guidelines

If you do not specify any parameters, this command displays information about all local users.

Examples

Display information about all local users.

```
<Sysname> display local-user
Device management user root:
  State:                     Active
  Service type:              SSH/Telnet/Terminal
  Access limit:              Enabled           Max access number: 3
  Current access number:     1
```

```
  User group:                system
  Bind attributes:
  Authorization attributes:
    Work directory:          flash:
    User role list:          network-admin
  Password control configurations:
    Password aging:          3 days
  Password history was last reset: 0 days ago
Network access user jj:
  State:                     Active
  Service type:              SSL VPN
  User group:                system
  Bind attributes:
    Location bound:          GigabitEthernet1/0/1
    MAC address:             0001-0001-0001
    VLAN ID:                 2
  Authorization attributes:
    Idle timeout:            33 minutes
    Work directory:          flash:
    ACL number:              2000
    User role list:          network-operator, level-0, level-3
    SSL VPN policy group:    spg
  Description:               A network access user
  Validity period:
    Start date and time:     2016/01/01-00:01:01
    Expiration date and time:2019/12/01-01:01:01
  Password control configurations:
    Password length:         4 characters
 Network access guest user user1:
  State:                     Active
  Service type:              Portal
  User group:                guest1
  Full name:                 Jack
  Company:                   cc
  Email:                     Jack@cc.com
  Phone:                     131129237
  Description:               A guest from company cc
  Sponsor full name:         Sam
  Sponsor department:        security
  Sponsor email:             Sam@aa.com
  Description:               A guest from company cc
  Validity period:
    Start date and time:     2016/04/01-08:00:00
    Expiration date and time:2019/12/03-18:00:00
Total 3 local users matched.
```

Table 4 Command output

Field	Description
State	Status of the local user: active or blocked.
Service type	Service types that the local user can use.
Access limit	Whether the concurrent login limit is enabled.
Max access number	Maximum number of concurrent logins using the local user name.
Current access number	Current number of concurrent logins using the local user name.
User group	Group to which the local user belongs.
Bind attributes	Binding attributes of the local user.
Location bound	Binding port of the local user.
MAC address	MAC address of the local user.
VLAN ID	Binding VLAN of the local user.
Authorization attributes	Authorization attributes of the local user.
Idle timeout	Idle timeout period of the user, in minutes.
Session-timeout	Session timeout timer for the user, in minutes.
Callback number	Authorized PPP callback number of the local user.
Work directory	Directory that the FTP, SFTP, or SCP user can access.
ACL number	Authorization ACL of the local user.
VLAN ID	Authorized VLAN of the local user.
User role list	Authorized roles of the local user.
IP pool	IPv4 address pool authorized to the local user.
SSL VPN policy group	SSL VPN policy group authorized to the local user.
IP address	IPv4 address authorized to the local user.
IPv6 address	IPv6 address authorized to the local user.
IPv6 prefix	IPv6 address prefix authorized to the local user.
IPv6 pool	IPv6 address pool authorized to the local user.
Primary DNS server	IPv4 address of the primary DNS server for the local user.
Secondary DNS server	IPv4 address of the secondary DNS server for the local user.
Primary DNSV6 server	IPv6 address of the primary DNS server for the local user.
Secondary DNSV6 server	IPv6 address of the secondary DNS server for the local user.
URL	Authorization PADM URL for the local user.
VPN instance	Authorization VPN instance for the local user.
Password control configurations	Password control attributes that are configured for the local user. Non-default vSystems do not support this field.
Password aging	Password expiration time. Non-default vSystems do not support this field.
Password length	Minimum number of characters that a password must contain. Non-default vSystems do not support this field.

Field	Description
Password composition	Password composition policy: • Minimum number of character types that a password must contain. • Minimum number of characters from each type in a password. Non-default vSystems do not support this field.
Password complexity	Password complexity checking policy: • Reject a password that contains the username or the reverse of the username. • Reject a password that contains any character repeated consecutively three or more times. Non-default vSystems do not support this field.
Maximum login attempts	Maximum number of consecutive failed login attempts. Non-default vSystems do not support this field.
Action for exceeding login attempts	Action to take on the user that failed to log in after using up all login attempts. Non-default vSystems do not support this field.
Password history was last reset	The most recent time that the history password records were cleared. Non-default vSystems do not support this field.
Full name	Name of the local guest.
Company	Company name of the local guest.
Email	Email address of the local guest.
Phone	Phone number of the local guest.
Sponsor full name	Name of the guest sponsor.
Sponsor department	Department of the guest sponsor.
Sponsor email	Email address of the guest sponsor.
Description	Description of the network access user.
Period of validity	Validity period of the network access user.
Start date and time	Date and time from which the network access user begins to take effect.
Expiration date and time	Date and time at which the network access user expires.

display user-group

Use **display user-group** to display user group configuration.

Syntax

display user-group { **all** | **name** *group-name* } [**identity-member** { **all** | **group** | **user** }]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

all: Specifies all user groups.

name *group-name*: Specifies a user group by its name, a case-insensitive string of 1 to 32 characters.

identity-member { **all** | **group** | **user** }: Specifies identity members in the specified user group or all user groups. If you do not specify these keywords, the command does not display identity member information.

all: Specifies all identity members, including identity users and identity groups.

group: Specifies identity groups.

user: Specifies identity users.

Examples

Display the configuration of all user groups.

```
<Sysname> display user-group all
Total 2 user groups matched.

User group: system
  Authorization attributes:
    Work directory:          flash:
User group: jj
  Authorization attributes:
    Idle timeout:            2 minutes
    Callback number:         2:2
    Work directory:          flash:/
    ACL number:              2000
    VLAN ID:                 2
    SSL VPN policy group:    policygroup1
  Password control configurations:
    Password aging:          2 days
```

Display information about all identity members for all user groups.

```
<Sysname> display user-group all identity-member all
Total 2 user groups matched.

User group: system
  Identity groups: 0
User group: jj
  Identity groups: 2
  Group ID        Group name
  0xffffffff      group1
  0x567           group2
  Identity users: 2
  User ID         Username
  0x234           user1
```

```
0xffffffff      user2
```

Table 5 Command output

Field	Description
User group	User group name.
Authorization attributes	Authorization attributes of the user group.
Idle timeout	Idle timeout period, in minutes.
Session-timeout	Session timeout timer, in minutes.
Callback number	Authorized PPP callback number.
Work directory	Directory that FTP, SFTP, or SCP users in the group can access.
ACL number	Authorization ACL.
VLAN ID	Authorized VLAN.
IP pool	IPv4 address pool authorized to the user group.
SSL VPN policy group	SSL VPN policy group authorized to the user group.
IPv6 prefix	IPv6 address prefix authorized to the user group.
IPv6 pool	IPv6 address pool authorized to the user group.
Primary DNS server	IPv4 address of the primary DNS server authorized to the user group.
Secondary DNS server	IPv4 address of the secondary DNS server authorized to the user group.
Primary DNSV6 server	IPv6 address of the primary DNS server authorized to the user group.
Secondary DNSV6 server	IPv6 address of the secondary DNS server authorized to the user group.
URL	Authorization PADM URL for the user group.
VPN instance	Authorization VPN instance for the user group.
Password control configurations	Password control attributes that are configured for the user group.
Password aging	Password expiration time.
Password length	Minimum number of characters that a password must contain.
Password composition	Password composition policy: • Minimum number of character types that a password must contain. • Minimum number of characters from each type in a password.
Password complexity	Password complexity checking policy: • Reject a password that contains the username or the reverse of the username. • Reject a password that contains any character repeated consecutively three or more times.
Maximum login attempts	Maximum number of consecutive failed login attempts.
Action for exceeding login attempts	Action to take on the user that failed to log in after using up all login attempts.
Identity users	Number of identity users.
Identity groups	Number of identity groups.
User ID	Identity user ID.

Field	Description
Group ID	Identity group ID.
Username	Identity user name.
Group name	Identity group name.

email

Use **email** to configure an email address for a local guest.

Use **undo email** to restore the default.

Syntax

email *email-string*

undo email

Default

No email address is configured for a local guest.

Views

Local guest view

Predefined user roles

network-admin

context-admin

Parameters

email-string: Specifies the email address for the local guest, a case-sensitive string of 1 to 255 characters. The string must contain an at sign (@), and it can contain only one at sign (@). In addition, the string cannot contain only the at sign (@).

Usage guidelines

The local guest uses the email address to receive notifications from the device.

Examples

Configure the email address as **abc@yyy.com** for local guest **abc**.

```
<Sysname> system-view
[Sysname] local-user abc class network guest
[Sysname-luser-network(guest)-abc] email abc@yyy.com
```

Related commands

display local-user

full-name

Use **full-name** to configure the name of a local guest.

Use **undo full-name** to restore the default.

Syntax

full-name *name-string*

undo full-name

Default

No name is configured for a local guest.

Views

Local guest view

Predefined user roles

network-admin

context-admin

Parameters

name-string: Specifies the local guest name, a case-sensitive string of 1 to 255 characters.

Examples

Configure the name as **abc Snow** for local guest **abc**.

```
<Sysname> system-view
[Sysname] local-user abc class network guest
[Sysname-luser-network(guest)-abc] full-name abc Snow
```

Related commands

display local-user

group

Use **group** to assign a local user to a user group.

Use **undo group** to restore the default.

Syntax

group *group-name*

undo group

Default

A local user belongs to user group **system**.

Views

Local user view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies the user group name, a case-insensitive string of 1 to 32 characters.

Examples

Assign device management user **111** to user group **abc**.

```
<Sysname> system-view
[Sysname] local-user 111 class manage
[Sysname-luser-manage-111] group abc
```

Related commands

display local-user

identity-group

Use **identity-group** to add a network access user to an identity group.

Use **undo identity-group** to remove a network access user from identity groups.

Syntax

identity-group *group-name*

undo identity-group [*group-name*]

Default

A network access user does not belong to any identity groups.

Views

Network access user view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies an identity group by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

Add users to an identity group as identity members for centralized management.

A user can belong to multiple identity groups.

After you add a user to an identity group in network access user view, the system automatically synchronizes the configuration to the identity group. Then, the user is available in user group view of the identity group.

If you do not specify a group name, the **undo identity-group** command removes the user from all identity groups.

Examples

Add network access user **user1** to identity group **group1**.

```
<Sysname> system-view
[Sysname] local-user user1 class network
[Sysname-luser-network-user1] identity-group group1
```

Related commands

identity-member

user-group

identity-member

Use **identity-member** to add an identity member to a user group.

Use **undo identity-member** to remove identity members from a user group.

Syntax

identity-member { **group** *group-name* | **user** *user-name* }

undo identity-member { **group** [*group-name*] | **user** [*user-name*] }

Default

No identity members exist in a user group.

Views

User group view

Predefined user roles

network-admin

context-admin

Parameters

group *group-name*: Specifies an identity group by its name, a case-insensitive string of 1 to 32 characters.

user *user-name*: Specifies an identity user by its name, a string of 1 to 55 characters. The username can be a pure username or a username containing a domain name.

- If the username does not contain an at sign (@), all characters in the username string are case sensitive. The device parses the username as a pure username. The username cannot be **a**, **al**, or **all**, and it cannot contain a forward slash (/), backslash (\), vertical bar (|), colon (:), asterisk (*), question mark (?), left angle bracket (<), or right angle bracket (>).
- If the username contains an at sign (@), it must be in the format of xxx@yyy. The at sign (@) is the delimiter between the pure username and the domain name.
  - The xxx part is case sensitive. It cannot contain a forward slash (/), backslash (\), vertical bar (|), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or at sign (@), and cannot be **a**, **al**, or **all**.
  - The yyy part is case insensitive and cannot contain an at sign (@).

Usage guidelines

Assign users or users groups that have the same user identification requirements to the same group.

When you add identity members, follow these restrictions and guidelines:

- You can add network access users as identity members.
- After you add an identity user to an identity group in user group view, the system automatically synchronizes the configuration to the identity user if the user exists. Then, the identity group is available in network access user view of the identity user.
- You cannot add an identity group to a lower-level group that is an identity member of the group.

If you do not specify a user name or group name, the **undo identity-member** command removes all identity users or groups from the user group.

If an identity group has been specified for a security policy, do not remove member identity groups from the identity group. A violation will cause the truncation of the tree where the identity group resides and further affect user traffic matching of the security policy.

Examples

Add identity user **user1** and identity group **group2** to user group **group1**.

```
<Sysname> system-view
[Sysname] user-group group1
[Sysname-ugroup-group1] identity-member user user1
[Sysname-ugroup-group1] identity-member group group2
```

Related commands

display user-group

identity-group

local-guest auto-delete enable

Use **local-guest auto-delete enable** to enable the guest auto-delete feature.

Use **undo local-guest auto-delete enable** to restore the default.

Syntax

local-guest auto-delete enable

undo local-guest auto-delete enable

Default

The guest auto-delete feature is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This feature enables the device to automatically delete the local guest accounts when they expire.

Examples

Enable the guest auto-delete feature.

```
<Sysname> system-view
[Sysname] local-guest auto-delete enable
```

Related commands

validity-datetime

local-guest email format

Use **local-guest email format** to configure the subject and body for the email notifications of local guest information.

Use **undo local-guest email format** to delete the configured subject or body for the email notifications of local guest information.

Syntax

local-guest email format to { **guest** | **manager** | **sponsor** } { **body** *body-string* | **subject** *sub-string* }

undo local-guest email format to { **guest** | **manager** | **sponsor** } { **body** | **subject** }

Default

No subject or body is configured for the email notifications of local guest information.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

to: Specifies the email recipient.

guest: Specifies the local guest.

manager: Specifies the guest manager.

sponsor: Specifies the guest sponsor.

body *body-string*: Configures the body content. The *body-string* argument is a case-sensitive string of 1 to 255 characters.

subject *sub-string*: Configures the email subject. The *sub-string* argument is a case-sensitive string of 1 to 127 characters.

Usage guidelines

Email notifications need to be sent to notify the local guests, guest sponsors, or guest managers of the guest account information or guest registration requests. Use this command to configure the subject and body for the email notifications to be sent by the device.

You can configure one subject and one body for each email recipient. If you configure the subject or body content multiple times for the same recipient, the most recent configuration takes effect.

You must configure both the subject and body for each recipient.

Examples

Configure the subject and body for the email notifications to send to the local guest.

```
<Sysname> system-view
[Sysname] local-guest email format to guest subject Guest account information
[Sysname] local-guest email format to guest body A guest account has been created for you.
The username, password, and validity period of the account are given below.
```

Related commands

local-guest email sender

local-guest email smtp-server

local-guest manager-email

local-guest send-email

local-guest email sender

Use **local-guest email sender** to configure the email sender address in email notifications of local guests sent by the device.

Use **undo local-guest email sender** to restore the default.

Syntax

local-guest email sender *email-address*

undo local-guest email sender

Default

No email sender address is configured for the email notifications of local guests sent by the device.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

email-address: Specifies the email sender address, a case-sensitive string of 1 to 255 characters. The string must contain an at sign (@), and it can contain only one at sign (@). In addition, the string cannot contain only the at sign (@).

Usage guidelines

If you do not specify the email sender address, the device cannot send email notifications of local guests.

The device supports only one email sender address for local guests. If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the email sender address as **abc@yyy.com** for email notifications of local guests.

```
<Sysname> system-view
[Sysname] local-guest email sender abc@yyy.com
```

Related commands

local-guest email format

local-guest email smtp-server

local-guest manager-email

local-guest send-email

local-guest email smtp-server

Use **local-guest email smtp-server** to specify an SMTP server to send email notifications of local guests.

Use **undo local-guest email smtp-server** to restore the default.

Syntax

local-guest email smtp-server *url-string*

undo local-guest email smtp-server

Default

No SMTP server is specified to send email notifications of local guests.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

url-string: Specifies the path of the SMTP server, a case-sensitive string of 1 to 255 characters. The path must comply with the standard SMTP protocol and start with **smtp://**.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the SMTP server at **smtp://www.test.com/smtp** to send local guest email notifications.

```
<Sysname> system-view
[Sysname] local-guest email smtp-server smtp://www.test.com/smtp
```

Related commands

local-guest email format

local-guest email sender

local-guest manager-email

local-guest send-email

local-guest generate

Use **local-guest generate** to create local guests in batch.

Syntax

local-guest generate username-prefix *name-prefix* [**password-prefix** *password-prefix*] **suffix** *suffix-number* [**group** *group-name*] **count** *user-count* **validity-datetime** *start-date start-time* **to** *expiration-date expiration-time*

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

username-prefix *name-prefix*: Specifies the name prefix. The *name-prefix* argument is a case-sensitive string of 1 to 45 characters. The prefix cannot contain any of the following characters: forward slash (/), backslash (\), vertical bar (|), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), and at sign (@).

password-prefix *password-prefix*: Specifies a prefix for the plaintext password. The *password-prefix* argument is a case-sensitive string of 1 to 53 characters. If you do not specify a password prefix, the device randomly generates passwords for the local guests.

suffix *suffix-number*: Specifies the start suffix number of the username and password. The *suffix-number* argument is a numeric string of 1 to 10 digits.

group *group-name*: Specifies a user group by its name. The *group-name* argument is a case-sensitive string of 1 to 32 characters. If you do not specify a user group, the guests are assigned to the system-defined user group **system**.

count *user-count*: Specifies the number of local guests to be created. The value range for the *user-count* argument is 1 to 256.

validity-datetime: Specifies the validity period of the local guests. The expiration date and time must be later than the start date and time.

start-date: Specifies the start date of the validity period, in the format of MM/DD/YYYY or YYYY/MM/DD. The value range for the MM argument is 1 to 12. The value range for the DD argument varies with the specified month. The value range for the YYYY argument is 2000 to 2035.

start-time: Specifies the start time of the validity period, in the format of hh:mm:ss. The value range for the hh argument is 0 to 23. The value range for the mm and ss arguments is 0 to 59. The mm and ss arguments are optional. For example, enter 1 to indicate 1:00:00. A value of 0 indicates 00:00:00.

to: Specifies the end date and time of the validity period.

expiration-date: Specifies the expiration date in the format of MM/DD/YYYY or YYYY/MM/DD. The value range for the MM argument is 1 to 12. The value range for the DD argument varies with the specified month. The value range for the YYYY argument is 2000 to 2035.

expiration-time: Specifies the expiration time in the format of hh:mm:ss. The value range for the hh argument is 0 to 23. The value range for the mm and ss arguments is 0 to 59. The mm and ss arguments are optional. For example, enter 1 to indicate 1:00:00. A value of 0 indicates 00:00:00.

Usage guidelines

Account names of batch created local guests start with the same string specified by the name prefix, and end with a different number as the suffix. The system increases the start suffix number by 1 for each new local guest created in the batch.

The device generates plaintext passwords by using the password prefix and suffix number in the same way it batch creates the local guest names.

Consider the system resources when you specify the number of local guests to create. The device might fail to create all accounts for a large batch of local guests because of insufficient resources.

If a local guest to be created has the same name as an existing local guest on the device, the new guest overrides the existing guest.

Examples

Create 20 local guests in batch with user names **abc01** through **abc20** for user group **visit**. The user accounts are effective from 2018/10/01 00:00:00 to 2019/10/02 12:00:00.

```
<Sysname> system-view
[Sysname] local-guest generate username-prefix abc suffix 01 group visit count 20
validity-datetime 2018/10/01 00:00:00 to 2019/10/02 12:00:00
```

Related commands

local-user

display local-user

local-guest manager-email

Use **local-guest manager-email** to configure the email address of the guest manager.

Use **undo local-guest manager-email** to restore the default.

Syntax

local-guest manager-email *email-address*

undo local-guest manager-email

Default

No email address is configured for the guest manager.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

email-address: Specifies the email address, a case-sensitive string of 1 to 255 characters. For example, sec@abc.com. The address must comply with RFC 822.

Usage guidelines

Use this command to specify the email address to which the device sends the local guest registration requests for approval.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure the email address of the guest manager as **xyz@yyy.com**.

```
<Sysname> system-view
[Sysname] local-guest manager-email xyz@yyy.com
```

Related commands

local-guest email format

local-guest email sender

local-guest email smtp-server

local-guest send-email

local-guest send-email

Use **local-guest send-email** to send emails to a local guest or guest sponsor.

Syntax

local-guest send-email user-name *user-name* **to** { **guest** | **sponsor** }

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

user-name *user-name*: Specifies a local guest by its username, a string of 1 to 55 characters. The username can be a pure username or a username containing a domain name.

- If the username does not contain an at sign (@), all characters in the username string are case sensitive. The device parses the username as a pure username. The username cannot be **a**, **al**, or **all**, and it cannot contain a forward slash (/), backslash (\), vertical bar (|), colon (:), asterisk (*), question mark (?), left angle bracket (<), or right angle bracket (>).
- If the username contains an at sign (@), it must be in the format of xxx@yyy. The at sign (@) is the delimiter between the pure username and the domain name.
  - The xxx part is case sensitive. It cannot contain a forward slash (/), backslash (\), vertical bar (|), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or at sign (@), and cannot be **a**, **al**, or **all**.
  - The yyy part is case insensitive and cannot contain an at sign (@).

to: Specifies the email recipient.

guest: Specifies the local guest.

sponsor: Specifies the guest sponsor.

Usage guidelines

Guest managers can use this command to inform local guests or guest sponsors of the guest password and validity period information.

Examples

Send an email to notify local guest **abc** of the guest password and validity period information.

```
<Sysname> local-guest send-email user-name abc to guest
```

Related commands

email

sponsor-email

local-guest timer

Use **local-guest timer** to set the waiting-approval timeout timer for local guests.

Syntax

local-guest timer waiting-approval *time-value*

undo local-guest timer waiting-approval

Default

The setting is 24 hours.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

time-value: Specifies the waiting-approval timeout timer in the range of 1 to 720, in hours.

Usage guidelines

The waiting-approval timeout timer starts when the registration request of a local guest is sent for approval. If the request is not approved within the timer, the device deletes the registration request.

Examples

Set the waiting-approval timeout timer to 12 hours.

```
<Sysname> system-view
[Sysname] local-guest timer waiting-approval 12
```

local-user

Use **local-user** to add a local user and enter its view, or enter the view of an existing local user.

Use **undo local-user** to delete local users.

Syntax

local-user *user-name* [**class** { **manage** | **network** [**guest**] }]

undo local-user { *user-name* **class** { **manage** | **network** [**guest**] } | **all** [**service-type** { **advpn** | **ftp** | **http** | **https** | **ike** | **ipoe** | **portal** | **ppp** | **ssh** | **sslvpn** | **telnet** | **terminal** } | **class** { **manage** | **network** [**guest**] }] }

Default

No local users exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

user-name: Specifies the local user name, a string of 1 to 55 characters. The username can be a pure username or a username containing a domain name.

- If the username does not contain an at sign (@), all characters in the username string are case sensitive. The device parses the username as a pure username. The username cannot be **a**, **al**, or **all**, and it cannot contain a forward slash (/), backslash (\), vertical bar (|), colon (:), asterisk (*), question mark (?), left angle bracket (<), or right angle bracket (>).
- If the username contains an at sign (@), it must be in the format of xxx@yyy. The at sign (@) is the delimiter between the pure username and the domain name.
  - The xxx part is case sensitive. It cannot contain a forward slash (/), backslash (\), vertical bar (|), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or at sign (@), and cannot be **a**, **al**, or **all**.
  - The yyy part is case insensitive and cannot contain an at sign (@).

class: Specifies the local user type. If you do not specify this keyword, the command adds a device management user.

manage: Device management user that can configure and monitor the device after login. Device management users can use FTP, HTTP, HTTPS, Telnet, SSH, and terminal services.

network: Network access user that accesses network resources through the device. Network access users can use ADVPN, IKE, IPoE, LAN access, portal, PPP, and SSL VPN services.

guest: Guest that can access network resources through the device during a specific validity period. Guests can use portal service.

all: Specifies all users.

service-type: Specifies the local users that use a specific type of service.

advpn: ADVPN tunnel users.

ftp: FTP users.

http: HTTP users.

https: HTTPS users.

ike: IKE users that access the network through IKE extended authentication.

ipoe: IPoE users that access the network through Layer 2 or Layer 3 leased lines or STBs.

portal: Portal users.

ppp: PPP users.

ssh: SSH users.

sslvpn: SSL VPN users.

telnet: Telnet users.

terminal: Terminal users that log in through console ports.

Usage guidelines

In local authentication, a username and user type uniquely identifiy a local user. The username is used to match the pure username parsed from the username entered by the user. The user type restricts the service types that can be used by the user.

In the current software version, only the pure username of an SSL VPN user can contain an at sign (@).

The device supports multiple local users. The maximum number of device management users varies by device model. The maximum number of network access users varies by device model.

If the local username contains Chinese characters, make sure the endpoint software used at device login uses the same character set encoding format as the encoding format (GB18030) used by the device to save local user configuration. If they use different encoding formats, the username cannot be correctly decoded on the device, which might cause local authentication failure.

Examples

Add a device management user named **user1** and enter local user view.

```
<Sysname> system-view
[Sysname] local-user user1 class manage
[Sysname-luser-manage-user1]
```

Add a network access user named **user2** and enter local user view.

```
<Sysname> system-view
[Sysname] local-user user2 class network
[Sysname-luser-network-user2]
```

Add a local guest named **user3** and enter local guest view.

```
Sysname> system-view
[Sysname] local-user user3 class network guest
[Sysname-luser-network(guest)-user3]
```

Related commands

display local-user

service-type (local user view)

local-user-export class network

Use **local-user-export class network** to export network access user account information from the device to a .csv file in the specified path.

Syntax

local-user-export class network url *url-string* [**from** { **group** *group-name* | **user** *user-name* }]

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

url *url-string*: Specifies the URL of the destination file, a case-insensitive string of 1 to 255 characters.

from: Specifies the range of users to be exported. If you do not specify this keyword, the command exports all network access users on the device.

group *group-name*: Specifies a user group by its name, a case-insensitive string of 1 to 32 characters.

user *user-name*: Specifies a user by its name, a string of 1 to 55 characters. The username can be a pure username or a username containing a domain name.

- If the username does not contain an at sign (@), all characters in the username string are case sensitive. The device parses the username as a pure username. The username cannot be **a**, **al**, or **all**, and it cannot contain a forward slash (/), backslash (\), vertical bar (|), colon (:), asterisk (*), question mark (?), left angle bracket (<), or right angle bracket (>).
- If the username contains an at sign (@), it must be in the format of xxx@yyy. The at sign (@) is the delimiter between the pure username and the domain name.
  - The xxx part is case sensitive. It cannot contain a forward slash (/), backslash (\), vertical bar (|), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or at sign (@), and cannot be **a**, **al**, or **all**.
  - The yyy part is case insensitive and cannot contain an at sign (@).

Usage guidelines

You can import the user account information back to the device or to other devices that support the **local-user-import class network** command. Before the import, you can edit the .csv file as needed. However, you must follow the restrictions in "local-user-import class network."

The device supports TFTP and FTP file transfer modes. Table 6 describes the valid URL formats of the .csv file.

Table 6 URL formats

Protocol	URL format	Description
TFTP	**tftp://***server*/*path*/*filename*	Specify a TFTP server by IP address or hostname. For example, tftp://1.1.1.1/user/user.csv.
FTP	• With FTP user name and password: **ftp://***username*:*password*@*server*/*path*/*filename* • Without FTP user name and password: **ftp://***server*/*path*/*filename*	Specify an FTP server by IP address or hostname. The device ignores the domain name in the FTP user name. For example, specify the file path as **ftp://1:1@1.1.1.1/user/user.csv** or **ftp://1.1.1.1/user/user.csv**.

Examples

Export network access user account information to the **identityuser.csv** file in the **ftp://1.1.1.1/user/** path.

```
<Sysname> system-view
[Sysname] local-user-export class network url ftp://1.1.1.1/user/identityuser.csv
```

Related commands

display local-user

local-user-import class network

local-user-export class network guest

Use **local-user-export class network guest** to export local guest account information to a .csv file in the specified path.

Syntax

local-user-export class network guest url *url-string*

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

url *url-string*: Specifies the URL of the destination file, a case-insensitive string of 1 to 255 characters.

Usage guidelines

You can import the user account information back to the device or to other devices that support the **local-user-import class network guest** command. Before the import, you can edit the .csv file as needed. However, you must follow the restrictions in "local-user-import class network guest."

The device supports TFTP and FTP file transfer modes. Table 7 describes the valid URL formats of the .csv file.

Table 7 URL formats

Protocol	URL format	Description
TFTP	**tftp://***server/path/filename*	Specify a TFTP server by IP address or hostname. For example, specify the file path as **tftp://1.1.1.1/user/user.csv**.
FTP	• With FTP user name and password: **ftp://***username*:*password@server/path/filename* • Without FTP user name and password: **ftp://***server/path/filename*	Specify an FTP server by IP address or hostname. The device ignores the domain name in the FTP user name. For example, specify the file path as **ftp://1:1@1.1.1.1/user/user.csv** or **ftp://1.1.1.1/user/user.csv**.

Examples

Export local guest account information to the **guest.csv** file in the **ftp://1.1.1.1/user/** path.

```
<Sysname> system-view
[Sysname] local-user-export class network guest url ftp://1.1.1.1/user/guest.csv
```

Related commands

display local-user

local-user-import class network guest

local-user-import class network

Use **local-user-import class network** to import user information from a .csv file in the specified path and create network access users based on the imported information.

Syntax

local-user-import class network url *url-string* [**auto-create-group** | **override** | **start-line** *line-number*] *

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

url *url-string*: Specifies the URL of the source file, a case-insensitive string of 1 to 255 characters.

auto-create-group: Enables the device to automatically create user groups for the imported network access users if the groups do not exist on the device. If you do not specify this keyword, the device ignores the nonexistent user groups of the network access users and assigns them to the predefined user group **system**.

override: Specifies the device to override the existing account with the same name as a user account to be imported. If you do not specify this keyword, the device retains the existing account information.

start-line *line-number*: Specifies the number of the line at which the account import begins. If you do not specify this option, the command imports information about all user accounts in the file.

Usage guidelines

The .csv file contains multiple parameters for each account and the parameters must be strictly arranged in the following order:

- **Username**—Username of an account. This parameter is required for each user account. The username is a case-sensitive string of 1 to 55 characters. The name cannot be **a**, **al**, or **all**. It cannot contain a forward slash (/), backslash (\), vertical bar (|), colon (:), asterisk (*), question mark (?), left angle bracket (<), or right angle bracket (>). If the username of an account contains an invalid character, the import process interrupts.
- **Password form**—Plaintext or encrypted form. By default, a password is in encrypted form.
- **Password**—Password of an account. A password in encrypted form is a case-sensitive string of 1 to 117 characters. A password in plaintext form is a case-sensitive string of 1 to 63 characters. If the device fails to parse the password or the password is empty, the device imports the account without a password.
- **Authorization user group**—User group to which a user belongs after the user passes local authentication. The group name is a case-insensitive string of 1 to 32 characters. If the parameter is empty, the device assigns the user to the system-defined user group **system**.
- **Identity groups**—Groups for identity-based access control. A user can belong to multiple identity groups. An identity group name is a case-insensitive string of 1 to 32 characters. Separate identity group names by the string of 0x0A. If the parameter is empty for a user, the user does not belong to any identity group.
- **Service types**—Services to assign to the user. Available services include portal, PPP, IPoE, LAN access, ADVPN, SSL VPN, and IKE. A service name is case insensitive. Separate service types by the string of 0x0A. If the parameter is empty for a user, the user cannot use any service.

- **Max concurrent logins**—The maximum number of online users with the same user name. The value range is 1 to 1024. If the parameter is empty, the device does not restrict the number of online users with the same user name.

Separate different accounts by a carriage return and separate each parameter value of the same account by a comma (,). To ensure a successful user information import, make sure no spaces are included in the contents. For example,

```
Jack,$c$3$uM6DH5empTfbsx341Qk/ORGozkbxNE0=,author-group1,parent-group1(0x0A)parent-group2,portal,1024
Mary,$c$3$YpVonswJTN1dVMEev+zu2pgrCIIJ,author-group2,parent-group1(0x0A)parent-group2,portal,800
```

When you edit the .csv file, follow these restrictions and guidelines:

- Start lines with pound signs (#) to contain explanation information for usage guidelines. The device does not import the lines as user account information.
- Separate parameter values by a comma (,). To avoid ambiguity, you must enclose the value of a parameter into single quotation marks (') if the value contains a comma (,). For example, if the authorization user group of a user is named as **author,group**, you must specify the authorization user group name as **'author,group'** in the .csv file.

The device supports TFTP and FTP file transfer modes. Table 8 describes the valid URL formats of the .csv file.

Table 8 URL formats

Protocol	URL format	Description
TFTP	**tftp://***server*/*path*/*filename*	Specify a TFTP server by IP address or hostname. For example, tftp://1.1.1.1/user/user.csv.
FTP	• With FTP user name and password: **ftp://***username*:*password*@*server*/*path*/*filename* • Without FTP user name and password: **ftp://***server*/*path*/*filename*	Specify an FTP server by IP address or hostname. The device ignores the domain name in the FTP user name. For example, specify the file path as **ftp://1:1@1.1.1.1/user/user.csv** or **ftp://1.1.1.1/user/user.csv**.

Examples

Import user account information from the **localuser.csv** file in the **ftp://1.1.1.1/user/** path, and create network access users based on the imported information. Specify the device to ignore the accounts that have the same name as the existing accounts on the device. Enable the device to automatically create the user group of an imported network access user if the user group does not exist on the device.

```
<Sysname> system-view
[Sysname] local-user-import class network url ftp://1.1.1.1/user/localuser.csv auto-create-group
```

Related commands

display local-user

local-user-export class network

local-user-import class network guest

Use **local-user-import class network guest** to import local guest account information from a .csv file in the specified path to the device to create local guests based on the imported information.

Syntax

local-user-import class network guest url *url-string* **validity-datetime** *start-date start-time* **to** *expiration-date expiration-time* [**auto-create-group** | **override** | **start-line** *line-number*] *

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

url *url-string*: Specifies the source file path. The *url-string* argument is a case-insensitive string of 1 to 255 characters.

validity-datetime: Specifies the guest validity period of the local guests. The expiration date and time must be later than the start date and time.

start-date: Specifies the start date of the validity period, in the format of MM/DD/YYYY or YYYY/MM/DD. The value range for the MM argument is 1 to 12. The value range for the DD argument varies with the specified month. The value range for the YYYY argument is 2000 to 2035.

start-time: Specifies the start time of the validity period, in the format of hh:mm:ss. The value range for the hh argument is 0 to 23. The value range for the mm and ss arguments is 0 to 59. The mm and ss arguments are optional. For example, enter 1 to indicate 1:00:00. A value of 0 indicates 00:00:00.

to: Specifies the end date and time of the validity period.

expiration-date: Specifies the expiration date in the format of MM/DD/YYYY or YYYY/MM/DD. The value range for the MM argument is 1 to 12. The value range for the DD argument varies with the specified month. The value range for the YYYY argument is 2000 to 2035.

expiration-time: Specifies the expiration time in the format of hh:mm:ss. The value range for the hh argument is 0 to 23. The value range for the mm and ss arguments is 0 to 59. The mm and ss arguments are optional. For example, enter 1 to indicate 1:00:00. A value of 0 indicates 00:00:00.

auto-create-group: Enables the device to automatically create user groups for the imported local guests if the groups in the imported information do not exist on the device. If you do not specify this keyword, the device adds all imported local guests to the system-defined user group named **system**.

override: Enables the device to override the existing account with the same name as an imported guest account. If you do not specify this keyword, the device retains the existing account and does not import the local guest with the same name.

start-line *line-number*: Specifies the number of the line at which the account import begins. If you do not specify a line number, this command imports all accounts in the .csv file.

Usage guidelines

The .csv file contains multiple parameters for each account and the parameters must be strictly arranged in the following order:

- **Username**—Username of the guest account. The username is required for each guest account. The username cannot contain any of the following characters: forward slash (/), backslash (\), vertical bar (|), colon (:), asterisk (*), question mark (?), left angle bracket (<), or right angle bracket (>). The name cannot be **a**, **al**, or **all**. Any invalid character results in account import failure and interruption.
- **Password**—Password of the guest account in plaintext form. If the password is empty, the device generates a random password in encrypted form for the guest.
- **User group**—User group to which the guest belongs. If the user group is empty, the device assigns the guest to the system-defined user group named **system**.
- **Guest full name**—Name of the guest.
- **Guest company**—Company of the guest.
- **Guest email**—Email address of the guest.
- **Guest phone**—Phone number of the guest.
- **Guest description**—Description of the guest.
- **Sponsor full name**—Name of the guest sponsor.
- **Sponsor department**—Department of the guest sponsor.
- **Sponsor email**—Email address of the guest sponsor.

The value of each parameter in the file must meet the requirements of the local user attributes on the device. Any violation results in account import failure and interruption. The system displays the number of the line where the account import is interrupted.

Separate different account entries by a carriage return and separate each parameter value in an account entry by a comma (,). If the value of a parameter contains a comma (,), you must enclose the value within a pair of quotation marks ("") to avoid ambiguity. For example,

```
Jack,abc,visit,Jack Chen,ETP,jack@etp.com,1399899,"The manager of ETP, come from TP.",Sam Wang,Ministry of personnel,Sam@yy.com
```

The device supports TFTP and FTP file transfer modes. Table 9 describes the valid URL formats of the .csv file.

Table 9 URL formats

Protocol	URL format	Description
TFTP	**tftp://***server*/*path*/*filename*	Specify a TFTP server by IP address or hostname. For example, specify the file path as **tftp://1.1.1.1/user/user.csv**.
FTP	• With FTP user name and password: **ftp://***username*:*password*@*server*/*path*/*filename* • Without FTP user name and password: **ftp://***server*/*path*/*filename*	Specify an FTP server by IP address or hostname. The device ignores the domain name in the FTP user name. For example, specify the file path as **ftp://1:1@1.1.1.1/user/user.csv** or **ftp://1.1.1.1/user/user.csv**.

Examples

Import guest account information from the **ftp://1.1.1.1/user/guest.csv** file and specify a validity period for the imported guests.

```
<Sysname> system-view
[Sysname] local-user-import class network guest url ftp://1.1.1.1/user/guest.csv
validity-datetime 2018/10/01 00:00:00 to 2019/10/02 12:00:00
```

Related commands

display local-user

local-user-export class network guest

password (device management user view)

Use **password** to configure a password for a device management user.

Use **undo password** to restore the default.

Syntax

password [{ **hash** | **simple** } *string*]

undo password

Default

A device management user does not have a password and cannot pass authentication.

Views

Local user view

Predefined user roles

network-admin

context-admin

Parameters

hash: Specifies a password encrypted by the hash algorithm.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in hashed form.

string: Specifies the password string. This argument is case sensitive. The hashed form of the password is a string of 1 to 110 characters. The plaintext form of the password is a string of 1 to 63 characters.

Usage guidelines

If you do not specify any parameters, you enter the interactive mode to set a plaintext password.

A device management user for which no password is specified can pass authentication after entering the correct username and passing attribute checks. To enhance security, configure a password for each device management user.

When global password control is enabled, the device handles passwords of device management users as follows:

- All passwords in the history records are saved in hashed form.
- If a user changes its own password in plaintext form, the system requests the user to enter the current plaintext password. The new password must be different from all passwords in the history records and the current password. In addition, the new password must have a minimum of four characters different from the current password.
- If a user changes the password for another user in plaintext form, the new password must be different from the latter user's all passwords in the history records and current password.
- If a user deletes its own password, the system requests the user to enter the current plaintext password.
- Except the above listed situations, the system does not request a user to enter the current plaintext password or compare the new password with passwords in the history records and the current password.

Examples

Set the password to **123456TESTplat&!** in plaintext form for device management user **user1**.

```
<Sysname> system-view
[Sysname] local-user user1 class manage
[Sysname-luser-manage-user1] password simple 123456TESTplat&!
```

Configure the password in interactive mode for device management user **test**.

```
<Sysname> system-view
[Sysname] local-user test class manage
[Sysname-luser-manage-test] password
Password:
confirm :
```

Related commands

display local-user

password (network access user view)

Use **password** to configure a password for a network access user.

Use **undo password** to restore the default.

Syntax

password { **cipher** | **simple** } *string*

undo password

Default

A network access user does not have a password and cannot pass authentication.

Views

Network access user view

Predefined user roles

network-admin

context-admin

Parameters

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password string. Its plaintext form is a case-sensitive string of 1 to 63 characters. Its encrypted form is a case-sensitive string of 1 to 117 characters.

Usage guidelines

As a best practice to enhance security, configure a password for each network access user.

Examples

Set the password to **123456TESTuser&!** in plaintext form for network access user **user1**.

```
<Sysname> system-view
[Sysname] local-user user1 class network
[Sysname-luser-network-user1] password simple 123456TESTuser&!
```

Related commands

display local-user

phone

Use **phone** to specify the phone number of a local guest.

Use **undo phone** to restore the default.

Syntax

phone *phone-number*

undo phone

Default

No phone number is specified for a local guest.

Views

Local guest view

Predefined user roles

network-admin

context-admin

Parameters

phone-number: Specifies the phone number, a string of 1 to 32 characters.

Examples

Specify the phone number as **13813723920** for local guest **abc**.

```
<Sysname> system-view
[Sysname] local-user abc class network guest
[Sysname-luser-network(guest)-abc] phone 13813723920
```

Related commands

display local-user

reset local-guest waiting-approval

Use **reset local-guest waiting-approval** to clear pending registration requests for local guests.

Syntax

reset local-guest waiting-approval [**user-name** *user-name*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

user-name *user-name*: Specifies a local guest by its username, a string of 1 to 55 characters. If you do not specify a guest, this command clears information about all registration requests for local guests. The username can be a pure username or a username containing a domain name.

- If the username does not contain an at sign (@), all characters in the username string are case sensitive. The device parses the username as a pure username. The username cannot be **a**, **al**, or **all**, and it cannot contain a forward slash (/), backslash (\), vertical bar (|), colon (:), asterisk (*), question mark (?), left angle bracket (<), or right angle bracket (>).
- If the username contains an at sign (@), it must be in the format of xxx@yyy. The at sign (@) is the delimiter between the pure username and the domain name.
  - The xxx part is case sensitive. It cannot contain a forward slash (/), backslash (\), vertical bar (|), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or at sign (@), and cannot be **a**, **al**, or **all**.
  - The yyy part is case insensitive and cannot contain an at sign (@).

Examples

Clear information about all registration requests for local guests.

```
<Sysname> reset local-guest waiting-approval
```

Related commands

display local-guest waiting-approval

service-type (local user view)

Use **service-type** to specify the service types that a local user can use.

Use **undo service-type** to remove service types configured for a local user.

Syntax

service-type { **advpn** | **ftp** | **ike** | **ipoe** | **lan-access** | { **http** | **https** | **ssh** | **telnet** | **terminal** } * | **portal** | **ppp** | **sslvpn** }

undo service-type { **advpn** | **ftp** | **ike** | **ipoe** | **lan-access** | { **http** | **https** | **ssh** | **telnet** | **terminal** } * | **portal** | **ppp** | **sslvpn** }

Default

A local user is not authorized to use any service.

Views

Local user view

Predefined user roles

network-admin

context-admin

Parameters

advpn: Authorizes the user to use the ADVPN service.

ftp: Authorizes the user to use the FTP service. The authorized directory can be modified by using the **authorization-attribute work-directory** command.

http: Authorizes the user to use the HTTP service.

https: Authorizes the user to use the HTTPS service.

ike: Authorizes the user to use the IKE extended authentication service.

ipoe: Authorizes the user to use the IPoE service.

ssh: Authorizes the user to use the SSH service.

telnet: Authorizes the user to use the Telnet service.

terminal: Authorizes the user to use the terminal service and log in from a console port.

portal: Authorizes the user to use the portal service.

ppp: Authorizes the user to use the PPP service.

sslvpn: Authorizes the user to use the SSL VPN service.

Usage guidelines

You can assign multiple service types to a user.

Examples

Authorize device management user **user1** to use the Telnet and FTP services.

```
<Sysname> system-view
[Sysname] local-user user1 class manage
[Sysname-luser-manage-user1] service-type telnet
[Sysname-luser-manage-user1] service-type ftp
```

Related commands

display local-user

sponsor-department

Use **sponsor-department** to specify the department of the guest sponsor for a local guest.

Use **undo sponsor-department** to restore the default.

Syntax

sponsor-department *department-string*

undo sponsor-department

Default

No department is specified for the guest sponsor of a local guest.

Views

Local guest view

Predefined user roles

network-admin

context-admin

Parameters

department-string: Specifies the department name, a case-sensitive string of 1 to 127 characters.

Examples

Specify the department as **test** for the guest sponsor of local guest **abc**.

```
<Sysname> system-view
[Sysname] local-user abc class network guest
[Sysname-luser-network(guest)-abc] sponsor-department test
```

Related commands

display local-user

sponsor-email

Use **sponsor-email** to specify the email address of the guest sponsor for a local guest.

Use **undo sponsor-email** to restore the default.

Syntax

sponsor-email *email-string*

undo sponsor-email

Default

No email address is specified for the guest sponsor.

Views

Local guest view

Predefined user roles

network-admin

context-admin

Parameters

email-string: Specifies the email address, a case-sensitive string of 1 to 255 characters. The string must contain an at sign (@), and it can contain only one at sign (@). In addition, the string cannot contain only the at sign (@).

Examples

Specify the email address as **Sam@a.com** for the guest sponsor of local guest **abc**.

```
<Sysname> system-view
[Sysname] local-user abc class network guest
[Sysname-luser-network(guest)-abc] sponsor-email Sam@a.com
```

Related commands

display local-user

sponsor-full-name

Use **sponsor-full-name** to specify the guest sponsor name for a local guest.

Use **undo sponsor-full-name** to restore the default.

Syntax

sponsor-full-name *name-string*

undo sponsor-full-name

Default

No guest sponsor name is specified for a local guest.

Views

Local guest view

Predefined user roles

network-admin

context-admin

Parameters

name-string: Specifies the guest sponsor name, a case-sensitive string of 1 to 255 characters.

Examples

Specify the guest sponsor name as **Sam Li** for local guest **abc**.

```
<Sysname> system-view
[Sysname] local-user abc class network guest
[Sysname-luser-network(guest)-abc] sponsor-full-name Sam Li
```

Related commands

display local-user

state (local user view)

Use **state** to set the status of a local user.

Use **undo state** to restore the default.

Syntax

state { **active** | **block** }

undo state

Default

A local user is in active state.

Views

Local user view

Predefined user roles

network-admin

context-admin

Parameters

active: Places the local user in active state to allow the local user to request network services.

block: Places the local user in blocked state to prevent the local user from requesting network services.

Examples

Place device management user **user1** in blocked state.

```
<Sysname> system-view
[Sysname] local-user user1 class manage
[Sysname-luser-manage-user1] state block
```

Related commands

display local-user

user-group

Use **user-group** to create a user group and enter its view, or enter the view of an existing user group.

Use **undo user-group** to delete a user group.

Syntax

user-group *group-name*

undo user-group *group-name*

Default

A system-defined user group exists. The group name is **system**.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies the user group name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

A user group consists of a group of local users and has a set of local user attributes. You can configure local user attributes for a user group to implement centralized management of user attributes for the local users in the group.

You cannot use the **undo user-group** command to delete a user group that has local users.

You can modify settings for the system-defined user group named **system**, but you cannot delete the user group.

Examples

Create a user group named **abc** and enter user group view.

```
<Sysname> system-view
[Sysname] user-group abc
[Sysname-ugroup-abc]
```

Related commands

display user-group

validity-datetime

Use **validity-datetime** to specify the validity period for a network access user.

Use **undo validity-datetime** to restore the default.

Syntax

Network access user view:

validity-datetime { **from** *start-date start-time* **to** *expiration-date expiration-time* | **from** *start-date start-time* | **to** *expiration-date expiration-time* }

undo validity-datetime

Local guest view:

validity-datetime from *start-date start-time* **to** *expiration-date expiration-time*

undo validity-datetime

Default

The validity period for a network access user does not expire.

Views

Network access user view

Local guest view

Predefined user roles

network-admin

context-admin

Parameters

from: Specifies the validity start date and time for the user. If you do not specify this option, the command defines only the expiration date and time of the user.

start-date: Specifies the date on which the user becomes effective. The date is in the format of MM/DD/YYYY or YYYY/MM/DD. The value range for the MM argument is 1 to 12. The value range for the DD argument varies with the specified month. The value range for the YYYY argument is 2000 to 2035.

start-time: Specifies the time on the day when the user becomes effective. The time is in the format of hh:mm:ss. The value range for the hh argument is 0 to 23. The value range for the mm and ss arguments is 0 to 59. The mm and ss arguments are optional. For example, enter 1 to indicate 1:00:00. A value of 0 indicates 00:00:00.

to: Specifies the expiration date and time for the user. If you do not specify this option, the command defines only the validity start date and time of the user.

expiration-date: Specifies the expiration date in the format of MM/DD/YYYY or YYYY/MM/DD. The value range for the MM argument is 1 to 12. The value range for the DD argument varies with the specified month. The value range for the YYYY argument is 2000 to 2035.

expiration-time: Specifies the expiration time in the format of hh:mm:ss. The value range for the hh argument is 0 to 23. The value range for the mm and ss arguments is 0 to 59. The mm and ss arguments are optional. For example, enter 1 to indicate 1:00:00. A value of 0 indicates 00:00:00.

Usage guidelines

Expired network access user accounts cannot be used for authentication.

When both **from** and **to** options are specified, the expiration date and time must be later than the validity start date and time.

When only the **from** option is specified, the network access user is valid since the specified date and time.

When only the **to** option is specified, the network access user is valid until the specified date and time.

Examples

Specify the validity period for network access user **123**.

```
<Sysname> system-view
[Sysname] local-user 123 class network
[Sysname-luser-network-123] validity-datetime from 2018/10/01 00:00:00 to 2019/10/02
12:00:00
```

Related commands

display local-user

RADIUS commands

aaa device-id

Use **aaa device-id** to configure the device ID.

Use **undo aaa device-id** to restore the default.

Syntax

aaa device-id *device-id*

undo aaa device-id

Default

The device ID is 0.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

device-id: Specifies a device ID in the range of 1 to 255.

Usage guidelines

RADIUS uses the value of the Acct-Session-ID attribute as the accounting ID for a user. The device generates an Acct-Session-ID value that includes the device ID for each online user.

If you modify the device ID, the new device ID does not take effect on users that have been online during the change.

Examples

Configure the device ID as 1.

```
<Sysname> system-view
[Sysname] aaa device-id 1
```

accounting-on enable

Use **accounting-on enable** to configure the accounting-on feature.

Use **undo accounting-on enable** to disable the accounting-on feature.

Syntax

accounting-on enable [**interval** *interval* | **send** *send-times*] *

undo accounting-on enable

Default

The accounting-on feature is disabled.

Views

RADIUS scheme view

Predefined user roles

network-admin

context-admin

Parameters

interval *interval*: Specifies the time interval for retransmitting an accounting-on packet in seconds. The value range for the *interval* argument is 1 to 15, and the default setting is 3.

send *send-times*: Specifies the maximum number of accounting-on packet transmission attempts. The value range for the *send-times* argument is 1 to 255, and the default setting is 50.

Usage guidelines

This feature enables the device to automatically monitor the status of all accounting servers in the RADIUS scheme and then send accounting-on packets to the reachable servers after a reboot. The accounting-on packets are used to request the RADIUS servers to stop accounting on all online users on the device and to log out the users.

Execute the **save** command to ensure that the **accounting-on enable** command takes effect at the next device reboot. For information about the **save** command, see *Fundamentals Command Reference*.

Parameters set by using the **accounting-on enable** command take effect immediately.

Examples

Enable the accounting-on feature for RADIUS scheme **radius1**, and set the retransmission interval to 5 seconds and the transmission attempts to 15.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] accounting-on enable interval 5 send 15
```

Related commands

display radius scheme

attribute 15 check-mode

Use **attribute 15 check-mode** to configure the Login-Service attribute check method for SSH, FTP, and terminal users.

Use **undo attribute 15 check-mode** to restore the default.

Syntax

attribute 15 check-mode { **loose** | **strict** }

undo attribute 15 check-mode

Default

The strict check method applies for SSH, FTP, and terminal users.

Views

RADIUS scheme view

Predefined user roles

network-admin

context-admin

Parameters

loose: Matches the standard Login-Service attribute value 0 for SSH, FTP, and terminal services.

strict: Matches Login-Service attribute values 50, 51, and 52 for SSH, FTP, and terminal services, respectively.

Usage guidelines

Use the loose check method only when the server does not issue Login-Service attribute values 50, 51, and 52 for SSH, FTP, and terminal users.

Examples

Configure the Login-Service attribute check method as **loose** for SSH, FTP, and terminal users in RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] attribute 15 check-mode loose
```

Related commands

display radius scheme

attribute 17 old-password

Use **attribute 17 old-password** to enable online user password change by using RADIUS attribute 17.

Use **undo attribute 17 old-password** to restore the default.

Syntax

attribute 17 old-password

undo attribute 17 old-password

Default

Online user password change is disabled.

Views

RADIUS scheme view

Predefined user roles

network-admin

context-admin

Usage guidelines

When this feature is enabled, the process of online password change is as follows for a user when the user passes authentication:

1. If the RADIUS authentication server sends an Access-Challenge packet that includes the Reply-Message attribute when a user passes authentication, the device prompts the user to change its password.
2. After receiving the password change request from the user, the device sends a RADIUS authentication request to the RADIUS authentication server.

   In the authentication request, the device uses attribute 2 to carry the new user password.
3. When the device receives a response from the RADIUS authentication server, the online user's password is changed successfully.

When this feature is enabled, the process of online password change is as follows for an online user:

1. After receiving the password change request from the user, the device sends a RADIUS authentication request to a reachable RADIUS server. In the authentication request, the device uses attribute 2 and attribute 17 to carry the new user password and old user password, respectively.

   The RADIUS server selection process for online password change is the same as the process used to select a RADIUS authentication server. Online password change might fail because the device selects a RADIUS server different from the RADIUS server that authenticated the user.
2. When the device receives a response from the selected RADIUS server, the online user's password is changed successfully.

This feature is applicable only to SSL VPN users.

Do not enable this feature if the RADIUS server does not support online user password change.

In a RADIUS scheme with this feature enabled, do not configure parsing rules for the Reply-Message attribute by using the **attribute 18 match** command. A violation will cause this feature fail to take effect.

Examples

In RADIUS scheme **radius1**, enable online user password change by using RADIUS attribute 17.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] attribute 17 old-password
```

Related commands

attribute 18 match

display radius scheme

attribute 18 match

Use **attribute 18 match** to configure a parsing rule for the RADIUS Reply-Message attribute.

Use **undo attribute 18 match** to remove a parsing rule for the RADIUS Reply-Message attribute.

Syntax

attribute 18 match *string* **action** { **new-password** | **next-token** }

undo attribute 18 match *string* **action**

Default

No parsing rules for the RADIUS Reply-Message attribute are configured. The device parses the Reply-Message attribute as to prompt users to enter the next authentication factor for double-factor authentication.

Views

RADIUS scheme view

Predefined user roles

network-admin

context-admin

Parameters

string: Specifies a match criterion, a case-sensitive string of 1 to 255 characters. To include spaces in the string, enclose the entire string in double quotation marks ("").

action: Specifies the action that the device prompts users to take if the attribute value matches the match criterion.

new-password: Enters the new password.

next-token: Enters the next authentication factor for double-factor authentication.

Usage guidelines

The RADIUS Reply-Message attribute (attribute 18) is intended for the RADIUS server to return a message to users. In the Access-Challenge packets, this attribute indicates the action that the RADIUS server expects users to take. For the access device to correctly parse this attribute, you can configure parsing rules for this attribute. For example, the device needs to parse the Reply-Message attribute containing the **new pin** string as to prompt users to change the passwords online.

Each parsing rule contains a match criterion and an action. The device uses the fuzzy match method to match the Reply-Message attribute value against the match criterion. If the attribute value partially matches the match criterion, the device prompts the users to take the action specified in the parsing rule.

This feature is applicable only to SSL VPN users.

Before you configure parsing rules, make sure you fully understand the implications of the Reply-Message attribute defined by the RADIUS server.

For a RADIUS scheme, you can configure a maximum of 18 parsing rules for the Reply-Message attribute. Make sure the match criterion in each parsing rule is not contained by the match criterion of another parsing rule.

When parsing rules for the Reply-Message attribute are configured, the online user password change feature configured by using the **attribute 17 old-password** command does not take effect. As a best practice, do not configure both parsing rules and online user password change in the same RADIUS scheme.

Examples

In RADIUS scheme **radius1**, configure a parsing rule for the Reply-Message attribute. According to this rule, the device will prompt users to enter the new password if the Reply-Message attribute contain string **new pin**.

```
<Sysname> system-view
[sysname] radius scheme radius1
[sysname-radius-radius1] attribute 18 match “new pin” action new-password
```

Related commands

attribute 17 old-password

display radius scheme

attribute 25 car

Use **attribute 25 car** to configure the device to interpret the RADIUS class attribute (attribute 25) as CAR parameters.

Use **undo attribute 25 car** to restore the default.

Syntax

attribute 25 car

undo attribute 25 car

Default

The RADIUS class attribute is not interpreted as CAR parameters.

Views

RADIUS scheme view

Predefined user roles

network-admin

context-admin

Usage guidelines

Configure the device to interpret the RADIUS class attribute if the RADIUS server uses the attribute to deliver CAR parameters for user-based traffic monitoring and control.

Examples

In RADIUS scheme **radius1**, configure the device to interpret the RADIUS class attribute as CAR parameters.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] attribute 25 car
```

Related commands

display radius scheme

attribute 30 mac-format

Use **attribute 30 mac-format** to configure the format of the MAC address in the RADIUS Called-Station-Id attribute.

Use **undo attribute 30 mac-format** to restore the default.

Syntax

attribute 30 mac-format section { **one** | { **six** | **three** } **separator** *separator-character* } { **lowercase** | **uppercase** }

undo attribute 30 mac-format

Default

The MAC address in the RADIUS Called-Station-Id attribute is in the format of HH-HH-HH-HH-HH-HH. The MAC address is separated by hyphens (-) into six sections with letters in upper case.

Views

RADIUS scheme view

Predefined user roles

network-admin

context-admin

Parameters

section: Specifies the number of sections that a MAC address contains.

one: Specifies the one-section format HHHHHHHHHHHH.

six: Specifies the six-section format HH-HH-HH-HH-HH-HH.

three: Specifies the three-section format HHHH-HHHH-HHHH.

separator *separator-character*: Specifies a case-sensitive character that separates the sections.

lowercase: Specifies the letters in a MAC address to be in lower case.

uppercase: Specifies the letters in a MAC address to be in upper case.

Usage guidelines

Configure the format of the MAC address in the RADIUS Called-Station-Id attribute to meet the requirements of the RADIUS servers.

Examples

In RADIUS scheme **radius1**, specify **hhhhhhhhhhhh** as the format of the MAC address in the RADIUS Called-Station-Id attribute.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] attribute 30 mac-format section one lowercase
```

Related commands

display radius scheme

attribute 31 mac-format

Use **attribute 31 mac-format** to configure the format of the MAC address in the RADIUS Calling-Station-Id attribute.

Use **undo attribute 31 mac-format** to restore the default.

Syntax

attribute 31 mac-format section { **one** | { **six** | **three** } **separator** *separator-character* } { **lowercase** | **uppercase** }

undo attribute 31 mac-format

Default

The MAC address in the RADIUS Calling-Station-Id attribute (attribute 31) is in the format of HH-HH-HH-HH-HH-HH. The MAC address is separated by hyphens (-) into six sections with letters in upper case.

Views

RADIUS scheme view

Predefined user roles

network-admin

context-admin

Parameters

section: Specifies the number of sections that a MAC address contains.

one: Specifies the one-section format HHHHHHHHHHHH.

six: Specifies the six-section format HH-HH-HH-HH-HH-HH.

three: Specifies the three-section format HHHH-HHHH-HHHH.

separator *separator-character*: Specifies a case-sensitive character that separates the sections.

lowercase: Specifies the letters in a MAC address to be in lower case.

uppercase: Specifies the letters in a MAC address to be in upper case.

Usage guidelines

Configure the format of the MAC address in the RADIUS Calling-Station-Id attribute to meet the requirements of the RADIUS servers.

Examples

In RADIUS scheme **radius1**, specify **hh:hh:hh:hh:hh:hh** as the format of the MAC address in the RADIUS Calling-Station-Id attribute.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] attribute 31 mac-format section six separator : lowercase
```

Related commands

display radius scheme

attribute 182 vendor-id 25506 vlan

Use **attribute 182 vendor-id 25506 vlan** to enable the device to interpret the Microsegment-Id attribute to an authorization VLAN.

Use **undo attribute 182 vendor-id 25506 vlan** to disable the device from interpreting the Microsegment-Id attribute to an authorization VLAN.

Syntax

attribute 182 vendor-id 25506 vlan

undo attribute 182 vendor-id 25506 vlan

Default

The device is disabled from interpreting the Microsegment-Id attribute to an authorization VLAN.

Views

RADIUS scheme view

Predefined user roles

network-admin

context-admin

Usage guidelines

Use this command only when the RADIUS server uses authorization microsegment IDs for granular user access control and the access device uses authorization VLANs to implement microsegment-based access control.

This feature enables the device to interpret the RADIUS Microsegment-Id attribute (attribute 182 with vendor ID 25506) assigned by the RADIUS server to an authorization VLAN.

- If the attribute value is an integer, the device interprets this attribute to a VLAN ID.
- If the attribute value is not an integer, the device interprets this attribute to a VLAN name.

If the RADIUS server uses a RADIUS attribute other than the Microsegment-Id attribute to assign microsegment IDs, you must first convert the attribute to the Microsegment-Id attribute. To enable RADIUS attribute translation feature, use the **attribute translate** command.

Examples

In RADIUS scheme **radius1**, enable the device to interpret the Microsegment-Id attribute to an authorization VLAN.

```
<Sysname> system-view
[Sysname] radius scheme radius1
```

```
[Sysname-radius-radius1] attribute 182 vendor-id 25506 vlan
```

Related commands

attribute translate

display radius scheme

attribute convert (RADIUS DAS view)

Use **attribute convert** to configure a RADIUS attribute conversion rule.

Use **undo attribute convert** to delete RADIUS attribute conversion rules.

Syntax

attribute convert *src-attr-name* **to** *dest-attr-name* { { **coa-ack** | **coa-request** } * | { **received** | **sent** } * }

undo attribute convert [*src-attr-name*]

Default

No RADIUS attribute conversion rules exist. The system processes RADIUS attributes according to the principles of the standard RADIUS protocol.

Views

RADIUS DAS view

Predefined user roles

network-admin

context-admin

Parameters

src-attr-name: Specifies the source RADIUS attribute by its name, a case-insensitive string of 1 to 63 characters. The attribute must be supported by the system.

dest-attr-name: Specifies the destination RADIUS attribute by its name, a case-insensitive string of 1 to 63 characters. The attribute must be supported by the system.

coa-ack: Specifies the CoA acknowledgment packets.

coa-request: Specifies the CoA request packets.

received: Specifies the received DAE packets.

sent: Specifies the sent DAE packets.

Usage guidelines

The device replaces the attribute in packets that match a RADIUS attribute conversion rule with the destination RADIUS attribute in the rule.

The conversion rules take effect only when the RADIUS attribute translation feature is enabled.

When you configure RADIUS attribute conversion rules, follow these restrictions and guidelines:

- The source and destination RADIUS attributes in a rule must use the same data type.
- The source and destination RADIUS attributes in a rule cannot use the same name.
- A source RADIUS attribute can be converted only by one criterion, packet type or direction.
- One source RADIUS attribute cannot be converted to multiple destination attributes.

If you do not specify a source RADIUS attribute, the **undo attribute convert** command deletes all RADIUS attribute conversion rules.

Examples

In RADIUS DAS view, configure a RADIUS attribute conversion rule to replace the Hw-Server-String attribute in the received DAE packets with the Connect-Info attribute.

```
<Sysname> system-view
[Sysname] radius dynamic-author server
[Sysname-radius-da-server] attribute convert Hw-Server-String to Connect-Info received
```

Related commands

attribute translate

attribute convert (RADIUS scheme view)

Use **attribute convert** to configure a RADIUS attribute conversion rule.

Use **undo attribute convert** to delete RADIUS attribute conversion rules.

Syntax

attribute convert *src-attr-name* **to** *dest-attr-name* { { **access-accept** | **access-request** | **accounting** } * | { **received** | **sent** } * }

undo attribute convert [*src-attr-name*]

Default

No RADIUS attribute conversion rules exist. The system processes RADIUS attributes according to the principles of the standard RADIUS protocol.

Views

RADIUS scheme view

Predefined user roles

network-admin

context-admin

Parameters

src-attr-name: Specifies the source RADIUS attribute by its name, a case-insensitive string of 1 to 63 characters. The attribute must be supported by the system.

dest-attr-name: Specifies the destination RADIUS attribute by its name, a case-insensitive string of 1 to 63 characters. The attribute must be supported by the system.

access-accept: Specifies the RADIUS Access-Accept packets.

access-request: Specifies the RADIUS Access-Request packets.

accounting: Specifies the RADIUS accounting packets.

received: Specifies the received RADIUS packets.

sent: Specifies the sent RADIUS packets.

Usage guidelines

The device replaces the attribute in packets that match a RADIUS attribute conversion rule with the destination RADIUS attribute in the rule.

The conversion rules take effect only when the RADIUS attribute translation feature is enabled.

When you configure RADIUS attribute conversion rules, follow these restrictions and guidelines:

- The source and destination RADIUS attributes in a rule must use the same data type.
- The source and destination RADIUS attributes in a rule cannot use the same name.

- A source RADIUS attribute can be converted only by one criterion, packet type or direction.
- One source RADIUS attribute cannot be converted to multiple destination attributes.

If you do not specify a source RADIUS attribute, the **undo attribute convert** command deletes all RADIUS attribute conversion rules.

Examples

In RADIUS scheme **radius1**, configure a RADIUS attribute conversion rule to replace the Hw-Server-String attribute of received RADIUS packets with the Connect-Info attribute.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] attribute convert Hw-Server-String to Connect-Info received
```

Related commands

attribute translate

attribute reject (RADIUS DAS view)

Use **attribute reject** to configure a RADIUS attribute rejection rule.

Use **undo attribute reject** to delete RADIUS attribute rejection rules.

Syntax

attribute reject *attr-name* { { **coa-ack** | **coa-request** } * | { **received** | **sent** } * }

undo attribute reject [*attr-name*]

Default

No RADIUS attribute rejection rules exist.

Views

RADIUS DAS view

Predefined user roles

network-admin

context-admin

Parameters

attr-name: Specifies a RADIUS attribute by its name, a case-insensitive string of 1 to 63 characters. The attribute must be supported by the system.

coa-ack: Specifies the CoA acknowledgment packets.

coa-request: Specifies the CoA request packets.

received: Specifies the received DAE packets.

sent: Specifies the sent DAE packets.

Usage guidelines

Configure RADIUS attribute rejection rules for the following purposes:

- Delete attributes from the RADIUS packets to be sent if the destination RADIUS server does not identify the attributes.
- Ignore unwanted attributes in the RADIUS packets received from a RADIUS server.

The RADIUS attribute rejection rules take effect only when the RADIUS attribute translation feature is enabled.

A RADIUS attribute can be rejected only by one criterion, packet type or direction.

If you do not specify a RADIUS attribute, the **undo attribute reject** command deletes all RADIUS attribute rejection rules.

Examples

In RADIUS DAS view, configure a RADIUS attribute rejection rule to delete the Connect-Info attribute from the DAE packets to be sent.

```
<Sysname> system-view
[Sysname] radius dynamic-author server
[Sysname-radius-da-server] attribute reject Connect-Info sent
```

Related commands

attribute translate

attribute reject (RADIUS scheme view)

Use **attribute reject** to configure a RADIUS attribute rejection rule.

Use **undo attribute reject** to delete RADIUS attribute rejection rules.

Syntax

attribute reject *attr-name* { { **access-accept** | **access-request** | **accounting** } * | { **received** | **sent** } * }

undo attribute reject [*attr-name*]

Default

No RADIUS attribute rejection rules exist.

Views

RADIUS scheme view

Predefined user roles

network-admin

context-admin

Parameters

attr-name: Specifies a RADIUS attribute by its name, a case-insensitive string of 1 to 63 characters. The attribute must be supported by the system.

access-accept: Specifies the RADIUS Access-Accept packets.

access-request: Specifies the RADIUS Access-Request packets.

accounting: Specifies the RADIUS accounting packets.

received: Specifies the received RADIUS packets.

sent: Specifies the sent RADIUS packets.

Usage guidelines

Configure RADIUS attribute rejection rules for the following purposes:

- Delete attributes from the RADIUS packets to be sent if the destination RADIUS server does not identify the attributes.
- Ignore unwanted attributes in the RADIUS packets received from a RADIUS server.

The RADIUS attribute rejection rules take effect only when the RADIUS attribute translation feature is enabled.

A RADIUS attribute can be rejected only by one criterion, packet type or direction.

If you do not specify a RADIUS attribute, the **undo attribute reject** command deletes all RADIUS attribute rejection rules.

Examples

In RADIUS scheme **radius1**, configure a RADIUS attribute rejection rule to delete the Connect-Info attribute from the RADIUS packets to be sent.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] attribute reject Connect-Info sent
```

Related commands

attribute translate

attribute remanent-volume

Use **attribute remanent-volume** to set the data measurement unit for the Remanent_Volume attribute.

Use **undo attribute remanent-volume** to restore the default.

Syntax

attribute remanent-volume unit { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** }

undo attribute remanent-volume unit

Default

The data measurement unit is kilobyte for the Remanent_Volume attribute.

Views

RADIUS scheme view

Predefined user roles

network-admin

context-admin

Parameters

byte: Specifies the unit as byte.

giga-byte: Specifies the unit as gigabyte.

kilo-byte: Specifies the unit as kilobyte.

mega-byte: Specifies the unit as megabyte.

Usage guidelines

Make sure the measurement unit is the same as the user data measurement unit on the RADIUS server.

Examples

In RADIUS scheme **radius1**, set the data measurement unit to **kilobyte** for the Remanent_Volume attribute.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] attribute remanent-volume unit kilo-byte
```

Related commands

display radius scheme

attribute translate

Use **attribute translate** to enable the RADIUS attribute translation feature.

Use **undo attribute translate** to disable the RADIUS attribute translation feature.

Syntax

attribute translate

undo attribute translate

Default

The RADIUS attribute translation feature is disabled.

Views

RADIUS DAS view

RADIUS scheme view

Predefined user roles

network-admin

context-admin

Usage guidelines

To cooperate with RADIUS servers of different vendors, enable the RADIUS attribute translation feature. Configure RADIUS attribute conversion rules and rejection rules to ensure that RADIUS attributes in the packets exchanged between the device and the server are supported by both sides.

Examples

Enable the RADIUS attribute translation feature for RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] attribute translate
```

Related commands

attribute convert (RADIUS DAS view)

attribute convert (RADIUS scheme view)

attribute reject (RADIUS DAS view)

attribute reject (RADIUS scheme view)

attribute vendor-id 2011 version

Use **attribute vendor-id 2011 version** to specify the version of the RADIUS servers with a vendor ID of 2011.

Use **undo attribute vendor-id 2011 version** to restore the default.

Syntax

attribute vendor-id 2011 version { **1.0** | **1.1** }

undo attribute vendor-id 2011 version

Default

The version is 1.0.

Views

RADIUS scheme view

Predefined user roles

network-admin

context-admin

Parameters

`1.0`: Specifies version 1.0.

`1.1`: Specifies version 1.1.

Usage guidelines

For the device to correctly interpret RADIUS attributes from the servers with a vendor ID of 2011, specify a server version the same as the actual version of the RADIUS servers.

The following table shows the differences in the way that the device interprets the vendor-specific RADIUS attributes assigned by different versions of RADIUS servers with vendor ID 2011.

RADIUS attribute	RADIUS server with version 1.0	RADIUS server with version 1.1
HW_ARRT_26_1	Upstream peak rate	Upstream burst size
HW_ARRT_26_2	Upstream average rate	Upstream average rate
HW_ARRT_26_3	N/A	Upstream peak rate
HW_ARRT_26_4	Downstream peak rate	Downstream burst size
HW_ARRT_26_5	Downstream average rate	Downstream average rate
HW_ARRT_26_6	N/A	Downstream peak rate

Examples

In RADIUS scheme **radius1**, specify the version of the RADIUS servers with a vendor ID of 2011 as version 1.1.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] attribute vendor-id 2011 version 1.1
```

Related commands

`display radius scheme`

client

Use **`client`** to specify a RADIUS DAC.

Use **`undo client`** to remove a RADIUS DAC.

Syntax

client { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**key** { **cipher** | **simple** } *string* | **vendor-id 2011 version** { **1.0** | **1.1** } | **vpn-instance** *vpn-instance-name*] *

undo client { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]

Default

No RADIUS DACs are specified.

Views

RADIUS DAS view

Predefined user roles

network-admin

context-admin

Parameters

ip *ipv4-address*: Specifies a DAC by its IPv4 address.

ipv6 *ipv6-address*: Specifies a DAC by its IPv6 address.

key: Specifies the shared key for secure communication between the RADIUS DAC and server. Make sure the shared key is the same as the key configured on the RADIUS DAC. If the RADIUS DAC does not have any shared key, do not specify this option.

cipher: Specifies the key in encrypted form.

simple: Specifies the key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. This argument is case sensitive. The encrypted form of the key is a string of 1 to 117 characters. The plaintext form of the key is a string of 1 to 64 characters.

vendor-id 2011: Specifies the vendor-ID of the DAC as 2011.

version: Specifies the version of the DAC.

1.0: Specifies the DAC version as version 1.0.

1.1: Specifies the DAC version as version 1.1.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance to which the RADIUS DAC belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the server is on the public network, do not specify this option.

Usage guidelines

With the RADIUS DAS feature, the device listens to the default or specified UDP port to receive DAE requests from the specified DACs. The device processes the requests and sends DAE responses to the DACs.

The device discards any DAE packets sent from DACs that are not specified for the DAS.

You can execute the **client** command multiple times to specify multiple DACs for the DAS.

To work with a DAC with vendor-ID 2011 and version 1.0, you do not need to specify the vendor-ID or version attribute. To work with a DAC with vendor-ID 2011 and version 1.1, you must specify the **vendor-id 2011 version 1.1** keywords.

Examples

Specify the DAC as 10.110.1.2. Set the shared key to **123456** in plaintext form for secure communication between the DAS and DAC.

```
<Sysname> system-view
[Sysname] radius dynamic-author server
[Sysname-radius-da-server] client ip 10.110.1.2 key simple 123456
```

Related commands

radius dynamic-author server

port

data-flow-format (RADIUS scheme view)

Use **data-flow-format** to set the data flow and packet measurement units for traffic statistics.

Use **undo data-flow-format** to restore the default.

Syntax

data-flow-format { **data** { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** } | **packet** { **giga-packet** | **kilo-packet** | **mega-packet** | **one-packet** } } *

undo data-flow-format { **data** | **packet** }

Default

Traffic is counted in bytes and packets.

Views

RADIUS scheme view

Predefined user roles

network-admin

context-admin

Parameters

data: Specifies the unit for data flows.

byte: Specifies the unit as byte.

giga-byte: Specifies the unit as gigabyte.

kilo-byte: Specifies the unit as kilobyte.

mega-byte: Specifies the unit as megabyte.

packet: Specifies the unit for data packets.

giga-packet: Specifies the unit as giga-packet.

kilo-packet: Specifies the unit as kilo-packet.

mega-packet: Specifies the unit as mega-packet.

one-packet: Specifies the unit as one-packet.

Usage guidelines

The data flow and packet measurement units for traffic statistics must be the same as configured on the RADIUS accounting servers. Otherwise, accounting results might be incorrect.

Examples

In RADIUS scheme **radius1**, set the data flow and packet measurement units for traffic statistics to kilobyte and kilo-packet, respectively.

```
<Sysname> system-view
```

```
[Sysname] radius scheme radius1
[Sysname-radius-radius1] data-flow-format data kilo-byte packet kilo-packet
```

Related commands

display radius scheme

display radius scheme

Use **display radius scheme** to display RADIUS scheme configuration.

Syntax

display radius scheme [*radius-scheme-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

radius-scheme-name: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters. If you do not specify a RADIUS scheme, this command displays the configuration of all RADIUS schemes.

Usage guidelines

When displaying configuration only for one scheme, this command also displays the active state duration for each active server and the most recent five state changes for all servers in the scheme.

When displaying configuration for all schemes, this command also displays the active state duration for each active server and the most recent blocked period for all servers in all schemes.

Examples

Display the configuration of all RADIUS schemes.

```
<Sysname> display radius scheme
Total 1 RADIUS schemes


------------------------------------------------------------------
RADIUS scheme name: radius1
  Index : 0
  Primary authentication server:
    IP   : 2.2.2.2                                Port: 1812
    VPN  : vpn1
    State: Active (duration: 1 weeks, 2 days, 1 hours, 32 minutes, 34 seconds)
    Most recent blocked period: 2019/08/08 20:33:45 – 2019/08/08 20:38:45
    Test profile: 132
      Probe username: test
      Probe interval: 60 minutes
  Primary accounting server:
    IP   : 1.1.1.1                                Port: 1813
```

```
    VPN  : Not configured
    State: Active (duration: 1 weeks, 2 days, 1 hours, 32 minutes, 34 seconds)
    Most recent blocked period: 2019/08/08 20:33:45 - 2019/08/08 20:38:45
  Second authentication server:
    IP   : 3.3.3.3                                Port: 1812
    VPN  : Not configured
    State: Blocked
    Most recent blocked period: 2019/08/08 20:33:45 - now
    Test profile: Not configured
  Second accounting server:
    Host name: Not configured
    IP   : 3.3.3.3                                Port: 1813
    VPN  : Not configured
    State: Blocked (mandatory)
    Most recent blocked period: 2019/08/08 20:33:45 - now
    Weight: 0
  Accounting-On function                     : Enabled
    extended function                        : Disabled
    retransmission times                     : 5
    retransmission interval(seconds)         : 2
  Timeout Interval(seconds)                  : 3
  Retransmission Times                       : 3
  Retransmission Times for Accounting Update : 5
  Server Quiet Period(minutes)               : 5
  Realtime Accounting Interval(seconds)      : 22
  NAS IP Address                             : 1.1.1.1
  VPN                                        : Not configured
  User Name Format                           : with-domain
  Data flow unit                             : Megabyte
  Packet unit                                : One
  Attribute 15 check-mode                    : Strict
  Attribute 25                               : CAR
  Attribute Remanent-Volume unit             : Mega
  RADIUS server version (vendor ID 2011)     : 1.0
  Attribute 30 MAC format                    : hh:hh:hh:hh:hh:hh
  Attribute 31 MAC format                    : hh:hh:hh:hh:hh:hh
  Attribute 17 carry old password            : Disabled
  Attribute 182 vendor-ID 25506 VLAN         : Enabled
  Stop-accounting-packet send-force          : Disabled
-------------------------------------------------------------------
```

Display the configuration of RADIUS scheme **radius1**.

```
<Sysname> display radius scheme radius1
RADIUS scheme name: radius1
  Index: 0
  Primary authentication server:
    IP   : 2.2.2.2                                Port: 1812
    VPN  : Not configured
    State: Active (duration: 1 weeks, 2 days, 1 hours, 32 minutes, 34 seconds)
```

```
  Most recent state changes:
    2019/08/08 20:38:45 Changed to active state
    2019/08/08 20:33:45 Changed to blocked state
    2019/08/08 20:31:19 Changed to active state
    2019/08/08 20:26:19 Changed to blocked state
    2019/08/08 20:26:00 Changed to active state
  Test profile: 132
    Probe username: test
    Probe interval: 60 minutes
Primary accounting server:
  IP   : 1.1.1.1                                Port: 1813
  VPN  : Not configured
  State: Active (duration: 1 weeks, 2 days, 1 hours, 32 minutes, 34 seconds)
  Most recent state changes:
    2019/08/08 20:38:45   Changed to active state
    2019/08/08 20:33:45   Changed to blocked state
    2019/08/08 20:31:19   Changed to active state
    2019/08/08 20:26:19   Changed to blocked state
    2019/08/08 20:26:00   Changed to active state
Second authentication server:
  IP   : 3.3.3.3                                Port: 1812
  VPN  : Not configured
  State: Blocked
  Most recent state changes:
    2019/08/08 20:56:22   Changed to blocked state
    2019/08/08 20:48:45   Changed to active state
    2019/08/08 20:43:45   Changed to blocked state
    2019/08/08 20:41:19   Changed to active state
    2019/08/08 20:46:19   Changed to blocked state
  Test profile: Not configured
Second accounting server:
  IP   : 3.3.3.3                                Port: 1813
  VPN  : Not configured
  State: Blocked (mandatory)
  Most recent state changes:
    2019/08/08 20:56:22   Changed to blocked state
    2019/08/08 20:48:45   Changed to active state
    2019/08/08 20:43:45   Changed to blocked state
    2019/08/08 20:41:19   Changed to active state
    2019/08/08 20:46:19   Changed to blocked state
Accounting-On function                     : Disabled
  extended function                        : Disabled
  retransmission times                     : 5
  retransmission interval(seconds)         : 2
Timeout Interval(seconds)                  : 3
Retransmission Times                       : 3
Retransmission Times for Accounting Update : 5
Server Quiet Period(minutes)               : 5
```

```
Realtime Accounting Interval(seconds)      : 22
NAS IP Address                             : 1.1.1.1
VPN                                        : Not configured
User Name Format                           : with-domain
Data flow unit                             : Megabyte
Packet unit                                : One
Attribute 15 check-mode                    : Strict
Attribute 25                               : CAR
Attribute Remanent-Volume unit             : Mega
RADIUS server version (vendor ID 2011)     : 1.0
Attribute 30 MAC format                    : HH-HH-HH-HH-HH-HH
Attribute 31 MAC format                    : hh:hh:hh:hh:hh:hh
Attribute 17 carry old password            : Disabled
Attribute 182 vendor-ID 25506 VLAN         : Enabled
Parsing rules for attribute 18:
  If match: "new pin"
    Action: New password
  If match: "challenge"
    Action: Next token
```

Table 10 Command output

Field	Description
Index	Index number of the RADIUS scheme.
Primary authentication server	Information about the primary authentication server.
Primary accounting server	Information about the primary accounting server.
Second authentication server	Information about the secondary authentication server.
Second accounting server	Information about the secondary accounting server.
IP	IP address of the server. This field displays **Not configured** if the server is not configured.
Port	Service port number of the server. If no port number is specified, this field displays the default port number.
State	Status of the server: • **Active**—The server is in active state. • **Blocked**—The server is changed to blocked state automatically. • **Blocked (mandatory)**—The server is set to blocked state manually.
duration	The duration of the current active state for the server. This field is displayed only when the server is in active state.
Most recent blocked period	Most recent blocking start time and end time when the server stayed in blocked state. If the server still remains in blocked state, **now** is displayed for the end time.
Most recent state changes	Most recent five state changes of the server.
VPN	MPLS L3VPN instance to which the server or the RADIUS scheme belongs. If no VPN instance is specified for the server, this field displays **Not configured**.
Test profile	Test profile used for RADIUS server status detection.
Probe username	Username used for RADIUS server status detection.

Field	Description
Probe interval	Server status detection interval, in minutes.
Accounting-On function	Whether the accounting-on feature is enabled.
extended function	Whether the extended accounting-on feature is enabled.
retransmission times	Number of accounting-on packet transmission attempts.
retransmission interval(seconds)	Interval at which the device retransmits accounting-on packets, in seconds.
Timeout Interval(seconds)	RADIUS server response timeout period, in seconds.
Retransmission times	Maximum number of attempts for transmitting a RADIUS packet to a single RADIUS server.
Retransmission Times for Accounting Update	Maximum number of accounting attempts.
Server Quiet Period(minutes)	Quiet period for the servers, in minutes.
Realtime Accounting Interval(seconds)	Interval for sending real-time accounting updates, in seconds.
NAS IP Address	Source IP addresses for outgoing RADIUS packets. This field displays **Not configured** if no source IP addresses are specified for outgoing RADIUS packets.
User Name Format	Format for the usernames sent to the RADIUS server: • **with-domain**—Includes the domain name. • **without-domain**—Excludes the domain name. • **keep-original**—Forwards the username as the username is entered.
Data flow unit	Measurement unit for data flow.
Packet unit	Measurement unit for packets.
Attribute 15 check-mode	RADIUS Login-Service attribute check method for SSH, FTP, and terminal users: • **Strict**—Matches Login-Service attribute values 50, 51, and 52 for SSH, FTP, and terminal services, respectively. • **Loose**—Matches the standard Login-Service attribute value 0 for SSH, FTP, and terminal services.
Attribute 25	RADIUS attribute 25 interpretation status: • **Standard**—The attribute is not interpreted as CAR parameters. • **CAR**—The attribute is interpreted as CAR parameters.
Attribute Remanent-Volume unit	Data measurement unit for the RADIUS Remanent_Volume attribute.
RADIUS server version (vendor ID 2011)	Version of the RADIUS servers with a vendor ID of 2011: • 1.0. • 1.1.
Attribute 30 MAC format	Format of the MAC address in the RADIUS Called-Station-Id attribute.
Attribute 31 MAC format	Format of the MAC address in the RADIUS Calling-Station-Id attribute.
Attribute 17 carry old password	Status of online user password change by using RADIUS attribute 17: • **Enabled**—Online user password change by using RADIUS attribute 17 is enabled. The device uses RADIUS attribute 17 to carry a user's old password. • **Disabled**—Online user password change by using RADIUS attribute

Field	Description
	17 is disabled.
Attribute 182 vendor-ID 25506 VLAN	Whether the device is enabled to interpret the Microsegment-Id attribute (attribute 182 with vendor ID 25506) to an authorization VLAN.
Parsing rules for attribute 18	Rules for the device to parse the RADIUS Reply-Message attribute.
If match	Match criterion, a string enclosed by double quotation marks ("").
Action	Action for users to take when the Reply-Message attribute value matches the criterion: • **New password**—Enters the new password. • **Next token**—Enters the netxt authentication factor for double-factor authentication.

display radius statistics

Use **display radius statistics** to display RADIUS packet statistics.

Syntax

display radius statistics

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display RADIUS packet statistics.

```
<Sysname> display radius statistics

                            Auth.         Acct.       SessCtrl.
          Request Packet:     0             0             0
            Retry Packet:     0             0             -
          Timeout Packet:     0             0             -
       Access Challenge:      0             -             -
          Account Start:      -             0             -
         Account Update:      -             0             -
           Account Stop:      -             0             -
      Terminate Request:      -             -             0
             Set Policy:      -             -             0
   Packet With Response:      0             0             0
Packet Without Response:      0             0             -
          Access Rejects:     0             -             -
          Dropped Packet:     0             0             0
          Check Failures:     0             0             0
```

Table 11 Command output

Field	Description
Auth.	Authentication packets.
Acct.	Accounting packets.
SessCtrl.	Session-control packets.
Request Packet	Number of request packets.
Retry Packet	Number of retransmitted request packets.
Timeout Packet	Number of request packets timed out.
Access Challenge	Number of access challenge packets.
Account Start	Number of start-accounting packets.
Account Update	Number of accounting update packets.
Account Stop	Number of stop-accounting packets.
Terminate Request	Number of packets for logging off users forcibly.
Set Policy	Number of packets for updating user authorization information.
Packet With Response	Number of packets for which responses were received.
Packet Without Response	Number of packets for which no responses were received.
Access Rejects	Number of Access-Reject packets.
Dropped Packet	Number of discarded packets.
Check Failures	Number of packets with checksum errors.

Related commands

`reset radius statistics`

exclude

Use **`exclude`** to exclude an attribute from RADIUS requests.

Use **`undo exclude`** to cancel the configuration of excluding an attribute from RADIUS requests.

Syntax

`exclude` { **`accounting`** | **`authentication`** } **`name`** *`attribute-name`*

`undo exclude` { **`accounting`** | **`authentication`** } **`name`** *`attribute-name`*

Default

No attributes are configured to be excluded from RADIUS requests.

Views

RADIUS attribute test group view

Predefined user roles

network-admin

context-admin

Parameters

`accounting`: Specifies RADIUS accounting requests.

authentication: Specifies RADIUS authentication requests.

name *attribute-name*: Specifies a RADIUS attribute by its name, a case-insensitive string of 1 to 63 characters. The specified attribute must be an attribute that RADIUS requests carry by default. Available attributes that you can specify for RADIUS authentication requests include Service-Type, Framed-Protocol, NAS-Identifier, Acct-Session-Id, and NAS-Port-Type. Available attributes that you can specify for RADIUS accounting requests include NAS-Identifier, Acct-Delay-Time, Acct-Session-Id, and Acct-Terminate-Cause.

Usage guidelines

Use this command to exclude an attribute from RADIUS requests sent during an AAA test to help troubleshoot authentication or accounting failures.

Before you exclude an attribute that is already configured to be included in RADIUS requests, you must cancel the inclusion configuration by using the **undo include** command.

Examples

In RADIUS attribute test group **t1**, exclude Service-Type attribute from RADIUS authentication requests.

```
<Sysname> system-view
[Sysname] radius attribute-test-group t1
[Sysname-radius-attr-test-grp-t1] exclude authentication name Service-Type
```

Related commands

include

test-aaa

include

Use **include** to include an attribute in RADIUS requests.

Use **undo include** to cancel the configuration of including an attribute in RADIUS requests.

Syntax

include { **accounting** | **authentication** } { **name** *attribute-name* | [**vendor** *vendor-id*] **code** *attribute-code* } **type** { **binary** | **date** | **integer** | **interface-id** | **ip** | **ipv6** | **ipv6-prefix** | **octets** | **string** } **value** *attribute-value*

undo include { **accounting** | **authentication**} { **name** *attribute-name* | [**vendor** *vendor-id*] **code** *attribute-code* }

Default

No attributes are configured to be included in RADIUS authentication or accounting requests.

Views

RADIUS attribute test group view

Predefined user roles

network-admin

context-admin

Parameters

accounting: Specifies RADIUS accounting requests.

authentication: Specifies RADIUS authentication requests.

name *attribute-name*: Specifies a standard RADIUS attribute by its name, a case-insensitive string of 1 to 63 characters.

vendor *vendor-id*: Specifies a vendor by its ID in the range of 1 to 65535. If you do not specify a vendor, this command includes a standard attribute in RADIUS requests. Table 12 shows the vendor IDs of supported vendors.

Table 12 Supported vendors and vendor IDs

Vendor	Vendor ID	Vendor	Vendor ID	Vendor	Vendor ID
HUAWEI	2011	NSFOCUS	25506	Microsoft	311
3COM	43	DSL Forum	3561	China Telecom	20942
Wi-Fi Alliance	40808	Juniper	2636	CMCC	28357
Cisco	9				

code *attribute-code*: Specifies a RADIUS attribute by its code in the range of 1 to 255.

type: Specifies a data type for the attribute content.

binary: Binary type.

date: Date type.

integer: Integer type.

interface-id: Interface ID type.

ip: IPv4 address type.

ipv6: IPv6 address type.

ipv6-prefix: IPv6 address prefix type.

octets: Octet type.

string: String type.

value *attribute-value*: Specifies the value for the attribute of the data type. The value range of the *attribute-value* argument varies by data type.

- For the binary type, the value is a string of 1 to 256 hexadecimal characters, which represents a binary number with a maximum of 128 bytes.
- For the date type, the value range is 0 to 4294967295.
- For the integer type, the value range is 0 to 4294967295.
- For the interface ID type, the value range is 1 to ffffffffffffffff.
- For the IPv6 address prefix type, the value is in the format of *prefix*/*prefix-length*.
- For the octet type, the value is a string of 1 to 256 hexadecimal characters, which represents an octet number with a maximum of 128 bytes.
- For the string type, the value of this argument is a string of 1 to 253 characters.

Usage guidelines

RADIUS requests carry some attributes by default. For these attributes, you can use the **include** command to change its value or use the **undo include** command to restore its value to the default. Table 13 shows the attributes that RADIUS requests carry by default.

Table 13 Attributes that RADIUS requests carry by default

Packet type	Attributes that the type of packets carry by default
RADIUS authentication request	User-Name CHAP-Password (or User-Password) CHAP-Challenge NAS-IP-Address (or NAS-IPv6-Address) Service-Type Framed-Protocol NAS-Identifier NAS-Port-Type Acct-Session-Id
RADIUS accounting request	User-Name Acct-Status-Type NAS-IP-Address (or NAS-IPv6-Address) NAS-Identifier Acct-Session-Id Acct-Delay-Time Acct-Terminate-Cause

For the accuracy of AAA tests, the value of an attribute must be of the data type specified for that attribute.

The attribute names of standard attributes saved in the configuration file will be converted to attribute codes.

Before you include an attribute that is already configured to be excluded from RADIUS requests, you must cancel the exclusion configuration by using the **undo exclude** command.

You can include multiple attributes in RADIUS requests. The device adds the included attributes to RADIUS packets in the order they are configured. If the length of a RADIUS request reaches 4096 bytes, the device will not add the remaining attributes to the request. As a best practice, include a reasonable number of attributes in RADIUS requests.

Examples

In RADIUS attribute test group **t1**, include Calling-Station-Id attribute with value 08-00-27-00-34-D8 in RADIUS authentication requests.

```
<Sysname> system-view
[Sysname] radius attribute-test-group t1
[Sysname-radius-attr-test-grp-t1] include authentication name Calling-Station-Id type
string value 08-00-27-00-34-d8
```

Related commands

exclude

test-aaa

key (RADIUS scheme view)

Use **key** to set the shared key for secure RADIUS authentication or accounting communication.

Use **undo key** to delete the shared key for secure RADIUS authentication or accounting communication.

Syntax

key { **accounting** | **authentication** } { **cipher** | **simple** } *string*

undo key { **accounting** | **authentication** }

Default

No shared key is configured for secure RADIUS authentication or accounting communication.

Views

RADIUS scheme view

Predefined user roles

network-admin

context-admin

Parameters

accounting: Specifies the shared key for secure RADIUS accounting communication.

authentication: Specifies the shared key for secure RADIUS authentication communication.

cipher: Specifies the key in encrypted form.

simple: Specifies the key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. This argument is case sensitive. The encrypted form of the key is a string of 1 to 117 characters. The plaintext form of the key is a string of 1 to 64 characters.

Usage guidelines

The shared keys configured by using this command apply to all servers in the scheme. Make sure the settings match the shared keys configured on the RADIUS servers.

The shared keys specified for specific RADIUS servers take precedence over the shared key specified with this command.

Examples

In RADIUS scheme **radius1**, set the shared key to **ok** in plaintext form for secure accounting communication.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] key accounting simple ok
```

Related commands

display radius scheme

nas-ip (RADIUS scheme view)

Use **nas-ip** to specify a source IP address for outgoing RADIUS packets.

Use **undo nas-ip** to delete the specified source IP address for outgoing RADIUS packets.

Syntax

nas-ip { *ipv4-address* | **ipv6** *ipv6-address* }

undo nas-ip [**ipv6**]

Default

The source IP address of an outgoing RADIUS packet is that specified by using the **radius nas-ip** command in system view.

If the **radius nas-ip** command is not used, the source IP address is the primary IP address of the outbound interface.

Views

RADIUS scheme view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-address: Specifies an IPv4 address, which must be an address of the device. The IP address cannot be 0.0.0.0, 255.255.255.255, a class D address, a class E address, or a loopback address.

ipv6 *ipv6-address*: Specifies an IPv6 address, which must be a unicast address of the device and cannot be a loopback address or a link-local address.

Usage guidelines

The source IP address of RADIUS packets that a NAS sends must match the IP address of the NAS that is configured on the RADIUS server. A RADIUS server identifies a NAS by its IP address. Upon receiving a RADIUS packet, the RADIUS server checks the source IP address of the packet.

- If the source IP address of the packet is the IP address of a managed NAS, the server processes the packet.
- If the source IP address of the packet is not the IP address of a managed NAS, the server drops the packet.

As a best practice, specify a loopback interface address as the source IP address for outgoing RADIUS packets to avoid RADIUS packet loss caused by physical port errors.

If you use both the **nas-ip** command and **radius nas-ip** command, the following guidelines apply:

- The setting configured by using the **nas-ip** command in RADIUS scheme view applies only to the RADIUS scheme.
- The setting configured by using the **radius nas-ip** command in system view applies to all RADIUS schemes.
- The setting in RADIUS scheme view takes precedence over the setting in system view.

For a RADIUS scheme, you can specify only one source IPv4 address and one source IPv6 address for outgoing RADIUS packets.

If you do not specify any parameter for the **undo nas-ip** command, the command deletes the specified source IPv4 address for outgoing RADIUS packets.

Examples

In RADIUS scheme **radius1**, specify IP address 10.1.1.1 as the source IP address for outgoing RADIUS packets.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] nas-ip 10.1.1.1
```

Related commands

display radius scheme

radius nas-ip

port

Use **port** to specify the RADIUS DAS port.

Use **undo port** to restore the default.

Syntax

port *port-number*

undo port

Default

The RADIUS DAS port number is 3799.

Views

RADIUS DAS view

Predefined user roles

network-admin

context-admin

Parameters

port-number: Specifies a UDP port number in the range of 1 to 65535.

Usage guidelines

The destination port in DAE packets on the DAC must be the same as the RADIUS DAS port on the DAS.

Examples

Enable the RADIUS DAS to listen to UDP port 3790 for DAE requests.

```
<Sysname> system-view
[Sysname] radius dynamic-author server
[Sysname-radius-da-server] port 3790
```

Related commands

client

radius dynamic-author server

primary accounting (RADIUS scheme view)

Use **primary accounting** to specify the primary RADIUS accounting server.

Use **undo primary accounting** to restore the default.

Syntax

primary accounting { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **vpn-instance** *vpn-instance-name*] *

undo primary accounting

Default

The primary RADIUS accounting server is not specified.

Views

RADIUS scheme view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-address: Specifies the IPv4 address of the primary RADIUS accounting server.

ipv6 *ipv6-address*: Specifies the IPv6 address of the primary RADIUS accounting server.

port-number: Specifies the service port number of the primary RADIUS accounting server. The value range for the UDP port number is 1 to 65535. The default setting is 1813.

key: Specifies the shared key for secure communication with the primary RADIUS accounting server.

cipher: Specifies the key in encrypted form.

simple: Specifies the key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. This argument is case sensitive. The encrypted form of the key is a string of 1 to 117 characters. The plaintext form of the key is a string of 1 to 64 characters.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance to which the primary RADIUS accounting server belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the server is on the public network, do not specify this option.

Usage guidelines

Make sure the port number and shared key settings of the primary RADIUS accounting server are the same as those configured on the server.

Two accounting servers specified for a scheme, primary or secondary, cannot have identical VPN instance, IP address, and port number settings.

The shared key configured by using this command takes precedence over the shared key configured with the **key accounting** command.

If the specified server resides on an MPLS L3VPN, specify the VPN instance by using the **vpn-instance** *vpn-instance-name* option. The VPN instance specified by this command takes precedence over the VPN instance specified for the RADIUS scheme.

If you use the **primary accounting** command to modify or delete the primary accounting server to which the device is sending a start-accounting request, communication with the primary server times out. The device tries to communicate with an active server that has the highest priority for accounting.

If you remove an actively used accounting server, the device no longer sends users' real-time accounting requests and stop-accounting requests. It does not buffer the stop-accounting requests. The device can generate incorrect accounting results.

Examples

In RADIUS scheme **radius1**, specify the primary accounting server with IP address 10.110.1.2, UDP port number 1813, and plaintext shared key **123456TESTacct&!**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] primary accounting 10.110.1.2 1813 key simple 123456TESTacct&!
```

Related commands

display radius scheme

key (RADIUS scheme view)

secondary accounting (RADIUS scheme view)

vpn-instance (RADIUS scheme view)

primary authentication (RADIUS scheme view)

Use **primary authentication** to specify the primary RADIUS authentication server.

Use **undo primary authentication** to restore the default.

Syntax

primary authentication { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **test-profile** *profile-name* | **vpn-instance** *vpn-instance-name*] *

undo primary authentication

Default

The primary RADIUS authentication server is not specified.

Views

RADIUS scheme view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-address: Specifies the IPv4 address of the primary RADIUS authentication server.

ipv6 *ipv6-address*: Specifies the IPv6 address of the primary RADIUS authentication server.

port-number: Specifies the service port number of the primary RADIUS authentication server. The value range for the UDP port number is 1 to 65535. The default setting is 1812.

key: Specifies the shared key for secure communication with the primary RADIUS authentication server.

cipher: Specifies the key in encrypted form.

simple: Specifies the key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. This argument is case sensitive. The encrypted form of the key is a string of 1 to 117 characters. The plaintext form of the key is a string of 1 to 64 characters.

test-profile *profile-name*: Specifies a test profile for detecting the RADIUS server status. The *profile-name* argument is a case-sensitive string of 1 to 31 characters.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance to which the primary RADIUS authentication server belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the server is on the public network, do not specify this option.

Usage guidelines

Make sure the service port and shared key settings of the primary RADIUS authentication server are the same as those configured on the server.

Two authentication servers specified for a scheme, primary or secondary, cannot have identical VPN instance, IP address, and port number settings.

The shared key configured by this command takes precedence over the shared key configured with the **key authentication** command.

The server status detection is triggered for the server if the specified test profile exists on the device.

If the specified server resides on an MPLS L3VPN, specify the VPN instance by using the **vpn-instance** *vpn-instance-name* option. The VPN instance specified by this command takes precedence over the VPN instance specified for the RADIUS scheme.

If you use the **primary authentication** command to modify or delete the primary authentication server during an authentication process, communication with the primary server times out. The device tries to communicate with an active server that has the highest priority for authentication.

Examples

In RADIUS scheme **radius1**, specify the primary authentication server with IP address 10.110.1.1, UDP port number 1812, and plaintext shared key **123456TESTauth&!**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] primary authentication 10.110.1.1 1812 key simple
123456TESTauth&!
```

Related commands

display radius scheme

key (RADIUS scheme view)

radius-server test-profile

secondary authentication (RADIUS scheme view)

vpn-instance (RADIUS scheme view)

radius attribute extended

Use **radius attribute extended** to define an extended RADIUS attribute.

Use **undo radius attribute extended** to delete user-defined extended RADIUS attributes.

Syntax

radius attribute extended *attribute-name* [**vendor** *vendor-id*] **code** *attribute-code* **type** { **binary** | **date** | **integer** | **interface-id** | **ip** | **ipv6** | **ipv6-prefix** | **octets** | **string** }

undo radius attribute extended [*attribute-name*]

Default

No user-defined extended RADIUS attributes exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

attribute-name: Specifies the RADIUS attribute name, a case-insensitive string of 1 to 63 characters. The name must be unique among all RADIUS attributes, including the standard and extended RADIUS attributes.

vendor *vendor-id*: Specifies a vendor ID in the range of 1 to 65535. If you do not specify a vendor ID, the device processes the RADIUS attribute as a standard RADIUS attribute.

code *attribute-code*: Specifies the ID of the RADIUS attribute in the attribute set. The value range for the *attribute-code* argument is 1 to 255.

type: Specifies a data type for the attribute content.

binary: Binary type.

date: Date type.

integer: Integer type.

interface-id: Interface ID type.

ip: IPv4 address type.

ipv6: IPv6 address type.

ipv6-prefix: IPv6 prefix type.

octets: Octet type.

string: String type.

Usage guidelines

To support the proprietary RADIUS attributes of other vendors, perform the following tasks:

1. Use this command to define the attributes as extended RADIUS attributes.
2. Use the **attribute convert** command to map the extended RADIUS attributes to attributes supported by the system.
3. Use the **attribute translate** command to enable the RADIUS attribute translation feature for the mappings to take effect.

To cooperate with RADIUS servers of a third-party vendor, map attributes that cannot be identified by the server to server-supported attributes.

Two RADIUS attributes cannot have the same combination of attribute name, vendor ID, and attribute ID.

If you do not specify a RADIUS attribute name, the **undo radius attribute extended** command deletes all user-defined extended RADIUS attributes.

Examples

Define a string-type extended RADIUS attribute with attribute name **Owner-Password**, vendor ID 122, and attribute ID 80.

```
<Sysname> system-view
[Sysname] radius attribute extended Owner-Password vendor 122 code 80 type string
```

Related commands

attribute convert (RADIUS DAS view)

attribute convert (RADIUS scheme view)

attribute reject (RADIUS DAS view)

attribute reject (RADIUS scheme view)

radius attribute-test-group

Use **radius attribute-test-group** to create a RADIUS attribute test group and enter its view, or enter the view of an existing RADIUS attribute test group.

Use **undo radius attribute-test-group** to remove a RADIUS attribute test group.

Syntax

radius attribute-test-group *attr-test-group-name*

undo radius attribute-test-group *attr-test-group-name*

Default

No RADIUS attribute test groups exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

attr-test-group-name: Specifies the name of a RADIUS attribute test group, a case-insensitive string of 1 to 31 characters.

Usage guidelines

A RADIUS attribute test group is a collection of RADIUS attributes that will be included in or excluded from RADIUS requests.

The system can have multiple RADIUS attribute test groups.

Examples

Create a RADIUS attribute test group named **t1** and enter its view.

```
<Sysname> system-view
[Sysname] radius attribute-test-group t1
[Sysname-radius-attr-test-grp-t1]
```

Related commands

exclude

include

test-aaa

radius dscp

Use **radius dscp** to change the DSCP priority of RADIUS packets.

Use **undo radius dscp** to restore the default.

Syntax

radius [**ipv6**] **dscp** *dscp-value*

undo radius [**ipv6**] **dscp**

Default

The DSCP priority of RADIUS packets is 0.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ipv6: Specifies the IPv6 RADIUS packets. If you do not specify this keyword, the command sets the DSCP priority for the IPv4 RADIUS packets.

dscp-value: Specifies the DSCP priority of RADIUS packets, in the range of 0 to 63. A larger value represents a higher priority.

Usage guidelines

Use this command to set the DSCP priority in the ToS field of RADIUS packets for changing their transmission priority.

Examples

Set the DSCP priority of IPv4 RADIUS packets to 10.

```
<Sysname> system-view
[Sysname] radius dscp 10
```

radius dynamic-author server

Use **radius dynamic-author server** to enable the RADIUS DAS feature and enter RADIUS DAS view.

Use **undo radius dynamic-author server** to disable the RADIUS DAS feature.

Syntax

radius dynamic-author server

undo radius dynamic-author server

Default

The RADIUS DAS feature is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

After you enable the RADIUS DAS feature, the device listens to the RADIUS DAS port to receive DAE packets from specified DACs. Based on the DAE packet type and contents, the device performs one of the following operations:

- Log off online users.
- Change online user authorization information.

Examples

Enable the RADIUS DAS feature and enter RADIUS DAS view.

```
<Sysname> system-view
```

```
[Sysname] radius dynamic-author server
[Sysname-radius-da-server]
```

Related commands

client

port

radius nas-ip

Use **radius nas-ip** to specify a source IP address for outgoing RADIUS packets.

Use **undo radius nas-ip** to delete the specified source IP address for outgoing RADIUS packets.

Syntax

radius nas-ip { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]

undo radius nas-ip { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]

Default

The source IP address of an outgoing RADIUS packet is the primary IPv4 address or the IPv6 address of the outbound interface.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-address: Specifies an IPv4 address, which must be an address of the device. The IP address cannot be 0.0.0.0, 255.255.255.255, a class D address, a class E address, or a loopback address.

ipv6 *ipv6-address*: Specifies an IPv6 address, which must be a unicast address of the device and cannot be a loopback address or a link-local address.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance to which the source IP address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. To configure a public-network source IP address, do not specify this option.

Usage guidelines

The source IP address of RADIUS packets that a NAS sends must match the IP address of the NAS that is configured on the RADIUS server. A RADIUS server identifies a NAS by its IP address. Upon receiving a RADIUS packet, the RADIUS server checks the source IP address of the packet.

- If the source IP address of the packet is the IP address of a managed NAS, the server processes the packet.
- If the source IP address of the packet is not the IP address of a managed NAS, the server drops the packet.

As a best practice, specify a loopback interface address as the source IP address for outgoing RADIUS packets to avoid RADIUS packet loss caused by physical port errors.

If you use both the **nas-ip** command and **radius nas-ip** command, the following guidelines apply:

- The setting configured by using the **nas-ip** command in RADIUS scheme view applies only to the RADIUS scheme.
- The setting configured by using the **radius nas-ip** command in system view applies to all RADIUS schemes.
- The setting in RADIUS scheme view takes precedence over the setting in system view.

You can specify a maximum of 16 source IP addresses in system view, including:

- Zero or one public-network source IPv4 address.
- Zero or one public-network source IPv6 address.
- Private-network source IP addresses.

Each VPN instance can have only one private-network source IPv4 address and one private-network source IPv6 address in system view.

Examples

Specify IP address 129.10.10.1 as the source IP address for outgoing RADIUS packets.

```
<Sysname> system-view
[Sysname] radius nas-ip 129.10.10.1
```

Related commands

nas-ip (RADIUS scheme view)

radius scheme

Use **radius scheme** to create a RADIUS scheme and enter its view, or enter the view of an existing RADIUS scheme.

Use **undo radius scheme** to delete a RADIUS scheme.

Syntax

radius scheme *radius-scheme-name*

undo radius scheme *radius-scheme-name*

Default

No RADIUS schemes exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

radius-scheme-name: Specifies the RADIUS scheme name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

A RADIUS scheme can be used by more than one ISP domain at the same time.

The device supports a maximum of 16 RADIUS schemes.

Examples

Create a RADIUS scheme named **radius1** and enter RADIUS scheme view.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1]
```

Related commands

display radius scheme

radius session-control client

Use **radius session-control client** to specify a RADIUS session-control client.

Use **undo radius session-control client** to remove the specified RADIUS session-control clients.

Syntax

radius session-control client { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**key** { **cipher** | **simple** } *string* | **vpn-instance** *vpn-instance-name*] *

undo radius session-control client { **all** | { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] }

Default

No RADIUS session-control clients are specified.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ip *ipv4-address*: Specifies a session-control client by its IPv4 address.

ipv6 *ipv6-address*: Specifies a session-control client by its IPv6 address.

key: Specifies the shared key for secure communication with the session-control client.

cipher: Specifies the key in encrypted form.

simple: Specifies the key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. This argument is case sensitive. The encrypted form of the key is a string of 1 to 117 characters. The plaintext form of the key is a string of 1 to 64 characters.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance to which the RADIUS session-control client belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the client is on the public network, do not specify this option.

all: Specifies all session-control clients.

Usage guidelines

To verify the session-control packets sent from a RADIUS server running on IMC, specify the RADIUS server as a session-control client to the device. The device matches a session-control packet to a session-control client based on the IP address and VPN instance, and then uses the shared key of the matched client to validate the packet.

The device searches the session-control client settings prior to searching all RADIUS scheme settings for a server with matching settings. This process narrows the search scope for finding the matched RADIUS server.

The session-control client settings take effect only when the RADIUS session-control feature is enabled.

The session-control client settings must be the same as the corresponding settings of the RADIUS server.

You can specify multiple session-control clients on the device.

Examples

Specify a session-control client with IP address 10.110.1.2 and shared key **12345** in plaintext form.

```
<Sysname> system-view
[Sysname] radius session-control client ip 10.110.1.2 key simple 12345
```

Related commands

radius session-control enable

radius session-control enable

Use **radius session-control enable** to enable the RADIUS session-control feature.

Use **undo radius session-control enable** to disable the RADIUS session-control feature.

Syntax

radius session-control enable

undo radius session-control enable

Default

The RADIUS session-control feature is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

An IMC RADIUS server uses session-control packets to deliver dynamic authorization change requests or disconnection requests to the device. The session-control feature enables the device to receive the RADIUS session-control packets on UDP port 1812.

This feature must work with IMC servers.

Examples

Enable the RADIUS session-control feature.

```
<Sysname> system-view
[Sysname] radius session-control enable
```

radius-server test-profile

Use **radius-server test-profile** to configure a test profile for detecting the RADIUS server status.

Use **undo radius-server test-profile** to delete a RADIUS test profile.

Syntax

radius-server test-profile *profile-name* **username** *name* [**interval** *interval*]

undo radius-server test-profile *profile-name*

Default

No RADIUS test profiles exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

profile-name: Specifies the name of the test profile, which is a case-sensitive string of 1 to 31 characters.

username *name*: Specifies the username in the detection packets. The *name* argument is a case-sensitive string of 1 to 253 characters.

interval *interval*: Specifies the interval for sending a detection packet, in minutes. The value range for the *interval* argument is 1 to 3600, and the default value is 60.

Usage guidelines

The device starts detecting the status of a RADIUS server only if the test profile specified for the server exists. If you specify a nonexistent test profile for a RADIUS server, the device does not detect the status of the server until you create the test profile on the device.

When you delete a test profile, the device stops detecting the status of RADIUS servers that use the test profile.

You can execute this command multiple times to configure multiple test profiles.

Examples

Configure a test profile named **abc** for RADIUS server status detection. A detection packet that uses username **admin** is sent every 10 minutes.

```
<Sysname> system-view
[Sysname] radius-server test-profile abc username admin interval 10
```

Related commands

primary authentication (RADIUS scheme view)

secondary authentication (RADIUS scheme view)

reset radius statistics

Use **reset radius statistics** to clear RADIUS statistics.

Syntax

reset radius statistics

Views

User view

Predefined user roles

network-admin

context-admin

Examples

Clear RADIUS statistics.

```
<Sysname> reset radius statistics
```

Related commands

display radius statistics

retry

Use **retry** to set the maximum number of attempts for transmitting a RADIUS packet to a single RADIUS server.

Use **undo retry** to restore the default.

Syntax

retry *retries*

undo retry

Default

The maximum number of RADIUS packet transmission attempts is 3.

Views

RADIUS scheme view

Predefined user roles

network-admin

context-admin

Parameters

retries: Specifies the maximum number of RADIUS packet transmission attempts, in the range of 1 to 20.

Usage guidelines

Because RADIUS uses UDP packets to transmit data, the communication is not reliable.

If the device does not receive a response to its request from the RADIUS server within the response timeout period, the device retransmits the RADIUS request. To set the response timeout period, use the **timer response-timeout** command.

If the device does not receive a response from the RADIUS server after the maximum number of transmission attempts is reached, the device considers the request a failure.

If the client times out during the authentication process, the user is immediately logged off. To avoid user logoffs, the value multiplied by the following items cannot be larger than the client timeout period defined by the access module:

- The maximum number of RADIUS packet transmission attempts.
- The RADIUS server response timeout period.
- The number of RADIUS authentication servers in the RADIUS scheme.

When the device sends a RADIUS request to a new RADIUS server, it checks the total amount of time it has taken to transmit the RADIUS packet. If the amount of time has reached 300 seconds, the device stops sending the RADIUS request to the next RADIUS server. As a best practice, consider

the number of RADIUS servers when you configure the maximum number of packet transmission attempts and the RADIUS server response timeout period.

Examples

In RADIUS scheme **radius1**, set the maximum number of RADIUS packet transmission attempts to 5.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] retry 5
```

Related commands

radius scheme

timer response-timeout (RADIUS scheme view)

retry realtime-accounting

Use **retry realtime-accounting** to set the maximum number of accounting attempts.

Use **undo retry realtime-accounting** to restore the default.

Syntax

retry realtime-accounting *retries*

undo retry realtime-accounting

Default

The maximum number of accounting attempts is 5.

Views

RADIUS scheme view

Predefined user roles

network-admin

context-admin

Parameters

retries: Specifies the maximum number of accounting attempts, in the range of 1 to 255.

Usage guidelines

Typically, a RADIUS accounting server checks whether a user is online by using a timeout timer. If the server does not receive a real-time accounting request for a user in the timeout period, it considers that a line or device failure has occurred. The server stops accounting for the user.

To work with the RADIUS server, the NAS needs to send real-time accounting requests to the server before the timer on the server expires and to keep pace with the server in disconnecting the user when a failure occurs. The NAS disconnects from a user according to the maximum number of accounting attempts and specific parameters.

For example, the following conditions exist:

- The RADIUS server response timeout period is 3 seconds (set by using the **timer response-timeout** command).
- The maximum number of RADIUS packet transmission attempts is 3 (set by using the **retry** command).
- The real-time accounting interval is 12 minutes (set by using the **timer realtime-accounting** command).

- The maximum number of accounting attempts is 5 (set by using the **retry realtime-accounting** command).

In the above case, the device generates an accounting request every 12 minutes, and retransmits the request if it sends the request but receives no response within 3 seconds. If the device receives no response after transmitting the request three times, it considers the accounting attempt a failure, and makes another accounting attempt. If five consecutive accounting attempts fail, the device cuts the user connection.

Examples

In RADIUS scheme **radius1**, set the maximum number of accounting attempts to 10.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] retry realtime-accounting 10
```

Related commands

retry

timer realtime-accounting (RADIUS scheme view)

timer response-timeout (RADIUS scheme view)

secondary accounting (RADIUS scheme view)

Use **secondary accounting** to specify a secondary RADIUS accounting server.

Use **undo secondary accounting** to remove a secondary RADIUS accounting server.

Syntax

secondary accounting { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **vpn-instance** *vpn-instance-name*] *

undo secondary accounting [{ *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **vpn-instance** *vpn-instance-name*] *]

Default

No secondary RADIUS accounting servers are specified.

Views

RADIUS scheme view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-address: Specifies the IPv4 address of a secondary RADIUS accounting server.

ipv6 *ipv6-address*: Specifies the IPv6 address of a secondary RADIUS accounting server.

port-number: Specifies the service port number of the secondary RADIUS accounting server. The value range for the UDP port number is 1 to 65535. The default setting is 1813.

key: Specifies the shared key for secure communication with the secondary RADIUS accounting server.

cipher: Specifies the key in encrypted form.

simple: Specifies the key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. This argument is case sensitive. The encrypted form of the key is a string of 1 to 117 characters. The plaintext form of the key is a string of 1 to 64 characters.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance to which the secondary RADIUS accounting server belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the server is on the public network, do not specify this option.

Usage guidelines

Make sure the port number and shared key settings of each secondary RADIUS accounting server are the same as those configured on the corresponding server.

A RADIUS scheme supports a maximum of 16 secondary RADIUS accounting servers. If the primary server fails, the device tries to communicate with a secondary server in active state. The device connects to the secondary servers in the order they are configured.

Two accounting servers specified for a scheme, primary or secondary, cannot have identical VPN instance, IP address, and port number settings.

The shared key configured by this command takes precedence over the shared key configured with the **key accounting** command.

If the specified server resides on an MPLS L3VPN, specify the VPN instance by using the **vpn-instance** *vpn-instance-name* option. The VPN instance specified by this command takes precedence over the VPN instance specified for the RADIUS scheme.

If you use the **secondary accounting** command to modify or delete a secondary accounting server to which the device is sending a start-accounting request, communication with the secondary server times out. The device tries to communicate with an active server that has the highest priority for accounting.

If you remove an actively used accounting server, the device no longer sends users' real-time accounting requests and stop-accounting requests. The device does not buffer the stop-accounting requests, either.

Examples

In RADIUS scheme **radius1**, specify a secondary accounting server with IP address 10.110.1.1 and UDP port 1813.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] secondary accounting 10.110.1.1 1813
```

In RADIUS scheme **radius2**, specify two secondary accounting servers with IP addresses 10.110.1.1 and 10.110.1.2 and UDP port 1813.

```
<Sysname> system-view
[Sysname] radius scheme radius2
[Sysname-radius-radius2] secondary accounting 10.110.1.1 1813
[Sysname-radius-radius2] secondary accounting 10.110.1.2 1813
```

Related commands

display radius scheme

key (RADIUS scheme view)

primary accounting (RADIUS scheme view)

vpn-instance (RADIUS scheme view)

secondary authentication (RADIUS scheme view)

Use **secondary authentication** to specify a secondary RADIUS authentication server.

Use **undo secondary authentication** to remove a secondary RADIUS authentication server.

Syntax

secondary authentication { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **test-profile** *profile-name* | **vpn-instance** *vpn-instance-name*] *

undo secondary authentication [{ *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **vpn-instance** *vpn-instance-name*] *]

Default

No secondary RADIUS authentication servers are specified.

Views

RADIUS scheme view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-address: Specifies the IPv4 address of a secondary RADIUS authentication server.

ipv6 *ipv6-address*: Specifies the IPv6 address of a secondary RADIUS authentication server.

port-number: Specifies the service port number of the secondary RADIUS authentication server. The value range for the UDP port number is 1 to 65535. The default setting is 1812.

key: Specifies the shared key for secure communication with the secondary RADIUS authentication server.

cipher: Specifies the key in encrypted form.

simple: Specifies the key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. This argument is case sensitive. The encrypted form of the key is a string of 1 to 117 characters. The plaintext form of the key is a string of 1 to 64 characters.

test-profile *profile-name*: Specifies a test profile for detecting the RADIUS server status. The *profile-name* argument is a case-sensitive string of 1 to 31 characters.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance to which the secondary RADIUS authentication server belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the server is on the public network, do not specify this option.

Usage guidelines

Make sure the port number and shared key settings of each secondary RADIUS authentication server are the same as those configured on the corresponding server.

A RADIUS scheme supports a maximum of 16 secondary RADIUS authentication servers. If the primary server fails, the device tries to communicate with a secondary server in active state. The device connects to the secondary servers in the order they are configured.

The server status detection is triggered for a server if the specified test profile exists on the device.

Two authentication servers specified for a scheme, primary or secondary, cannot have identical VPN instance, IP address, and port number settings.

The shared key configured by this command takes precedence over the shared key configured with the **key authentication** command.

If the specified server resides on an MPLS L3VPN, specify the VPN instance by using the **vpn-instance** *vpn-instance-name* option. The VPN instance specified by this command takes precedence over the VPN instance specified for the RADIUS scheme.

If you use the **secondary authentication** command to modify or delete a secondary authentication server during an authentication process, communication with the secondary server times out. The device tries to communicate with an active server that has the highest priority for authentication.

Examples

In RADIUS scheme **radius1**, specify a secondary authentication server with IP address 10.110.1.2 and UDP port 1812.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] secondary authentication 10.110.1.2 1812
```

In RADIUS scheme **radius2**, specify two secondary authentication servers with IP addresses 10.110.1.1 and 10.110.1.2 and UDP port 1812.

```
<Sysname> system-view
[Sysname] radius scheme radius2
[Sysname-radius-radius2] secondary authentication 10.110.1.1 1812
[Sysname-radius-radius2] secondary authentication 10.110.1.2 1812
```

Related commands

display radius scheme

key (RADIUS scheme view)

primary authentication (RADIUS scheme view)

radius-server test-profile

vpn-instance (RADIUS scheme view)

snmp-agent trap enable radius

Use **snmp-agent trap enable radius** to enable SNMP notifications for RADIUS.

Use **undo snmp-agent trap enable radius** to disable SNMP notifications for RADIUS.

Syntax

snmp-agent trap enable radius [**accounting-server-down** | **accounting-server-up** | **authentication-error-threshold** | **authentication-server-down** | **authentication-server-up**] *

undo snmp-agent trap enable radius [**accounting-server-down** | **accounting-server-up** | **authentication-error-threshold** | **authentication-server-down** | **authentication-server-up**] *

Default

All RADIUS SNMP notifications are disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

accounting-server-down: Specifies notifications to be sent when the RADIUS accounting server becomes unreachable.

accounting-server-up: Specifies notifications to be sent when the RADIUS accounting server becomes reachable.

authentication-error-threshold: Specifies notifications to be sent when the number of authentication failures exceeds the specified threshold. The threshold is represented by the ratio of the authentication failures to the total number of authentication attempts. The value range is 1 to 100, and the default value is 30. This threshold can only be configured through the MIB.

authentication-server-down: Specifies notifications to be sent when the RADIUS authentication server becomes unreachable.

authentication-server-up: Specifies notifications to be sent when the RADIUS authentication server becomes reachable.

Usage guidelines

If you do not specify any keywords, this command enables or disables all types of notifications for RADIUS.

When SNMP notifications for RADIUS are enabled, the device supports the following notifications generated by RADIUS:

- **RADIUS server unreachable notification**—The RADIUS server cannot be reached. RADIUS generates this notification if it cannot receive any response to an accounting or authentication request within the specified RADIUS request transmission attempts.
- **RADIUS server reachable notification**—The RADIUS server can be reached. RADIUS generates this notification for a previously blocked RADIUS server after the quiet timer expires.
- **Excessive authentication failures notification**—RADIUS generates this notification when the number of authentication failures to the total number of authentication attempts exceeds the specified threshold.

Examples

Enable the device to send RADIUS accounting server unreachable notifications.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable radius accounting-server-down
```

state primary

Use **state primary** to set the status of a primary RADIUS server.

Syntax

state primary { **accounting** | **authentication** } { **active** | **block** }

Default

A primary RADIUS server is in active state.

Views

RADIUS scheme view

Predefined user roles

network-admin

context-admin

Parameters

accounting: Specifies the primary RADIUS accounting server.

authentication: Specifies the primary RADIUS authentication server.

active: Specifies the active state, the normal operation state.

block: Specifies the blocked state, the out-of-service state.

Usage guidelines

During an authentication or accounting process, the device first tries to communicate with the primary server if the primary server is in active state. If the primary server is unavailable, the device performs the following operations:

- Changes the status of the primary server to blocked.
- Starts a quiet timer for the server.
- Tries to communicate with a secondary server in active state.

When the quiet timer of the primary server times out, the status of the server automatically changes to active. If you set the server status to blocked before the quiet timer times out, the server status cannot change back to active unless you manually set the status to active.

When all servers are in blocked state, the device tries to communicate with a server as follows:

- If the primary server is placed in blocked state automatically, the device only tries to communicate with the primary server.
- If the primary server is placed in blocked state manually, the device tries to communicate with secondary servers automatically placed in blocked state in the sequence they are configured.

This command can affect the RADIUS server status detection feature when a valid test profile is specified for a primary RADIUS authentication server.

- If you set the status of the server to blocked, the device stops detecting the status of the server.
- If you set the status of the server to active, the device starts to detect the status of the server.

Examples

In RADIUS scheme **radius1**, set the status of the primary authentication server to blocked.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] state primary authentication block
```

Related commands

display radius scheme

radius-server test-profile

state secondary

state secondary

Use **state secondary** to set the status of a secondary RADIUS server.

Syntax

state secondary { **accounting** | **authentication** } [{ *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **vpn-instance** *vpn-instance-name*] *] { **active** | **block** }

Default

A secondary RADIUS server is in active state.

Views

RADIUS scheme view

Predefined user roles

network-admin

context-admin

Parameters

accounting: Specifies a secondary RADIUS accounting server.

authentication: Specifies a secondary RADIUS authentication server.

ipv4-address: Specifies the IPv4 address of a secondary RADIUS server.

ipv6 *ipv6-address*: Specifies the IPv6 address of a secondary RADIUS server.

port-number: Specifies the service port number of a secondary RADIUS server. The value range for the UDP port number is 1 to 65535. The default port numbers for authentication and accounting are 1812 and 1813, respectively.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance to which the secondary RADIUS server belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters.

active: Specifies the active state, the normal operation state.

block: Specifies the blocked state, the out-of-service state.

Usage guidelines

If you do not specify an IP address, this command changes the status of all configured secondary RADIUS servers.

If the device finds that a secondary server in active state is unreachable, the device performs the following operations:

- Changes the status of the secondary server to blocked.
- Starts a quiet timer for the server.
- Tries to communicate with another secondary server in active state.

When the quiet timer of a server times out, the status of the server automatically changes to active. If you set the server status to blocked before the quiet timer times out, the server status cannot change back to active unless you manually set the status to active. If all configured secondary servers are unreachable, the device considers the authentication or accounting attempt a failure.

This command can affect the RADIUS server status detection feature when a valid test profile is specified for a secondary RADIUS authentication server.

- If you set the status of the server to blocked, the device stops detecting the status of the server.
- If you set the status of the server to active, the device starts to detect the status of the server.

Examples

In RADIUS scheme **radius1**, set the status of all the secondary authentication servers to blocked.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] state secondary authentication block
```

Related commands

display radius scheme

radius-server test-profile

state primary

test-aaa

Use **test-aaa** to perform an AAA test.

Syntax

test-aaa user *user-name* **password** *password* **radius-scheme** *radius-scheme-name* [**radius-server** { *ipv4-address* | **ipv6** *ipv6-address* } *port-number* [**vpn-instance** *vpn-instance-name*]] [**chap** | **pap**] [**attribute-test-group** attr-*test-group-name*] [**trace**]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

user *user-name*: Specifies the test username, a string of 1 to 80 characters. The username can be a pure username or contain a domain name. The format for a username containing a domain name is *pure-username@domain-name*. The pure username is case sensitive and the domain name is case insensitive.

password *password*: Specifies the password of the test user, a case-sensitive string of 1 to 63 characters.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

radius-server: Specifies a RADIUS server.

ipv4-address: Specifies the IPv4 address of the RADIUS server.

ipv6 *ipv6-address*: Specifies the IPv6 address of the RADIUS server.

port-number: Specifies the UDP port number of the RADIUS server, in the range of 1 to 65535.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the RADIUS server belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the server is on the public network, do not specify this option.

chap: Specifies the CHAP authentication method (the default).

pap: Specifies the PAP authentication method.

attribute-test-group *attr-test-group-name*: Specifies a RADIUS attribute test group by its name, a case-insensitive string of 1 to 31 characters. If you do not specify a RADIUS attribute test group or the specified RADIUS attribute test group does not exist, the device does not change the attributes carried in authentication or accounting requests.

trace: Displays detailed information about RADIUS packets exchanged during the AAA test. If you do not specify this keyword, the command displays brief information about the AAA test, including the sent and received packets and the test result.

Usage guidelines

Use this command to identify the reasons for the failure of interaction between the device and the AAA servers.

The device might communicate with the AAA servers incorrectly during an AAA test. Make sure no users come online or go offline during an AAA text.

If the configuration of the specified RADIUS scheme changes, the new configuration does not affect the current AAA test. The modification will take effect in the next test.

The system can have only one AAA test at a time. Another AAA test can be performed only after the current test finishes.

Examples

Perform an AAA test and display detailed information about the test. The test uses username **user1**, password **123456**, the CHAP authentication method, and RADIUS scheme **test**.

```
<Sysname> test-aaa user user1 password 123456 radius-scheme test chap trace
Sent a RADIUS authentication request.
  Server  IP   : 192.168.1.110
  Source  IP   : 192.168.1.166
  VPN instance : N/A
  Server port  : 1812
  Packet type  : Authentication request
  Packet length: 118 bytes
  Packet ID    : 0
  Attribute list:
    [User-Name(1)]                [6]   [user1]
    [CHAP-Password(3)]            [19]  [******]
    [NAS-IP-Address(4)]           [6]   [192.168.1.166]
    [Service-Type(6)]             [6]   [2] [Framed]
    [Framed-Protocol(7)]          [6]   [1] [PPP]
    [NAS-Identifier(32)]          [5]   [Sysname]
    [Acct-Session-Id(44)]         [40]  [00000008201707241008280000000c16100171]
    [CHAP-Challenge(60)]          [18]  [******]
    [NAS-Port-Type(61)]           [6]   [15] [Ethernet]

Received a RADIUS authentication response.
  Server IP    : 192.168.1.110
  Source IP    : 192.168.1.166
  VPN instance : N/A
  Server port  : 1812
  Packet type  : Access-Reject
  Packet length: 20 bytes
  Packet ID    : 0
  Reply-Message: "E63032: Incorrect password. You can retry 9 times."

Sent a RADIUS start-accounting request.
  Server IP    : 192.168.1.110
  Source  IP   : 192.168.1.166
  VPN instance : N/A
  Server port  : 1813
  Packet type  : Start-accounting request
  Packet length: 63 bytes
  Packet ID    : 1
  Attribute list:
    [User-Name(1)]                [6]   [user1]
    [Acct-Status-Type(40)]        [6]   [1] [Start]
```

```
    [NAS-IP-Address(4)]             [6]   [192.168.1.166]
    [NAS-Identifier(32)]            [5]   [Sysname]
    [Acct-Session-Id(44)]           [40]  [00000008201707241008280000000c16100171]

Received a RADIUS start-accounting response.
  Server  IP   : 192.168.1.110
  Source  IP   : 192.168.1.166
  VPN instance : N/A
  Server port  : 1813
  Packet type  : Start-accounting response
  Packet length: 20 bytes
  Packet ID    : 1

Sent a RADIUS stop-accounting request.
  Server  IP   : 192.168.1.110
  Source  IP   : 192.168.1.166
  VPN instance : N/A
  Server port  : 1813
  Packet type  : Stop-accounting request
  Packet length: 91 bytes
  Packet ID    : 1
  Attribute list:
    [User-Name(1)]                  [6]   [user1]
    [Acct-Status-Type(40)]          [6]   [2] [Stop]
    [NAS-IP-Address(4)]             [6]   [192.168.1.166]
    [NAS-Identifier(32)]            [5]   [Sysname]
    [Acct-Delay-Time(41)]           [6]   [0]
    [Acct-Session-Id(44)]           [40]  [00000008201707241008280000000c16100171]
    [Acct-Terminate-Cause(49)]      [6]   [1] [User Request]

Received a RADIUS stop-accounting response.
  Server  IP   : 192.168.1.110
  Source  IP   : 192.168.1.166
  VPN instance : N/A
  Server port  : 1813
  Packet type  : Stop-accounting response
  Packet length: 20 bytes
  Packet ID    : 1


Test result: Failed
```

Perform an AAA test and display brief information about the test. The test uses username **user1**, password **123456** and the CHAP authentication method to test RADIUS server at 192.168.1.110 in RADIUS scheme **test**.

```
<Sysname> test-aaa user user1 password 123456 radius-scheme test radius-server
192.168.1.110 1812
Sent a RADIUS authentication request.
Received a RADIUS authentication response.


Test result: Successful
```

Table 14 Command output

Field	Description
Server IP	IP address of the server.
Source IP	Source IP address of the RADIUS packet.
VPN instance	MPLS L3VPN instance to which the server belongs. This field displays **N/A** if the server belongs to the public network.
Server port	UDP port number of the server.
Packet type	Type of the RADIUS packet: • Authentication request. • Access-Accept. • Access-Reject. • Start-accounting request. • Start-accounting response. • Stop-accounting request. • Stop-accounting response.
Packet length	Total length of the RADIUS packet, in bytes.
Packet ID	ID of the RADIUS packet. This field is used to identity a pair of request and response packets.
[*attribute-name* (*code*)] [*length*] [*value*] [*description*]	Information about a RADIUS attribute: • ***attribute-name***—Name of the attribute. • ***code***—Code of the attribute. • ***length***—Length of the attribute, in bytes. • ***value***—Value of the attribute. • ***description***—Description of the attribute.
Reply-Message:	The RADIUS server rejected the authentication request and replied a message.
Test result	Result of the AAA test: • **Successful**—The test has succeeded. • **Failed**—The test has failed. If any request is rejected, the test fails.

Related commands

`radius attribute-test-group`

`radius scheme`

timer quiet (RADIUS scheme view)

Use **`timer quiet`** to set the quiet timer for the servers specified in a RADIUS scheme.

Use **`undo timer quiet`** to restore the default.

Syntax

`timer quiet` *`minutes`*

`undo timer quiet`

Default

The server quiet timer period is 5 minutes in a RADIUS scheme.

Views

RADIUS scheme view

Predefined user roles

network-admin

context-admin

Parameters

minutes: Specifies the server quiet period in minutes, in the range of 1 to 255.

Usage guidelines

Make sure the server quiet timer is set correctly.

A timer that is too short might result in frequent authentication or accounting failures. This is because the device will continue to attempt to communicate with an unreachable server that is in active state.

A timer that is too long might temporarily block a reachable server that has recovered from a failure. This is because the server will remain in blocked state until the timer expires.

Examples

In RADIUS scheme **radius1**, set the quiet timer to 10 minutes for the servers.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] timer quiet 10
```

Related commands

display radius scheme

timer realtime-accounting (RADIUS scheme view)

Use **timer realtime-accounting** to set the real-time accounting interval.

Use **undo timer realtime-accounting** to restore the default.

Syntax

timer realtime-accounting *interval* [**second**]

undo timer realtime-accounting

Default

The real-time accounting interval is 12 minutes.

Views

RADIUS scheme view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies the real-time accounting interval in the range of 0 to 71582.

second: Specifies the measurement unit as second. If you do not specify this keyword, the real-time accounting interval is measured in minutes.

Usage guidelines

When the real-time accounting interval on the device is not zero, the device sends online user accounting information to the RADIUS accounting server at the configured interval.

When the real-time accounting interval on the device is zero, the device sends online user accounting information to the RADIUS accounting server at the real-time accounting interval configured on the server. If the real-time accounting interval is not configured on the server, the device does not send online user accounting information.

If a user uses RADIUS accounting but not RADIUS authentication and authorization, the device performs real-time accounting for that user only based on the real-time accounting interval set in the user's RADIUS accounting scheme. The real-time accounting interval assigned by the RADIUS accounting server does not take effect.

A short interval helps improve accounting precision but requires many system resources.

Table 15 Recommended real-time accounting intervals

Number of users	Real-time accounting interval
1 to 99	3 minutes
100 to 499	6 minutes
500 to 999	12 minutes
1000 or more	15 minutes or longer

When you modify the real-time accounting interval, the following rules apply to users that have been online before the modification:

- If you modify the real-time accounting interval from a non-zero value to zero or from zero to a non-zero value, the modification does not take effect on these users. These users still use the old real-time accounting interval.
- If you modify the real-time accounting interval from a non-zero value to another non-zero value, the modification takes effect immediately on these users.

The device sends a start-accounting packet for a dual-stack user after the user obtains an IP address of one stack. No matter how long the real-time accounting interval is, the device sends an update-accounting packet for the user immediately after the user obtains an IP address of another stack.

Examples

In RADIUS scheme **radius1**, set the real-time accounting interval to 51 minutes.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] timer realtime-accounting 51
```

Related commands

retry realtime-accounting

timer response-timeout (RADIUS scheme view)

Use **timer response-timeout** to set the RADIUS server response timeout timer.

Use **undo timer response-timeout** to restore the default.

Syntax

timer response-timeout *seconds*

undo timer response-timeout

Default

The RADIUS server response timeout period is 3 seconds.

Views

RADIUS scheme view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies the RADIUS server response timeout period, in the range of 1 to 10 seconds.

Usage guidelines

If a NAS receives no response from the RADIUS server in a period of time after sending a RADIUS request, it resends the request so that the user has more opportunity to obtain the RADIUS service. The NAS uses the RADIUS server response timeout timer to control the transmission interval.

If the client times out during the authentication process, the user is immediately logged off. To avoid user logoffs, the value multiplied by the following items cannot be larger than the client timeout period defined by the access module:

- The maximum number of RADIUS packet transmission attempts.
- The RADIUS server response timeout period.
- The number of RADIUS servers in the RADIUS scheme.

When the device sends a RADIUS request to a new RADIUS server, it checks the total amount of time it has taken to transmit the RADIUS packet. If the amount of time has reached 300 seconds, the device stops sending the RADIUS request to the next RADIUS server. As a best practice, consider the number of RADIUS servers when you configure the maximum number of packet transmission attempts and the RADIUS server response timeout period.

Examples

In RADIUS scheme **radius1**, set the RADIUS server response timeout timer to 5 seconds.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] timer response-timeout 5
```

Related commands

display radius scheme

retry

user-name-format (RADIUS scheme view)

Use **user-name-format** to specify the format of the username to be sent to a RADIUS server.

Use **undo user-name-format** to restore the default.

Syntax

user-name-format { **keep-original** | **with-domain** | **without-domain** }

undo user-name-format

Default

The ISP domain name is included in the usernames sent to a RADIUS server.

Views

RADIUS scheme view

Predefined user roles

network-admin

context-admin

Parameters

keep-original: Sends the username to the RADIUS server as the username is entered.

with-domain: Includes the ISP domain name in the username sent to the RADIUS server.

without-domain: Excludes the ISP domain name from the username sent to the RADIUS server.

Usage guidelines

A username is generally in the *userid@isp-name* format, of which the *isp-name* argument is used by the device to determine the ISP domain to which a user belongs. Some earlier RADIUS servers, however, cannot recognize a username containing an ISP domain name. Before sending a username including a domain name to such a RADIUS server, the device must remove the domain name. This command allows you to specify whether to include a domain name in a username sent to a RADIUS server.

If a RADIUS scheme defines that the username is sent without the ISP domain name, do not apply the scheme to more than one ISP domain. Otherwise, the RADIUS server will consider two users in different ISP domains but with the same *userid* as one user.

Examples

In RADIUS scheme **radius1**, configure the device to remove the domain name from the usernames sent to the RADIUS servers.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] user-name-format without-domain
```

Related commands

display radius scheme

vpn-instance (RADIUS scheme view)

Use **vpn-instance** to specify an MPLS L3VPN instance for a RADIUS scheme.

Use **undo vpn-instance** to restore the default.

Syntax

vpn-instance *vpn-instance-name*

undo vpn-instance

Default

The RADIUS scheme belongs to the public network.

Views

RADIUS scheme view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance-name: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

The VPN instance specified for a RADIUS scheme applies to all authentication and accounting servers in that scheme. If a VPN instance is also configured for an individual RADIUS server, the VPN instance specified for the RADIUS scheme does not take effect on that server.

Examples

Specify VPN instance **test** for RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] vpn-instance test
```

Related commands

display radius scheme

HWTACACS commands

data-flow-format (HWTACACS scheme view)

Use **data-flow-format** to set the data flow and packet measurement units for traffic statistics.

Use **undo data-flow-format** to restore the default.

Syntax

data-flow-format { **data** { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** } | **packet** { **giga-packet** | **kilo-packet** | **mega-packet** | **one-packet** } } *

undo data-flow-format { **data** | **packet** }

Default

Traffic is counted in bytes and packets.

Views

HWTACACS scheme view

Predefined user roles

network-admin

context-admin

Parameters

data: Specifies the unit for data flows.

byte: Specifies the unit as byte.

giga-byte: Specifies the unit as gigabyte.

kilo-byte: Specifies the unit as kilobyte.

mega-byte: Specifies the unit as megabyte.

packet: Specifies the unit for data packets.

giga-packet: Specifies the unit as giga-packet.

kilo-packet: Specifies the unit as kilo-packet.

mega-packet: Specifies the unit as mega-packet.

one-packet: Specifies the unit as one-packet.

Usage guidelines

The data flow and packet measurement units for traffic statistics must be the same as configured on the HWTACACS accounting servers. Otherwise, accounting results might be incorrect.

Examples

In HWTACACS scheme **hwt1**, set the data flow and packet measurement units for traffic statistics to kilobyte and kilo-packet, respectively.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] data-flow-format data kilo-byte packet kilo-packet
```

Related commands

display hwtacacs scheme

display hwtacacs scheme

Use **display hwtacacs scheme** to display the configuration or statistics of HWTACACS schemes.

Syntax

display hwtacacs scheme [*hwtacacs-scheme-name* [**statistics**]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

hwtacacs-scheme-name: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters. If you do not specify an HWTACACS scheme, this command displays the configuration of all HWTACACS schemes.

statistics: Displays the HWTACACS service statistics. If you do not specify this keyword, the command displays the configuration of the specified HWTACACS scheme.

Usage guidelines

When displaying configuration only for one scheme, this command also displays the active state duration for each active server and the most recent five state changes for all servers in the scheme.

When displaying configuration for all schemes, this command also displays the active state duration for each active server and the most recent blocked period for all servers in all schemes.

Examples

Displays the configuration of all HWTACACS schemes.

```
<Sysname> display hwtacacs scheme
Total 1 HWTACACS schemes
```

```
-----------------------------------------------------------------------------
HWTACACS Scheme Name  : hwtac
  Index : 0
  Primary Auth Server:
    IP  : 2.2.2.2         Port: 49     State: Active
    VPN Instance: 2
    State: Active (duration: 1 weeks, 2 days, 1 hours, 32 minutes, 34 seconds)
    Most recent blocked period: 2019/08/08 20:33:45 - 2019/08/08 20:38:45
    Single-connection: Enabled
    Track ID: 1
  Primary Author Server:
    IP  : 2.2.2.2         Port: 49     State: Active
    VPN Instance: 2
    State: Active (duration: 1 weeks, 2 days, 1 hours, 32 minutes, 34 seconds)
    Most recent blocked period: 2019/08/08 20:33:45 - 2019/08/08 20:38:45
    Single-connection: Disabled
    Track ID: 1
  Primary Acct Server:
    IP  : Not Configured  Port: 49     State: Block
    VPN Instance: Not configured
    State: Blocked
    Most recent blocked period: 2019/08/08 20:33:45 - now
    Single-connection: Disabled

  VPN Instance                          : 2
  NAS IP Address                        : 2.2.2.3
  Server Quiet Period(minutes)          : 5
  Realtime Accounting Interval(minutes) : 12
  Response Timeout Interval(seconds)    : 5
  Username Format                       : with-domain
  Data flow unit                        : Byte
  Packet unit                           : one
  All-server-block action               : Attempt the top-priority server
-----------------------------------------------------------------------------
```

Display the configuration of HWTACACS scheme **hwtac**.

```
<Sysname> display hwtacacs scheme hwtac
HWTACACS Scheme Name  : hwtac
  Index : 0
  Primary Auth Server:
    IP  : 2.2.2.2         Port: 49
    VPN Instance: 2
    State: Active (duration: 1 weeks, 2 days, 1 hours, 32 minutes, 34 seconds)
    Most recent state changes:
      2019/08/08 21:01:23 Changed to active state
      2019/08/08 20:56:22 Changed to blocked state
    Single-connection: Enabled
    Track ID: 1
  Primary Author Server:
```

```
  IP  : 2.2.2.2         Port: 49
  VPN Instance: 2
  State: Active (duration: 1 weeks, 2 days, 1 hours, 32 minutes, 34 seconds)
  Most recent state changes:
    2019/08/08 21:01:23 Changed to active state
    2019/08/08 20:56:22 Changed to blocked state
  Single-connection: Disabled
  Track ID: 1
Primary Acct Server:
  IP  : Not Configured  Port: 49
  VPN Instance: Not configured
  State: Blocked
  Most recent state changes:
    2019/08/08 22:16:52 Changed to blocked state
    2019/08/08 22:01:25 Changed to active state
    2019/08/08 21:56:22 Changed to blocked state
  Single-connection: Disabled

VPN Instance                          : 2
NAS IP Address                        : 2.2.2.3
Server Quiet Period(minutes)          : 5
Realtime Accounting Interval(minutes) : 12
Response Timeout Interval(seconds)    : 5
Username Format                       : with-domain
Data flow unit                        : Byte
Packet unit                           : one
All-server-block action               : Attempt the top-priority server
```

Table 16 Command output

Field	Description
Index	Index number of the HWTACACS scheme.
Primary Auth Server	Primary HWTACACS authentication server.
Primary Author Server	Primary HWTACACS authorization server.
Primary Acct Server	Primary HWTACACS accounting server.
Secondary Auth Server	Secondary HWTACACS authentication server.
Secondary Author Server	Secondary HWTACACS authorization server.
Secondary Acct Server	Secondary HWTACACS accounting server.
IP	IP address of the server. This field displays **Not configured** if the server is not configured.
Port	Service port of the HWTACACS server. If no port configuration is performed, this field displays the default port number.
VPN Instance	MPLS L3VPN instance to which the HWTACACS server or scheme belongs. If no VPN instance is specified for the server or scheme, this field displays **Not configured**.
State	Status of the server: • **Active**—The server is in active state.

Field	Description
	• **Blocked**—The server is in blocked state.
duration	The duration of the current active state for the server. This field is displayed only when the server is in active state.
Most recent blocked period	Most recent blocking start time and end time when the server stayed in blocked state. If the server still remains in blocked state, **now** is displayed for the end time.
Most recent state changes	Most recent five state changes of the server.
Single-connection	Single connection status: • **Enabled**—Establish only one TCP connection for all users to communicate with the server. • **Disabled**—Establish a TCP connection for each user to communicate with the server.
Track ID	ID of the track entry associated with the server. This field is not available if the server is not associated with a track entry.
NAS IP Address	Source IP addresses for outgoing HWTACACS packets. This field displays **Not configured** if no source IP addresses are specified for outgoing HWTACACS packets.
Server Quiet Period(minutes)	Quiet period for the primary servers, in minutes.
Realtime Accounting Interval(minutes)	Real-time accounting interval, in minutes.
Response Timeout Interval(seconds)	HWTACACS server response timeout period, in seconds.
Username Format	Format for the usernames sent to the HWTACACS server: • **with-domain**—Includes the domain name. • **without-domain**—Excludes the domain name. • **keep-original**—Forwards the username as the username is entered.
Data flow unit	Measurement unit for data flows.
Packet unit	Measurement unit for packets.
All-server-block action	Action to take for AAA requests when all servers in the scheme are blocked: • Attempt the top-priority server. • Skip all servers in the scheme.

Display the HWTACACS service statistics.

```
<Sysname> display hwtacacs scheme tac statistics
HWTACACS scheme name: tac
  Primary authentication server: 3.3.3.3
    Round trip time:                                0 seconds
    Request packets:                                1
    Login request packets:                          1
    Change-password request packets:                0
    Request packets including plaintext password:   0
    Request packets including ciphertext password:  0
    Response packets:                               2
    Pass response packets:                          1
```

```
  Failure response packets:                    0
  Get-data response packets:                   0
  Get-username response packets:               0
  Get-password response packets:               1
  Restart response packets:                    0
  Error response packets:                      0
  Follow response packets:                     0
  Malformed response packets:                  0
  Continue packets:                            1
  Continue-abort packets:                      0
  Pending request packets:                     0
  Timeout packets:                             0
  Unknown type response packets:               0
  Dropped response packets:                    0

Primary authorization server: 3.3.3.3
  Round trip time:                             1 seconds
  Request packets:                             1
  Response packets:                            1
  PassAdd response packets:                    1
  PassReply response packets:                  0
  Failure response packets:                    0
  Error response packets:                      0
  Follow response packets:                     0
  Malformed response packets:                  0
  Pending request packets:                     0
  Timeout packets:                             0
  Unknown type response packets:               0
  Dropped response packets:                    0

Primary accounting server: 3.3.3.3
  Round trip time:                             0 seconds
  Request packets:                             2
  Accounting start request packets:            1
  Accounting stop request packets:             1
  Accounting update request packets:           0
  Pending request packets:                     0
  Response packets:                            2
  Success response packets:                    2
  Error response packets:                      0
  Follow response packets:                     0
  Malformed response packets:                  0
  Timeout response packets:                    0
  Unknown type response packets:               0
  Dropped response packets:                    0
```

Table 17 Command output

Field	Description
Primary authentication server	Primary HWTACACS authentication server.
Primary authorization server	Primary HWTACACS authorization server.
Primary accounting server	Primary HWTACACS accounting server.
Secondary authentication server	Secondary HWTACACS authentication server.
Secondary authorization server	Secondary HWTACACS authorization server.
Secondary accounting server	Secondary HWTACACS accounting server.
Round trip time	Time between the device processes the latest pair of request and response, in seconds.
Request packets	Number of sent requests.
Response packets	Number of received responses.
Failure response packets	Number of responses for authentication or authorization failure.
Error response packets	Number of error authentication responses.
Follow response packets	Number of follow authentication responses.
Malformed response packets	Number of invalid responses.
Pending request packets	Number of requests for which the device waits for responses.
Timeout packets	Number of requests that timed out.
Unknown type response packets	Number of unknown responses.
Dropped response packets	Number of dropped responses.
Login request packets	Number of sent packets that request to log in to the device.
Change-password request packets	Number of sent packets that request to change user passwords.
Request packets including plaintext passwords	Number of sent requests that include user passwords in plaintext form.
Request packets including ciphertext passwords	Number of requests that include user passwords in encrypted form.
Pass response packets	Number of responses that indicate users pass authentication.
Get-data response packets	Number of responses that get data.
Get-username response packets	Number of responses that get usernames.
Get-password response packets	Number of responses that get user passwords.
Restart response packets	Number of responses that indicate reauthentication.
Continue packets	Number of sent continue packets.
Continue-abort packets	Number of sent continue-abort packets.
PassAdd response packets	Number of received PassAdd responses. This type of responses indicate that the server agrees to assign all requested authorization attributes and adds other authorization attributes.
PassReply response packets	Number of received PassReply responses. This type of responses indicate that the server uses the authorization attributes in the responses to replace the requested authorization attributes.
Accounting start request packets	Number of sent start-accounting requests.

Field	Description
Accounting stop request packets	Number of sent stop-accounting requests.
Accounting update request packets	Number of sent accounting-update requests.
Success response packets	Number of received responses that indicate accounting success.

Related commands

reset hwtacacs statistics

hwtacacs nas-ip

Use **hwtacacs nas-ip** to specify a source IP address for outgoing HWTACACS packets.

Use **undo hwtacacs nas-ip** to delete the specified source IP address for outgoing HWTACACS packets.

Syntax

hwtacacs nas-ip { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]

undo hwtacacs nas-ip { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]

Default

The source IP address of an HWTACACS packet sent to the server is the primary IPv4 address or the IPv6 address of the outbound interface.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-address: Specifies an IPv4 address, which must be an address of the device. The IP address cannot be 0.0.0.0, 255.255.255.255, a class D address, a class E address, or a loopback address.

ipv6 *ipv6-address*: Specifies an IPv6 address, which must be a unicast address of the device and cannot be a loopback address or a link-local address.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance to which the source IP address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. To configure a public-network source IP address, do not specify this option.

Usage guidelines

The source IP address of HWTACACS packets that a NAS sends must match the IP address of the NAS that is configured on the HWTACACS server. An HWTACACS server identifies a NAS by IP address. Upon receiving an HWTACACS packet, the HWTACACS server checks the source IP address of the packet.

- If the source IP address of the packet is the IP address of a managed NAS, the server processes the packet.
- If the source IP address of the packet is not the IP address of a managed NAS, the server drops the packet.

As a best practice, specify a loopback interface address as the source IP address for outgoing HWTACACS packets to avoid HWTACACS packet loss caused by physical port errors.

If you use both the **nas-ip** command and **hwtacacs nas-ip** command, the following guidelines apply:

- The setting configured by using the **nas-ip** command in HWTACACS scheme view applies only to the HWTACACS scheme.
- The setting configured by using the **hwtacacs nas-ip** command in system view applies to all HWTACACS schemes.
- The setting in HWTACACS scheme view takes precedence over the setting in system view.

You can specify a maximum of 16 source IP addresses in system view, including:

- Zero or one public-network source IPv4 address.
- Zero or one public-network source IPv6 address.
- Private-network source IP addresses.

Each VPN instance can have only one private-network source IPv4 address and one private-network source IPv6 address in system view.

Examples

Specify IP address 129.10.10.1 as the source IP address for HWTACACS packets.

```
<Sysname> system-view
[Sysname] hwtacacs nas-ip 129.10.10.1
```

Related commands

nas-ip (HWTACACS scheme view)

hwtacacs scheme

Use **hwtacacs scheme** to create an HWTACACS scheme and enter its view, or enter the view of an existing HWTACACS scheme.

Use **undo hwtacacs scheme** to delete an HWTACACS scheme.

Syntax

hwtacacs scheme *hwtacacs-scheme-name*

undo hwtacacs scheme *hwtacacs-scheme-name*

Default

No HWTACACS schemes exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

hwtacacs-scheme-name: Specifies the HWTACACS scheme name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

An HWTACACS scheme can be used by more than one ISP domain at the same time.

You can configure a maximum of 16 HWTACACS schemes.

Examples

Create an HWTACACS scheme named **hwt1** and enter HWTACACS scheme view.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1]
```

Related commands

display hwtacacs scheme

hwtacacs server-probe track

Use **hwtacacs server-probe track** to associate an HWTACACS server with a track entry.

Use **undo hwtacacs server-probe track** to remove the association between an HWTACACS server and a track entry.

Syntax

hwtacacs server-probe { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**port** *port-number*] **track** *track-entry-number*

undo hwtacacs server-probe { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**port** *port-number*] **track**

Default

An HWTACACS server is not associated with any track entry.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ip *ipv4-address*: Specifies an HWTACACS server by its IPv4 address.

ipv6 *ipv6-address*: Specifies an HWTACACS server by its IPv6 address.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance to which the HWTACACS server belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the server is on the public network, do not specify this option.

port *port-number*: Specifies the service port number of the HWTACACS server. The value range for the TCP port number is 1 to 65535. The default setting is 49.

track-entry-number: Specifies a track entry by its ID, in the range of 1 to 1024.

Usage guidelines

Use this command on a network that has high real-time requirements for HWTACACS authentication, authorization, and accounting.

By default, the device does not actively detect the status of an HWTACACS server. It changes the state of an HWTACACS server to active or blocked based on the server response timeout timer and the server quiet timer. This timer-based state transition mechanism needs time to determine the server state, and it cannot ensure that the device obtains the actual server state in time. To resolve this issue, associate the server with a track entry and associate the track entry with a TCP-type NQA

operation. This HWTACACS server-Track-NQA collaboration can actively detect the reachability of the server in real time.

By using HWTACACS server-Track-NQA collaboration, the device determines the status of an HWTACACS server only based on the detection result.

1. The NQA operation starts to detect the reachability of the server and obtains the result. NQA sends the detection result to the Track module for the Track module to set the state of the track entry.
   - If the server is reachable, the Track module sets the state of the track entry to Positive.
   - If the server is unreachable, the Track module sets the state of the track entry to Negative.
   - If the Track-NQA collaboration does not take effect, the Track module keeps the track entry in NotReady state or changes its state to NotReady.
2. AAA sets the status of the server based on the track entry state.
   - If the track entry is in Positive state, AAA sets the state of the server to active.
   - If the track entry is in Negative state, AAA sets the state of the server to blocked and disables the quiet timer for the server.
   - If the track entry stays in NotReady state or its state changes to NotReady, AAA sets the state of the server to active.

To start the NQA operation to detect the reachability of the server, use the **nqa schedule** command with appropriate settings for the scheduling parameters. For more information about associating Track with NQA, see Track configuration in *Network Management and Monitoring Configuration guide*. For more information about configuring a TCP-type NQA operation and scheduling the NQA operation, see NQA configuration in *Network Management and Monitoring Configuration Guide*.

Examples

Associate HWTACACS server that uses IP address 10.163.155.13 and TCP port number 49 with track entry 1.

```
<Sysname> system-view
[Sysname] hwtacacs server-probe ip 10.163.155.13 port 49 track 1
```

Related commands

display hwtacacs scheme

nqa schedule (*Network Monitoring and Management Command Reference*)

track nqa (*Network Management and Monitoring Command Reference*)

key (HWTACACS scheme view)

Use **key** to set the shared key for secure HWTACACS authentication, authorization, or accounting communication.

Use **undo key** to delete the shared key for secure HWTACACS authentication, authorization, or accounting communication.

Syntax

key { **accounting** | **authentication** | **authorization** } { **cipher** | **simple** } *string*

undo key { **accounting** | **authentication** | **authorization** }

Default

No shared key is configured for secure HWTACACS authentication, authorization, or accounting communication.

Views

HWTACACS scheme view

Predefined user roles

network-admin

context-admin

Parameters

accounting: Specifies the shared key for secure HWTACACS accounting communication.

authentication: Specifies the shared key for secure HWTACACS authentication communication.

authorization: Specifies the shared key for secure HWTACACS authorization communication.

cipher: Specifies the key in encrypted form.

simple: Specifies the key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. This argument is case sensitive. The encrypted form of the key is a string of 1 to 373 characters. The plaintext form of the key is a string of 1 to 255 characters.

Usage guidelines

The shared keys configured on the device must match those configured on the HWTACACS servers.

Examples

In HWTACACS scheme **hwt1**, set the shared key to **123456TESTauth&!** in plaintext form for secure HWTACACS authentication communication.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] key authentication simple 123456TESTauth&!
```

Set the shared key to **123456TESTautr&!** in plaintext form for secure HWTACACS authorization communication.

```
[Sysname-hwtacacs-hwt1] key authorization simple 123456TESTautr&!
```

Set the shared key to **123456TESTacct&!** in plaintext form for secure HWTACACS accounting communication.

```
[Sysname-hwtacacs-hwt1] key accounting simple 123456TESTacct&!
```

Related commands

display hwtacacs scheme

nas-ip (HWTACACS scheme view)

Use **nas-ip** to specify a source IP address for outgoing HWTACACS packets.

Use **undo nas-ip** to delete the specified source IP address for outgoing HWTACACS packets.

Syntax

nas-ip { *ipv4-address* | **ipv6** *ipv6-address* }

undo nas-ip [**ipv6**]

Default

The source IP address of an outgoing HWTACACS packet is that configured by using the **hwtacacs nas-ip** command in system view.

If the **hwtacacs nas-ip** command is not used, the source IP address is the primary IP address of the outbound interface.

Views

HWTACACS scheme view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-address: Specifies an IPv4 address, which must be an address of the device. The IP address cannot be 0.0.0.0, 255.255.255.255, a class D address, a class E address, or a loopback address.

ipv6 *ipv6-address*: Specifies an IPv6 address, which must be a unicast address of the device and cannot be a loopback address or a link-local address.

Usage guidelines

The source IP address of HWTACACS packets that a NAS sends must match the IP address of the NAS that is configured on the HWTACACS server. An HWTACACS server identifies a NAS by IP address. Upon receiving an HWTACACS packet, the HWTACACS server checks the source IP address of the packet.

- If the source IP address of the packet is the IP address of a managed NAS, the server processes the packet.
- If the source IP address of the packet is not the IP address of a managed NAS, the server drops the packet.

As a best practice, specify a loopback interface address as the source IP address for outgoing HWTACACS packets to avoid HWTACACS packet loss caused by physical port errors.

If you use both the **nas-ip** command and **hwtacacs nas-ip** command, the following guidelines apply:

- The setting configured by using the **nas-ip** command in HWTACACS scheme view applies only to the HWTACACS scheme.
- The setting configured by using the **hwtacacs nas-ip** command in system view applies to all HWTACACS schemes.
- The setting in HWTACACS scheme view takes precedence over the setting in system view.

For an HWTACACS scheme, you can specify only one source IPv4 address and one source IPv6 address for outgoing HWTACACS packets.

If you do not specify any parameter for the **undo nas-ip** command, the command deletes the configured source IPv4 address for outgoing HWTACACS packets.

Examples

In HWTACACS scheme **hwt1**, specify IP address 10.1.1.1 as the source address for outgoing HWTACACS packets.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] nas-ip 10.1.1.1
```

Related commands

display hwtacacs scheme

hwtacacs nas-ip

primary accounting (HWTACACS scheme view)

Use **primary accounting** to specify the primary HWTACACS accounting server.

Use **undo primary accounting** to restore the default.

Syntax

primary accounting { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **single-connection** | **vpn-instance** *vpn-instance-name*] *

undo primary accounting

Default

The primary HWTACACS accounting server is not specified.

Views

HWTACACS scheme view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-address: Specifies an IPv4 address of the primary HWTACACS accounting server.

ipv6 *ipv6-address*: Specifies an IPv6 address of the primary HWTACACS accounting server.

port-number: Specifies the service port number of the primary HWTACACS accounting server. The value range for the TCP port number is 1 to 65535. The default setting is 49.

key: Specifies the shared key for secure communication with the primary HWTACACS accounting server.

cipher: Specifies the key in encrypted form.

simple: Specifies the key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. This argument is case sensitive. The encrypted form of the key is a string of 1 to 373 characters. The plaintext form of the key is a string of 1 to 255 characters.

single-connection: The device and the primary HWTACACS accounting server use the same TCP connection to exchange accounting packets for all users. If you do not specify this keyword, the device establishes a new TCP connection each time it exchanges accounting packets with the primary accounting server for a user.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance to which the primary HWTACACS accounting server belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the server is on the public network, do not specify this option.

Usage guidelines

Make sure the port number and shared key settings of the primary HWTACACS accounting server are the same as those configured on the server.

Two accounting servers specified for a scheme, primary or secondary, cannot have identical VPN instance, IP address, and port number settings.

As a best practice, specify the **single-connection** keyword to reduce TCP connections for improving system performance if the HWTACACS server supports the single-connection method.

If the specified server resides on an MPLS L3VPN, specify the VPN instance by using the **vpn-instance** *vpn-instance-name* option. The VPN instance specified by this command takes precedence over the VPN instance specified for the HWTACACS scheme.

You can remove an accounting server only when it is not used for user accounting. Removing an accounting server affects only accounting processes that occur after the remove operation.

Examples

In HWTACACS scheme **hwt1**, specify the primary accounting server with IP address 10.163.155.12, TCP port number 49, and plaintext shared key **123456TESTacct&!**.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] primary accounting 10.163.155.12 49 key simple 123456TESTacct&!
```

Related commands

display hwtacacs scheme

key (HWTACACS scheme view)

secondary accounting (HWTACACS scheme view)

vpn-instance (HWTACACS scheme view)

primary authentication (HWTACACS scheme view)

Use **primary authentication** to specify the primary HWTACACS authentication server.

Use **undo primary authentication** to restore the default.

Syntax

primary authentication { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **single-connection** | **vpn-instance** *vpn-instance-name*] *

undo primary authentication

Default

The primary HWTACACS authentication server is not specified.

Views

HWTACACS scheme view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-address: Specifies the IPv4 address of the primary HWTACACS authentication server.

ipv6 *ipv6-address*: Specifies the IPv6 address of the primary HWTACACS authentication server.

port-number: Specifies the service port number of the primary HWTACACS authentication server. The value range for the TCP port number is 1 to 65535. The default setting is 49.

key: Specifies the shared key for secure communication with the primary HWTACACS authentication server.

cipher: Specifies the key in encrypted form.

simple: Specifies the key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. This argument is case sensitive. The encrypted form of the key is a string of 1 to 373 characters. The plaintext form of the key is a string of 1 to 255 characters.

single-connection: The device and the primary HWTACACS authentication server use the same TCP connection to exchange all authentication packets for all users. If you do not specify this keyword, the device establishes a new TCP connection each time it exchanges authentication packets with the primary authentication server for a user.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance to which the primary HWTACACS authentication server belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the server is on the public network, do not specify this option.

Usage guidelines

Make sure the port number and shared key settings of the primary HWTACACS authentication server are the same as those configured on the server.

Two authentication servers specified for a scheme, primary or secondary, cannot have identical VPN instance, IP address, and port number settings.

As a best practice, specify the **single-connection** keyword to reduce TCP connections for improving system performance if the HWTACACS server supports the single-connection method.

If the specified server resides on an MPLS L3VPN, specify the VPN instance by using the **vpn-instance** *vpn-instance-name* option. The VPN instance specified by this command takes precedence over the VPN instance specified for the HWTACACS scheme.

You can remove an authentication server only when it is not used for user authentication. Removing an authentication server affects only authentication processes that occur after the remove operation.

Examples

In HWTACACS scheme **hwt1**, specify the primary authentication server with IP address 10.163.155.13, TCP port number 49, and plaintext shared key **123456TESTauth&!**.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] primary authentication 10.163.155.13 49 key simple
123456TESTauth&!
```

Related commands

display hwtacacs scheme

key (HWTACACS scheme view)

secondary authentication (HWTACACS scheme view)

vpn-instance (HWTACACS scheme view)

primary authorization

Use **primary authorization** to specify the primary HWTACACS authorization server.

Use **undo primary authorization** to restore the default.

Syntax

primary authorization { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **single-connection** | **vpn-instance** *vpn-instance-name*] *

undo primary authorization

Default

The primary HWTACACS authorization server is not specified.

Views

HWTACACS scheme view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-address: Specifies the IPv4 address of the primary HWTACACS authorization server.

ipv6 *ipv6-address*: Specifies the IPv6 address of the primary HWTACACS authorization server.

port-number: Specifies the service port number of the primary HWTACACS authorization server. The value range for the TCP port number is 1 to 65535. The default setting is 49.

key: Specifies the shared key for secure communication with the primary HWTACACS authorization server.

cipher: Specifies the key in encrypted form.

simple: Specifies the key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. This argument is case sensitive. The encrypted form of the key is a string of 1 to 373 characters. The plaintext form of the key is a string of 1 to 255 characters.

single-connection: The device and the primary HWTACACS authorization server use the same TCP connection to exchange all authorization packets for all users. If you do not specify this keyword, the device establishes a new TCP connection each time it exchanges authorization packets with the primary authorization server for a user.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance to which the primary HWTACACS authorization server belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the server is on the public network, do not specify this option.

Usage guidelines

Make sure the port number and shared key settings of the primary HWTACACS authorization server are the same as those configured on the server.

Two authorization servers specified for a scheme, primary or secondary, cannot have identical VPN instance, IP address, and port number settings.

As a best practice, specify the **single-connection** keyword to reduce TCP connections for improving system performance if the HWTACACS server supports the single-connection method.

If the specified server resides on an MPLS L3VPN, specify the VPN instance by using the **vpn-instance** *vpn-instance-name* option. The VPN instance specified by this command takes precedence over the VPN instance specified for the HWTACACS scheme.

You can remove an authorization server only when it is not used for user authorization. Removing an authorization server affects only authorization processes that occur after the remove operation.

Examples

In HWTACACS scheme **hwt1**, specify the primary authorization server with IP address 10.163.155.13, TCP port number 49, and plaintext shared key **123456TESTautr&!**.

```
<Sysname> system-view
```

```
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] primary authorization 10.163.155.13 49 key simple
123456TESTautr&!
```

Related commands

display hwtacacs scheme

key (HWTACACS scheme view)

secondary authorization (HWTACACS scheme view)

vpn-instance (HWTACACS scheme view)

reset hwtacacs statistics

Use **reset hwtacacs statistics** to clear HWTACACS statistics.

Syntax

reset hwtacacs statistics { **accounting** | **all** | **authentication** | **authorization** }

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

accounting: Clears the HWTACACS accounting statistics.

all: Clears all HWTACACS statistics.

authentication: Clears the HWTACACS authentication statistics.

authorization: Clears the HWTACACS authorization statistics.

Examples

Clear all HWTACACS statistics.

```
<Sysname> reset hwtacacs statistics all
```

Related commands

display hwtacacs scheme

secondary accounting (HWTACACS scheme view)

Use **secondary accounting** to specify a secondary HWTACACS accounting server.

Use **undo secondary accounting** to remove a secondary HWTACACS accounting server.

Syntax

secondary accounting { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **single-connection** | **vpn-instance** *vpn-instance-name*] *

undo secondary accounting [{ *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **vpn-instance** *vpn-instance-name*] *]

Default

No secondary HWTACACS accounting servers are specified.

Views

HWTACACS scheme view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-address: Specifies the IPv4 address of a secondary HWTACACS accounting server.

ipv6 *ipv6-address*: Specifies the IPv6 address of a secondary HWTACACS accounting server.

port-number: Specifies the service port number of the secondary HWTACACS accounting server. The value range for the TCP port number is 1 to 65535. The default setting is 49.

key: Specifies the shared key for secure communication with the secondary HWTACACS accounting server.

cipher: Specifies the key in encrypted form.

simple: Specifies the key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. This argument is case sensitive. The encrypted form of the key is a string of 1 to 373 characters. The plaintext form of the key is a string of 1 to 255 characters.

single-connection: The device and the secondary HWTACACS accounting server use the same TCP connection to exchange all accounting packets for all users. If you do not specify this keyword, the device establishes a new TCP connection each time it exchanges accounting packets with the secondary accounting server for a user.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance to which the secondary HWTACACS accounting server belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the server is on the public network, do not specify this option.

Usage guidelines

Make sure the port number and shared key settings of the secondary HWTACACS accounting server are the same as those configured on the server.

An HWTACACS scheme supports a maximum of 16 secondary HWTACACS accounting servers. If the primary server fails, the device tries to communicate with a secondary server in active state. The device connects to the secondary servers in the order they are configured.

If you do not specify any parameters for the **undo secondary accounting** command, the command removes all secondary accounting servers.

Two accounting servers specified for a scheme, primary or secondary, cannot have identical VPN instance, IP address, and port number settings.

As a best practice, specify the **single-connection** keyword to reduce TCP connections for improving system performance if the HWTACACS server supports the single-connection method.

If the specified server resides on an MPLS L3VPN, specify the VPN instance by using the **vpn-instance** *vpn-instance-name* option. The VPN instance specified by this command takes precedence over the VPN instance specified for the HWTACACS scheme.

You can remove an accounting server only when it is not used for user accounting. Removing an accounting server affects only accounting processes that occur after the remove operation.

Examples

In HWTACACS scheme **hwt1**, specify a secondary accounting server with IP address 10.163.155.12, TCP port number 49, and plaintext shared key **123456TESTacct&!**.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] secondary accounting 10.163.155.12 49 key simple 123456TESTacct&!
```

Related commands

display hwtacacs scheme

key (HWTACACS scheme view)

primary accounting (HWTACACS scheme view)

vpn-instance (HWTACACS scheme view)

secondary authentication (HWTACACS scheme view)

Use **secondary authentication** to specify a secondary HWTACACS authentication server.

Use **undo secondary authentication** to remove a secondary HWTACACS authentication server.

Syntax

secondary authentication { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **single-connection** | **vpn-instance** *vpn-instance-name*] *

undo secondary authentication [{ *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **vpn-instance** *vpn-instance-name*] *]

Default

No secondary HWTACACS authentication servers are specified.

Views

HWTACACS scheme view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-address: Specifies the IPv4 address of a secondary HWTACACS authentication server.

ipv6 *ipv6-address*: Specifies the IPv6 address of a secondary HWTACACS authentication server.

port-number: Specifies the service port number of the secondary HWTACACS authentication server. The value range for the TCP port number is 1 to 65535. The default setting is 49.

key: Specifies the shared key for secure communication with the secondary HWTACACS authentication server.

cipher: Specifies the key in encrypted form.

simple: Specifies the key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. This argument is case sensitive. The encrypted form of the key is a string of 1 to 373 characters. The plaintext form of the key is a string of 1 to 255 characters.

single-connection: The device and the secondary HWTACACS authentication server use the same TCP connection to exchange all authentication packets for all users. If you do not specify this keyword, the device establishes a new TCP connection each time it exchanges authentication packets with the secondary authentication server for a user.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance to which the secondary HWTACACS authentication server belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the server is on the public network, do not specify this option.

Usage guidelines

Make sure the port number and shared key settings of each secondary HWTACACS authentication server are the same as those configured on the corresponding server.

An HWTACACS scheme supports a maximum of 16 secondary HWTACACS authentication servers. If the primary server fails, the device tries to communicate with a secondary server in active state. The device connects to the secondary servers in the order they are configured.

If you do not specify any parameters for the **undo secondary authentication** command, the command removes all secondary authentication servers.

Two authentication servers specified for a scheme, primary or secondary, cannot have identical VPN instance, IP address, and port number settings.

As a best practice, specify the **single-connection** keyword to reduce TCP connections for improving system performance if the HWTACACS server supports the single-connection method.

If the specified server resides on an MPLS L3VPN, specify the VPN instance by using the **vpn-instance** *vpn-instance-name* option. The VPN instance specified by this command takes precedence over the VPN instance specified for the HWTACACS scheme.

You can remove an authentication server only when it is not used for user authentication. Removing an authentication server affects only authentication processes that occur after the remove operation.

Examples

In HWTACACS scheme **hwt1**, specify a secondary authentication server with IP address 10.163.155.13, TCP port number 49, and plaintext shared key **123456TESTauth&!**.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] secondary authentication 10.163.155.13 49 key simple
123456TESTauth&!
```

Related commands

display hwtacacs scheme

key (HWTACACS scheme view)

primary authentication (HWTACACS scheme view)

vpn-instance (HWTACACS scheme view)

secondary authorization

Use **secondary authorization** to specify a secondary HWTACACS authorization server.

Use **undo secondary authorization** to remove a secondary HWTACACS authorization server.

Syntax

secondary authorization { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **single-connection** | **vpn-instance** *vpn-instance-name*] *

undo secondary authorization [{ *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **vpn-instance** *vpn-instance-name*] *]

Default

No secondary HWTACACS authorization servers are specified.

Views

HWTACACS scheme view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-address: Specifies the IPv4 address of a secondary HWTACACS authorization server.

ipv6 *ipv6-address*: Specifies the IPv6 address of a secondary HWTACACS authorization server.

port-number: Specifies the service port number of the secondary HWTACACS authorization server. The value range for the TCP port number is 1 to 65535. The default setting is 49.

key: Specifies the shared key for secure communication with the secondary HWTACACS authorization server.

cipher: Specifies the key in encrypted form.

simple: Specifies the key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. This argument is case sensitive. The encrypted form of the key is a string of 1 to 373 characters. The plaintext form of the key is a string of 1 to 255 characters.

single-connection: The device and the secondary HWTACACS authorization server use the same TCP connection to exchange all authorization packets for all users. If you do not specify this keyword, the device establishes a new TCP connection each time it exchanges authorization packets with the secondary authorization server for a user.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance to which the secondary HWTACACS authorization server belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the server is on the public network, do not specify this option.

Usage guidelines

Make sure the port number and shared key settings of the secondary HWTACACS authorization server are the same as those configured on the server.

An HWTACACS scheme supports a maximum of 16 secondary HWTACACS authorization servers. If the primary server fails, the device tries to communicate with a secondary server in active state. The device connects to the secondary servers in the order they are configured.

If you do not specify any parameters for the **undo secondary authorization** command, the command removes all secondary authorization servers.

Two authorization servers specified for a scheme, primary or secondary, cannot have identical VPN instance, IP address, and port number settings.

As a best practice, specify the **single-connection** keyword to reduce TCP connections for improving system performance if the HWTACACS server supports the single-connection method.

If the specified server resides on an MPLS L3VPN, specify the VPN instance by using the **vpn-instance** *vpn-instance-name* option. The VPN instance specified by this command takes precedence over the VPN instance specified for the HWTACACS scheme.

You can remove an authorization server only when it is not used for user authorization. Removing an authorization server affects only authorization processes that occur after the remove operation.

Examples

In HWTACACS scheme **hwt1**, specify a secondary authorization server with IP address 10.163.155.13, TCP port number 49, and plaintext shared key **123456TESTautr&!**.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] secondary authorization 10.163.155.13 49 key simple
123456TESTautr&!
```

Related commands

display hwtacacs scheme

key (HWTACACS scheme view)

primary authorization (HWTACACS scheme view)

vpn-instance (HWTACACS scheme view)

server-block-action

Use **server-block-action** to specify the action to take for AAA requests if all servers in an HWTACACS scheme are blocked.

Use **undo server-block-action** to restore the default.

Syntax

server-block-action { **attempt** | **skip** }

undo server-block-action

Default

The device attempts to connect to the server with the highest priority in an HWTACACS scheme upon receiving AAA requests if all servers in the scheme are blocked.

Views

HWTACACS scheme view

Predefined user roles

network-admin

context-admin

Parameters

attempt: Attempts to connect to the server that has the highest priority in the scheme. (Typically, the highest-priority server is the primary server. If no primary server is specified, it is the firstly configured secondary server.) If the device fails to connect to the server, it turns to the backup method.

skip: Skips all servers in the scheme and turns to the backup method.

Usage guidelines

The **attempt** action gives the device a chance to use the scheme in case the server with the highest priority in the scheme might be available. However, the attempt to communicate with an unavailable server increases the response time for AAA requests. As a best practice, specify the **skip** action in scenarios that require quick responses to AAA requests.

When processing an AAA request, the device does not turn back to a skipped scheme even though the state of the servers in the scheme changes from blocked to active.

Examples

In HWTACACS scheme **hwt1**, configure the device to skip all servers in the scheme upon receiving AAA requests if all servers in the scheme are blocked.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] server-block-action skip
```

Related commands

display hwtacacs scheme

timer quiet (HWTACACS scheme view)

Use **timer quiet** to set the quiet timer for the servers specified in an HWTACACS scheme.

Use **undo timer quiet** to restore the default.

Syntax

timer quiet *minutes*

undo timer quiet

Default

The server quiet period is 5 minutes.

Views

HWTACACS scheme view

Predefined user roles

network-admin

context-admin

Parameters

minutes: Specifies the server quiet period in minutes, in the range of 1 to 255.

Examples

In HWTACACS scheme **hwt1**, set the server quiet timer to 10 minutes.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] timer quiet 10
```

Related commands

display hwtacacs scheme

timer realtime-accounting (HWTACACS scheme view)

Use **timer realtime-accounting** to set the real-time accounting interval.

Use **undo timer realtime-accounting** to restore the default.

Syntax

timer realtime-accounting *minutes*

undo timer realtime-accounting

Default

The real-time accounting interval is 12 minutes.

Views

HWTACACS scheme view

Predefined user roles

network-admin

context-admin

Parameters

minutes: Specifies the real-time accounting interval in minutes, in the range of 0 to 60. Setting this interval to 0 disables the device from sending online user accounting information to the HWTACACS accounting server.

Usage guidelines

For real-time accounting, a NAS must transmit the accounting information of online users to the HWTACACS accounting server periodically. This command is used to set the interval.

A short interval helps improve accounting precision but requires many system resources.

Table 18 Recommended real-time accounting intervals

Number of users	Real-time accounting interval
1 to 99	3 minutes
100 to 499	6 minutes
500 to 999	12 minutes
1000 or more	15 minutes or longer

The device sends a start-accounting packet for a dual-stack user after the user obtains an IP address of one stack. No matter how long the real-time accounting interval is, the device sends an update-accounting packet for the user immediately after the user obtains an IP address of another stack.

Examples

In HWTACACS scheme **hwt1**, set the real-time accounting interval to 51 minutes.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] timer realtime-accounting 51
```

Related commands

display hwtacacs scheme

timer response-timeout (HWTACACS scheme view)

Use **timer response-timeout** to set the HWTACACS server response timeout timer.

Use **undo timer response-timeout** to restore the default.

Syntax

timer response-timeout *seconds*

undo timer response-timeout

Default

The HWTACACS server response timeout time is 5 seconds.

Views

HWTACACS scheme view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies the HWTACACS server response timeout time, in the range of 1 to 300 seconds.

Usage guidelines

HWTACACS is based on TCP. When the server response timeout timer or the TCP timeout timer times out, the device is disconnected from the HWTACACS server.

The client timeout period of the associated access module cannot be shorter than the total response timeout timer of all HWTACACS servers in the scheme. Any violation will result in user logoffs before the authentication, authorization, or accounting process is complete.

Examples

In HWTACACS scheme **hwt1**, set the HWTACACS server response timeout timer to 30 seconds.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] timer response-timeout 30
```

Related commands

display hwtacacs scheme

user-name-format (HWTACACS scheme view)

Use **user-name-format** to specify the format of the username to be sent to an HWTACACS server.

Use **undo user-name-format** to restore the default.

Syntax

user-name-format { **keep-original** | **with-domain** | **without-domain** }

undo user-name-format

Default

The ISP domain name is included in the usernames sent to an HWTACACS server.

Views

HWTACACS scheme view

Predefined user roles

network-admin

context-admin

Parameters

keep-original: Sends the username to the HWTACACS server as the username is entered.

with-domain: Includes the ISP domain name in the username sent to the HWTACACS server.

without-domain: Excludes the ISP domain name from the username sent to the HWTACACS server.

Usage guidelines

A username is generally in the *userid@isp-name* format, of which the *isp-name* argument is used by the device to determine the ISP domain to which a user belongs. However, some HWTACACS servers cannot recognize a username containing an ISP domain name. Before sending a username including a domain name to such an HWTACACS server, the device must remove the domain name. This command allows you to specify whether to include a domain name in a username to be sent to an HWTACACS server.

If an HWTACACS scheme defines that the username is sent without the ISP domain name, do not apply the scheme to more than one ISP domain. Otherwise, the HWTACACS server will consider two users in different ISP domains but with the same *userid* as one user.

Examples

In HWTACACS scheme **hwt1**, configure the device to remove the ISP domain name from the usernames sent to the HWTACACS servers.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] user-name-format without-domain
```

Related commands

display hwtacacs scheme

vpn-instance (HWTACACS scheme view)

Use **vpn-instance** to specify an MPLS L3VPN instance for an HWTACACS scheme.

Use **undo vpn-instance** to restore the default.

Syntax

vpn-instance *vpn-instance-name*

undo vpn-instance

Default

The HWTACACS scheme belongs to the public network.

Views

HWTACACS scheme view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance-name: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

The VPN instance specified for an HWTACACS scheme applies to all servers in that scheme. If a VPN instance is also configured for an individual HWTACACS server, the VPN instance specified for the HWTACACS scheme does not take effect on that server.

Examples

Specify VPN instance **test** for HWTACACS scheme **hwt1**.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] vpn-instance test
```

Related commands

display hwtacacs scheme

LDAP commands

attribute-map

Use **attribute-map** to specify the LDAP attribute map in an LDAP scheme.

Use **undo attribute-map** to restore the default.

Syntax

attribute-map *map-name*

undo attribute-map

Default

An LDAP scheme does not use an LDAP attribute map.

Views

LDAP scheme view

Predefined user roles

network-admin

context-admin

Parameters

map-name: Specifies an LDAP attribute map by its name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

When the LDAP scheme used for authorization contains an LDAP attribute map, the device converts server-assigned LDAP attributes to device-recognizable AAA attributes based on the mapping entries.

You can specify only one LDAP attribute map in an LDAP scheme. If you execute this command multiple times, the most recent configuration takes effect.

If you specify another attribute map or change the mapping entries, the new settings take effect only on the LDAP authorization that occurs after your operation.

Examples

Specify LDAP attribute map **map1** in LDAP scheme **ldap1**.

```
<Sysname> system-view
```

```
[Sysname] ldap scheme ldap1
[Sysname-ldap-ldap1] attribute-map map1
```

Related commands

display ldap scheme

ldap attribute-map

authentication-server

Use **authentication-server** to specify the LDAP authentication server for an LDAP scheme.

Use **undo authentication-server** to restore the default.

Syntax

authentication-server *server-name*

undo authentication-server

Default

No LDAP authentication server is specified for an LDAP scheme.

Views

LDAP scheme view

Predefined user roles

network-admin

context-admin

Parameters

server-name: Specifies the name of an LDAP server, a case-sensitive string of 1 to 64 characters.

Usage guidelines

You can specify only one LDAP authentication server in an LDAP scheme. If you execute this command multiple times, the most recent configuration takes effect.

Examples

In LDAP scheme **ldap1**, specify the LDAP authentication server as **ccc**.

```
<Sysname> system-view
[Sysname] ldap scheme ldap1
[Sysname-ldap-ldap1] authentication-server ccc
```

Related commands

display ldap scheme

ldap server

authorization-server

Use **authorization-server** to specify the LDAP authorization server for an LDAP scheme.

Use **undo authorization-server** to restore the default.

Syntax

authorization-server *server-name*

undo authorization-server

Default

No LDAP authorization server is specified for an LDAP scheme.

Views

LDAP scheme view

Predefined user roles

network-admin

context-admin

Parameters

server-name: Specifies the name of an LDAP server, a case-sensitive string of 1 to 64 characters.

Usage guidelines

You can specify only one LDAP authorization server in an LDAP scheme. If you execute this command multiple times, the most recent configuration takes effect.

Examples

In LDAP scheme **ldap1**, specify the LDAP authorization server as **ccc**.

```
<Sysname> system-view
[Sysname] ldap scheme ldap1
[Sysname-ldap-ldap1] authorization-server ccc
```

Related commands

display ldap scheme

ldap server

character-encoding

Use **character-encoding** to specify the character encoding format for an LDAP server.

Use **undo character-encoding** to restore the default.

Syntax

character-encoding { **gb18030** | **utf-8** }

undo character-encoding

Default

No character encoding format is specified for an LDAP server. The device does not change the character encoding format for information exchanged with the LDAP server.

Views

LDAP server view

Predefined user roles

network-admin

context-admin

Parameters

gb18030: Specifies the GB18030 character encoding format.

utf-8: Specifies the UTF-8 character encoding format.

Usage guidelines

By default, the device encodes the configuration made through the Web interface in GB18030 and that made through terminal software in the character encoding format used by the software. If the device and the LDAP server use different character encoding formats, some characters in the exchanged information might fail to be interpreted, causing further issues. For example, if user DNs on the LDAP server are Chinese and the user DNs on the device are English, user DN search will fail and the users will fail to come online. To resolve this issue, use this command to ensure that the device and the LDAP server use the same character encoding format.

After you specify the character encoding format for an LDAP server, the device processes LDAP packets exchanged with the LDAP server as follows:

- For an LDAP packet sent to the LDAP server, the device first decodes the information in the packet by using GB18030. Then, the device uses the specified character encoding format to encode the information.
- For an LDAP packet received form the LDAP server, the device first uses the specified character encoding format to decode the information in the packet. Then, the device uses GB18030 to encode the information and saves the information.

As a best practice to avoid LDAP authentication failure caused by inconsistent character encoding format, change the character encoding format before using the LDAP server to perform authentication on users.

Examples

Specify UTF-8 as the character encoding format for LDAP server **ccc**.

```
<Sysname> system-view
[Sysname] ldap server ccc
[Sysname-ldap-server-ccc] character-encoding utf-8
```

Related commands

display ldap scheme

display ldap scheme

Use **display ldap scheme** to display LDAP scheme configuration.

Syntax

display ldap scheme [*ldap-scheme-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ldap-scheme-name: Specifies an LDAP scheme by its name, a case-insensitive string of 1 to 32 characters. If you do not specify an LDAP scheme, this command displays the configuration of all LDAP schemes.

Examples

Display the configuration of all LDAP schemes.

```
<Sysname> display ldap scheme
Total 1 LDAP schemes

------------------------------------------------------------------
LDAP scheme name             : aaa
  Authentication server      : aaa
    IP                       : 1.1.1.1
    Port                     : 111
    VPN instance             : Not configured
    Source IP                : Provided by interface
                               GigabitEthernet1/0/1
    LDAP protocol version    : LDAPv3
    Server timeout interval  : 10 seconds
    Login account DN         : Not configured
    Base DN                  : Not configured
    Search scope             : all-level
    User searching parameters:
      User object class      : Not configured
      Username attribute     : cn
      Username format        : with-domain
    Group filter             : (objectclass=group)
    Character encoding       : UTF-8
  Authorization server       : aaa
    IP                       : 1.1.1.1
    Port                     : 111
    VPN instance             : Not configured
    Source IP                : 2.2.2.2
    LDAP protocol version    : LDAPv3
    Server timeout interval  : 10 seconds
    Login account DN         : Not configured
    Base DN                  : Not configured
    Search scope             : all-level
    User searching parameters:
      User object class      : Not configured
      Username attribute     : cn
      Username format        : with-domain
    Group filter             : (objectclass=group)
    Character encoding       : GB18030
  Attribute map              : map1
 ------------------------------------------------------------------
```

Table 19 Command output

Field	Description
Authentication server	Name of the LDAP authentication server. If no server is configured, this field displays **Not configured**.
Authorization server	Name of the LDAP authorization server. If no server is configured, this field displays **Not configured**.
IP	IP address of the LDAP server. If no server is specified, this field

Field	Description
	displays **Not configured**.
Port	Port number of the server. If no port number is specified, this field displays the default port number.
VPN instance	MPLS L3VPN instance to which the LDAP server belongs. If no VPN instance is specified, this field displays **Not configured**.
Source IP	Source IP address of the LDAP packets sent to the LDAP server. If no source IP is specified, this field displays **Not configured**.
LDAP protocol version	LDAP version, LDAPv2 or LDAPv3.
Server timeout interval	LDAP server timeout period, in seconds.
Login account DN	DN of the administrator.
Base DN	Base DN for user search.
Search scope	User DN search scope, including: • **all-level**—All subdirectories. • **single-level**—Next lower level of subdirectories under the base DN.
User searching parameters	User search parameters.
User object class	User object class for user DN search. If no user object class is configured, this field displays **Not configured**.
Username attribute	User account attribute for login.
Username format	Format for the username sent to the server.
Group filter	User group filter.
Character encoding	Character encoding format for the LDAP server: • GB18030. • UTF-8. This field is not available if no character encoding format has been specified for the LDAP server.
Attribute map	LDAP attribute map used by the scheme. If no LDAP attribute map is used, this field displays **Not configured**.

group-filter

Use **group-filter** to configure the user group filter.

Use **undo group-filter** to restore the default.

Syntax

group-filter *group-filter*

undo group-filter

Default

The user group filter is **(objectclass=group)**.

Views

LDAP server view

Predefined user roles

network-admin

context-admin

Parameters

group-filter: Specifies the user group filter, a case-sensitive string of 1 to 127 characters. The syntax of the filter must meet the filter syntax requirements defined by LDAP servers.

Usage guidelines

When the device requests to import user group information from an LDAP server, the LDAP server sends only user groups that match the user group filter to the device.

Examples

Configure the user group filter as **(&(objectclass=group)(name=group1))** for LDAP server **ccc**.

```
<Sysname> system-view
[Sysname] ldap server ccc
[Sysname-ldap-server-ccc] group-filter (&(objectclass=group)(name=group1))
```

Related commands

display ldap scheme

ip

Use **ip** to configure the IP address of the LDAP server.

Use **undo ip** to restore the default.

Syntax

ip *ip-address* [**port** *port-number*] [**vpn-instance** *vpn-instance-name*]

undo ip

Default

An LDAP server does not have an IP address.

Views

LDAP server view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the IP address of the LDAP server.

port *port-number*: Specifies the TCP port number of the LDAP server. The value range for the *port-number* argument is 1 to 65535, and the default value is 389.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance to which the LDAP server belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the server is on the public network, do not specify this option.

Usage guidelines

The LDAP service port configured on the device must be consistent with the service port of the LDAP server.

If you change the IP address and port number of the LDAP server, the change takes effect only on the LDAP authentication that occurs after the change.

Examples

Specify the IP address and port number as 192.168.0.10 and 4300 for LDAP server **ccc**.

```
<Sysname> system-view
[Sysname] ldap server ccc
[Sysname-ldap-server-ccc] ip 192.168.0.10 port 4300
```

Related commands

ldap server

ipv6

Use **ipv6** to configure the IPv6 address of the LDAP server.

Use **undo ipv6** to restore the default.

Syntax

ipv6 *ipv6-address* [**port** *port-number*] [**vpn-instance** *vpn-instance-name*]

undo ipv6

Default

An LDAP server does not have an IPv6 address.

Views

LDAP server view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address: Specifies the IPv6 address of the LDAP server.

port *port-number*: Specifies the TCP port number of the LDAP server. The value range for the *port-number* argument is 1 to 65535, and the default value is 389.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance to which the LDAP server belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the server is on the public network, do not specify this option.

Usage guidelines

The LDAP service port configured on the device must be consistent with the service port of the LDAP server.

If you change the IP address and port number of the LDAP server, the change takes effect only on the LDAP authentication that occurs after the change.

Examples

Specify the IPv6 address and port number as 1:2::3:4 and 4300 for LDAP server **ccc**.

```
<Sysname> system-view
[Sysname] ldap server ccc
[Sysname-ldap-server-ccc] ipv6 1:2::3:4 port 4300
```

Related commands

ldap server

ldap attribute-map

Use **ldap attribute-map** to create an LDAP attribute map and enter its view, or enter the view of an existing LDAP attribute map.

Use **undo ldap attribute-map** to delete an LDAP attribute map.

Syntax

ldap attribute-map *map-name*

undo ldap attribute-map *map-name*

Default

No LDAP attribute maps exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

map-name: Specifies the name of the LDAP attribute map, a case-sensitive string of 1 to 31 characters.

Usage guidelines

Execute this command multiple times to create multiple LDAP attribute maps. You can add multiple mapping entries to an LDAP attribute map. Each entry defines the mapping between an LDAP attribute and an AAA attribute.

Examples

Create an LDAP attribute map named **map1** and enter LDAP attribute map view.

```
<Sysname> system-view
[Sysname] ldap attribute-map map1
[Sysname-ldap-map-map1]
```

Related commands

attribute-map

ldap scheme

map

ldap scheme

Use **ldap scheme** to create an LDAP scheme and enter its view, or enter the view of an existing LDAP scheme.

Use **undo ldap scheme** to delete an LDAP scheme.

Syntax

ldap scheme *ldap-scheme-name*

undo ldap scheme *ldap-scheme-name*

Default

No LDAP schemes exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ldap-scheme-name: Specifies the LDAP scheme name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

An LDAP scheme can be used by more than one ISP domain at the same time.

You can configure a maximum of 16 LDAP schemes.

Examples

Create an LDAP scheme named **ldap1** and enter LDAP scheme view.

```
<Sysname> system-view
[Sysname] ldap scheme ldap1
[Sysname-ldap-ldap1]
```

Related commands

display ldap scheme

ldap server

Use **ldap server** to create an LDAP server and enter its view, or enter the view of an existing LDAP server.

Use **undo ldap server** to delete an LDAP server.

Syntax

ldap server *server-name*

undo ldap server *server-name*

Default

No LDAP servers exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

server-name: Specifies the LDAP server name, a case-insensitive string of 1 to 64 characters.

Examples

Create an LDAP server named **ccc** and enter LDAP server view.

```
<Sysname> system-view
[Sysname] ldap server ccc
[Sysname-ldap-server-ccc]
```

Related commands

display ldap scheme

login-dn

Use **login-dn** to specify the administrator DN.

Use **undo login-dn** to restore the default.

Syntax

login-dn *dn-string*

undo login-dn

Default

No administrator DN is specified.

Views

LDAP server view

Predefined user roles

network-admin

context-admin

Parameters

dn-string: Specifies the administrator DN for binding with the server, a case-insensitive string of 1 to 255 characters.

Usage guidelines

The administrator DN specified on the device must be consistent with the administrator DN configured on the LDAP server.

If you change the administrator DN, the change takes effect only on the LDAP authentication that occurs after the change.

Examples

Specify the administrator DN as **uid=test, ou=people, o=example, c=city** for LDAP server **ccc**.

```
<Sysname> system-view
[Sysname] ldap server ccc
[Sysname-ldap-server-ccc] login-dn uid=test,ou=people,o=example,c=city
```

Related commands

display ldap scheme

login-password

Use **login-password** to configure the administrator password for binding with the LDAP server during LDAP authentication.

Use **undo login-password** to restore the default.

Syntax

login-password { **cipher** | **simple** } *string*

undo login-password

Default

No administrator password is configured.

Views

LDAP server view

Predefined user roles

network-admin

context-admin

Parameters

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 128 characters. Its encrypted form is a case-sensitive string of 1 to 201 characters.

Usage guidelines

This command takes effect only after the **login-dn** command is used.

Examples

Specify the administrator password as **abcdefg** in plaintext form for LDAP server **ccc**.

```
<Sysname> system-view
[Sysname] ldap server ccc
[Sysname-ldap-server-ccc] login-password simple abcdefg
```

Related commands

display ldap scheme

login-dn

map

Use **map** to configure a mapping entry in an LDAP attribute map.

Use **undo map** to delete the specified mapping entries from the LDAP attribute map.

Syntax

map ldap-attribute *ldap-attribute-name* [**prefix** *prefix-value* **delimiter** *delimiter-value*] **aaa-attribute user-group**

undo map [**ldap-attribute** *ldap-attribute-name*]

Default

An LDAP attribute map does not contain mapping entries.

Views

LDAP attribute map view

Predefined user roles

network-admin

context-admin

Parameters

ldap-attribute *ldap-attribute-name*: Specifies an LDAP attribute by its name. The *ldap-attribute-name* argument is a case-sensitive string of 1 to 63 characters.

prefix *prefix-value* **delimiter** *delimiter-value*: Specifies a partial value string of the LDAP attribute for attribute mapping. The *prefix-value* argument represents the position where the partial string starts. The prefix is a case-sensitive string of 1 to 7 characters, such as **cn=**. The *delimiter-value* argument represents the position where the partial string ends, such as a comma (,). If you do not specify the **prefix** *prefix-value* **delimiter** *delimiter-value* option, the mapping entry uses the entire value string of the LDAP attribute.

aaa-attribute: Specifies an AAA attribute.

user-group: Specifies the user group attribute.

Usage guidelines

Because the device ignores unrecognized LDAP attributes, configure the mapping entries to include important LDAP attributes that should not be ignored.

An LDAP attribute can be mapped only to one AAA attribute. Different LDAP attributes can be mapped to the same AAA attribute.

If you do not specify an LDAP attribute for the **undo map** command, the command deletes all mapping entries from the LDAP attribute map.

Examples

In LDAP attribute map **map1**, map a partial value string of the LDAP attribute named **memberof** to AAA attribute named **user-group**.

```
<Sysname> system-view
[Sysname] ldap attribute-map map1
[Sysname-ldap-map-map1] map ldap-attribute memberof prefix cn= delimiter , aaa-attribute user-group
```

Related commands

ldap attribute-map

user-group

protocol-version

Use **protocol-version** to specify the LDAP version.

Use **undo protocol-version** to restore the default.

Syntax

protocol-version { **v2** | **v3** }

undo protocol-version

Default

The LDAP version is LDAPv3.

Views

LDAP server view

Predefined user roles

network-admin

context-admin

Parameters

v2: Specifies the LDAP version LDAPv2.

v3: Specifies the LDAP version LDAPv3.

Usage guidelines

For successful LDAP authentication, the LDAP version used by the device must be consistent with the version used by the LDAP server.

If you change the LDAP version, the change takes effect only on the LDAP authentication that occurs after the change.

A Microsoft LDAP server supports only LDAPv3.

Examples

Specify the LDAP version as LDAPv2 for LDAP server **ccc**.

```
<Sysname> system-view
[Sysname] ldap server ccc
[Sysname-ldap-server-ccc] protocol-version v2
```

Related commands

display ldap scheme

search-base-dn

Use **search-base-dn to** specify the base DN for user search.

Use **undo search-base-dn** to restore the default.

Syntax

search-base-dn *base-dn*

undo search-base-dn

Default

No base DN is specified for user search.

Views

LDAP server view

Predefined user roles

network-admin

context-admin

Parameters

base-dn: Specifies the base DN for user search, a case-insensitive string of 1 to 255 characters.

Examples

Specify the base DN for user search as **dc=ldap,dc=com** for LDAP server **ccc**.

```
<Sysname> system-view
[Sysname] ldap server ccc
[Sysname-ldap-server-ccc] search-base-dn dc=ldap,dc=com
```

Related commands

display ldap scheme

ldap server

search-scope

Use **search-scope** to specify the user search scope.

Use **undo search-scope** to restore the default.

Syntax

search-scope { **all-level** | **single-level** }

undo search-scope

Default

The user search scope is **all-level**.

Views

LDAP server view

Predefined user roles

network-admin

context-admin

Parameters

all-level: Specifies that the search goes through all subdirectories of the base DN.

single-level: Specifies that the search goes through only the next lower level of subdirectories under the base DN.

Examples

Specify the search scope for the LDAP authentication as all subdirectories of the base DN for LDAP server **ccc**.

```
<Sysname> system-view
[Sysname] ldap server ccc
[Sysname-ldap-server-ccc] search-scope all-level
```

Related commands

display ldap scheme

ldap server

server-timeout

Use **server-timeout** to set the LDAP server timeout period, the maximum time that the device waits for an LDAP response.

Use **undo server-timeout** to restore the default.

Syntax

server-timeout *time-interval*

undo server-timeout

Default

The LDAP server timeout period is 10 seconds.

Views

LDAP server view

Predefined user roles

network-admin

context-admin

Parameters

time-interval: Specifies the LDAP server timeout period in the range of 5 to 20 seconds.

Usage guidelines

If you change the LDAP server timeout period, the change takes effect only on the LDAP authentication that occurs after the change.

Examples

Set the LDAP server timeout period to 15 seconds for LDAP server **ccc**.

```
<Sysname> system-view
[Sysname] ldap server ccc
[Sysname-ldap-server-ccc] server-timeout 15
```

Related commands

display ldap scheme

source-ip

Use **source-ip** to specify a source interface or source IP address for outgoing LDAP packets.

Use **undo source-ip** to remove the source interface or the source IP address of the specified type for outgoing LDAP packets.

Syntax

source-ip { *ipv4-address* | **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }

undo source-ip [**interface** | **ipv6**]

Default

No IP address is specified as the source IP address of LDAP packets sent to an LDAP server. The device uses the primary IPv4 address or the IPv6 address of the outbound interface that can reach the server as the source IP address of LDAP packets sent to the server.

Views

LDAP server view

Predefined user roles

network-admin

context-admin

Parameters

interface *interface-type interface-number*: Specifies a source interface by its type and number. The device uses the primary IPv4 address or the IPv6 address of the interface as the source IP address of an outgoing LDAP packet.

ipv4-address: Specifies an IPv4 address, which must be an address of the device. The IP address cannot be 0.0.0.0, 255.255.255.255, a class D address, a class E address, or a loopback address.

ipv6 *ipv6-address*: Specifies an IPv6 address, which must be a unicast address of the device and cannot be a loopback address or a link-local address.

Usage guidelines

When you use this command for an LDAP server, follow these restrictions and guidelines:

- You can specify only one source IPv4 address and one source IPv6 address for LDAP packets sent to the server.
- You can specify only one source interface. Make sure the source interface can reach the server.
- To have the source interface configuration take effect, make sure the source interface is in the same VPN instance as the server.
- To have the source address configuration take effect, the IP version of the specified source address must be the same as that of the server IP address.
- The source interface configuration and the source address configuration overwrite each other.

Examples

Specify 3.3.3.3 as the source IP address of the LDAP packets sent to LDAP server **ccc**.

```
<Sysname> system-view
[Sysname] ldap server ccc
[Sysname-ldap-server-ccc] source-ip 3.3.3.3
```

Specify GigabitEthernet 1/0/1 as the source interface of the LDAP packets sent to LDAP server **ddd**.

```
<Sysname> system-view
[Sysname] ldap server ddd
[Sysname-ldap-server-ddd] source-ip interface gigabitethernet 1/0/1
```

user-parameters

Use **user-parameters** to configure LDAP user attributes, including the username attribute, username format, and user-defined user object class.

Use **undo user-parameters** to restore the default of an LDAP user attribute.

Syntax

user-parameters { **user-name-attribute** { *name-attribute* | **cn** | **uid** } | **user-name-format** { **with-domain** | **without-domain** } | **user-object-class** *object-class-name* }

undo user-parameters { **user-name-attribute** | **user-name-format** | **user-object-class** }

Default

The LDAP username attribute is **cn** and the username format is **without-domain**. No user object class is specified and the default user object class of the LDAP server is used.

Views

LDAP server view

Predefined user roles

network-admin

context-admin

Parameters

user-name-attribute { *name-attribute* | **cn** | **uid** }: Specifies the username attribute. The *name-attribute* argument represents an attribute value, a case-insensitive string of 1 to 64 characters. The **cn** keyword represents the user account attribute of common name, and the **uid** keyword represents the user account attribute of user ID.

user-name-format { **with-domain** | **without-domain** }: Specifies the format of the username to be sent to the server. The **with-domain** keyword means that the username contains the domain name, and the **without-domain** keyword means that the username does not contain the domain name.

user-object-class *object-class-name*: Specifies the user object class for user search. The *object-class-name* argument represents a class value, a case-insensitive string of 1 to 64 characters.

Usage guidelines

If the username on the LDAP server does not contain the domain name, specify the **without-domain** keyword. If the username contains the domain name, specify the **with-domain** keyword.

Examples

Set the user object class to **person** for LDAP server **ccc**.

```
<Sysname> system-view
[Sysname] ldap server ccc
[Sysname-ldap-server-ccc] user-parameters user-object-class person
```

Related commands

display ldap scheme

login-dn

Contents

802.1X commands

The following compatibility matrixes shows the support of hardware platforms for 802.1X:

Models	802.1X compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080	Yes
NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	No

display dot1x

Use **`display dot1x`** to display information about 802.1X.

Syntax

`display dot1x` [**`sessions`** | **`statistics`**] [**`interface`** *`interface-type interface-number`*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

`sessions`: Displays 802.1X session information.

`statistics`: Displays 802.1X statistics.

`interface` *`interface-type interface-number`*: Specifies a port by its type and number.

Usage guidelines

If you do not specify the **`sessions`** keyword or the **`statistics`** keyword, this command displays all information about 802.1X, including session information, statistics, and settings.

If you do not specify any parameters, this command displays all 802.1X information.

Examples

Display all information about 802.1X.

```
<Sysname> display dot1x
Global 802.1X parameters:
   802.1X authentication  : Enabled
   CHAP authentication    : Enabled
   Max-tx period          : 30 s
   Handshake period       : 15 s
```

```
  Quiet timer            : Disabled
        Quiet period     : 60 s
  Supp timeout           : 30 s
  Server timeout         : 100 s
  Reauth period          : 3600 s
  Max auth requests      : 2
  SmartOn switch ID      : 30
  SmartOn supp timeout   : 30 s
  SmartOn retry counts   : 3
  EAD assistant function : Disabled
      URL                : http://www.dwsoft.com
      Free IP            : 6.6.6.0         255.255.255.0
      EAD timeout        : 30 min
  Domain delimiter       : @
Online 802.1X wired users    : 1
Online 802.1X wireless users : 1

GigabitEthernet1/0/1  is link-up
  802.1X authentication      : Enabled
  Handshake                  : Enabled
  Handshake reply            : Disabled
  Handshake security         : Disabled
  Unicast trigger            : Disabled
  Periodic reauth            : Disabled
  Port role                  : Authenticator
  Authorization mode         : Auto
  Port access control        : Port-based
  Multicast trigger          : Enabled
  Mandatory auth domain      : Not configured
  Guest VLAN                 : 3
  Auth-Fail VLAN             : Not configured
  Critical VLAN              : Not configured
  Re-auth server-unreachable : Logoff
  Max online users           : 256
  SmartOn                    : Disabled

  EAPOL packets: Tx 3, Rx 4
  Sent EAP Request/Identity packets : 1
       EAP Request/Challenge packets: 1
       EAP Success packets: 1
       EAP Failure packets: 0
  Received EAPOL Start packets : 1
           EAPOL LogOff packets: 1
           EAP Response/Identity packets : 1
           EAP Response/Challenge packets: 1
           Error packets: 0
  Online 802.1X users: 1
         MAC address         Auth state
```

```
          0001-0000-0000      Authenticated
```

Table 1 Command output

Field	Description
Global 802.1X parameters	Global 802.1X configuration.
802.1X authentication	Whether 802.1X is enabled globally.
CHAP authentication	Performs EAP termination and uses CHAP to communicate with the RADIUS server.
EAP authentication	Relays EAP packets and supports any of the EAP authentication methods to communicate with the RADIUS server.
PAP authentication	Performs EAP termination and uses PAP to communicate with the RADIUS server.
Max-tx period	Username request timeout timer in seconds.
Handshake period	Handshake timer in seconds.
Quiet timer	Status of the quiet timer, enabled or disabled.
Quiet period	Quiet timer in seconds.
Supp timeout	Client timeout timer in seconds.
Server timeout	Server timeout timer in seconds.
Reauth period	Periodic reauthentication timer in seconds.
Max auth requests	Maximum number of attempts for sending an authentication request to a client.
SmartOn switch ID	Switch ID for SmartOn authentication.
SmartOn supp timeout	SmartOn client timeout timer in seconds.
SmartOn retry counts	Maximum number of attempts for retransmitting an EAP-Request/Notification packet to a client.
EAD assistant function	Whether EAD assistant is enabled.
URL	Redirect URL for unauthenticated users using a Web browser to access the network.
Free IP	Network segment accessible to unauthenticated users.
EAD timeout	EAD rule timer in minutes.
Domain delimiter	Domain delimiters supported by the device.
Online 802.1X wired users	Number of wired online 802.1X users, including users that have passed 802.1X authentication and users that are performing 802.1X authentication.
Online 802.1X wireless users	Number of wireless online 802.1X users, including users that have passed 802.1X authentication and users that are performing 802.1X authentication.
GigabitEthernet1/0/1 is link-up	Status of the port. In this example, GigabitEthernet 1/0/1 is up.
802.1X authentication	Whether 802.1X is enabled on the port.
Handshake	Whether the online user handshake feature is enabled on the port.
Handshake reply	Whether the online user handshake reply feature is enabled on the port.
Handshake security	Whether the online user handshake security feature is enabled on the port.

Field	Description
Unicast trigger	Whether the 802.1X unicast trigger is enabled on the port.
Periodic reauth	Whether 802.1X periodic reauthentication is enabled on the port.
Port role	Role of the port. The port functions only as an **Authenticator**.
Authorization mode	Authorization state of the port, which can be Force-Authorized, Auto, or Force-Unauthorized.
Port access control	Access control method of the port: • **MAC-based**—MAC-based access control. • **Port-based**—Port-based access control.
Multicast trigger	Whether the 802.1X multicast trigger feature is enabled.
Mandatory auth domain	Mandatory authentication domain on the port.
Guest VLAN	802.1X guest VLAN configured on the port. If no 802.1X guest VLAN is configured on the port, this field displays **Not configured**.
Auth-Fail VLAN	802.1X Auth-Fail VLAN configured on the port. If no 802.1X Auth-Fail VLAN is configured on the port, this field displays **Not configured**.
Critical VLAN	802.1X critical VLAN configured on the port. If no 802.1X critical VLAN is configured on the port, this field displays **Not configured**.
Re-auth server-unreachable	Whether to log off online 802.1X users or keep them online when no server is reachable for 802.1X reauthentication.
Max online users	Maximum number of concurrent 802.1X users on the port.
SmartOn	Whether SmartOn authentication is enabled on the port.
EAPOL packets	Number of sent (Tx) and received (Rx) EAPOL packets.
Sent EAP Request/Identity packets	Number of sent EAP-Request/Identity packets.
EAP Request/Challenge packets	Number of sent EAP-Request/MD5-Challenge packets.
EAP Success packets	Number of sent EAP-Success packets.
EAP Failure packets	Number of sent EAP-Failure packets.
Received EAPOL Start packets	Number of received EAPOL-Start packets.
EAPOL LogOff packets	Number of received EAPOL-LogOff packets.
EAP Response/Identity packets	Number of received EAP-Response/Identity packets.
EAP Response/Challenge packets	Number of received EAP-Response/MD5-Challenge packets.
Error packets	Number of received error packets.
Online 802.1X users	Number of online 802.1X users on the port, including users that have passed 802.1X authentication and users that are performing 802.1X authentication.
MAC address	MAC addresses of the online 802.1X users.
Auth state	Authentication status of the online 802.1X users.
SSID	SSID with which users are associated.
BSSID	ID of the BSS with which users are associated.

display dot1x connection

Use **display dot1x connection** to display information about online 802.1X users.

Syntax

display dot1x connection [**interface** *interface-type interface-number* | **slot** *slot-number* | **user-mac** *mac-address* | **user-name** *name-string*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify a port, this command displays online 802.1X user information for all ports.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays online 802.1X user information for all member devices.

user-mac *mac-address*: Specifies an 802.1X user by MAC address. The *mac-address* argument represents the MAC address of the user, in the form of H-H-H. If you do not specify an 802.1X user, this command displays online user information for all 802.1X users.

user-name *name-string*: Specifies an 802.1X user by its name. The *name-string* argument represents the username, a case-sensitive string of 1 to 253 characters. If you do not specify an 802.1X user, this command displays online user information for all 802.1X users.

Usage guidelines

If you do not specify any parameters, this command displays information about online 802.1X users for all ports.

If you do not specify any parameters, this command displays information about online 802.1X users for all member devices.

Examples

Display all online 802.1X user information.

```
<Sysname> display dot1x connection
Total connections: 1

Slot ID: 0
User MAC address: 0015-e9a6-7cfe
Access interface: GigabitEthernet1/0/1
Username: ias
Authentication domain: abc
IPv4 address: 192.168.1.1
IPv6 address: 2000:0:0:0:1:2345:6789:abcd
Authentication method: CHAP
Initial VLAN: 1
Authorization untagged VLAN: 6
```

```
Authorization tagged VLAN list: 1 to 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 29 31 33
                                35 37 40 to 100
Authorization ACL number/name: 3001
Authorization user profile: N/A
Termination action: Default
Session timeout period: 2 s
Online from: 2013/03/02  13:14:15
Online duration: 0h 2m 15s

User MAC address                : 0016-ecb7-a879
User name                       : ias
Authentication domain           : 1
IPv4 address                    : 192.168.1.1
IPv6 address                    : 2000:0:0:0:1:2345:6789:abcd
Authentication method           : CHAP
Initial VLAN                    : 1
Authorization VLAN              : N/A
Authorization ACL number        : 3001
Authorization user profile      : N/A
Authorization CAR               :
  Average input rate            : 102400 bps
  Average output rate           : 102400 bps
Termination action              : Default
Session timeout period          : 2 sec
Online from                     : 2013/03/02 13:14:15
Online duration                 : 0 h 2 m 15 s
Level flow statistic            :
Level-0     Sent packets/bates  : 1/54
        Received packets/bates  : 0/0
Level-1     Sent packets/bates  : 0/0
        Received packets/bates  : 45/1248
```

Table 2 Command output

Field	Description
Total connections	Number of online 802.1X users.
User MAC address	MAC address of the user.
Access interface	Interface through which the user access the device.
AP name	Name of the AP with which the user is associated.
Radio ID	ID of the radio with which the user is associated.
Authentication domain	ISP domain used for 802.1X authentication.
IPv4 address	IPv4 address of the user. If the device does not get the IPv4 address of the user, this field is not available.
IPv6 address	IPv6 address of the user. If the device does not get the IPv6 address of the user, this field is not available.

Field	Description
Authentication method	EAP message handling method: • **CHAP**—Performs EAP termination and uses CHAP to communicate with the RADIUS server. • **EAP**—Relays EAP packets and supports any of the EAP authentication methods to communicate with the RADIUS server. • **PAP**—Performs EAP termination and uses PAP to communicate with the RADIUS server.
Initial VLAN	VLAN to which the user belongs before 802.1X authentication.
Authorization untagged VLAN	Untagged VLAN authorized to the user.
Authorization tagged VLAN list	Tagged VLANs authorized to the user.
Authorization ACL number/name	Number or name of the ACL authorized to the user. If no ACL is authorized, this field displays **N/A**. If ACL authorization fails, this field displays **(Not effective)** after the ACL number or name.
Authorization user profile	User profile authorized to the user.
Authorization CAR	Authorization CAR attributes assigned by the server. • **Average input rate**—Average rate of inbound traffic in bps. • **Average output rate**—Average rate of outbound traffic in bps. If no authorization CAR attributes are assigned, this field displays **N/A**.
Termination action	Action attribute assigned by the server to terminate the user session: • **Default**—Logs off the online authenticated 802.1X user when the session timeout timer expires. This attribute does not take effect when 802.1X periodic reauthentication is enabled and the periodic reauthentication timer is shorter than the session timeout timer. • **Radius-request**—Reauthenticates the online user when the session timeout timer expires, regardless of whether the 802.1X periodic reauthentication feature is enabled or not. If the device performs local authentication, this field displays **N/A**.
Session timeout period	Session timeout timer assigned by the server. If the device performs local authentication, this field displays **N/A**.
Online from	Time from which the 802.1X user came online.
Online duration	Online duration of the 802.1X user.

dot1x

Use **dot1x** to enable 802.1X globally or on a port.

Use **undo dot1x** to disable 802.1X globally or on a port.

Syntax

dot1x

undo dot1x

Default

802.1X is neither enabled globally nor enabled for any port.

Views

System view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

For the 802.1X feature to take effect on a port, you must enable the feature both globally and on the port.

Examples

Enable 802.1X globally.

```
<Sysname> system-view
[Sysname] dot1x
```

Enable 802.1X on GigabitEthernet 1/0/1.

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x
[Sysname-GigabitEthernet1/0/1] quit
```

Related commands

display dot1x

dot1x authentication-method

Use **dot1x authentication-method** to specify an EAP message handling method.

Use **undo dot1x authentication-method** to restore the default.

Syntax

dot1x authentication-method { **chap** | **eap** | **pap** }

undo dot1x authentication-method

Default

The access device performs EAP termination and uses CHAP to communicate with the RADIUS server.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

chap: Configures the access device to perform Extensible Authentication Protocol (EAP) termination and use the Challenge Handshake Authentication Protocol (CHAP) to communicate with the RADIUS server.

eap: Configures the access device to relay EAP packets, and supports any of the EAP authentication methods to communicate with the RADIUS server.

pap: Configures the access device to perform EAP termination and use the Password Authentication Protocol (PAP) to communicate with the RADIUS server.

Usage guidelines

The access device terminates or relays EAP packets.

- **In EAP termination mode**—The access device re-encapsulates and sends the authentication data from the client in standard RADIUS packets to the RADIUS server. The device performs either CHAP or PAP authentication with the RADIUS server. In this mode, the RADIUS server supports only MD5-Challenge EAP authentication and the username and password EAP authentication initiated by an iNode client.
  - PAP transports usernames and passwords in plain text. The authentication method applies to scenarios that do not require high security. To use PAP, the client can be an iNode 802.1X client.
  - CHAP transports usernames in plain text and passwords in encrypted form over the network. CHAP is more secure than PAP.
- **In EAP relay mode**—The access device relays EAP messages between the client and the RADIUS server. The EAP relay mode supports multiple EAP authentication methods, such as MD5-Challenge, EAP-TLS, and PEAP. To use this mode, make sure the RADIUS server meets the following requirements:
  - Supports the EAP-Message and Message-Authenticator attributes.
  - Uses the same EAP authentication method as the client.

  If this mode is used, the **user-name-format** command configured in RADIUS scheme view does not take effect. For more information about the **user-name-format** command, see "RADIUS commands."

If RADIUS authentication is used, you must configure the access device to use the same authentication method (PAP, CHAP, or EAP) as the RADIUS server.

Examples

Enable the access device to terminate EAP packets and perform PAP authentication with the RADIUS server.

```
<Sysname> system-view
[Sysname] dot1x authentication-method pap
```

Related commands

display dot1x

dot1x auth-fail vlan

Use **dot1x auth-fail vlan** to configure an 802.1X Auth-Fail VLAN on a port.

Use **undo dot1x auth-fail vlan** to restore the default.

Syntax

dot1x auth-fail vlan *authfail-vlan-id*

undo dot1x auth-fail vlan

Default

No 802.1X Auth-Fail VLAN exists on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

context-admin

Parameters

authfail-vlan-id: Specifies the ID of the 802.1X Auth-Fail VLAN on the port. The value range for the VLAN ID is 1 to 4094. Make sure the VLAN has been created. If the port type is hybrid, verify that the VLAN to be specified as the Auth-Fail VLAN is not in the tagged VLAN list on the port.

Usage guidelines

An 802.1X Auth-Fail VLAN accommodates users that have failed 802.1X authentication for any reason other than unreachable servers. Users in the Auth-Fail VLAN can access a limited set of network resources.

To delete a VLAN that has been configured as an 802.1X Auth-Fail VLAN, you must first use the **undo dot1x auth-fail vlan** command.

Examples

Configure VLAN 100 as the Auth-Fail VLAN on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x auth-fail vlan 100
```

Related commands

display dot1x

dot1x critical vlan

Use **dot1x critical vlan** to configure an 802.1X critical VLAN on a port.

Use **undo dot1x critical vlan** to restore the default.

Syntax

dot1x critical vlan *critical-vlan-id*

undo dot1x critical vlan

Default

No 802.1X critical VLAN exists on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

context-admin

Parameters

critical-vlan-id: Specifies the ID of the 802.1X critical VLAN on the port. The value range for the VLAN ID is 1 to 4094. Make sure the VLAN has been created. If the port type is hybrid, verify that the VLAN to be specified as the critical VLAN is not in the tagged VLAN list on the port.

Usage guidelines

An 802.1X critical VLAN accommodates users that fail 802.1X authentication because all the RADIUS servers in their ISP domains are unreachable. Users in the critical VLAN can access a limited set of network resources depending on the configuration.

To delete a VLAN that has been configured as an 802.1X critical VLAN, you must first use the **undo dot1x critical vlan** command.

Examples

Specify VLAN 100 as the 802.1X critical VLAN on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x critical vlan 100
```

Related commands

display dot1x

dot1x domain-delimiter

Use **dot1x domain-delimiter** to specify a set of domain name delimiters supported by the device.

Use **undo dot1x domain-delimiter** to restore the default.

Syntax

dot1x domain-delimiter *string*

undo dot1x domain-delimiter

Default

The device supports only the at sign (@) delimiter for 802.1X users.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

string: Specifies a set of 1 to 16 domain name delimiters for 802.1X users. No space is required between delimiters. Available delimiters include the at sign (@), backslash (\), dot (.), and forward slash (/). If you want to use backslash (\) as the domain name delimiter, you must enter the escape character (\) along with the backslash (\) sign.

Usage guidelines

Any character in the configured set can be used as the domain name delimiter for 802.1X authentication users. Usernames that include domain names can use the format of *username*@*domain-name*, *domain-name**username*, *username*.*domain-name*, or *username*/*domain-name*.

The delimiter set you configured overrides the default setting. If the at sign (@) is not included in the delimiter set, the device does not support the 802.1X users that use this sign as the domain name delimiter.

If a username string contains multiple configured delimiters, the device takes the rightmost delimiter in the username string as the domain name delimiter. For example, if you configure the forward slash (/), dot (.), and backslash (\) as delimiters, the domain name delimiter for the username string 121.123/22\@abc is the backslash (\). The username is **@abc** and the domain name is **121.123/22**.

Examples

Specify the at sign (@) and forward slash (/) as domain name delimiters.

```
<Sysname> system-view
[Sysname] dot1x domain-delimiter @/
```

Related commands

display dot1x

dot1x ead-assistant enable

Use **dot1x ead-assistant enable** to enable the EAD assistant feature.

Use **undo dot1x ead-assistant enable** to disable the EAD assistant feature.

Syntax

dot1x ead-assistant enable

undo dot1x ead-assistant enable

Default

The EAD assistant feature is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

The EAD assistant feature enables the access device to redirect the HTTP requests of a user to a URL to download and install EAD client. This feature eliminates the tedious job of the administrator to deploy EAD clients.

For the EAD assistant feature to take effect on a port, you must set the port authorization mode to **auto**.

Examples

Enable the EAD assistant feature.

```
<Sysname> system-view
[Sysname] dot1x ead-assistant enable
```

Related commands

display dot1x

dot1x ead-assistant free-ip

dot1x ead-assistant url

dot1x ead-assistant free-ip

Use **dot1x ead-assistant free-ip** to configure a free IP.

Use **undo dot1x ead-assistant free-ip** to remove the specified or all free IP addresses.

Syntax

dot1x ead-assistant free-ip *ip-address* { *mask-address* | *mask-length* }

undo dot1x ead-assistant free-ip { *ip-address* { *mask-address* | *mask-length* } | **all** }

Default

No free IPs exist. Users cannot access any segments before they pass 802.1X authentication.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies a freely accessible IP address segment, also called a free IP.

mask: Specifies an IP address mask.

mask-length: Specifies IP address mask length in the range of 1 to 32.

all: Removes all free IP addresses.

Usage guidelines

With EAD assistant enabled on the device, unauthenticated 802.1X users can access the network resources in the free IP segments before they pass 802.1X authentication.

Execute this command multiple times to configure multiple free IPs.

Examples

Configure 192.168.1.1/16 as a free IP.

```
<Sysname> system-view
[Sysname] dot1x ead-assistant free-ip 192.168.1.1 255.255.0.0
```

Related commands

display dot1x

dot1x ead-assistant enable

dot1x ead-assistant url

dot1x ead-assistant url

Use **dot1x ead-assistant url** to configure a redirect URL for EAD assistant.

Use **undo dot1x ead-assistant url** to restore the default.

Syntax

dot1x ead-assistant url *url-string*

undo dot1x ead-assistant url

Default

No redirect URL exists for EAD assistant.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

url-string: Specifies the redirect URL, a case-sensitive string of 1 to 64 characters.

Usage guidelines

When an unauthenticated user uses a Web browser to access any network other than the free IP, the device redirects the HTTP requests of the user to the redirect URL.

The redirect URL must be on the free IP subnet.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure the redirect URL as http://test.com.

```
<Sysname> system-view
[Sysname] dot1x ead-assistant url http://test.com
```

Related commands

display dot1x

dot1x ead-assistant enable

dot1x ead-assistant free-ip

dot1x guest-vlan

Use **dot1x guest-vlan** to configure an 802.1X guest VLAN on a port.

Use **undo dot1x guest-vlan** to restore the default.

Syntax

dot1x guest-vlan *guest-vlan-id*

undo dot1x guest-vlan

Default

No 802.1X guest VLAN exists on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

context-admin

Parameters

guest-vlan-id: Specifies the ID of the 802.1X guest VLAN. The value range for the VLAN ID is 1 to 4094. Make sure the VLAN has been created. If the port type is hybrid, verify that the VLAN to be specified as the guest VLAN is not in the tagged VLAN list on the port.

Usage guidelines

An 802.1X guest VLAN accommodates users that have not performed 802.1X authentication. In the guest VLAN, users can access a limited set of network resources, such as a software server, to download anti-virus software and system patches.

To delete a VLAN that has been configured as a guest VLAN, you must use the **undo dot1x guest-vlan** command first.

Examples

Specify VLAN 100 as the 802.1X guest VLAN on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] dot1x guest-vlan 100
```

Related commands

display dot1x

dot1x handshake

Use **dot1x handshake** to enable the online user handshake feature.

Use **undo dot1x handshake** to disable the online user handshake feature.

Syntax

dot1x handshake

undo dot1x handshake

Default

The online user handshake feature is enabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

The online user handshake feature enables the device to periodically send EAP-Request/Identity packets to the client for verifying the connectivity status of online 802.1X users. The device sets a user to the offline state if it does not receive an EAP-Response/Identity packet from the user after making the maximum attempts within the handshake period. To set the handshake timer, use the **dot1x timer handshake-period** command. To set the maximum handshake attempts, use the **dot1x retry** command.

Examples

Enable the online user handshake feature on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x handshake
```

Related commands

display dot1x

dot1x timer handshake-period

dot1x retry

dot1x handshake reply enable

Use **dot1x handshake reply enable** to enable the 802.1X online user handshake reply feature.

Use **undo dot1x handshake reply enable** to disable the 802.1X online user handshake reply feature.

Syntax

dot1x handshake reply enable

undo dot1x handshake reply enable

Default

The 802.1X online user handshake reply feature is disabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command enables the device to reply to 802.1X clients' EAP-Response/Identity packets with EAP-Success packets during the online handshake process.

Use this command only if 802.1X clients will go offline without receiving EAP-Success packets from the device.

Examples

Enable the 802.1X online user handshake reply feature on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x handshake reply enable
```

Related commands

dot1x handshake

dot1x handshake secure

Use **dot1x handshake secure** to enable the online user handshake security feature.

Use **undo dot1x handshake secure** to disable the online user handshake security feature.

Syntax

dot1x handshake secure

undo dot1x handshake secure

Default

The online user handshake security feature is disabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

The online user handshake security feature enables the device to prevent users from using illegal client software.

The feature is implemented based on the online user handshake feature. To bring the security function into effect, make sure the online user handshake feature is enabled.

The online user handshake security feature takes effect only on the network where the iNode client and IMC server are used.

Examples

Enable the online user handshake security feature on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x handshake secure
```

Related commands

display dot1x

dot1x handshake

dot1x mandatory-domain

Use **dot1x mandatory-domain** to specify a mandatory 802.1X authentication domain on a port.

Use **undo dot1x mandatory-domain** to restore the default.

Syntax

dot1x mandatory-domain *domain-name*

undo dot1x mandatory-domain

Default

No mandatory 802.1X authentication domain is specified on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

context-admin

Parameters

domain-name: Specifies the ISP domain name, a case-insensitive string of 1 to 255 characters.

Usage guidelines

When the system authenticates an 802.1X user trying to access a port, it selects an authentication domain in the following order:

1. Mandatory domain.
2. ISP domain specified in the username.
3. Default ISP domain.

Examples

Specify **my-domain** as the mandatory authentication domain for 802.1X users on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x mandatory-domain my-domain
```

Related commands

display dot1x

dot1x max-user

Use **dot1x max-user** to set the maximum number of concurrent 802.1X users on a port.

Use **undo dot1x max-user** to restore the default.

Syntax

dot1x max-user *max-number*

undo dot1x max-user

Default

The default is 4294967295.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

context-admin

Parameters

max-number: Sets the maximum number of concurrent 802.1X users on a port. The value range is 1 to 4294967295.

Usage guidelines

Set the maximum number of concurrent 802.1X users on a port to prevent the system resources from being overused. When the maximum number is reached, the port denies subsequent 802.1X users.

Examples

Set the maximum number of concurrent 802.1X users to 32 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x max-user 32
```

dot1x multicast-trigger

Use **dot1x multicast-trigger** to enable the 802.1X multicast trigger feature.

Use **undo dot1x multicast-trigger** to disable the 802.1X multicast trigger feature.

Syntax

dot1x multicast-trigger

undo dot1x multicast-trigger

Default

The 802.1X multicast trigger feature is enabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

The multicast trigger feature enables the device to act as the initiator. The device periodically multicasts EAP-Request/Identity packets out of a port to detect 802.1X clients and trigger authentication. You can use the **dot1x timer tx-period** command to set the interval for sending multicast EAP-Request/Identity packets.

Disable the multicast trigger in a wireless LAN. Wireless clients and the wireless module of the access device can both initiate 802.1X authentication.

Examples

Enable the multicast trigger feature on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x multicast-trigger
```

Related commands

display dot1x

dot1x timer tx-period

dot1x unicast-trigger

dot1x port-control

Use **dot1x port-control** to set the authorization state for the port.

Use **undo dot1x port-control** to restore the default.

Syntax

dot1x port-control { **authorized-force** | **auto** | **unauthorized-force** }

undo dot1x port-control

Default

The default port authorization state is **auto**.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

context-admin

Parameters

authorized-force: Places the port in authorized state, enabling users on the port to access the network without authentication.

auto: Places the port initially in unauthorized state to allow only EAPOL packets to pass, and places the port in authorized state after a user passes authentication. You can use this option in most scenarios.

unauthorized-force: Places the port in unauthorized state, denying any access requests from users on the port.

Usage guidelines

You can use this command to set the port authorization state to determine whether a client is granted access to the network.

Examples

Set the authorization state of GigabitEthernet 1/0/1 to **unauthorized-force**.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x port-control unauthorized-force
```

Related commands

display dot1x

dot1x port-method

Use **dot1x port-method** to specify an access control method for the port.

Use **undo dot1x port-method** to restore the default.

Syntax

dot1x port-method { **macbased** | **portbased** }

undo dot1x port-method

Default

MAC-based access control applies.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

context-admin

Parameters

macbased: Uses MAC-based access control on the port to separately authenticate each user attempting to access the network. Using this method, when an authenticated user logs off, no other online users are affected.

portbased: Uses port-based access control on the port. Using this method, once an 802.1X user passes authentication on the port, any subsequent user can access the network through the port without authentication. When the authenticated user logs off, all other users are logged off.

Usage guidelines

CAUTION:

If online 802.1X users are present on a port, changing its access control method will cause the online users to go offline.

MAC-based access control provides higher security than port-based access control.

Examples

Configure GigabitEthernet 1/0/1 to implement port-based access control.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x port-method portbased
```

Related commands

display dot1x

dot1x quiet-period

Use **dot1x quiet-period** to enable the quiet timer.

Use **undo dot1x quiet-period** to disable the quiet timer.

Syntax

dot1x quiet-period

undo dot1x quiet-period

Default

The quiet timer is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

When a client fails 802.1X authentication, the device must wait a period of time before it can process authentication requests from the client. You can use the **dot1x timer quiet-period** command to set the quiet timer.

Examples

Enable the quiet timer and set the quiet timer to 100 seconds.

```
<Sysname> system-view
[Sysname] dot1x quiet-period
[Sysname] dot1x timer quiet-period 100
```

Related commands

display dot1x

dot1x timer

dot1x re-authenticate

Use **dot1x re-authenticate** to enable the 802.1X periodic reauthentication feature.

Use **undo dot1x re-authenticate** to disable the 802.1X periodic reauthentication feature.

Syntax

dot1x re-authenticate

undo dot1x re-authenticate

Default

The 802.1X periodic reauthentication feature is disabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

Periodic reauthentication enables the access device to periodically authenticate online 802.1X users on a port. This feature tracks the connection status of online users and updates the authorization attributes assigned by the server, such as the ACL and VLAN.

You can use the **dot1x timer reauth-period** command to configure the interval for reauthentication.

Examples

Enable the 802.1X periodic reauthentication feature on GigabitEthernet 1/0/1, and set the periodic reauthentication interval to 1800 seconds.

```
<Sysname> system-view
[Sysname] dot1x timer reauth-period 1800
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x re-authenticate
```

Related commands

display dot1x

dot1x timer

dot1x re-authenticate server-unreachable keep-online

Use **dot1x re-authenticate server-unreachable keep-online** to enable the keep-online feature on a port.

Use **undo dot1x re-authenticate server-unreachable** to restore the default.

Syntax

dot1x re-authenticate server-unreachable keep-online

undo dot1x re-authenticate server-unreachable

Default

The keep-online feature is disabled on a port. The device logs off online 802.1X authenticated users if no server is reachable for 802.1X reauthentication.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

This feature keeps authenticated 802.1X users online when no server is reachable for 802.1X reauthentication.

Examples

Enable the keep-online feature on GigabitEthernet 1/0/1 for 802.1X reauthentication.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x re-authenticate server-unreachable keep-online
```

Related commands

display dot1x

dot1x re-authenticate

dot1x retry

Use **dot1x retry** to set the maximum number of attempts for sending an authentication request to a client.

Use **undo dot1x retry** to restore the default.

Syntax

dot1x retry *retries*

undo dot1x retry

Default

A maximum of two attempts are made to send an authentication request to a client.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

retries: Specifies the maximum number of attempts for sending an authentication request to a client. The value range is 1 to 10.

Usage guidelines

The access device retransmits an authentication request to a client in any of the following situations:

- The device does not receive any responses from the client within the username request timeout interval. The timer is set by using the **dot1x timer tx-period** *tx-period-value* command for the EAP-Request/Identity packet.
- The device does not receive any responses from the client within the client timeout interval. The timer is set by using the **dot1x timer supp-timeout** *supp-timeout-value* command for the EAP-Request/MD5-Challenge packet.

The access device stops retransmitting the request, if it has made the maximum number of request transmission attempts but still received no response.

Examples

Set the maximum number of attempts to 9 for sending an authentication request to a client.

```
<Sysname> system-view
[Sysname] dot1x retry 9
```

Related commands

display dot1x

dot1x timer

dot1x smarton

Use **dot1x smarton** to enable the SmartOn feature on a port.

Use **undo dot1x smarton** to disable the SmartOn feature on a port.

Syntax

dot1x smarton

undo dot1x smarton

Default

The SmartOn feature is disabled on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

When a SmartOn-enabled port receives an EAPOL-Start packet from an 802.1X client, it sends a unicast EAP-Request/Notification packet to the client. The client will respond with an EAP-Response/Notification packet, which contains the SmartOn switch ID and the MD5 digest of the SmartOn password. The device compares the digest in the packet with the digest on the device. If they are the same, the device continues to perform 802.1X authentication for the client. Otherwise, the device denies the client's 802.1X authentication request.

The SmartOn feature and the online user handshake feature are mutually exclusive.

Examples

Enable the SmartOn feature on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x smarton
```

Related commands

display dot1x

dot1x smarton switched

dot1x smarton password

dot1x smarton password

Use **dot1x smarton password** to set a SmartOn password.

Use **undo dot1x smarton password** to restore the default.

Syntax

dot1x smarton password { **cipher** | **simple** } *string*

undo dot1x smarton password

Default

No SmartOn password is set.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

cipher: Specifies a password in encrypted form.

simple: Specifies password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 16 characters. Its encrypted form is a case-sensitive string of 1 to 53 characters

Usage guidelines

The device checks the MD5 digest of the SmartOn password in each received EAP-Response/Notification packet. If the digest is different from the SmartOn password digest on the device, the device stops the 802.1X authentication process for the client that sends this packet.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the SmartOn password to **abc** in plaintext form.

```
<Sysname> system-view
[Sysname] dot1x smarton password simple abc
```

Related commands

display dot1x

dot1x smarton

dot1x smarton switched

dot1x smarton retry

Use **dot1x smarton retry** to set the maximum number of attempts for retransmitting an EAP-Request/Notification packet to a client.

Use **undo dot1x smarton retry** to restore the default.

Syntax

dot1x smarton retry *retries*

undo dot1x smarton retry

Default

A maximum of three attempts are made to retransmit an EAP-Request/Notification packet to a client.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

retries: Specifies the maximum attempts for retransmitting an EAP-Request/Notification packet to a client. The value range is 1 to 10.

Usage guidelines

When the device sends an EAP-Request/Notification packet to the client, the SmartOn client timeout timer (set by using the **dot1x smarton timer supp-timeout** command) starts. If the device does not receive any EAP-Response/Notification packets from the client before the timer expires, it retransmits the EAP-Request/Notification packet to the client. After the device has made the maximum retransmission attempts but received no response, it stops the 802.1X authentication process for the client.

Examples

Set the maximum attempts to 5 for retransmitting an EAP-Request/Notification packet.

```
<Sysname> system-view
[Sysname] dot1x smarton retry 5
```

Related commands

display dot1x

dot1x smarton timer supp-timeout

dot1x smarton switchid

Use **dot1x smarton switchid** to set a SmartOn switch ID.

Use **undo dot1x smarton switchid** to restore the default.

Syntax

dot1x smarton switchid *switch-string*

undo dot1x smarton switchid

Default

No SmartOn switch ID exists.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

switch-string: Specifies the SmartOn switch ID, a case-sensitive string of 1 to 30 characters.

Usage guidelines

The device checks the SmartOn switch ID in each received EAP-Response/Notification packet. If the switch ID is not the same as the switch ID on the device, the device stops the 802.1X authentication process for the client that sends this packet.

Examples

Set the SmartOn switch ID to **abc**.

```
<Sysname> system-view
[Sysname] dot1x smarton switchid abc
```

Related commands

display dot1x

dot1x smarton

dot1x smarton password

dot1x smarton timer supp-timeout

Use **dot1x smarton timer supp-timeout** to set the SmartOn client timeout timer.

Use **undo dot1x smarton timer supp-timeout** to restore the default.

Syntax

dot1x smarton timer supp-timeout *supp-timeout-value*

undo dot1x smarton timer supp-timeout

Default

The SmartOn client timeout timer is 30 seconds.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

supp-timeout-value: Sets the SmartOn client timeout timer in seconds. The value range is 10 to 120.

Usage guidelines

The SmartOn client timeout timer starts when the device sends an EAP-Request/Notification packet to the client. If the device does not receive any EAP-Response/Notification packets from the client within the timer interval, it retransmits the EAP-Request/Notification packet. After the device has made the maximum retransmission attempts but received no response, it stops the 802.1X authentication process for the client. To set the maximum retransmission attempts, use the **dot1x smarton retry** command.

Examples

Set the SmartOn client timeout timer to 20 seconds.

```
<Sysname> system-view
[Sysname] dot1x smarton timer supp-timeout 20
```

Related commands

display dot1x

dot1x smarton retry

dot1x timer

Use **dot1x timer** to set an 802.1X timer.

Use **undo dot1x timer** to restore the default of an 802.1X timer.

Syntax

dot1x timer { **ead-timeout** *ead-timeout-value* | **handshake-period** *handshake-period-value* | **quiet-period** *quiet-period-value* | **reauth-period** *reauth-period-value* | **server-timeout** *server-timeout-value* | **supp-timeout** *supp-timeout-value* | **tx-period** *tx-period-value* }

undo dot1x timer { **ead-timeout** | **handshake-period** | **quiet-period** | **reauth-period** | **server-timeout** | **supp-timeout** | **tx-period** }

Default

The following 802.1X timers apply:

- EAD rule timer: 30 minutes.
- Handshake timer: 15 seconds.
- Quiet timer: 60 seconds.
- Periodic reauthentication timer: 3600 seconds.
- Server timeout timer: 100 seconds.
- Client timeout timer: 30 seconds.
- Username request timeout timer: 30 seconds.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ead-timeout *ead-timeout-value*: Sets the EAD rule timer in minutes. The value range for the *ead-timeout-value* argument is 1 to 1440.

handshake-period *handshake-period-value*: Sets the handshake timer in seconds. The value range for the *handshake-period-value* argument is 5 to 1024.

quiet-period *quiet-period-value*: Sets the quiet timer in seconds. The value range for the *quiet-period-value* argument is 10 to 120.

reauth-period *reauth-period-value*: Sets the periodic reauthentication timer in seconds. The value range for the *reauth-period-value* argument is 60 to 7200.

server-timeout *server-timeout-value*: Sets the server timeout timer in seconds. The value range for the *server-timeout-value* argument is 100 to 300.

supp-timeout *supp-timeout-value*: Sets the client timeout timer in seconds. The value range for the *supp-timeout-value* argument is 1 to 120.

tx-period *tx-period-value*: Sets the username request timeout timer in seconds. The value range for the *tx-period-value* argument is 1 to 120.

Usage guidelines

In most cases, the default settings are sufficient. You can edit the timers, depending on the network conditions.

- In a low-speed network, increase the client timeout timer.
- In a vulnerable network, set the quiet timer to a high value.
- In a high-performance network with quick authentication response, set the quiet timer to a low value.
- In a network with authentication servers of different performance, adjust the server timeout timer.

The network device uses the following 802.1X timers:

- **EAD rule timer (ead-timeout)**—Sets the lifetime of each EAD rule. When the timer expires or the user passes authentication, the rule is removed. If users fail to download the EAD client

or fail to pass authentication within the timer interval, they must reconnect to the network to access the free IP.

- **Handshake timer (`handshake-period`)**—Sets the interval at which the access device sends client handshake requests to check the online status of a client that has passed authentication. If the device does not receive a response after sending the maximum number of handshake requests, it considers that the client has logged off.
- **Quiet timer (`quiet-period`)**—Starts when a client fails authentication. The access device must wait the time period before it can process the authentication attempts from the client.
- **Periodic reauthentication timer (`reauth-period`)**—Sets the interval at which the access device periodically reauthenticates online 802.1X users. To enable 802.1X periodic reauthentication on a port, use the **`dot1x re-authenticate`** command.
- **Server timeout timer (`server-timeout`)**—Starts when the access device sends a RADIUS Access-Request packet to the authentication server. If no response is received when this timer expires, 802.1X authentication fails.
- **Client timeout timer (`supp-timeout`)**—Starts when the access device sends an EAP-Request/MD5-Challenge packet to a client. If no response is received when this timer expires, the access device retransmits the request to the client.
- **Username request timeout timer (`tx-period`)**—Starts when the access device sends an EAP-Request/Identity packet to a client in response to an authentication request. If the device does not receive a response before this timer expires, it retransmits the request. The timer also sets the interval at which the access device sends multicast EAP-Request/Identity packets to detect clients that cannot actively request authentication.

The change to the periodic reauthentication timer applies to the users that have been online only after the old timer expires. Other timer changes take effect immediately on the device.

Examples

Set the server timeout timer to 150 seconds.

```
<Sysname> system-view
[Sysname] dot1x timer server-timeout 150
```

Related commands

`display dot1x`

dot1x unicast-trigger

Use **`dot1x unicast-trigger`** to enable the 802.1X unicast trigger feature.

Use **`undo dot1x unicast-trigger`** to disable the 802.1X unicast trigger feature.

Syntax

`dot1x unicast-trigger`

`undo dot1x unicast-trigger`

Default

The 802.1X unicast trigger feature is disabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

The unicast trigger feature enables the access device to initiate 802.1X authentication when the device receives a data frame from an unknown source MAC address. The device sends a unicast EAP-Request/Identity packet to the unknown source MAC address. It will retransmit the packet if it does not receive any responses within a period of time (set by using the **dot1x timer tx-period** command). This process continues until the maximum number of request attempts (set by using the **dot1x retry** command) is reached.

As a best practice, do not use the unicast trigger on a port that performs port-based access control. If you do so, users on that port might fail to come online.

Examples

Enable the unicast trigger feature on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x unicast-trigger
```

Related commands

display dot1x

dot1x multicast-trigger

dot1x port-method

dot1x retry

dot1x timer

reset dot1x guest-vlan

Use **reset dot1x guest-vlan** to remove users from the 802.1X guest VLAN on a port.

Syntax

reset dot1x guest-vlan interface *interface-type interface-number* [**mac-address** *mac-address*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number.

mac-address *mac-address*: Specifies the MAC address of an 802.1X user in the guest VLAN. If you do not specify this option, the command removes all 802.1X users from the 802.1X guest VLAN on the port.

Examples

Remove the 802.1X user with MAC address 1-1-1 from the 802.1X guest VLAN on GigabitEthernet 1/0/1.

```
<Sysname> reset dot1x guest-vlan interface gigabitethernet 1/0/1 mac-address 1-1-1
```

Related commands

dot1x guest-vlan

reset dot1x statistics

Use **reset dot1x statistics** to clear 802.1X statistics.

Syntax

reset dot1x statistics [**interface** *interface-type interface-number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify a port, this command clears 802.1X statistics on all ports.

Usage guidelines

If you do not specify any parameters, this command clears all 802.1X statistics.

Examples

Clear 802.1X statistics on GigabitEthernet 1/0/1.

```
<Sysname> reset dot1x statistics interface gigabitethernet 1/0/1
```

Related commands

display dot1x

Contents

User identification commands

account-update-interval

Use **account-update-interval** to set the interval for automatic identity user account import.

Use **undo account-update-interval** to restore the default.

Syntax

account-update-interval *interval*

undo account-update-interval

Default

The interval is 24 hours for automatic identity user account import.

Views

Identity user import policy view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies an interval in the range of 1 to 65536 hours.

Usage guidelines

After you enable automatic import for an identity user import policy, the device automatically imports identity user accounts from the servers specified in the policy at the specified interval. Periodic auto-import ensures account consistency between the device and the servers.

Examples

Set the interval for automatic identity user account import to 12 hours for identity user import policy **policy1**.

```
<Sysname> system-view
[Sysname] user-identity user-import-policy policy1
[Sysname-identity-user-impt-policy-policy1] account-update-interval 12
```

Related commands

user-identity user-account auto-import policy

connection-detect

Use **connection-detect** to configure parameters for RESTful server reachability detection.

Use **undo connection-detect** to restore the default.

Syntax

connection-detect { **interval** *interval* | **maximum** *max-times* }

undo connection-detect { **interval** | **maximum** }

Default

The reachability detection interval is 5 minutes and the maximum number of probes per detection is 3.

Views

RESTful server view

Predefined user roles

network-admin

context-admin

Parameters

interval *interval*: Specifies the reachability detection interval, in minutes. The value range for the *interval* argument is 1 to 10.

maximum *max-times*: Specifies the maximum number of probes per detection, in the range of 1 to 5.

Usage guidelines

A smaller reachability detection interval and a larger number of probes provide more accurate detection results but increase the burden of the RESTful server. Considering the network connectivity requirement and the performance of the RESTful server, set reasonable values for the parameters.

Examples

Configure reachability detection parameters for RESTful server **rest1**. Set the reachability detection interval to 2 minutes and the maximum number of probes per detection to 3.

```
<Sysname> system-view
[Sysname] user-identity restful-server rest1
[Sysname-restfulserver-rest1] connection-detect interval 2
[Sysname-restfulserver-rest1] connection-detect maximum 3
```

Related commands

connection-detect enable

display user-identity restful-server

login-name

uri

user-identity restful-server

connection-detect enable

Use **connection-detect enable** to enable RESTful server reachability detection.

Use **undo connection-detect enable** to disable RESTful server reachability detection.

Syntax

connection-detect enable

undo connection-detect enable

Default

RESTful server reachability detection is disabled.

Views

RESTful server view

Predefined user roles

network-admin

context-admin

Usage guidelines

Use this command to detect the reachability of a RESTful server. The detection results can be used as references to define user access control policies for other security modules.

Before you use this command, you must complete the following tasks:

- Specify the username and password used for logging in to the RESTful server by using the **login-name** command.
- Specify a URI for the RESTful server by using the **uri** command.

When RESTful server reachability detection is enabled, the device periodically starts a reachability detection and initiates probes within the detection interval.

- If the device receives a response from the RESTful server, it determines that the server is reachable and stops probe.
- If the device does not receive a response from the RESTful server after the maximum number of probes is reached, it determines that the server is unreachable.

The interval at which the device starts a detection and the maximum number of probes that the device can initiate per detection are set by using the **connection-detect** { **interval** *interval* | **maximum** *max-times* } command.

When RESTful server reachability detection is disabled, the device immediately stops detecting the reachability of the RESTful server.

Examples

Enable reachability detection for RESTful server **rest1**.

```
<Sysname> system-view
[Sysname] user-identity restful-server rest1
[Sysname-restfulserver-rest1] connection-detect enable
```

Related commands

connection-detect

display user-identity restful-server

login-name

uri

user-identity restful-server

display user-identity

Use **display user-identity** to display information about the specified identity users or identity groups.

Syntax

display user-identity { **domain** *domain-name* | **null-domain** } { **user** [*user-name* [**group**]] | **user-group** [*group-name* [**member** { **group** | **user** }]] }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

domain *domain-name*: Specifies an identity domain by its domain name, a case-insensitive string of 1 to 255 characters.

null-domain: Specifies identity users or identity groups that do not belong to any identity domain.

user: Displays identity user information.

user-name: Specifies an identity user by its name, a case-sensitive string of 1 to 55 characters. If you do not specify an identity user, this command displays information about all identity users.

group: Displays information about the identity groups to which the identity user belongs. If you do not specify this keyword, the command does not display identity group information.

user-group: Display identity group information.

group-name: Specifies an identity group by its group name, a case-insensitive string of 1 to 200 characters. If you do not specify an identity group, this command displays information about all identity groups.

member: Displays information about members in the specified identity group. If you do not specify this keyword, the command does not display member information.

group: Specifies identity group members in the specified identity group.

user: Specifies identity user members in the specified identity group.

Usage guidelines

This command displays information about identity users or identity groups, including the information learned from the local user database and information imported from remote servers and .csv files.

Examples

Display information about all identity groups in identity domain **system**.

```
<Sysname> display user-identity domain system user-group
Identity domain: system
  Group ID      Group name
  0x888         abc
  0x123         gp1

Total 2 records matched.
```

Display information about identity group **abc** in identity domain **system**.

```
<Sysname> display user-identity domain system user-group abc
Identity domain: system
  Group ID      Group name
  0x888         abc

Total 1 records matched.
```

Display information about identity user members of identity group **abc** in identity domain **system**.

```
<Sysname> display user-identity domain system user-group abc member user
Identity domain: system
  User ID      Username
  0x234        user1
  0xffffffff   user2
```

```
Total 2 records matched.
```

Display information about identity group members of identity group **abc** in identity domain **system**.

```
<Sysname> display user-identity domain system user-group abc member group
Identity domain: system
  Group ID      Group name
  0x567         group1
  0x111         group2

Total 2 records matched.
```

Display information about all identity users in identity domain **system**.

```
<Sysname> display user-identity domain system user
Identity domain: system
  User ID       Username
  0x234         user1
  0xffffffff    user2

Total 2 records matched.
```

Display information about identity user **user1** in identity domain **system**.

```
<Sysname> display user-identity domain system user user1
Identity domain: system
  User ID       Username
  0x234         user1

Total 1 records matched.
```

Display information about identity groups to which identity user **user1** belongs in identity domain **system**.

```
<Sysname> display user-identity domain system user user1 group
Identity domain: system
  Group ID      Group name
  0x888         abc
  0x123         gp1

Total 2 records matched.
```

Display information about identity users that do not belong to any identity domain.

```
<Sysname> display user-identity null-domain user
  User ID     Username
  0x1         test
  0x3         jj
  0x2         abc

Total 3 records matched.
```

Table 1 Command output

Field	Description
Identity domain	Name of the identity domain to which identity users or identity groups belong.

Field	Description
	This field is not displayed if identity users or identity groups do not belong to any identity domain.
User ID	ID of the identity user.
Username	Name of the identity user.
Group ID	ID of the identity group.
Group name	Name of the identity group.
Total *n* records matched.	Total number of matching identity users or identity groups.

Related commands

reset user-identity user-account

reset user-identity user-group

display user-identity active-user-group

Use **display user-identity active-user-group** to display information about active identity groups.

Syntax

display user-identity active-user-group { **all** | **domain** *domain-name* | **null-domain** }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

all: Specifies all identity domains.

domain *domain-name*: Specifies an identity domain by its domain name, a case-insensitive string of 1 to 255 characters.

null-domain: Specifies active identity groups that do not belong to any identity domain.

Usage guidelines

An identity group is active only when it is used by a security module for network access control.

Examples

Display information about active identity groups in identity domain **system**.

```
<Sysname> display user-identity active-user-group domain system
Identity domain: system
  Group ID      Group name
  0x888         abc
  0x123         gp1
```

```
Total 2 records matched.
```

Table 2 Command output

Field	Description
Identity domain	Name of the identity domain to which active identity groups belong. This field is not displayed if active identity groups do not belong to any identity domain.
Group ID	ID of the active identity group.
Group name	Name of the active identity group.
Total *n* records matched.	Total number of matching active identity groups.

Related commands

`reset user-identity user-group`

display user-identity all

Use **`display user-identity all`** to display information about all identity users or identity groups.

Syntax

`display user-identity all` { **`user`** | **`user-group`** }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

`user`: Specifies identity users.

`user-group`: Specifies identity groups.

Usage guidelines

This command displays information about all identity users or identity groups, including information learned from the local user database and information obtained from remote servers and .csv files.

Examples

Display information about all identity users.

```
<Sysname> display user-identity all user
Identity domain: system
  User ID       Username
  0x121         test1
  0x123         test2
Identity domain: 11
  User ID       Username
```

```
  0x888         test3
  0x899         test4

Total 4 records matched.
```

Table 3 Command output

Field	Description
Identity domain	Name of the identity domain to which identity users belong. This field is not displayed if identity users do not belong to any identity domain.
User ID	ID of the identity user.
Username	Name of the identity user.
Total *n* records matched.	Total number of matching identity users.

Display information about all identity groups.

```
<Sysname> display user-identity all user-group
Identity domain: system
  Group ID      Group name
  0x888         abc
  0x123         gp1
Identity domain: 11
  Group ID      Group name
  0x255         001
  0x256         002

Total 4 records matched.
```

Table 4 Command output

Field	Description
Identity domain	Name of the identity domain to which identity groups belong. This field is not displayed if identity groups do not belong to any identity domain.
Group ID	ID of the identity group.
Group name	Name of the identity group.
Total *n* records matched.	Total number of matching identity groups.

Related commands

`reset user-identity user-account`

`reset user-identity user-group`

display user-identity online-user

Use **`display user-identity online-user`** to display online identity user information.

Syntax

display user-identity online-user { **domain** *domain-name* | **null-domain** } **name** *user-name*

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

domain *domain-name*: Specifies an identity domain by its domain name, a case-insensitive string of 1 to 255 characters.

null-domain: Specifies online identity users that do not belong to any identity domain.

name *user-name*: Specifies an online identity user by its username, a case-sensitive string of 1 to 55 characters. The username cannot contain the domain name.

Usage guidelines

This command displays information about online identity users, including static online identity users and dynamic online identity users.

Examples

Display information about online identity user **user1** in identity domain **system**.

```
<Sysname> display user-identity online-user domain system name user1
User name: user1
  Identity domain: system
  IP  : 199.199.0.15
  MAC : 0001-0002-0003
  Type: Static

Total 1 records matched.
```

Table 5 Command output

Field	Description
User name	Name of the online identity user.
Identity domain	Name of the identity domain to which online identity users belong. This field is not displayed if online identity users do not belong to any identity domain.
IP	IP address of the online identity user. This field is not displayed if the device does not obtain the IP address.
MAC	MAC address of the online identity user. This field is not displayed if the MAC address of the online identity user is not obtained.
Type	Type of the online identity user:

Field	Description
	• Static. • Dynamic.
Total *n* records matched.	Total number of matching online identity users.

Related commands

reset user-identity dynamic-online-user

user-identity static-user

display user-identity restful-server

Use **display user-identity restful-server** to display RESTful server configuration.

Syntax

display user-identity restful-server [*server-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

server-name: Specifies a RESTful server by its server name, a case-insensitive string of 1 to 31 characters. If you do not specify a RESTful server, this command displays configuration information for all RESTful servers.

Examples

Display configuration information for RESTful server **rest1**.

```
<Sysname> display user-identity restful-server rest1
RESTful server name: rest1
  Login name: u1
  Vpn Instance: v1
  Get User URI: http://1.1.1.1:8080/imcrs/ssm/imcuser/accessUser
  Get User Group URI: http://1.1.1.1:8080/imcrs/ssm/imcuser/accessUserGroup
  Get Online User URI: http://1.1.1.1:8080/imcrs/ssm/imcuser/onlineUser
  Put Online User URI: http://1.1.1.1:8080/imcrs/ssm/imcuser/uploadOnlineUser
  Put Offline User URI: http://1.1.1.1:8080/imcrs/ssm/imcuser/uploadOfflineUser
  Connectivity detection: Enabled
    Detection interval: 1 minutes
    Maximum times: 1
  Connectivity status: Reachable
```

Display configuration information for RESTful server **rest2**.

```
<Sysname> display user-identity restful-server rest2
RESTful server name: rest2
  Login name: u2
```

```
Get User URI: http://1.1.1.1:8080/imcrs/uam/acmUser/acmUserList
Get User Group URI: http://1.1.1.1:8080/imcrs/uam/acmUser/userGroup
Get Online User URI: http://1.1.1.1:8080/imcrs/uam/online
Connectivity detection: Enabled
  Detection interval: 1 minutes
  Maximum times: 1
Connectivity status: Reachable
```

Table 6 Command output

Field	Description
Login name	Username used to log in to the RESTful server.
Vpn Instance	MPLS L3VPN instance to which the RESTful server belongs. This field is not displayed if the RESTful server belongs to the public network.
Get User URI	URI used to request user account information.
Get User Group URI	URI used to request user group information.
Get Online User URI	URI used to request online user information.
Put Online User URI	URI used to upload online user information.
Put Offline User URI	URI used to upload offline user information.
Connectivity detection	Whether RESTful server reachability detection is enabled: **Enabled** or **Disabled**.
Detection interval	Interval at which the device detects the reachability of the RESTful server, in minutes.
Maximum times	Maximum number of probes per detection.
Connectivity status	Status of the RESTful server: • Reachable. • Unreachable. This field is not displayed if RESTful server reachability detection is disabled.

Related commands

connection-detect

connection-detect enable

login-name

uri

user-identity restful-server

vpn-instance

display user-identity security-manage-server

Use **display user-identity security-manage-server** to display configuration information for security management server sets.

Syntax

display user-identity security-manage-server [*server-set-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

server-set-name: Specifies a security management server set by its name, a case-insensitive string of 1 to 31 characters. If you do not specify a security management server set, this command displays configuration information for all security management server sets. The system supports only one security management server set.

Examples

Display configuration information for security management server set **sec1**.

```
<Sysname> display user-identity security-manage-server sec1
Security management server set: sec1
  IP addresses: 192.168.0.1,10.113.0.1
  Listening port: 8200
  Encryption algorithm: 3DES

Total 1 records matched
```

Table 7 Command output

Field	Description
Security management server set	Name of the security management server set.
IP addresses	IP addresses of security management servers.
Listening port	Port for listening to security management servers.
Encryption algorithm	Algorithm for encrypting packets exchanged between the device and security management servers.
Total *n* records matched	Number of matched security management server sets.

Related commands

encryption

ip

listen-port

user-identity security-manage-server

display user-identity user-import-policy

Use **display user-identity user-import-policy** to display identity user import policy information.

Syntax

display user-identity user-import-policy [*policy-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

policy-name: Specifies an identity user import policy by its name, a case-insensitive string of 1 to 31 characters. If you do not specify an identity user import policy, this command displays information about all identity user import policies.

Examples

Display information about identity user import policy **policy1**.

```
<Sysname> display user-identity user-import-policy policy1
Policy name: policy1
  Interval time: 24 hours
  RESTful server name:
    ser1
  LDAP import type: All
  LDAP scheme name:
    ldap-scheme

 Total 1 records matched.
```

Table 8 Command output

Field	Description
Policy name	Name of the identity user import policy.
Interval time	Interval for automatic identity user account import, in hours.
RESTful server name	Name of the RESTful server.
LDAP import type	Type of user information imported from LDAP servers: • **All**—User and user group information. • **User**—User information. • **Group**—User group information.
LDAP scheme name	Name of an LDAP scheme.
Total *n* records matched	Total number of matching identity user import policies.

Related commands

import-type

user-identity user-import-policy

encryption

Use **encryption** to configure the encryption algorithm and shared key for securing communication with security management servers.

Use **undo encryption** to restore the default.

Syntax

encryption algorithm { **3des** | **aes128** } **key** { **simple** | **cipher** } *string*

undo encryption algorithm

Default

No encryption algorithm or shared key is configured for securing communication with security management servers.

Views

Security management server set view

Predefined user roles

network-admin

context-admin

Parameters

algorithm: Specifies the encryption algorithm.

3des: Specifies the 3DES algorithm.

aes128: Specifies the AES algorithm that uses a 128-bit key.

key: Specifies the shared key.

cipher: Specifies the key in encrypted form.

simple: Specifies the key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. The key string is case sensitive.

- If the encryption algorithm is 3DES, the plaintext form of the key is a string of 1 to 24 characters. The encrypted form of the key is a string of 1 to 65 characters.
- If the encryption algorithm is AES-128, the plaintext form of the key is a string of 1 to 16 characters. The encrypted form of the key is a string of 1 to 53 characters.

Usage guidelines

For the device to correctly exchange packets with security management servers, make sure the encryption algorithm and shared key are the same as those configured on the servers.

Examples

Configure 3DES as the encryption algorithm and plaintext string **123** as the shared key for securing communication with security management servers in security management sever set **sec1**.

```
<Sysname> system-view
[Sysname] user-identity security-manage-server sec1
[Sysname-identity-sec-manage-server-sec1] encryption algorithm 3des key simple 123
```

Related commands

display user-identity security-manage-server

import-type

Use **import-type** to specify the type of user information to be imported from LDAP servers.

Use **undo import-type** to restore the default.

Syntax

import-type { **all** | **group** | **user** }

undo import-type

Default

The type of user information to be imported from LDAP servers is not specified. The device imports both user information and user group information from LDAP servers.

Views

Identity user import policy view

Predefined user roles

network-admin

context-admin

Parameters

all: Specifies both the user and user group types.

group: Specifies the user group type.

user: Specifies the user type.

Usage guidelines

The device imports only user information of the specified type from LDAP servers.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure the device to import both user information and user group information from LDAP servers.

```
<Sysname> system-view
[Sysname] user-identity user-import-policy policy
[Sysname-identity-user-impt-policy-policy] import-type all
```

Related commands

display user-identity user-import-policy

ip

Use **ip** to specify IP addresses of security management servers.

Use **undo ip** to remove the specified IP addresses of security management servers.

Syntax

ip *ip-address*&<1-10>

undo ip { *ip-address*&<1-10> | **all** }

Default

No IP addresses of security management severs are specified.

Views

Security management server set view

Predefined user roles

network-admin

context-admin

Parameters

ip-address&<1-10>: Specifies a space-separated list of up to 10 IP addresses. The all-zero IP address is not allowed.

all: Specifies all the IP addresses of security management servers.

Usage guidelines

You can specify a maximum of 20 IP addresses of security management servers in a security management server set.

Examples

Specify security management servers at 192.168.0.1 and 10.113.0.1 for security management server set **sec1**.

```
<Sysname> system-view
[Sysname] user-identity security-manage-server sec1
[Sysname-identity-sec-manage-server-sec1] ip 192.168.0.1 10.113.0.1
```

Related commands

display user-identity security-manage-server

ldap-scheme

Use **ldap-scheme** to specify an LDAP scheme.

Use **undo ldap-scheme** to restore the default.

Syntax

ldap-scheme *ldap-scheme-name*

undo ldap-scheme *ldap-scheme-name*

Default

No LDAP schemes are specified.

Views

Identity user import policy view

Predefined user roles

network-admin

context-admin

Parameters

ldap-scheme-name: Specifies an LDAP scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

To import identity user account information from the LDAP server specified in the LDAP scheme, use the **user-identity user-account import policy** command. The device cannot import online identity user information from the LDAP server.

You can specify a maximum of 16 LDAP schemes in an identity user import policy for importing users from multiple LDAP servers in batch.

Examples

Specify LDAP scheme **ser2** for identity user import policy **policy1**.

```
<Sysname> system-view
[Sysname] user-identity user-import-policy policy1
[Sysname-identity-user-impt-policy-policy1] ldap-scheme ser2
```

Related commands

display user-identity user-import-policy

ldap scheme

listen-port

Use **listen-port** to set the port number for listening to security management servers.

Use **undo listen-port** to restore the default.

Syntax

listen-port *port-num*

undo listen-port

Default

The device listens to security management servers on port 8001.

Views

Security management server set view

Predefined user roles

network-admin

context-admin

Parameters

port-num: Specifies the UDP port number for listening to security management servers, in the range of 1 to 65535.

Usage guidelines

For the device to establish connections with security management servers, make sure the listening port is the same as the port that the servers use to send online user information.

Examples

Set the port to 8048 for listening to security management servers in security management server set **sec1**.

```
<Sysname> system-view
[Sysname] user-identity security-manage-server sec1
[Sysname-identity-sec-manage-server-sec1] listen-port 8084
```

Related commands

display user-identity security-manage-server

login-name

Use **login-name** to specify the username and password used for logging in to the RESTful server.

Use **undo login-name** to restore the default.

Syntax

login-name *user-name* **password** { **cipher** | **simple** } *string*

undo login-name

Default

No username or password is specified for logging in to the RESTful server.

Views

RESTful server view

Predefined user roles

network-admin

context-admin

Parameters

user-name: Specifies a username, a case-sensitive string of 1 to 55 characters.

password: Specifies a password.

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 63 characters. Its encrypted form is a case-sensitive string of 1 to 117 characters.

Usage guidelines

The device uses the specified username and password to establish a connection with the RESTful server. If the device is authenticated as legitimate, the RESTful server permits the connection request of the device. Then, the device can request resources on the server.

The specified username and password must exist on the RESTful server.

Examples

Configure the device to use username **abc** and plaintext password **123** to log in to the RESTful server.

```
<Sysname> system-view
[Sysname] user-identity restful-server rest1
[Sysname-restfulserver-rest1] login-name abc password simple 123
```

Related commands

display user-identity restful-server

user-identity restful-server

reset user-identity dynamic-online-user

Use **reset user-identity dynamic-online-user** to delete dynamic online identity users.

Syntax

reset user-identity dynamic-online-user { **all** | { **domain** *domain-name* | **null-domain** } [**name** *user-name*] | { { **ip** *ipv4-address* | **ipv6** *ipv6-address* } | **mac** *mac-address* } * }

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

all: Specifies all dynamic online identity users.

domain *domain-name*: Specifies an identity domain by its domain name, a case-insensitive string of 1 to 255 characters.

null-domain: Specifies dynamic online identity users that do not belong to any identity domain.

name *user-name*: Specifies a dynamic online identity user by its username, a case-sensitive string of 1 to 55 characters. If you do not specify this option, the command deletes dynamic online identity users that belong to the specified domain or that do not belong to any domain.

ip *ipv4-address*: Specifies the IPv4 address of a dynamic online identity user.

ipv6 *ipv6-address*: Specifies the IPv6 address of a dynamic online identity user.

mac *mac-address*: Specifies the MAC address of a dynamic online identity user, in the format H-H-H. If you do not specify a MAC address, this command deletes dynamic online identity users that have the specified username regardless of their MAC addresses.

Usage guidelines

This command deletes dynamic online identity users created based on user information obtained from remote servers and it cannot delete static online identity users. To delete static online identity users, use the **undo user-identity static-user** command.

Examples

Delete all dynamic online identity users.

```
<Sysname> reset user-identity dynamic-online-user all
```

Delete dynamic online identity users in identity domain **abc**.

```
<Sysname> reset user-identity dynamic-online-user domain abc
```

Delete dynamic online identity user **user1** in identity domain **dom1**.

```
<Sysname> reset user-identity dynamic-online-user domain dom1 name user1
```

Delete dynamic online identity users that use username **user2** and do not belong to any identity domain.

```
<Sysname> reset user-identity dynamic-online-user null-domain name user2
```

Delete the dynamic online identity user whose IP address is 1.2.3.4.

```
<Sysname> reset user-identity dynamic-online-user ip 1.2.3.4
```

Delete the dynamic online identity user whose IP address is 1.2.3.4 and MAC address is 2222-3333-4444.

```
<Sysname> reset user-identity dynamic-online-user ip 1.2.3.4 mac 2222-3333-4444
```

Delete the dynamic online identity user whose MAC address is 2222-3333-4444.

```
<Sysname> reset user-identity dynamic-online-user mac 2222-3333-4444
```

Related commands

display user-identity online-user

reset user-identity user-account

Use **reset user-identity user-account** to delete identity user accounts.

Syntax

reset user-identity user-account { **all** | { **domain** *domain-name* | **null-domain** } [**name** *user-name*] }

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

all: Specifies all identity user accounts.

domain *domain-name*: Specifies an identity domain by its domain name, a case-insensitive string of 1 to 255 characters.

null-domain: Specifies identity user accounts that do not belong to any identity domain.

name *user-name*: Specifies an identity user account by its name, a case-sensitive string of 1 to 55 characters. If you do not specify an identity user account, this command deletes identity user accounts that belong to the specified domain or that do not belong to any domain.

Usage guidelines

This command deletes identity user accounts created based on the information obtained from remote servers and .csv files. It cannot delete identity user accounts learned from the local user database.

Examples

Delete all identity user accounts.

```
<Sysname> reset user-identity user-account all
```

Delete identity user account **test** in identity domain **dom1**.

```
<Sysname> reset user-identity user-account domain dom1 name test
```

Related commands

display user-identity all user

reset user-identity user-group

Use **reset user-identity user-group** to delete identity groups.

Syntax

reset user-identity user-group { **all** | { **domain** *domain-name* | **null-domain** } [**name** *group-name*] }

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

all: Specifies all identity groups.

domain *domain-name*: Specifies an identity domain by its domain name, a case-insensitive string of 1 to 255 characters.

null-domain: Specifies identity groups that do not belong to any identity domain.

name *group-name*: Specifies an identity group by its group name, a case-insensitive string of 1 to 200 characters. If you do not specify an identity group, this command deletes identity groups that belong to the specified domain or that do not belong to any domain.

Usage guidelines

Use this command to delete identity groups created based on user group information obtained from remote servers and .csv files and it cannot delete identity groups learned from the local user database.

Examples

Delete all identity groups.

```
<Sysname> reset user-identity user-group all
```

Delete identity group **g1** in identity domain **dom1**.

```
<Sysname> reset user-identity user-group domain dom1 name g1
```

Related commands

display user-identity all user-group

restful-server

Use **restful-server** to specify a RESTful server.

Use **undo restful-server** to restore the default.

Syntax

restful-server *server-name*

undo restful-server *server-name*

Default

No RESTful server is specified.

Views

Identity user import policy view

Predefined user roles

network-admin

context-admin

Parameters

server-name: Specifies a RESTful server by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

To import identity user accounts from the RESTful server, use the **user-identity user-account import policy** command. To import online identity user information from the RESTful server, use the **user-identity online-user import policy** command.

You can specify only one RESTful server. To specify a new RESTful server, first remove the currently specified RESTful server by using the **undo restful-server** command.

Examples

Specify RESTful server **ser1** for identity user import policy **policy1**.

```
<Sysname> system-view
[Sysname] user-identity user-import-policy policy1
[Sysname-identity-user-impt-policy-policy1] restful-server ser1
```

Related commands

display user-identity restful-server

display user-identity user-import-policy

user-identity restful-server

uri

Use **uri** to specify a URI for the RESTful server.

Use **undo uri** to delete a URI specified for the RESTful server.

Syntax

uri { **get-online-user** | **get-user-database** | **get-user-group-database** | **put-offline-user** | **put-online-user** } *uri-string*

undo uri { **get-online-user** | **get-user-database** | **get-user-group-database** | **put-offline-user** | **put-online-user** }

Default

No URIs are specified for the RESTful server.

Views

RESTful server view

Predefined user roles

network-admin

context-admin

Parameters

get-online-user: Specifies the URI used to request online network access user information.

get-user-database: Specifies the URI used to request network access user account information.

get-user-group-database: Specifies the URI used to request user group information.

put-offline-user: Specifies the URI used to upload offline user information.

put-online-user: Specifies the URI used to upload online user information.

uri-string: Specifies a URI, a case-insensitive string of 1 to 255 characters.

Usage guidelines

The specified URIs must be the same as those provided by the RESTful server. Otherwise, user information interaction will fail.

If the device adds or deletes an identity user that is not imported from the RESTful server, the device uploads the online or offline user information to the RESTful server.

You can repeat this command to specify multiple URIs for the RESTful server.

Examples

Specify **http://1.1.1.1:8080/imcrs/ssm/imcuser/onlineUser** as the URI used to request online network access user information from RESTful server **rest1**.

```
<Sysname> system-view
[Sysname] user-identity restful-server rest1
[Sysname-restfulserver-rest1] uri get-online-user
http://1.1.1.1:8080/imcrs/ssm/imcuser/onlineUser
```

Specify **http://1.1.1.1:8080/imcrs/ssm/imcuser/accessUser** as the URI used to request network access user account information from RESTful server **rest1**.

```
<Sysname> system-view
[Sysname] user-identity restful-server rest1
[Sysname-restfulserver-rest1] uri get-user-database
http://1.1.1.1:8080/imcrs/ssm/imcuser/accessUser
```

Specify **http://1.1.1.1:8080/imcrs/ssm/imcuser/accessUserGroup** as the URI used to request user group information from RESTful server **rest1**.

```
<Sysname> system-view
[Sysname] user-identity restful-server rest1
[Sysname-restfulserver-rest1] uri get-user-group-database
http://1.1.1.1:8080/imcrs/ssm/imcuser/accessUserGroup
```

Specify **http://1.1.1.1:8080/imcrs/ssm/imcuser/uploadOfflineUser** as the URI used to upload offline user information to RESTful server **rest1**.

```
<Sysname> system-view
[Sysname] user-identity restful-server rest1
[Sysname-restfulserver-rest1] uri put-offline-user
http://1.1.1.1:8080/imcrs/ssm/imcuser/uploadOfflineUser
```

Specify **http://1.1.1.1:8080/imcrs/ssm/imcuser/uploadOnlineUser** as the URI used to upload online user information to RESTful server **rest1**.

```
<Sysname> system-view
[Sysname] user-identity restful-server rest1
[Sysname-restfulserver-rest1] uri put-online-user
http://1.1.1.1:8080/imcrs/ssm/imcuser/uploadOnlineUser
```

Specify **http://1.1.1.1:8080/imcrs/uam/online** as the URI used to request online network access user information from the EIA component of RESTful server **rest2**.

```
<Sysname> system-view
[Sysname] user-identity restful-server rest2
[Sysname-restfulserver-rest1] uri get-online-user http://1.1.1.1:8080/imcrs/uam/online
```

Specify **http://1.1.1.1:8080/imcrs/uam/acmUser/acmUserList** as the URI used to request network access user account information from the EIA component of RESTful server **rest2**.

```
<Sysname> system-view
[Sysname] user-identity restful-server rest2
[Sysname-restfulserver-rest1] uri get-user-database http://
1.1.1.1:8080/imcrs/uam/acmUser/acmUserList
```

Specify **http://1.1.1.1:8080/imcrs/uam/acmUser/userGroup** as the URI used to request user group information from the EIA component of RESTful server **rest2**.

```
<Sysname> system-view
[Sysname] user-identity restful-server rest2
[Sysname-restfulserver-rest1] uri get-user-group-database http://
1.1.1.1:8080/imcrs/uam/acmUser/userGroup
```

Related commands

display user-identity restful-server

user-identity restful-server

user-identity enable

Use **user-identity enable** to enable the user identification feature.

Use **undo user-identity enable** to disable the user identification feature.

Syntax

user-identity enable

undo user-identity enable

Default

The user identification feature is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

With the user identification feature, the device learns online user information from the user access modules. The device uses the obtained information for user identification and works with other security features for identity-based network access control.

Examples

Enable the user identification feature.

```
<Sysname> system-view
[Sysname] user-identity enable
```

user-identity online-user import policy

Use **user-identity online-user import policy** to import online identity users from a server.

Syntax

user-identity online-user import policy *policy-name*

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies an identity user import policy by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

After this command is executed, the device initiates a connection request to the server specified in the identity user import policy. Then, the device imports online network access user information from the server. The information includes the username, identity domain name, user group name, IP address, and MAC address of the users.

Before you execute this command, make sure the user identification feature is enabled.

Examples

Import online identity users from the server specified in identity user import policy **policy1**.

```
<Sysname> system-view
[Sysname] user-identity online-user import policy policy1
Loading...Done.
```

Related commands

user-identity user-account auto-import policy

user-identity user-import-policy

user-identity online-user-name-match

Use **user-identity online-user-name-match** to specify username match mode for user identification.

Use **undo user-identity online-user-name-match** to restore the default.

Syntax

user-identity online-user-name-match { **keep-original** | **with-domain** | **without-domain** }

undo user-identity online-user-name-match

Default

The username match mode for user identification is **keep-original**.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

keep-original: Uses the username entered by a user to perform username match. For example, if the authentication domain is **abc** and the entered username is **test@123**, the device searches username **test@123** in local user accounts.

with-domain: Uses the username that includes the authentication domain name of a user to perform username match. For example, if the authentication domain is **abc** and the entered username is **test@123**, the device searches username **test@abc** in local user accounts.

without-domain: Uses the username that excludes the domain name of a user to perform username match. For example, if the authentication domain is **abc** and the entered username is **test@123**, the device searches username **test** in local user accounts that do not join any identity domains.

Usage guidelines

This command specifies the username match mode for user identification. The device creates online identity users only for online users whose usernames can match the usernames in the local identity user accounts.

This command takes effect only on online identity users that access the current device.

Examples

Specify **with-domain** as the username match mode for user identification.

```
<Sysname> system-view
[Sysname] user-identity online-user-name-match with-domain
```

user-identity restful-server

Use **user-identity restful-server** to create a RESTful server and enter its view, or enter the view of an existing RESTful server.

Use **undo user-identity restful-server** to delete a RESTful server.

Syntax

user-identity restful-server *server-name*

undo user-identity restful-server *server-name*

Default

No RESTful server exists.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

server-name: Specifies the name of a RESTful server. The RESTful server name is a case-insensitive string of 1 to 31 characters.

Usage guidelines

You can configure parameters of the RESTful server in RESTful server view. The parameters include the URIs of the server and the login account.

You can create only one RESTful server.

Examples

Create a RESTful server named **rest1** and enter its view.

```
<Sysname> system-view
[Sysname] user-identity restful-server rest1
[Sysname-restfulserver-rest1]
```

Related commands

display user-identity restful-server

login-name

uri

user-identity user-import-policy

user-identity security-manage-server

Use **user-identity security-manage-server** to create a security management server set and enter its view, or enter the view of an existing security management server set.

Use **undo user-identity security-manage-server** to delete a security management server set.

Syntax

user-identity security-manage-server *server-set-name*

undo user-identity security-manage-server *server-set-name*

Default

No security management server set exists.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

server-set-name: Specifies the name of the security management server set, a case-insensitive string of 1 to 31 characters.

Usage guidelines

The security management server set view defines the related parameters of security management servers. The parameters include the IP addresses of the servers, the port number for listening to the servers, and the shared key to secure communication between the device and the servers.

You can create only one security management server set.

Examples

Create a security management server set named **sec1** and enter its view.

```
<Sysname> system-view
[Sysname] user-identity security-manage-server sec
[Sysname-identity-sec-manage-server-sec1]
```

Related commands

display user-identity security-manage-server

encryption

ip

listen-port

user-identity static-user

Use **user-identity static-user** to configure a static identity user.

Use **undo user-identity static-user** to delete a static identity user.

Syntax

user-identity static-user *user-name* [**domain** *domain-name*] **bind** { **ipv4** *ipv4-address* | **ipv6** *ipv6-address* } | **mac** *mac-address* } *

undo user-identity static-user *user-name* [**domain** *domain-name*] [**bind** { { **ipv4** *ipv4-address* | **ipv6** *ipv6-address* } | **mac** *mac-address* } *]

Default

No static identity users exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

user-name: Specifies the name of the static identity user, a case-sensitive string of 1 to 55 characters.

domain *domain-name*: Specifies the identity domain to which the static identity user belongs. The *domain-name* argument represents an identity domain name, a case-insensitive string of 1 to 255 characters. If you do not specify an identity domain, the static identity user does not belong to any identity domain.

bind: Specifies address attributes bound to the static identity user.

ipv4 *ipv4-address*: Specifies an IPv4 address. The IPv4 address cannot be an all-zero address, all-one address, or multicast address.

ipv6 *ipv6-address*: Specifies an IPv6 address. The IPv6 address cannot be an all-zero address, multicast address, loopback address, or link local address.

mac *mac-address*: Specifies a MAC address in the format of H-H-H. If you do not specify a MAC address, the static identity user can use any MAC address.

Usage guidelines

To allow users to access the network without identity authentication and to use security features to control their access to the network, configure the users as static identity users.

If you do not specify the **bind** keyword in the **undo** form of this command, all static identity users that use the specified username are deleted.

Execute this command multiple times to add multiple static identity users.

You can bind one username with multiple IP addresses, multiple MAC addresses, or multiple IP-MAC address combinations. You cannot bind one IP address, one MAC address, or one IP-MAC address combination with multiple usernames.

Only when the user identification feature is enabled and static identity users match local identity user accounts, the device can generate corresponding static online identity user entries.

Examples

Configure a static identity user of which the username is **test**, the identity domain is **dom1**, and the IP address is 109.15.0.15.

```
<Sysname> system-view
[Sysname] user-identity static-user test domain dom1 bind ipv4 109.15.0.15
```

Configure a static identity user of which the username is **abc**, the identity domain is **dom1**, and the MAC address is 1-1-1.

```
<Sysname> system-view
[Sysname] user-identity static-user abc domain dom1 bind mac 1-1-1
```

Related commands

display user-identity online-user

user-identity enable

user-identity user-account auto-import policy

Use **user-identity user-account auto-import policy** to enable automatic identity user account import.

Use **undo user-identity user-account auto-import policy** to disable automatic identity user account import.

Syntax

user-identity user-account auto-import policy *policy-name*

undo user-identity user-account auto-import policy *policy-name*

Default

Automatic identity user account import is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies an identity user import policy by its policy name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

After this feature is enabled, the device first imports all identity user accounts and online identity user information from the servers specified in the identity user import policy. Then, the device periodically imports identity user accounts from the servers at the interval set by the **account-update-interval** command.

For this feature to take effect, make sure the user identification feature is enabled. To enable the user identification feature, use the **user-identity enable** command.

Examples

Enable automatic identity user account import for identity user import policy **policy1**.

```
<Sysname> system-view
[Sysname] user-identity user-account auto-import policy policy1
```

Related commands

account-update-interval

user-identity user-import-policy

user-identity user-account export url

Use **user-identity user-account export url** to export identity user accounts to a .csv file.

Syntax

user-identity user-account export url *url-string* [{ **domain** *domain-name* | **null-domain** } [**user** *user-name*] | **template**] [**vpn-instance** *vpn-instance-name*]

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

url-string: Specifies a URL, a case-insensitive string of 1 to 255 characters.

domain *domain-name*: Specifies an identity domain by its domain name, a case-insensitive string of 1 to 255 characters.

null-domain: Specifies identity user accounts that do not belong to any identity domain.

user *user-name*: Specifies an identity user account by its account name, a case-sensitive string of 1 to 55 characters. If you do not specify an identity user account, this command exports all identity user accounts.

template: Exports a standard .csv file template. You can use this file template as a reference when editing .csv files.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance where the .csv file will be saved. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the .csv file will be saved on the public network, do not specify this option.

Usage guidelines

You must save the exported identity user account information to a .csv file.

If you do not specify any parameters, the device exports all identity user account information to a .csv file.

The device supports TFTP and FTP file transfer modes. Table 9 describes the valid URL formats of the .csv file.

Table 9 URL formats

Protocol	URL format	Description
TFTP	**tftp://***server*/*path*/*filename*	Specify a TFTP server by IP address or hostname. For example, specify the file path as **tftp://1.1.1.1/user/user.csv**.
FTP	• With FTP username and password: **ftp://***username*:*password*@*server*/*path*/*filename* • Without FTP username and password: **ftp://***server*/*path*/*filename*	Specify an FTP server by IP address or hostname. The device ignores the domain name in the FTP username. For example, specify the file path as **ftp://1:1@1.1.1.1/user/user.csv** or **ftp://1.1.1.1/user/user.csv**.

For identity user account information to be correctly exported by using FTP, follow the input formats in Table 10 when you use special characters in the URL.

Table 10 Input formats for special characters

Special character	Input format
\	\\
"	\"
/	%2F
:	%3A
@	%40

If this command is successfully executed, a .csv file with the specified file name will be created on the specified server. If you execute this command with the same parameters multiple times, the new file will override the old file.

Examples

Export all identity user accounts in identity domain **dom1** to a .csv file and save the file to the path **tftp://1.1.1.1/user.csv**.

```
<Sysname> system-view
[Sysname] user-identity user-account export url tftp://1.1.1.1/user.csv domain dom1
```

Related commands

user-identity user-account import url

user-identity user-account import policy

Use **user-identity user-account import policy** to import identity user accounts from servers.

Syntax

user-identity user-account import policy *policy-name*

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies an identity user import policy by its policy name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

After you execute this command, the device initiates an identity user account information request to the servers specified in the identity user import policy. Then, the device imports identity user account information from the servers.

Examples

Import identity user accounts from the servers specified in identity user import policy **policy1**.

```
<Sysname> system-view
[Sysname] user-identity user-account import policy policy1
```

Related commands

user-identity user-import-policy

user-identity user-account import url

Use **user-identity user-account import url** to import identity user accounts from a .csv file.

Syntax

user-identity user-account import url *url-string* [**vpn-instance** *vpn-instance-name*] [**auto-create-group** | **override** | **start-line** *line-number*] *

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

url-string: Specifies the URL of the .csv file. The URL is a case-insensitive string of 1 to 255 characters.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance where the .csv file will be saved. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the .csv file will be saved on the public network, do not specify this option.

auto-create-group: Enables the device to automatically create an identity group for an account if the identity group to which the account belongs does not exist on the device. If you do not specify this keyword, the device does not create nonexistent identity groups.

override: Enables the device to override the existing identity user account with the same name as an identity user account to be imported. If you do not specify this keyword, the device retains the existing identity user account.

start-line *line-number*: Specifies the number of the line at which the account import begins. If you do not specify this option, the command imports identity user account information from the first line.

Usage guidelines

The file from which identity user accounts are imported must be a .csv file.

You can use the **user-identity user-account export url** command to export a standard .csv file template.

Examples

Import identity user accounts from the second line of the **user.csv** file in path **ftp://1.1.1.1/newpath**.

```
<Sysname> system-view
[Sysname] user-identity user-account import url ftp://1.1.1.1/newpath/user.csv
start-line 2
```

Related commands

user-identity user-account export url

user-identity user-import-policy

Use **user-identity user-import-policy** to create an identity user import policy and enter its view, or enter the view of an existing identity user import policy.

Use **undo user-identity user-import-policy** to delete an identity user import policy.

Syntax

user-identity user-import-policy *policy-name*

undo user-identity user-import-policy *policy-name*

Default

No identity user import policy exists.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies an identity user import policy by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

An identity user import policy determines the policy that the user identification feature uses to import identity user information from servers. The imported user information includes information about identity user accounts and online identity users. Supported servers include IMC servers and LDAP servers.

You can create only one identity user import policy. Before you create a new identity user import policy, first delete the existing identity user import policy by using the **undo** form of this command.

Examples

Create an identity user import policy named **policy1** and enter its view.

```
<Sysname> system-view
[Sysname] user-identity user-import-policy policy1
[Sysname-identity-user-impt-policy-policy1]
```

Related commands

display user-identity user-import-policy

vpn-instance

Use **vpn-instance** to specify an MPLS L3VPN instance for a RESTful server.

Use **undo vpn-instance** to restore the default.

Syntax

vpn-instance *vpn-instance-name*

undo vpn-instance

Default

The RESTful server belongs to the public network.

Views

RESTful server view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance-name: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

Use this command to specify the VPN instance of the interfaces that the device and the RESTful server use to communicate with each other.

Examples

Specify VPN instance **v1** for RESTful server **r1**.

```
<Sysname> system-view
[Sysname] user-identity restful-server r1
[Sysname-restfulserver-r1] vpn-instance v1
```

Related commands

display user-identity restful-server

user-identity restful-server

Contents

Password control commands

display password-control

Use **display password-control** to display password control configuration.

Syntax

display password-control [**super**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

super: Displays the password control information for the super passwords. If you do not specify this keyword, the command displays the global password control configuration.

Examples

Display the global password control configuration.

```
<Sysname> display password-control
 Global password control configurations:
 Password control:                     Enabled (device management users)
                                       Enabled (network access users)
 Password aging:                       Enabled (90 days)
 Password length:                      Enabled (10 characters)
 Password composition:                 Enabled (1 types, 1 characters per type)
 Password history:                     Enabled (max history records:4)
 Early notice on password expiration:  7 days
 Maximum login attempts:               3
 Action for exceeding login attempts:  Lock user for 1 minutes
 Password history was last reset:      0 days ago (device management users)
                                       0 days ago (network access users)
 Minimum interval between two updates: 24 hours
 User account idle time:               90 days
 Logins with aged password:            3 times in 30 days
 Password complexity:                  Disabled (username checking)
                                       Disabled (repeated characters checking)
 Password change:                      Enabled (first login)
                                       Enabled (mandatory weak password change)
User information in blacklist:        Username-only
```

Display the password control configuration for super passwords.

```
<Sysname> display password-control super
 Super password control configurations:
```

```
Password aging:                    Enabled (90 days)
Password length:                   Enabled (10 characters)
Password composition:              Enabled (1 types, 1 characters per type)
```

Table 1 Command output

Field	Description
Password control	Whether the password control feature is enabled for device management users or network access users.
Password aging	Whether password expiration is enabled and, if enabled, the aging time.
Password length	Whether the minimum password length restriction feature is enabled and, if enabled, the setting.
Password composition	Whether the password composition restriction feature is enabled and, if enabled, the settings.
Password history	Whether the password history management feature is enabled and, if enabled, the setting.
Early notice on password expiration	Number of days during which the user is notified of the pending password expiration.
Maximum login attempts	Allowed maximum number of consecutive failed login attempts for FTP and VTY users.
Action for exceeding login attempts	Action to be taken after a user fails to log in after the specified number of attempts.
Password history was last reset	Last time when the password history records of the device management or network access users were deleted.
Minimum interval between two updates	Minimum password update interval.
Logins with aged password	Number of times and maximum number of days a user can log in using an expired password.
Password complexity	Whether the following password complexity checking is enabled: • **username checking**—Checks whether a password contains the username or the reverse of the username. • **repeated characters checking**—Checks whether a password contains any character that appears consecutively three or more times.
Password change	Status of the password change at first login feature: • Enabled (first login). • Disabled (first login). • Enabled (mandatory weak password change). • Disabled (mandatory weak password change).
User information in blacklist	User information items added to the password control blacklist: • **Username-only**—Only usernames are added to the password control blacklist. • **Username and IP**—Both usernames and IP addresses are added to the password control blacklist.

display password-control blacklist

Use **`display password-control blacklist`** to display password control blacklist information.

Syntax

display password-control blacklist [**user-name** *user-name* | **ip** *ipv4-address* | **ipv6** *ipv6-address*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

user-name *user-name*: Specifies a user by its username, a string of 1 to 55 characters. You can specify a pure username or specify a pure username and its domain name in the format of *pure usernname@domain name*. The pure username is case sensitive. The domain name is case-insensitive.

ipv6 *ipv6-address*: Specifies the IPv6 address of a user.

Usage guidelines

If you do not specify any parameters, this command displays the maximum number of blacklist entries for a user account, the total number of blacklisted users, and detailed information about the blacklisted users.

When the console users fail login, only their user accounts can be added to the password control blacklist because the system is unable to obtain the IP addresses of these users. When FTP, Web, or virtual terminal line (VTY) users fail login, both their IP addresses and user accounts can be added to the password control blacklist. The user information items specified by the **password-control blacklist user-info** command will be added to the password control blacklist.

The device will create a blacklist entry for each IP address for a user account when the following conditions are both met:

- Both usernames and IP addresses are added to the password control blacklist.
- A user uses the same user account to log in to the device from different IP addresses and fails the logins.

When the maximum number of blacklist entries for the user account is reached, a blacklist entry for a new IP address of the user account will overwrite the earliest blacklist entry for the user account.

Examples

Display password control blacklist where only usernames are added.

```
<Sysname> display password-control blacklist
 Per-user blacklist limit: 32.
 Blacklist items matched: 1.
 Username                    Login failures     Lock flag
 con                         2                  unlock
 abcd                        4                  lock
 admin                       1                  unlock
```

Display password control blacklist where both usernames and IP addresses are added.

```
<Sysname> display password-control blacklist
 Per-user blacklist limit: 100.
 Blacklist items matched: 2.
```

```
Username                    IP address          Login failures   Lock flag
abcd                        169::168:34:1       4                lock
admin                       192.168.34.1        1                unlock
```

Table 2 Command output

Field	Description
Per-user blacklist limit	Maximum number of blacklist entries for a user account.
Blacklist items matched	Number of blacklisted users.
IP address	IP address of the user. This field displays hyphens (**-**) for users that log in to the device through console ports. This field is not available if the password control blacklist contains only usernames.
Login failures	Number of login failures.
Lock flag	Whether the user account is locked for the user: • **unlock**—Not locked. • **lock**—Locked temporarily or permanently, depending on the **password-control login-attempt** command.

password-control { aging | composition | history | length } enable

Use **password-control** { **aging** | **composition** | **history** | **length** } **enable** to enable a password restriction feature.

Use **undo password-control** { **aging** | **composition** | **history** | **length** } **enable** to disable a password restriction feature.

Syntax

password-control { **aging** | **composition** | **history** | **length** } **enable**

undo password-control { **aging** | **composition** | **history** | **length** } **enable**

Default

The password restriction features are all enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

aging: Enables the password expiration feature.

composition: Enables the password composition restriction feature.

history: Enables the password history management feature.

length: Enables the minimum password length restriction feature.

Usage guidelines

The password expiration feature or the password history management feature takes effect only after the global password control feature is also enabled.

The password composition restriction and the minimum password length restriction are enabled by default regardless of whether or not the global password control feature is enabled. By default, a password must contain a minimum of four different characters.

If a password of a device management user is in hashed form, a restriction setting does not take effect for the password even when the following requirements are met:

- The global password control is enabled.
- The specific password restriction feature is enabled.

For more information about configuring a password for a device management user, see "AAA commands."

If the password history management is disabled, the system will not compare the new password with history passwords, but the system will not stop recording history passwords. When the number of history password records of a user reaches the maximum number set by the **password-control history** command, the newest history record overwrites the earliest one.

Examples

Enable the password control feature globally.

```
<Sysname> system-view
[Sysname] password-control enable
```

Enable the password composition restriction feature.

```
[Sysname] password-control composition enable
```

Enable the password expiration feature.

```
[Sysname] password-control aging enable
```

Enable the minimum password length restriction feature.

```
[Sysname] password-control length enable
```

Enable the password history management feature.

```
[Sysname] password-control history enable
```

Related commands

display password-control

password-control enable

password-control aging

Use **password-control aging** to set the password aging time.

Use **undo password-control aging** to restore the default.

Syntax

password-control aging *aging-time*

undo password-control aging

Default

A password expires after 90 days. The password aging time for a user group equals the global setting. The password aging time for a local user equals that of the user group to which the local user belongs.

Views

System view

User group view

Local user view

Predefined user roles

network-admin

context-admin

Parameters

aging-time: Specifies the password aging time in days, in the range of 1 to 365.

Usage guidelines

The aging time depends on the view:

- The time in system view has global significance and applies to all user groups.
- The time in user group view applies to all local users in the user group.
- The time in local user view applies only to the local user.

A password aging time with a smaller application scope has higher priority. The system prefers to use the password aging time in local user view for a local user.

- If no password aging time is configured for the local user, the system uses the password aging time for the user group to which the local user belongs.
- If no password aging time is configured for the user group, the system uses the global password aging time.

Examples

Globally set the passwords to expire after 80 days.

```
<Sysname> system-view
[Sysname] password-control aging 80
```

Set the passwords for user group **test** to expire after 90 days.

```
[Sysname] user-group test
[Sysname-ugroup-test] password-control aging 90
[Sysname-ugroup-test] quit
```

Set the password for device management user **abc** to expire after 100 days.

```
[Sysname] local-user abc class manage
[Sysname-luser-manage-abc] password-control aging 100
```

Related commands

display local-user

display password-control

display user-group

password-control aging enable

password-control alert-before-expire

Use **password-control alert-before-expire** to set the number of days before a user's password expires during which the user is notified of the pending password expiration.

Use **undo password-control alert-before-expire** to restore the default.

Syntax

password-control alert-before-expire *alert-time*

undo password-control alert-before-expire

Default

The default is 7 days.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

alert-time: Specifies the number of days before a user password expires during which the user is notified of the pending password expiration. The value range is 1 to 30.

Usage guidelines

This command is effective only for non-FTP users. FTP users can only have their passwords changed by the administrator.

Examples

Configure the device to notify a user about pending password expiration 10 days before the user's password expires.

```
<Sysname> system-view
[Sysname] password-control alert-before-expire 10
```

Related commands

display password-control

password-control blacklist user-info username-only

Use **password-control blacklist user-info username-only** to add only usernames of users failing authentication to the password control blacklist.

Use **undo password-control blacklist user-info** to restore the default.

Syntax

password-control blacklist user-info username-only

undo password-control blacklist user-info

Default

Both usernames and IP addresses are added to the password control blacklist when users fail authentication.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

If the user information items to add to the password control blacklist change, the system will clear the password control blacklist and restart the recording.

Examples

Add only usernames to the password control blacklist when users fail authentication.

```
<Sysname> system-view
[Sysname] password-control blacklist user-info username-only
```

Related commands

display password-control

display password-control blacklist

reset password-control blacklist

password-control change-password first-login enable

Use **password-control change-password first-login enable** to enable the password change at first login feature.

Use **undo password-control change-password first-login enable** to disable the password change at first login feature.

Syntax

password-control change-password first-login enable

undo password-control change-password first-login enable

Default

The password change at first login feature is enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

For the password change at first login feature to take effect, make sure the global password control is enabled.

Examples

Enable the password change at first login feature.

```
<Sysname> system-view
[Sysname] password-control change-password first-login enable
```

Related commands

display password-control

password-control enable

password-control change-password weak-password enable

Use **password-control change-password weak-password enable** to enable mandatory weak password change.

Use **undo password-control change-password weak-password enable** to disable mandatory weak password change.

Syntax

password-control change-password weak-password enable

undo password-control change-password weak-password enable

Default

The mandatory weak password change feature is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

The system checks for weak login passwords for Telnet, SSH, HTTP, or HTTPS device management users. A password is weak if it does not meet the following requirements:

- Password composition restriction.
- Minimum password length restriction.
- Password complexity checking policy.

The mandatory weak password change feature is disabled by default. The system displays a message about a weak password but does not force the user to change it. To improve the device security, you can enable the mandatory weak password change feature, which forces the users to change the identified weak passwords. The users can log in to the device only after their passwords meet the password requirements.

To view the current password control settings, use the **display password-control** command. To change the password composition restriction, minimum password length, and password complexity checking policy, use the **password-control composition**, **password-control length**, and **password-control complexity** commands, respectively.

Examples

Enable the mandatory weak password change feature.

```
<Sysname> system-view
[Sysname] password-control change-password weak-password enable
```

Related commands

display password-control

password-control { **aging** | **composition** | **history** | **length** }

password-control complexity

password-control composition

password-control length

password-control enable

password-control complexity

Use **password-control complexity** to configure the password complexity checking policy.

Use **undo password-control complexity** to remove a password complexity checking item.

Syntax

password-control complexity { **same-character** | **user-name** } **check**

undo password-control complexity { **same-character** | **user-name** } **check**

Default

The global password complexity checking policy is that username checking is enabled and repeated character checking is disabled.

The password complexity checking policy for a user group equals the global setting.

The password complexity checking policy for a local user equals that of the user group to which the local user belongs.

Views

System view

User group view

Local user view

Predefined user roles

network-admin

context-admin

Parameters

same-character: Refuses a password that contains a minimum of three consecutive identical characters. For example, the password **aaabc** is not complex enough.

user-name: Refuses a password that contains the username or the reverse of the username. For example, if the username is **123**, a password such as **abc123** or **321df** is not complex enough.

Usage guidelines

The password complexity checking policy depends on the view:

- The policy in system view has global significance and applies to all user groups.
- The policy in user group view applies to all local users in the user group.
- The policy in local user view applies only to the local user.

A password complexity checking policy with a smaller application scope has higher priority. The system prefers to use the password complexity checking policy in local user view for a local user.

- If no policy is configured for the local user, the system uses the policy for the user group to which the local user belongs.
- If no policy is configured for the user group, the system uses the global policy.

Username checking is independent of whether or not the global password control feature is enabled.

You can enable both username checking and repeated character checking.

Examples

Configure the password complexity checking policy, refusing any password that contains the username or the reverse of the username.

```
<Sysname> system-view
[Sysname] password-control complexity user-name check
```

Related commands

display local-user

display password-control

display user-group

password-control composition

Use **password-control composition** to configure the password composition policy.

Use **undo password-control composition** to restore the default.

Syntax

password-control composition type-number *type-number* [**type-length** *type-length*]

undo password-control composition

Default

The global composition policy requires that a password must contain a minimum of two character types and a minimum of one character for each type.The password composition policy for a user group is the same as the global policy. The password composition policy for a local user is the same as that of the user group to which the local user belongs.

Views

System view

User group view

Local user view

Predefined user roles

network-admin

context-admin

Parameters

type-number *type-number*: Specifies the minimum number of character types that a password must contain. The value range for the *type-number* argument is 1 to 4.

type-length *type-length*: Specifies the minimum number of characters that are from each type in the password. The value range for the *type-length* argument is 1 to 63.

Usage guidelines

The password composition policy depends on the view:

- The policy in system view has global significance and applies to all user groups.
- The policy in user group view applies to all local users in the user group.
- The policy in local user view applies only to the local user.

A password composition policy with a smaller application scope has higher priority. The system prefers to use the password composition policy in local user view for a local user.

- If no policy is configured for the local user, the system uses the policy for the user group to which the local user belongs.
- If no policy is configured for the user group, the system uses the global policy.

The product of the minimum number of character types and minimum number of characters for each type cannot be greater than the maximum length of passwords.

Examples

Specify that all passwords must each contain a minimum of four character types and a minimum of five characters for each type.

```
<Sysname> system-view
[Sysname] password-control composition type-number 4 type-length 5
```

Specify that passwords in user group **test** must contain a minimum of four character types and a minimum of five characters for each type.

```
[Sysname] user-group test
[Sysname-ugroup-test] password-control composition type-number 4 type-length 5
[Sysname-ugroup-test] quit
```

Specify that the password of device management user **abc** must contain a minimum of four character types and a minimum of five characters for each type.

```
[Sysname] local-user abc class manage
[Sysname-luser-manage-abc] password-control composition type-number 4 type-length 5
```

Related commands

display local-user

display password-control

display user-group

password-control composition enable

password-control enable

Use **password-control enable** to enable the password control feature globally.

Use **undo password-control enable** to disable the password control feature globally.

Syntax

password-control enable [**network-class**]

undo password-control enable [**network-class**]

Default

The password control feature is disabled globally for device management and network access users.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

network-class: Enables global password control for network access users. If you do not specify this keyword, the command enables global password control for device management users.

Usage guidelines

When you enable global password control, the device automatically generates a .dat file and saves the file to the storage media. The file is used to record authentication and login information of local users. Do not manually delete or modify the file.

The password composition policy, minimum password length, and username checking are independent of the global password control feature. Other password control features take effect only after the global password control feature is also enabled.

After the global password control feature is enabled, the passwords configured for local users must contain a minimum of four different characters.

After the global password control feature is enabled for device management users, you cannot display the password and super password configuration for device management users by using the corresponding **display** commands.

After the global password control feature is enabled for network access users, you cannot display the password configuration for network access users by using the corresponding **display** commands.

You can configure all password control features for device management users.

You can configure only the following password control features for network access users:

- Password complexity checking policy.
- Password composition policy.
- Minimum password length.
- Minimum password update interval.
- Maximum number of history password records for each user.

Examples

Enable the password control feature globally for device management users.

```
<Sysname> system-view
[Sysname] password-control enable
```

Enable the password control feature globally for network access users.

```
<Sysname> system-view
[Sysname] password-control enable network-class
```

Related commands

display password-control

password-control complexity

password-control { **aging** | **composition** | **history** | **length** } **enable**

password-control update-interval

password-control expired-user-login

Use **password-control expired-user-login** to set the maximum number of days and maximum number of times that a user can log in after the password expires.

Use **undo password-control expired-user-login** to restore the defaults.

Syntax

password-control expired-user-login delay *delay* **times** *times*

undo password-control expired-user-login

Default

A user can use an expired password to log in three times within 30 days after the password expires. If all the three attempts fail or the user makes a login attempt after 30 days, the system prompts the user to set a new password.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

delay *delay*: Specifies the maximum number of days during which a user can log in using an expired password. The value range for the *delay* argument is 1 to 90.

times *times*: Specifies the maximum number of times a user can log in after the password expires. The value range is 0 to 10. For a user to set a new password at the system prompt immediately after the password expires, set the value to 0.

Usage guidelines

This command is effective only on non-FTP login users. An FTP user cannot continue to log in after its password expires.

Examples

Allow a user to log in five times within 60 days after the password expires.

```
<Sysname> system-view
[Sysname] password-control expired-user-login delay 60 times 5
```

Related commands

display password-control

password-control history

Use **password-control history** to set the maximum number of history password records for each user.

Use **undo password-control history** to restore the default.

Syntax

password-control history *max-record-number*

undo password-control history

Default

The maximum number of history password records for each user is 4.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

max-record-number: Specifies the maximum number of history password records for each user. The value range is 2 to 15.

Usage guidelines

The global password control feature enables the system to record history passwords. When the number of history password records of a user reaches the maximum number, the newest history record overwrites the earliest one.

To delete the existing records, use one of the following methods:

- Use the **undo password-control enable** command to disable the password control feature globally.
- Use the **reset password-control history-record** command to clear the passwords manually.

Examples

Set the maximum number of history password records for each user to 10.

```
<Sysname> system-view
[Sysname] password-control history 10
```

Related commands

display password-control

password-control history enable

reset password-control blacklist

password-control length

Use **password-control length** to set the minimum password length.

Use **undo password-control length** to restore the default.

Syntax

password-control length *length*

undo password-control length

Default

The global minimum password length is 10 characters.The minimum password length for a user group equals the global setting. The minimum password length for a local user equals that of the user group to which the local user belongs.

Views

System view

User group view

Local user view

Predefined user roles

network-admin

context-admin

Parameters

length: Specifies the minimum password length in characters. The value range for this argument is 4 to 32.

Usage guidelines

The minimum length setting depends on the view:

- The setting in system view has global significance and applies to all user groups.

- The setting in user group view applies to all local users in the user group.
- The setting in local user view applies only to the local user.

A minimum password length with a smaller application scope has higher priority. The system prefers to use the minimum password length in local user view for a local user.

- If no minimum password length is configured for the local user, the system uses the minimum password length for the user group to which the local user belongs.
- If no minimum password length is configured for the user group, the system uses the global minimum password length.

Examples

Set the global minimum password length to 16 characters.

```
<Sysname> system-view
[Sysname] password-control length 16
```

Set the minimum password length to 16 characters for the user group **test**.

```
[Sysname] user-group test
[Sysname-ugroup-test] password-control length 16
[Sysname-ugroup-test] quit
```

Set the minimum password length to 16 characters for the device management user **abc**.

```
[Sysname] local-user abc class manage
[Sysname-luser-manage-abc] password-control length 16
```

Related commands

display local-user

display password-control

display user-group

password-control length enable

password-control login idle-time

Use **password-control login idle-time** to set the maximum account idle time.

Use **undo password-control login idle-time** to restore the default.

Syntax

password-control login idle-time *idle-time*

undo password-control login idle-time

Default

The maximum account idle time is 90 days.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

idle-time: Specifies the maximum account idle time in days. The value range is 0 to 365. 0 means no restriction for account idle time.

Usage guidelines

If a user account is idle for this period of time, the account becomes invalid and can no longer be used to log in to the device.

The account might become invalid if the system time changes after your last successful login. You cannot use an invalid account to log in. To disable the account idle time restriction, set the idle time value to 0.

Examples

Set the maximum account idle time to 30 days.

```
<Sysname> system-view
[Sysname] password-control login idle-time 30
```

Related commands

display password-control

password-control login-attempt

Use **password-control login-attempt** to configure the login attempt limit. The settings include the maximum number of consecutive login failures and the action to be taken when the maximum number is reached.

Use **undo password-control login-attempt** to restore the default.

Syntax

password-control login-attempt *login-times* [**exceed** { **lock** | **lock-time** *time* | **unlock** }]

undo password-control login-attempt

Default

The global login-attempt settings:

- The maximum number of consecutive login failures is 3.
- The locking period is 1 minute.

The login-attempt settings for a user group equal the global settings.

The login-attempt settings for a local user equal those for the user group to which the local user belongs.

Views

System view

User group view

Local user view

Predefined user roles

network-admin

context-admin

Parameters

login-times: Specifies the maximum number of consecutive login failures. The value range is 2 to 10.

exceed: Specifies an action if the user fails the maximum number of consecutive login attempts.

- **lock**: Locks the user account and the user's IP address permanently. No one can use this user account to log in from this locked IP address.

- **lock-time** *time*: Locks the user account and the user's IP address for a period of time. When the locking timer expires, users can use this user account to log in from the IP address. The value range for the *time* argument is 1 to 360 minutes.
- **unlock**: Does not lock the user account. The user can continue using this account to make login attempts from the current IP address.

Usage guidelines

The login-attempt policy depends on the view:

- The policy in system view has global significance and applies to all user groups.
- The policy in user group view applies to all local users in the user group.
- The policy in local user view applies only to the local user.

A login-attempt policy with a smaller application scope has higher priority. The system prefers to use the login-attempt policy in local user view for a local user.

- If no policy is configured for the local user, the system uses the policy for the user group to which the local user belongs.
- If no policy is configured for the user group, the system uses the global policy.

If an FTP, Web, or VTY user fails to log in, the system adds the user account and the user's IP address to the password control blacklist. When the maximum number of consecutive login failures is reached, the login attempt limit feature is triggered.

Whether a blacklisted user and user account are locked depends on the locking setting:

- If a user account is permanently locked for a user, the user cannot use this account unless this account is removed from the password control blacklist. To remove the user account, use the **reset password-control blacklist** command.
- To use a temporarily locked user account, the user can perform either of the following tasks:
  - Wait until the locking timer expires.
  - Remove the user account from the password control blacklist.
- If the user account and the user are blacklisted but not locked, the user can continue using this account to log in. The account and the user's IP address are removed from the password control blacklist when the user uses the account to successfully log in to the device.

NOTE:

This account is locked only for the user at the locked IP address. A user from an unlocked IP address can still use this account, and the user at the locked IP address can use other unlocked user accounts.

The **password-control login-attempt** command takes effect immediately after being executed, and can affect the users already in the password control blacklist.

Examples

Allow a maximum of four consecutive login failures on a user account, and lock the user account and the user's IP address permanently if the limit is reached.

```
<Sysname> system-view
[Sysname] password-control login-attempt 4 exceed lock
```

Use the user account **test** to log in to the device, and enter incorrect password for four times.

Display the password control blacklist. The output shows that the user account is on the blacklist, and its status is **lock**.

```
[Sysname] display password-control blacklist
 Per-user blacklist limit: 100.
 Blacklist items matched: 1.
```

```
 Username                    IP address          Login failures   Lock flag
 test                        192.168.44.1        4                lock
```

Verify that the user at 192.168.44.1 cannot use this user account to log in.

Allow a maximum of two consecutive login failures on a user account, and lock the account for 3 minutes if the limit is reached.

```
<Sysname> system-view
[Sysname] password-control login-attempt 2 exceed lock-time 3
```

Use the user account **test** to log in to the device, and enter incorrect password for two attempts.

Display the password control blacklist. The output shows that the user account is on the blacklist and its status is **lock**.

```
[Sysname] display password-control blacklist
 Per-user blacklist limit: 100.
 Blacklist items matched: 1.
 Username                    IP address          Login failures   Lock flag
 test                        192.168.44.1        2                lock
```

Verify that after 3 minutes, the user account is removed from the password control blacklist and the user at 192.168.44.1 can use this account.

Related commands

display local-user

display password-control

display password-control blacklist

display user-group

reset password-control blacklist

password-control per-user blacklist-limit

Use **password-control per-user blacklist-limit** to set the maximum number of blacklist entries for a user account.

Use **undo password-control per-user blacklist-limit** to restore the default.

Syntax

password-control per-user blacklist-limit *max-number*

undo password-control per-user blacklist-limit

Default

The maximum number of blacklist entries for a user account is 32.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

max-number: Maximum number of blacklist entries that the device can record for a single user account. The value range is 1 to 4294967295.

Usage guidelines

When the console users fail login, their user accounts are added to the password control blacklist. When FTP, Web, or virtual terminal line (VTY) users fail login, their IP addresses and user accounts are added to the password control blacklist.

If such a user uses the same user account to log in to the device from different IP addresses and fails the logins, the device will create a blacklist entry for each IP address for the user account. When the maximum number of blacklist entries for the user account is reached, a blacklist entry for a new IP address of the user account will overwrite the earliest blacklist entry for the user account.

Examples

Set the maximum number of blacklist entries for a user account to 100.

```
<Sysname> system-view
[Sysname] password-control per-user blacklist-limit 100
```

Related commands

display password-control blacklist

password-control login-attempt

reset password-control blacklist

password-control super aging

Use **password-control super aging** to set the aging time for super passwords.

Use **undo password-control super aging** to restore the default.

Syntax

password-control super aging *aging-time*

undo password-control super aging

Default

A super password expires after 90 days.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

aging-time: Specifies the super password aging time in days, in the range of 1 to 365.

Examples

Set the super passwords to expire after 10 days.

```
<Sysname> system-view
[Sysname] password-control super aging 10
```

Related commands

display password-control

password-control aging

password-control super composition

Use **password-control super composition** to configure the composition policy for super passwords.

Use **undo password-control super composition** to restore the default.

Syntax

password-control super composition type-number *type-number* [**type-length** *type-length*]

undo password-control super composition

Default

A super password must contain a minimum of two character types and a minimum of one character for each type.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

type-number *type-number*: Specifies the minimum number of character types that a super password must contain. The value range for the *type-number* argument is 1 to 4.

type-length *type-length*: Specifies the minimum number of characters that are from each character type. The value range for the *type-length* argument is 1 to 63.

Usage guidelines

The product of the minimum number of character types and minimum number of characters for each type cannot be greater than the maximum length of the super password.

Examples

Specify that a super password must contain a minimum of four character types and a minimum of five characters for each type.

```
<Sysname> system-view
[Sysname] password-control super composition type-number 4 type-length 5
```

Related commands

display password-control

password-control composition

password-control super length

Use **password-control super length** to set the minimum length for super passwords.

Use **undo password-control super length** to restore the default.

Syntax

password-control super length *length*

undo password-control super length

Default

The minimum super password length is 10 characters.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

length: Specifies the minimum length of super passwords in characters. The value range for this argument is 4 to 63.

Examples

Set the minimum length of super passwords to 16 characters.

```
<Sysname> system-view
[Sysname] password-control super length 16
```

Related commands

display password-control

password-control length

password-control update-interval

Use **password-control update-interval** to set the minimum password update interval, which is the minimum interval at which users can change their passwords.

Use **undo password-control update-interval** to restore the default.

Syntax

password-control update-interval *interval*

undo password-control update-interval

Default

The minimum password update interval is 24 hours.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies the minimum password update interval in hours, in the range of 0 to 168. 0 means no requirements for password update interval.

Usage guidelines

The set minimum interval is not effective on a user who is prompted to change the password at the first login or after the password expires.

Examples

Set the minimum password update interval to 36 hours.

```
<Sysname> system-view
[Sysname] password-control update-interval 36
```

Related commands

display password-control

reset password-control blacklist

Use **reset password-control blacklist** to remove blacklisted users.

Syntax

reset password-control blacklist [**user-name** *user-name*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

user-name *user-name*: Specifies the username of a user account to be removed from the password control blacklist. The username is a string of 1 to 55 characters. You can specify a pure username or specify a pure username and its domain name in the format of *pure usernname@domain name*. The pure username is case sensitive. The domain name is case-insensitive.

Usage guidelines

You can use this command to remove a user account and the user's IP address that are blacklisted due to excessive login failures. Then the user at this IP address can use this user account to log in.

Examples

Remove the user account named **test** from the password control blacklist.

```
<Sysname> reset password-control blacklist user-name test
Are you sure to delete the specified user in blacklist? [Y/N]:
```

Related commands

display password-control blacklist

reset password-control history-record

Use **reset password-control history-record** to delete history password records.

Syntax

reset password-control history-record [**super** [**role** *role name*] | **user-name** *user-name* | **network-class** [**user-name** *user-name*]]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

super: Deletes the history records of the specified super password or all super passwords.

role *role name*: Specifies a user role name, a case-sensitive string of 1 to 63 characters. If you do not specify this option, the command deletes the history records of all super passwords.

network-class: Deletes the history password records of network access users. If you do not specify this keyword, the command deletes the history password records of device management users.

user-name *user-name*: Specifies the username of the user whose password records are to be deleted. The *user-name* argument is a case-sensitive string of 1 to 55 characters. If you do not specify this option, the command deletes all history password records of the specified user type.

Usage guidelines

If you do not specify any parameters, this command deletes the history password records of all device management users.

Examples

Clear the history password records of all device management users.

```
<Sysname> reset password-control history-record
Are you sure to delete all local user's history records? [Y/N]:y
```

Delete the history password records of all network access users.

```
<Sysname> reset password-control history-record network-class
Are you sure you want to delete all network access users' history records? [Y/N]:y
```

Related commands

password-control history

Contents

Portal commands

aaa-fail nobinding enable

Use **aaa-fail nobinding enable** to enable AAA failure unbinding.

Use **undo aaa-fail nobinding enable** to restore the default.

Syntax

aaa-fail nobinding enable

undo aaa-fail nobinding enable

Default

AAA failure unbinding is disabled.

Views

MAC binding server view

Predefined user roles

network-admin

context-admin

Usage guidelines

If a portal user fails AAA in MAC-trigger authentication, the user cannot trigger authentication before the MAC-trigger entry of the user ages out. After the MAC-trigger entry ages out, the user triggers MAC-trigger authentication when it accesses the network.

After AAA failure unbinding is enabled, the device sets the MAC-trigger entry state for a user to unbound immediately after the user fails AAA in MAC-trigger authentication. Before the user's MAC-trigger entry ages out, the user can trigger normal portal authentication.

Examples

Enable AAA failure unbinding for MAC binding server **mts**.

```
<Sysname> system-view
[Sysname] portal mac-trigger-server mts
[Sysname-portal-mac-trigger-server-mts] aaa-fail nobinding enable
```

Related commands

display portal mac-trigger-server

ad-url

Use **ad-url** to configure an advertisement URL in an advertisement group.

Use **undo ad-url** to delete an advertisement URL from an advertisement group.

Syntax

ad-url *url-string* [**time-range** *time-range-name*]

undo ad-url *url-string*

Default

No advertisement URLs are configured in an advertisement group.

Views

Advertisement group view

Predefined user roles

network-admin

context-admin

Parameters

url-string: Specifies the URL of an advertisement, a case-sensitive string of 1 to 256 characters. The URL must begin with **http://**.

time-range *time-range-name*: Specifies a time range for portal advertisement push. The *time-range-name* argument represents the name of the time range, a case-insensitive string of 1 to 32 characters. The time range name must begin with a letter and cannot be **all**. For more information about time ranges, see time range configuration in *ACL and QoS Configuration Guide*.

Usage guidelines

You can configure a maximum of 16 advertisement URLs in an advertisement group.

If the advertisement push method is time range-based, you must specify a time range for each advertisement URL. The time ranges for all advertisement URLs in an advertisement group must be different from each other.

Examples

Configure advertisement URLs in advertisement group **test**.

```
<Sysname> system-view
[Sysname] portal ad-url-group test method interval
[Sysname-portal-ad-url-group-test] ad-url http://www.qq.com
[Sysname-portal-ad-url-group-test] ad-url http://www.sina.com
[Sysname-portal-ad-url-group-test] ad-url http://www.baidu.com
```

Related commands

ad-url-group

ad-url-group

Use **ad-url-group** to set the time interval or traffic threshold for portal advertisement push in an advertisement group.

Use **undo ad-url-group** to restore the default.

Syntax

ad-url-group { **interval** *interval* | **traffic-threshold** *traffic-threshold* }

undo ad-url-group

Default

The interval is 360 minutes and the traffic threshold is 100 MB for portal advertisement push in an an advertisement group.

Views

Advertisement group view

Predefined user roles

network-admin

context-admin

Parameters

interval *interval*: Specifies the advertisement push interval, in the range of 5 to 1440 minutes. The interval begins when a portal user comes online.

traffic-threshold *traffic-threshold*: Specifies the traffic threshold for portal advertisement push in the range of 1 to 1024 MB.

Usage guidelines

This command takes effect only when the advertisement push method is time-based or traffic-based. The advertisement push interval is applicable to time-based advertisement push. The traffic threshold is applicable to traffic-based advertisement push.

Each time the interval for a user ends or the user's consumed traffic since the last push reaches the traffic threshold, the device pushes an advertisement to the user. The advertisements in the advertisement group are pushed to the portal user in the order they are configured.

Examples

Set the advertisement push interval to 100 minutes in advertisement group **test**.

```
<Sysname> system-view
[Sysname] portal ad-url-group test
[Sysname-portal-ad-url-group-test] ad-url-group interval 100
```

Related commands

ad-url

portal ad-url-group

aging-time

Use **aging-time** to set the aging time for MAC-trigger entries.

Use **undo aging-time** to restore the default.

Syntax

aging-time *seconds*

undo aging-time

Default

The aging time for MAC-trigger entries is 300 seconds.

Views

MAC binding server view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies the aging time for MAC-trigger entries. The value range is 60 to 7200 seconds.

Usage guidelines

With MAC-based quick portal authentication enabled, the device generates a MAC-trigger entry for a user when the device detects traffic from the user for the first time. The MAC-trigger entry records the following information:

- MAC address of the user

- Interface index
- VLAN ID
- Traffic statistics
- Aging timer

When the aging time expires, the device deletes the MAC-trigger entry. The device re-creates a MAC-trigger entry for the user when it detects the user's traffic again.

Examples

Specify the aging time as 300 seconds for MAC-trigger entries.

```
<Sysname> system-view
[Sysname] portal mac-trigger-server mts
[Sysname-portal-mac-trigger-server-mts] aging-time 300
```

Related commands

display portal mac-trigger-server

app-id (Facebook authentication server view)

Use **app-id** to specify the app ID for Facebook authentication.

Use **undo app-id** to restore the default.

Syntax

app-id *app-id*

undo app-id

Default

No app ID is specified for Facebook authentication.

Views

Facebook authentication server view

Predefined user roles

network-admin

context-admin

Parameters

app-id: Specifies the app ID for Facebook authentication.

Usage guidelines

If a portal user uses Facebook authentication, the Facebook server authenticates and authorizes the user and sends an authorization code to the device after the authentication and authorization succeed. Then, the device sends the authorization code, app ID, and app key to the Facebook server to determine whether the user has passed authentication and authorization.

Examples

Specify **123456789** as the app ID for Facebook authentication.

```
<Sysname> system-view
[Sysname] portal extend-auth-server facebook
[Sysname-portal-extend-auth-server-fb] app-id 123456789
```

Related commands

display portal extend-auth-server

app-id (QQ authentication server view)

Use **app-id** to specify the app ID for QQ authentication.

Use **undo app-id** to restore the default.

Syntax

app-id *app-id*

undo app-id

Default

An app ID for QQ authentication exists.

Views

QQ authentication server view

Predefined user roles

network-admin

context-admin

Parameters

app-id: Specifies the app ID for QQ authentication.

Usage guidelines

To use QQ authentication for portal users, you must go to Tencent Open Platform (**http://connect.qq.com/intro/login**) to finish the following tasks:

1. Register as a developer by using a valid QQ account.
2. Apply the access to the platform for your website. The website is the webpage to which users are redirected after passing QQ authentication.

You will obtain the app ID and app key from the Tencent Open Platform after your application succeeds.

After a portal user passes QQ authentication, the QQ authentication server sends the authorization code of the user to the portal Web server. After the portal Web server receives the authorization code, it sends the authorization code of the user, the app ID, and the app key to the QQ authentication server for verification. If the information is verified as correct, the device determines that the user passes QQ authentication.

Examples

Specify **101235509** as the app ID for QQ authentication.

```
<Sysname> system-view
[Sysname] portal extend-auth-server qq
[Sysname-portal-extend-auth-server-qq] app-id 101235509
```

Related commands

display portal extend-auth-server

app-id (WeChat authentication server view)

Use **app-id** to specify the app ID for WeChat authentication.

Use **undo app-id** to restore the default.

Syntax

app-id *app-id*

undo app-id

Default

No app ID is specified for WeChat authentication.

Views

WeChat authentication server view

Predefined user roles

network-admin

context-admin

Parameters

app-id: Specifies the app ID for WeChat authentication.

Usage guidelines

The app ID specified in this command must be the same as the app ID obtained from the WeChat Official Account Admin Platform.

This configuration is required for the device to provide local WeChat authentication for portal users.

To obtain the app ID for WeChat authentication, you must perform the following tasks:

1. Go to the WeChat Official Account Admin Platform (**https://mp.weixin.qq.com**) to apply a WeChat official account.
2. Use the account to log in to the platform and enable the WeChat WiFi hotspot feature.
3. Click the device management tab, add the device: select the shop where the device is deployed, select the **portal** device type, and enter the deviec settings.

   After the previous configurations, you will obtain the credentials (app ID, app key, and shop ID) for WeChat authentication.

When a WeChat user attempts to connect to the WiFi network provided in the specified shop, the device sends the credentials to the WeChat Official Account Platform for verification. After the credentials are verified, the device continues the portal authentication and allows the user to use the WiFi network after the authentication.

Examples

Specify **wx23fb4aaf04b8491e** as the app ID for WeChat authentication.

```
<Sysname> system-view
[Sysname] portal extend-auth-server wechat
[Sysname-portal-extend-auth-server-wechat] app-id wx23fb4aaf04b8491e
```

Related commands

display portal extend-auth-server

app-key (Facebook authentication server view)

Use **app-key** to specify the app key for Facebook authentication.

Use **undo app-key** to restore the default.

Syntax

app-key { **cipher** | **simple** } *app-key*

undo app-key

Default

No app key is specified for Facebook authentication.

Views

Facebook authentication server view

Predefined user roles

network-admin

context-admin

Parameters

cipher: Specifies the app key in encrypted form.

simple: Specifies the app key in plaintext form.

app-key: Specifies the app key string. Its plaintext form is a case-sensitive string of 1 to 64 characters. Its encrypted form is a case-sensitive string of 1 to 117 characters.

Usage guidelines

If a portal user uses Facebook authentication, the Facebook server authenticates and authorizes the user and sends an authorization code to the device after the authentication and authorization succeed. Then, the device sends the authorization code, app ID, and app key to the Facebook server to determine whether the user has passed authentication and authorization.

Examples

Specify **123** in plaintext form as the app key for Facebook authentication.

```
<Sysname> system-view
[Sysname] portal extend-auth-server facebook
[Sysname-portal-extend-auth-server-fb] app-key simple 123
```

Related commands

display portal extend-auth-server

app-key (QQ authentication server view)

Use **app-key** to specify the app key for QQ authentication.

Use **undo app-key** to restore the default.

Syntax

app-key { **cipher** | **simple** } *app-key*

undo app-key

Default

An app key for QQ authentication exists.

Views

QQ authentication server view

Predefined user roles

network-admin

context-admin

Parameters

cipher: Specifies the app key in encrypted form.

simple: Specifies the app key in plaintext form.

app-key: Specifies the app key string. Its plaintext form is a case-sensitive string of 1 to 64 characters. Its encrypted form is a case-sensitive string of 1 to 117 characters.

Usage guidelines

To use QQ authentication for portal users, you must go to Tencent Open Platform (**http://connect.qq.com/intro/login**) to finish the following tasks:

1. Register as a developer by using a valid QQ account.
2. Apply the access to the platform for your website. The website is the webpage to which users are redirected after passing QQ authentication.

You will obtain the app ID and app key from the Tencent Open Platform after your application succeeds.

After a portal user passes QQ authentication, the QQ authentication server sends the authorization code of the user to the portal Web server. After the portal Web server receives the authorization code, it sends the authorization code of the user, the app ID, and the app key to the QQ authentication server for verification. If the information is verified as correct, the device determines that the user passes QQ authentication.

Examples

Specify **8a5428e6afdc3e2a2843087fe73f1507** in plaintext form as the app key for QQ authentication.

```
<Sysname> system-view
[Sysname] portal extend-auth-server qq
[Sysname-portal-extend-auth-server-qq] app-key simple 8a5428e6afdc3e2a2843087fe73f1507
```

Related commands

display portal extend-auth-server

app-key (WeChat authentication server view)

Use **app-key** to specify the app key for WeChat authentication.

Use **undo app-key** to restore the default.

Syntax

app-key { **cipher** | **simple** } *app-key*

undo app-key

Default

No app key is specified for WeChat authentication.

Views

WeChat authentication server view

Predefined user roles

network-admin

context-admin

Parameters

cipher: Specifies the app key in encrypted form.

simple: Specifies the app key in plaintext form.

app-key: Specifies the app key string. Its plaintext form is a case-sensitive string of 1 to 64 characters. Its encrypted form is a case-sensitive string of 1 to 117 characters.

Usage guidelines

This configuration is required for the device to provide local WeChat authentication for portal users. The app key specified in this command must be the same as the app key obtained from the WeChat Official Account Admin Platform.

To obtain the app key for WeChat authentication, you must perform the following tasks:

1. Go to the WeChat Official Account Admin Platform (**https://mp.weixin.qq.com**) to apply a WeChat official account.
2. Use the account to log in to the platform and enable the WeChat WiFi hotspot feature.
3. Click the device management tab, add the device: select the shop where the device is deployed, select the **portal** device type, and enter the device settings.

   After the previous configurations, you will obtain the credentials (app ID, app key, and shop ID) for WeChat authentication.

When a WeChat user attempts to connect to the WiFi network provided in the specified shop, the device sends the credentials to the WeChat Official Account Platform for verification. After the credentials are verified, the device continues the portal authentication and allows the user to use the WiFi network after the authentication.

Examples

Specify **nqduqg4816689geruhq3** in plaintext form as the app key for WeChat authentication.

```
<Sysname> system-view
[Sysname] portal extend-auth-server wechat
[Sysname-portal-extend-auth-server-wechat] app-key simple nqduqg4816689geruhq3
```

Related commands

display portal extend-auth-server

app-secret

Use **app-secret** to specify the app secret for WeChat authentication.

Use **undo app-secret** to restore the default.

Syntax

app-secret { **cipher** | **simple** } *string*

undo app-secret

Default

No app secret is specified for WeChat authentication.

Views

WeChat authentication server view

Predefined user roles

network-admin

context-admin

Parameters

cipher: Specifies the app secret in encrypted form.

simple: Specifies the app secret in plaintext form.

app-key: Specifies the app secret string. Its plaintext form is a case-sensitive string of 1 to 64 characters. Its encrypted form is a case-sensitive string of 1 to 117 characters.

Usage guidelines

When the subscribe-required feature is enabled, you must specify the app secret for WeChat authentication on the device.

To obtain the app secret for WeChat authentication, perform the following tasks:

1. Use a WeChat official account to log in to the WeChat Official Account Admin Platform.

   For more information about the WeChat official account, see WeChat authentication configuration in *Security Configuration Guide*.
2. From the navigation tree, select **Developer Centers**.

   In the **Configuration Items** area, you can see the app secret for the WeChat Official account.

Examples

Specify **nqduqg4816689geruhq3** in plaintext form as the app secret for WeChat authentication.

```
<Sysname> system-view
[Sysname] portal extend-auth-server wechat
[Sysname-portal-extend-auth-server-wechat] app-secret simple nqduqg4816689geruhq3
```

authentication-timeout

Use **authentication-timeout** to set the authentication timeout, which is the maximum amount of time the device waits for portal authentication to complete after receiving the MAC binding query response.

Use **undo authentication-timeout** to restore the default.

Syntax

authentication-timeout *minutes*

undo authentication-timeout

Default

The authentication timeout time is 3 minutes.

Views

MAC binding server view

Predefined user roles

network-admin

context-admin

Parameters

minutes: Specifies the authentication timeout in the range of 1 to 15 minutes.

Usage guidelines

Upon receiving the MAC binding query response of a user from the MAC binding server, the device starts an authentication timeout timer for the user. When the timer expires, the device deletes the MAC-trigger entry of the user.

Examples

Set the authentication timeout to 10 minutes.

```
<Sysname> system-view
[Sysname] portal mac-trigger-server mts
```

```
[Sysname-portal-mac-trigger-server-mts] authentication-timeout 10
```

Related commands

display portal mac-trigger-server

auth-url

Use **auth-url** to specify the URL of the QQ or Facebook authentication server.

Use **undo auth-url** to delete the URL of the QQ or Facebook authentication server.

Syntax

auth-url *url-string*

undo auth-url

Default

The URL of QQ authentication server is **https://graph.qq.com**.

The URL of Facebook authentication server is **https://graph.facebook.com**.

Views

QQ authentication server view

Facebook authentication server view

Predefined user roles

network-admin

context-admin

Parameters

url-string: Specifies the URL of the QQ or Facebook authentication server, a case-sensitive string of 1 to 256 characters. Make sure that you specify the actual URL of the QQ or Facebook authentication server. The URL string can include question marks (?). If you enter a question mark (?) in the place of this argument, the CLI does not display help information for this argument.

Examples

Specify **http://oauth.qq.com/** as the URL of the QQ authentication server.

```
<Sysname> system-view
[Sysname] portal extend-auth-server qq
[Sysname-portal-extend-auth-server-qq] auth-url http://oauth.qq.com
```

Specify **http://oauth.facebook.com** as the URL of the Facebook authentication server.

```
<Sysname> system-view
[Sysname] portal extend-auth-server facebook
[Sysname-portal-extend-auth-server-fb] auth-url http://oauth.facebook.com
```

Related commands

display portal extend-auth-server

binding-retry

Use **binding-retry** to specify the maximum number of attempts and the interval for sending MAC binding queries to the MAC binding server.

Use **undo binding-retry** to restore the default.

Syntax

binding-retry { *retries* | **interval** *interval* } *

undo binding-retry

Default

The maximum number of query attempts is 3 and the query interval is 1 second.

Views

MAC binding server view

Predefined user roles

network-admin

context-admin

Parameters

retries: Specifies the maximum number of MAC binding query attempts, in the range of 1 to 10.

interval *interval*: Specifies the query interval in the range of 1 to 60 seconds.

Usage guidelines

If the device does not receive a response from the MAC binding server after the maximum number is reached, the device determines that the MAC binding server is unreachable. The device performs normal portal authentication for the user. The user needs to enter the username and password for authentication.

If you execute this command multiple times in the same MAC binding server view, the most recent configuration takes effect.

Examples

Set the maximum number of MAC binding query attempts to 3 and the query interval to 60 seconds.

```
<Sysname> system-view
[Sysname] portal mac-trigger-server mts
[Sysname-portal-mac-trigger-server-mts] binding-retry 3 interval 60
```

Related commands

display portal mac-trigger-server

captive-bypass enable

Use **captive-bypass enable** to enable the captive-bypass feature.

Use **undo captive-bypass enable** to disable the captive-bypass feature.

Syntax

captive-bypass [**android** | **ios** [**optimize**]] **enable**

undo captive-bypass [**android** | **ios** [**optimize**]] **enable**

Default

The captive-bypass feature is disabled. The device automatically pushes the portal authentication page to the iOS devices and some Android devices when they are connected to the network.

Views

Portal Web server view

Predefined user roles

network-admin

context-admin

Parameters

android: Enables the captive-bypass feature for Android users.

ios: Enables the captive-bypass feature for iOS users.

optimize: Enables the optimized captive-bypass feature.

Usage guidelines

With the captive-bypass feature enabled, the device does not automatically push the portal authentication page to iOS devices and some Android devices when they are connected to the network. The device pushes the portal authentication page only when the user accesses the Internet by using a browser.

The optimized captive-bypass feature applies only to iOS mobile devices. The device automatically pushes the portal authentication page to iOS mobile devices when they are connected to the network. Users can press the home button to return to the desktop without triggering portal authentication, and the Wi-Fi connection is not terminated.

If you do not specify any parameters, this command enables the captive-bypass feature for both Android and iOS users.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Enable the captive-bypass feature.

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] captive-bypass enable
```

Enable the optimized captive-bypass feature for iOS users.

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] captive-bypass ios optimize enable
```

Enable the captive-bypass feature for Android users.

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] captive-bypass android enable
```

Related commands

display portal captive-bypass statistics

display portal web-server

cloud-binding enable

Use **cloud-binding enable** to enable cloud MAC-trigger authentication.

Use **undo cloud-binding enable** to disable cloud MAC-trigger authentication.

Syntax

cloud-binding enable

undo cloud-binding enable

Default

Cloud MAC-trigger authentication is disabled.

Views

MAC binding server view

Predefined user roles

network-admin

context-admin

Usage guidelines

The cloud MAC-trigger authentication feature enables the cloud server to provide automated authentication to users as a unified portal authentication, portal Web, and MAC binding server. Users are required to perform manual authentication (entering the username and password) only for the first network access. They are automatically connected to the network without manual authentication for subsequent network access attempts.

Examples

Enable cloud MAC-trigger authentication for MAC binding server **mts**.

```
<Sysname> system-view
[Sysname] portal mac-trigger-server mts
[Sysname-portal-mac-trigger-server-mts] cloud-binding enable
```

Related commands

display portal mac-trigger-server

cloud-server url

Use **cloud-server url** to specify the URL of the cloud portal authentication server.

Use **undo cloud-server url** to restore the default.

Syntax

cloud-server url *url-string*

undo cloud-server url

Default

The URL of the cloud portal authentication server is not specified. The device uses the URL of the portal Web server as the URL of the cloud portal authentication server.

Views

MAC binding server view

Predefined user roles

network-admin

context-admin

Parameters

url-string: Specifies the URL of a cloud portal authentication server. The specified URL must be a complete URL starting with **http://** or **https://**, a case-sensitive string of 1 to 256 characters. The URL string can include question marks (?). If you enter a question mark (?) in the place of this argument, the CLI does not display help information for this argument.

Usage guidelines

To separate portal authentication and Web servers, specify the cloud portal authentication server URL by using this command, and specify a different URL for the portal Web server. In this way, you can use a different portal Web server to provide customized authentication pages to users.

Examples

In the view of MAC binding server **mts**, specify **http://lvzhou.nsfocus.com.cn** as the URL of the cloud portal authentication server.

```
<Sysname> system-view
[Sysname] portal mac-trigger-server mts
[Sysname-portal-mac-trigger-server-mts] cloud-server url http://lvzhou.nsfocus.com.cn
```

Related commands

display portal mac-trigger-server

default-logon-page

Use **default-logon-page** to specify the default authentication page file for a local portal Web service.

Use **undo default-logon-page** to restore the default.

Syntax

default-logon-page *file-name*

undo default-logon-page

Default

Models	Default
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	The device does not provide a default authentication page file for a local portal Web service.
NFNX3-HDB680, NFNX3-HDB1080	The device provides a default authentication page file for a local portal Web service.

Views

Local portal Web service view

Predefined user roles

network-admin

context-admin

Parameters

file-name: Specifies the default authentication page file by the file name (without the file storage directory). The file name is a case-sensitive string of 1 to 91 characters. Valid characters are letters, digits, dots (.) and underscores (_).

Usage guidelines

You must edit the default authentication pages, compress them to a .zip file, and then upload the file to the root directory of the storage medium of the device.

After you use the **default-logon-page** command to specify the file, the device decompresses the file to get the authentication pages. The device then sets them as the default authentication pages for local portal authentication.

Examples

Specify file **pagefile1.zip** as the default authentication page file for local portal authentication.

```
<Sysname> system-view
[Sysname] portal local-web-server http
[Sysname-portal-local-websvr-http] default-logon-page pagefile1.zip
```

Related commands

portal local-web-server

display portal

Use **display portal** to display portal configuration and portal running state.

Syntax

display portal interface *interface-type interface-number*

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Examples

Display portal configuration and portal running state on GigabitEthernet 1/0/1.

```
<Sysname> display portal interface gigabitethernet 1/0/1
 Portal information of GigabitEthernet1/0/1
     NAS-ID profile: aaa
     Authorization : Strict checking
     ACL           : Enabled
     User profile  : Disabled
     Dual stack    : Disabled
     Dual IP       : Disabled
     Dual traffic-separate: Disabled
     Advertisement push: Enabled
     Embedded advertisement: Enabled
 IPv4:
     Portal status: Enabled
     Portal authentication method: Layer3
     Portal Web server: wbs(active)
     Secondary portal Web server: wbs sec
     Portal mac-trigger-server: mts
```

```
     Authentication domain: my-domain
     Pre-auth domain: abc
     Extend-auth domain: abc
     User-dhcp-only: Enabled
     Pre-auth IP pool: ab
     Max portal users: Not configured
     Bas-ip: Not configured
     User detection: Type: ICMP  Interval: 300s  Attempts: 5  Idle time: 180s
     Portal temp-pass: Enabled       Period: 30s
     Action for server detection:
         Server type    Server name                        Action
         Web server     wbs                                fail-permit
         Portal server  pts                                fail-permit
     Layer3 source network:
         IP address              Mask
         1.1.1.1                 255.255.0.0

     Destination authentication subnet:
         IP address              Mask
         2.2.2.2                 255.255.255.0
     Advertisement push URL: http://192.168.56.3/welcome
IPv6:
     Portal status: enabled
     Portal authentication method: Layer3
     Portal Web server: wbsv6(active)
     Secondary portal Web server: Not configured
     Portal mac-trigger-server: Not configured
     Authentication domain: my-domain
     Pre-auth domain: abc
     Extend-auth domain: Not configured
     User-dhcp-only: Enabled
     Pre-auth IP pool: ab
     Max portal users: Not configured
     Bas-ipv6:Not configured
     User detection: Type: ICMPv6   Interval: 300s   Attempts: 5   Idle time: 180s
     Portal temp-pass: Disabled
     Action for server detection:
         Server type    Server name                        Action
         Web server     wbsv6                              fail-permit
         Portal server  ptsv6                              fail-permit
     Layer3 source network:
         IP address                                        Prefix length
         11::5                                             64

     Destination authentication subnet:
         IP address                                        Prefix length
     Advertisement push: Not Configured
```

Table 1 Command output

Field	Description
Portal information of interface	Portal configuration on the interface.
NAS-ID profile	NAS-ID profile on the interface.
Authorization	Authorization information type: .
Strict checking	Whether strict checking is enabled on portal authorization information.
Dual stack	Status of the portal dual-stack feature on the interface: • Disabled. • Enabled.
Dual IP	Status of the dual IP feature, disabled or enabled. This feature enables the device to carry both an IPv4 address and an IPv6 address in RADIUS packets for single-stack users in remote portal authentication.
Dual traffic-separate	Status of separate IPv4 and IPv6 traffic statistics for dual-stack portal users on the interface: • Disabled. • Enabled.
Advertisement-push	Status of portal advertisement push: • Disabled. • Enabled.
Embedded advertisement	Status of embedded portal advertisement push: • Disabled. • Enabled.
IPv4	IPv4 portal configuration.
IPv6	IPv6 portal configuration.
Portal status	Portal authentication status on the interface: • **Disabled**—Portal authentication is disabled. • **Enabled**—Portal authentication is enabled. • **Authorized**—The portal authentication server or portal Web server is unreachable. The interface allows users to have network access without authentication.
Portal authentication method	Type of authentication enabled on the interface: • **Direct**—Direct authentication. • **Redhcp**—Re-DHCP authentication. • **Layer3**—Cross-subnet authentication.
Portal Web server	Name of the primary portal Web server specified on the interface. This field displays the **(active)** flag next to the server name if the server is being used.
Secondary portal Web server	Name of the backup portal Web server specified on the interface. This field displays the **(active)** flag next to the server name if the server is being used.
Portal mac-trigger-server	Name of the MAC binding server specified on the interface.
Authentication domain	Mandatory authentication domain on the interface.
Pre-auth domain	Preauthentication domain for portal users on the interface.
Extend-auth domain	Authentication domain configured for third-party authentication on an

Field	Description
	interface.
User-dhcp-only	Status of the user-dhcp-only feature: • **Enabled**—Only users with IP addresses obtained through DHCP can perform portal authentication. • **Disabled**—Both users with IP addresses obtained through DHCP and users with static IP addresses can pass authentication to get online.
Pre-auth ip-pool	Name of the IP address pool specified for portal users before authentication.
Max portal users	Maximum number of portal users allowed on an interface.
Bas-ip	BAS-IP attribute of the portal packets sent to the portal authentication server.
Bas-ipv6	BAS-IPv6 attribute of the portal packets sent to the portal authentication server.
User detection	Configuration for online detection of portal users on the interface, including detection method (ARP, ICMP, ND, or ICMPv6), detection interval, maximum number of detection attempts, and user idle time.
Portal temp-pass	Status of the temporary pass feature: • **Enabled**—The temporary pass feature is enabled. • **Disabled**—The temporary pass feature is disabled. • **Period**—Temporary pass period during which a user can access the Internet temporarily. This field is displayed only if the temporary pass feature is enabled.
Action for server detection	Portal server detection configuration on the interface: • **Server type**—Type of the server. **Portal server** represents the portal authentication server, and **Web server** represents the portal Web server. • **Server name**—Name of the server. • **Action**—Action triggered by the result of server detection. This field displays **fail-permit** when the portal fail-permit feature is enabled.
Layer3 source network	Information of the portal authentication source subnet.
Destination authentication subnet	Information of the portal authentication destination subnet.
IP address	IP address of the portal authentication subnet.
Mask	Subnet mask of the portal authentication subnet.
Prefix length	Prefix length of the IPv6 portal authentication subnet address.
Advertisement push URL	URL of the advertisement to be pushed to portal users and the push method related setting: Possible settings include: • **Interval**—Interval for time-based advertisement push, in minutes. • **Traffic**—Traffic threshold for traffic-based advertisement push, in MB. • **Time-range**—Time range for time range-based advertisement push.
Advertisement push url-group	Name of an advertisement group. The advertisements in the group are pushed to portal users.

display portal ad-push statistics

Use **display portal ad-push statistics** to display statistics about portal advertisement push.

Syntax

display portal ad-push statistics { **ad-url-group** | **url** }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ad-url-group: Displays statistics on an advertisement group basis.

url: Displays statistics on an advertisement URL basis.

Examples

Display URL-based statistics about portal advertisement push.

```
<Sysname> display portal ad-push statistics url
PV = Page View        IP = IP        UV = Unique Visitor
   URL                    PV    IP   UV
   www.sina.com.cn        10    5    5
   www.baidu.com.cn       1     1    1
```

Display advertisement group-based statistics about portal advertisement push.

```
<Sysname> display portal ad-push statistics ad-url-group
PV = Page View        IP = IP        UV = Unique Visitor
URL-group name: group1
   URL                    PV    IP    UV
   www.sina.com.cn        1     1     1
   www.dianying.com       2     1     1
URL-group name: group2
   URL                    PV    IP    UV
   www.sina.com.cn        1     1     1
   www.qq.com             2     1     1
```

Table 2 Command output

Field	Description
Url-group name	Name of an advertisement group.
URL	URL of an advertisement.
PV	Number of times that a portal user visits the advertisement page. This value increases by 1 each time the page is refreshed.
IP	Number of IP addresses from which portal users visit the advertisement page.

Field	Description
UV	Number of portal users with different usernames that visit the advertisement page.

Related commands

reset portal ad-push statistic

display portal auth-error-record

Use **display portal auth-error-record** to display portal authentication error records.

Syntax

display portal auth-error-record { **all** | **ipv4** *ipv4-address* | **ipv6** *ipv6-address* | **start-time** *start-date start-time* **end-time** *end-date end-time* }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

all: Specifies all portal authentication error records.

ipv4 *ipv4-address*: Specifies the IPv4 address of a portal user.

ipv6 *ipv6-address*: Specifies the IPv6 address of a portal user.

start-time *start-date start-time* **end-time** *end-date end-time*: Specifies a time range. The start date and end date must be in the format of MM/DD/YYYY or YYYY/MM/DD. The value range for MM is 1 to 12. The value range for DD varies with the specified month. The value range for YYYY is 1970 to 2037. The start time and end time must be in the format of hh:mm. The value range for the start time and end time is 00:00 to 23:59.

Examples

Display all portal authentication error records.

```
<Sysname> display portal auth-error-record all
Total authentication error records: 2
User MAC               : 0016-ecb7-a879
Interface              : Vlan-interface100
User IP address        : 192.168.0.188
Auth error time        : 2016-03-04 16:49:07
Auth error reason      : The maximum number of users already reached.

User MAC               : 0016-ecb7-a235
Interface              : Vlan-interface100
User IP address        : 192.168.0.10
Auth error time        : 2016-03-04 16:51:07
```

```
Auth error reason      : The maximum number of users already reached.
```

Display portal authentication error records for the portal user whose IPv4 address is **192.168.0.188**.

```
<Sysname> display portal auth-error-record ip 192.168.0.188
User MAC               : 0016-ecb7-a879
Interface              : Vlan-interface100
User IP address        : 192.168.0.188
Auth error time        : 2016-03-04 16:49:07
Auth error reason      : The maximum number of users already reached.
```

Display portal authentication error records for the portal user whose IPv6 address is **2000::2**.

```
<Sysname> display portal auth-error-record ipv6 2000::2
User MAC               : 0016-ecb7-a879
Interface              : Vlan-interface100
User IP address        : 2000::2
Auth error time        : 2016-03-04 16:49:07
Auth error reason      : The maximum number of users already reached.
```

Display portal authentication error records with the error time in the range of 2016/3/4 14:20 to 2016/3/4 14:23.

```
<Sysname> display portal auth-error-record start-time 2016/3/4 14:20 end-time 2016/3/4
14:23
User MAC               : 0016-ecb7-a879
Interface              : Vlan-interface100
User IP address        : 192.168.0.188
Auth error time        : 2016-03-04 14:22:25
Auth error reason      : The maximum number of users already reached.
```

Table 3 Command output

Field	Description
Total authentication error records	Total number of portal authentication error records.
User MAC	MAC address of the portal user.
Interface	Access interface of the portal user.
User IP address	IP address of the portal user.
Auth error time	Time when the portal user encountered an authentication error, in the format of YYYY-MM-DD hh:mm:ss.
Auth error reason	Reason for the authentication error: • The maximum number of users already reached. • Failed to obtain user physical information. • Failed to receive the packet because packet length is 0. • Packet source unknown. Server IP:X.X.X.X, VRF index:0. • Packet validity check failed because packet length and version don't match. • Packet type invalid. • Packet validity check failed due to invalid authenticator. • Memory insufficient. • Portal is disabled on the interface. • The maximum number of users on the interface already reached. • Failed to get the access token of the cloud user.

Field	Description
	• Failed to get the user information of the cloud user. • Failed to get the access token of the QQ user. • Failed to get the openID of the QQ user. • Failed to get the user information of the QQ user. • Email authentication failed.

Related commands

portal auth-error-record enable

reset auth-error-record

display portal auth-fail-record

Use **display portal auth-fail-record** to display portal authentication failure records.

Syntax

display portal auth-fail-record { **all** | **ipv4** *ipv4-address* | **ipv6** *ipv6-address* | **start-time** *start-*date *start-time* **end-time** *end-date end-time* | **username** *username* }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

all: Specifies all portal authentication failure records.

ipv4 *ipv4-address*: Specifies the IPv4 address of a portal user.

ipv6 *ipv6-address*: Specifies the IPv6 address of a portal user.

start-time *start-date start-time* **end-time** *end-date end-time*: Specifies a time range. The start date and end date must be in the format of MM/DD/YYYY or YYYY/MM/DD. The value range for MM is 1 to 12. The value range for DD varies with the specified month. The value range for YYYY is 1970 to 2037. The start time and end time must be in the format of hh:mm. The value range for the start time and end time is 00:00 to 23:59.

username *username*: Specifies the username of a portal user, a case-sensitive string of 1 to 253 characters. The username cannot contain the domain name.

Examples

Display all portal authentication failure records.

```
<Sysname> display portal auth-fail-record all
Total authentication fail records: 2
User name              : test@abc
User MAC               : 0016-ecb7-a879
Interface              : Vlan-interface100
User IP address        : 192.168.0.188
```

```
Auth failure time      : 2016-03-04 16:49:07
Auth failure reason    : Authorization information does not exist.

User name              : coco
User MAC               : 0016-ecb7-a235
Interface              : Vlan-interface100
User IP address        : 192.168.0.10
Auth failure time      : 2016-03-04 16:50:07
Auth failure reason    : Authorization information does not exist.
```

Display portal authentication failure records for the portal user whose IPv4 address is **192.168.0.8**.

```
<Sysname> display portal auth-fail-record ip 192.168.0.188
User name              : test@abc
User MAC               : 0016-ecb7-a879
Interface              : Vlan-interface100
User IP address        : 192.168.0.188
Auth failure time      : 2016-03-04 16:49:07
Auth failure reason    : Authorization information does not exist.
```

Display portal authentication failure records for the portal user whose IPv6 address is **2000::2**.

```
<Sysname> display portal auth-fail-record ipv6 2000::2
User name              : test@abc
User MAC               : 0016-ecb7-a879
Interface              : Vlan-interface100
User IP address        : 2000::2
Auth failure time      : 2016-03-04 16:49:07
Auth failure reason    : Authorization information does not exist.
```

Display portal authentication failure records for the portal user whose username is **chap1**.

```
<Sysname> display portal auth-fail-record username chap1
User name              : chap1
User MAC               : 0016-ecb7-a879
Interface              : Vlan-interface100
User IP address        : 192.168.0.188
Auth failure time      : 2016-03-04 16:49:07
Auth failure reason    : Authorization information does not exist.
```

Display portal authentication failure records with the failure time in the range of 2016/3/4 14:20 to 2016/3/4 14:23.

```
<Sysname> display portal auth-fail-record start-time 2016/3/4 14:20 end-time 2016/3/4
14:23
User name              : chap1
User MAC               : 0016-ecb7-a879
Interface              : Vlan-interface100
User IP address        : 192.168.0.188
Auth failure time      : 2016-03-04 14:22:25
Auth failure reason    : Authorization information does not exist.
```

Table 4 Command output

Field	Description
Total authentication fail records	Total number of portal authentication failure records.

Field	Description
User name	Username of the portal user.
User MAC	MAC address of the portal user.
Interface	Access interface of the portal user.
User IP address	IP address of the portal user.
Auth failure time	Time when the portal user failed authentication, in the format of YYYY/MM/DD hh:mm:ss.
Auth failure reason	Reason why the user failed portal authentication.

Related commands

portal auth-fail-record enable

reset portal auth-fail-record

display portal captive-bypass statistics

Use **display portal captive-bypass statistics** to display packet statistics for portal captive-bypass.

Syntax

display portal captive-bypass statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays portal captive-bypass packet statistics on all member devices.

Examples

Display portal captive-bypass packets on the specified slot.

```
<Sysname> display portal captive-bypass statistics slot 1
Slot 1:
User type       Packets
iOS             1
Android         0
```

Table 5 Command output

Field	Description
User type	Type of users: • iOS.

Field	Description
	• Android.
Packets	Number of portal captive-bypass packets sent to the users.

Related commands

captive-bypass enable

display portal dns free-rule-host

Use **display portal dns free-rule-host** to display IP addresses corresponding to host names in destination-based portal-free rules.

Syntax

display portal dns free-rule-host [*host-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

host-name: Specifies a host by its name, a case-insensitive string of 1 to 253 characters. Valid characters are letters, digits, hyphens (-), underscores (_), dots (.), and wildcards (asterisks *). The host name cannot be **ip** or **ipv6**. If you do not specify a host name, this command displays IP addresses corresponding to all host names in destination-based portal-free rules.

Examples

Display IP addresses corresponding to host name **http://www.baidu.com/** in a destination-based portal-free rule.

```
<Sysname> display portal dns free-rule-host www.baidu.com
 Host name                      IP
 www.baidu.com                  10.10.10.10
```

Display IP addresses corresponding to host name ***abc.com** in a destination-based portal-free rule.

```
<Sysname> display portal dns free-rule-host *abc.com
 Host name                      IP
 *abc.com                       12.12.12.12
                                111.8.33.100
                                3.3.3.3
```

Table 6 Command output

Field	Description
Host name	Host name specified in a destination-based portal-free rule.
IP	IP address corresponding to the host name.

display portal dns redirect-rule-host

Use **display portal dns redirect-rule-host** to display IP addresses resolved by host names in destination-based portal redirection rules.

Syntax

display portal dns redirect-rule-host [*host-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

host-name: Specifies a host name, a case-insensitive string of 1 to 253 characters. Valid characters include letters, digits, hyphens (-), underscores (_), and dots (.). If you do not specify a host name, this command displays IP addresses resolved by all host names in all destination-based portal redirection rules.

Usage guidelines

For destination-based portal redirection rules that specify host names, the device will resolve the host names to IP addresses. Use this command to display IP addresses that are resolved by the host names in redirection rules.

The system can save a maximum of 16 resolved IPv4 addresses and 16 resolved IPv6 addresses. If the maximum number is reached, the new resolved IP address will override the oldest resolved IP address.

Examples

Display IP addresses resolved by host name **www.baidu.com** in a destination-based portal redirection rule.

```
<Sysname> display portal dns redirect-rule-host www.baidu.com
 Host name                      IP
 www.baidu.com                  10.10.10.10
```

Display IP addresses resolved by host name **www.abc.com** in a destination-based portal redirection rule.

```
<Sysname> display portal dns redirect-rule-host www.abc.com
 Host name                      IP
 www.abc.com                    12.12.12.12
                                111.8.33.100
                                3.3.3.3
```

Display IP addresses resolved by all host names in all destination-based portal redirection rules.

```
<Sysname> display portal dns redirect-rule-host
 Host name                      IP
www.baidu.com                   10.10.10.10
 www.abc.com                    12.12.12.12
                                111.8.33.100
                                3.3.3.3
```

Table 7 Command output

Field	Description
Host name	Host name in a destination-based portal redirection rule.
IP	IP address resolved by the host name.

Related commands

portal redirect-rule destination

display portal extend-auth-server

Use **display portal extend-auth-server** to display information about third-party authentication servers.

Syntax

display portal extend-auth-server { **all** | **facebook** | **mail** | **qq** | **wechat** }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

all: Specifies all third-party authentication servers.

facebook: Specifies the Facebook authentication server.

mail: Specifies the email authentication server.

qq: Specifies the QQ authentication server.

wechat: Specifies the WeChat authentication server.

Examples

Display information about all third-party authentication servers.

```
<Sysname> display portal extend-auth-server all
Portal extend-auth-server: qq
   Authentication URL : http://graph.qq.com
   APP ID             : 101235509
   APP key            : ******
   Redirect URL       : http://oauthindev.nsfocus.com.cn/portal/qqlogin.html
Portal extend-auth-server: mail
   Mail protocol      : POP3
   Mail domain name   : @qq.com
Portal extend-auth-server: wechat
  App ID              : wx23fb4aaf04b8491e
  App key             : ******
  App secret          : ******
```

```
  Subscribe-required : Enabled
  Shop ID            : 6747662
Portal extend-auth-server: facebook
   Authentication URL : https://graph.facebook.com
   APP ID             : 123456789
   APP key            : ******
   Redirect URL       : http://oauthindev.nsfocus.com.cn/portal/fblogin.html
```

Table 8 Command output

Field	Description
Portal extend-auth-server	Type of the third-party authentication server.
Authentication URL	URL of the third-party authentication server.
APP ID	App ID for the third-party authentication.
APP key	App key for the third-party authentication.
APP secret	App secret for WeChat authentication.
Subscribe-required	Status of the subscribe-required feature: • Enabled. • Disabled.
Redirect URL	URL to which portal users are redirected after they pass third-party authentication.
Mail protocol	Protocols of the email authentication service.
Mail domain name	Email domain name of the email authentication service.
Shop ID	ID of the shop where the device is deployed as a portal device for WeChat authentication.

Related commands

portal extend-auth-server

display portal local-binding mac-address

Use **display portal local-binding mac-address** to display information about local MAC-account binding entries on the local MAC binding server.

Syntax

display portal local-binding mac-address { *mac-address* | **all** }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

mac-address: Specifies the MAC address of a portal user, in the format H-H-H.

all: Specifies all local MAC-account binding entries.

Examples

Display information about all local MAC-account binding entries.

```
<Sysname> display portal local-binding mac-address all
Total MAC addresses: 5
MAC address               Username            Aging(hh:mm:ss)
0015-e9a6-7cfe            wlan_user1          00:41:38
0000-e27c-6e80            wlan_user2          00:41:38
000f-e212-ff01            wlan_user3          00:41:38
001c-f08f-f804            wlan_user4          00:41:38
000f-e233-9000            wlan_user5          00:41:38
```

Display information about the local MAC-account binding entry for the user with MAC address 0015-e9a6-7cfe.

```
<Sysname> display portal local-binding mac-address 0015-e9a6-7cfe
Total MAC addresses: 1
MAC address               Username            Aging(hh:mm:ss)
0015-e9a6-7cfe            wlan_user1          00:41:38
```

Table 9 Command output

Field	Description
MAC address	MAC address of a portal user.
Username	Username of a portal user.
Aging	Remaining lifetime of the local MAC-account binding entry.

Related commands

local-binding enable

display portal logout-record

Use **display portal logout-record** to display portal user offline records.

Syntax

display portal logout-record { **all** | **ipv4** *ipv4-address* | **ipv6** *ipv6-address* | **start-time** *start-date start-time* **end-time** *end-date end-time* | **username** *username* }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

all: Specifies all portal user offline records.

ipv4 *ipv4-address*: Specifies the IPv4 address of a portal user.

ipv6 *ipv6-address*: Specifies the IPv6 address of a portal user.

start-time *start-date start-time* **end-time** *end-date end-time*: Specifies a time range. The start date and end date must be in the format of MM/DD/YYYY or YYYY/MM/DD. The value range for MM is 1 to 12. The value range for DD varies with the specified month. The value range for YYYY is 1970 to 2037. The start time and end time must be in the format of hh:mm. The value range for the start time and end time is 00:00 to 23:59.

username *username*: Specifies the username of a portal user, a case-sensitive string of 1 to 253 characters. The username cannot contain the domain name.

Examples

Display all portal user offline records.

```
<Sysname> display portal logout-record all
Total logout records: 2
User name              : test@abc
User MAC               : 0016-ecb7-a879
Interface              : Vlan-interface100
User IP address        : 192.168.0.8
User login time        : 2016-03-04 14:20:19
User logout time       : 2016-03-04 14:22:05
Logout reason          : Admin Reset

User name              : coco
User MAC               : 0016-ecb7-a235
Interface              : Vlan-interface100
User IP address        : 192.168.0.10
User login time        : 2016-03-04 14:10:15
User offline time      : 2016-03-04 14:22:05
Offline reason         : Admin Reset
```

Display offline records for the portal user whose IP address is **192.168.0.8**.

```
<Sysname> display portal logout-record ip 192.168.0.8
User name              : test@abc
User MAC               : 0016-ecb7-a879
Interface              : Vlan-interface100
User IP address        : 192.168.0.8
User login time        : 2016-03-04 14:26:12
User logout time       : 2016-03-04 14:27:35
Logout reason          : Admin Reset
```

Display offline records for the portal user whose username is **chap1**.

```
<Sysname> display portal logout-record username chap1
User name              : chap1
User MAC               : 0016-ecb7-a879
Interface              : Vlan-interface100
User IP address        : 192.168.0.8
User login time        : 2016-03-04 17:20:19
User logout time       : 2016-03-04 17:22:05
Logout reason          : Admin Reset
```

Display portal user offline records with the logout time in the range of 2016/3/4 14:20 to 2016/3/4 14:23.

```
<Sysname> display portal logout-record start-time 2016/3/4 14:20 end-time 2016/3/4 14:23
User name              : test@abc
User MAC               : 0016-ecb7-a879
Interface              : Vlan-interface100
User IP address        : 192.168.0.8
User login time        : 2016-03-04 14:20:19
User logout time       : 2016-03-04 14:22:05
Logout reason          : Admin Reset
```

Table 10 Command output

Field	Description
Total logout records	Total number of portal user offline records.
User name	Username of the portal user.
User MAC	MAC address of the portal user.
Interface	Access interface of the portal user.
User IP address	IP address of the portal user.
User login time	Time when the portal user came online, in the format of YYYY-MM-DD hh:mm:ss.
User logout time	Time when the portal user went offline, in the format of YYYY-MM-DD hh:mm:ss.
Logout reason	Reason why the portal user went offline: • User Request. • Carrier Lost. • Service Lost. • Admin Reset. • NAS Request. • Idle Timeout. • Port Suspended. • Port Error. • Admin Reboot. • Session Timeout. • User Error. • Service Unavailable. • NAS Error. • Other Errors.

Related commands

portal logout-record enable

reset portal logout-record

display portal mac-trigger user

Use **display portal mac-trigger user** to display information about MAC-trigger authentication users (portal users that perform MAC-trigger authentication).

Syntax

display portal mac-trigger user { **all** | **ip** *ipv4-address* | **mac** *mac-address* }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

all: Specifies all MAC-trigger authentication users.

ip *ipv4-address*: Specifies a MAC-trigger authentication user by its IP address.

mac *mac-address*: Specifies a MAC-trigger authentication user by its MAC address, in the format of H-H-H.

Examples

Display information about all MAC-trigger authentication users.

```
<Sysname> display portal mac-trigger user all
Total portal mac-trigger users: 8
MAC address      IP address     VLAN ID   Interface          Traffic(Bytes)  State
0050-ba50-732a   1.1.1.6        1         Vlan-interface1    0               NOBIND
0050-ba50-7328   1.1.1.4        1         Vlan-interface1    0               NOBIND
0050-ba50-7326   1.1.1.2        1         Vlan-interface1    0               NOBIND
0050-ba50-732c   1.1.1.8        1         Vlan-interface1    0               NOBIND
0050-ba50-7329   1.1.1.5        1         Vlan-interface1    0               NOBIND
```

Display information about the MAC-trigger authentication user whose MAC address is 0050-ba50-7777.

```
<Sysname> display portal mac-trigger user mac 0050-ba50-7777
MAC address      IP address     VLAN ID   Interface          Traffic(Bytes)  State
0050-ba50-777    1.1.5.83       1         Vlan-interface1    0               NOBIND
```

Display information about the MAC-trigger authentication user whose IP address is 1.1.2.126.

```
<Sysname> display portal mac-trigger user ip 1.1.2.126
MAC address      IP address     VLAN ID   Interface          Traffic(Bytes)  State
0050-ba50-74a2   1.1.2.126      1         Vlan-interface1    0               NOBIND
```

Table 11 Command output

Field	Description
MAC address	MAC address of the user.
IP address	IP address of the user.
VLAN ID	ID of the VLAN to which the user belongs.
Interface	Interface through which the user accesses the network.
Traffic(Bytes)	Traffic of the user, in bytes.
State	Status of the user: • **DEFAULT**—The user's traffic is below the free-traffic

Field	Description
	threshold and the user can access the network without authentication. • **WAIT**—The binding status between the user's MAC address and account is being queried. • **NOBIND**—The user's MAC address is not bound with the user's account. • **BIND**—The user's MAC address is bound with the user's account. • **DISABLE**—The MAC-trigger entry for the user is deleted on the device.

Related commands

portal apply mac-trigger-server

portal mac-trigger-server

display portal mac-trigger-server

Use **display portal mac-trigger-server** to display information about MAC binding servers.

Syntax

display portal mac-trigger-server { **all** | **name** *server-name* }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

all: Specifies all MAC binding servers.

name *server-name*: Specifies a MAC binding server by its name, a case-sensitive string of 1 to 32 characters.

Examples

Display information about all MAC binding servers.

```
<Sysname> display portal mac-trigger-server all
Portal mac-trigger server name: ms1
  Version                    : 2.0
  Server type                : CMCC
  IP                         : 10.1.1.1
  Port                       : 100
  VPN instance               : Not configured
  Aging time                 : 120 seconds
  Free-traffic threshold     : 1000 bytes
  NAS-Port-Type              : 255
```

```
  Binding retry times        : 5
  Binding retry interval     : 2 seconds
  Authentication timeout     : 5 minutes
  Local-binding              : Disabled
  Local-binding aging time   : 12 minutes
  aaa-fail nobinding         : Disabled
  Excluded attribute list    : 1
  Cloud-binding              : Disabled
  Cloud server URL           : Not configured
Portal mac-trigger server name: mts
  Version                    : 1.0
  Server type                : IMC
  IP                         : 4.4.4.2
  Port                       : 50100
  VPN instance               : Not configured
  Aging time                 : 300 seconds
  Free-traffic threshold     : 0 bytes
  NAS-Port-Type              : Not configured
  Binding retry times        : 3
  Binding retry interval     : 1 seconds
  Authentication timeout     : 3 minutes
  Local-binding              : Disabled
  Local-binding aging-time   : 12 minutes
  aaa-fail nobinding         : Disabled
  Excluded attribute list    : 1
  Cloud-binding              : Disabled
  Cloud server URL           : Not configured
```

Display information about MAC binding server **ms1**.

```
<Sysname> display portal mac-trigger-server name ms1
Portal mac-trigger server name: ms1
  Version                    : 2.0
  Server type                : CMCC
  IP                         : 10.1.1.1
  Port                       : 100
  VPN instance               : Not configured
  Aging time                 : 120 seconds
  Free-traffic threshold     : 1000 bytes
  NAS-Port-Type              : 255
  Binding retry times        : 5
  Binding retry interval     : 2 seconds
  Authentication timeout     : 5 minutes
  Local-binding              : Disabled
  Local-binding aging-time   : 12 minutes
  aaa-fail nobinding         : Disabled
  Excluded attribute list    : 1
  Cloud-binding              : Disabled
  Cloud server URL           : Not configured
```

Table 12 Command output

Field	Description
Portal mac trigger server name	Name of the MAC binding server.
Version	Version of the portal protocol: • **1.0**—Version 1. • **2.0**—Version 2. • **3.0**—Version 3.
Server type	Type of the MAC binding server: • **CMCC**—CMCC server. • **IMC**—IMC server.
IP	IP address of the MAC binding server.
Port	UDP port number on which the MAC binding server listens for MAC binding query packets.
VPN instance	MPLS L3VPN where the MAC binding server resides.
Aging time	Aging time in seconds. A MAC-trigger entry is aged out when the aging time expires.
Free-traffic threshold	Free-traffic threshold in bytes. If a user's traffic is below the threshold, the user can access the network without authentication.
NAS-Port-Type	NAS-Port-Type attribute value in RADIUS request packets sent to the RADIUS server.
Binding retry times	Maximum number of attempts for sending MAC binding queries to the MAC binding server.
Binding retry interval	Interval at which the device sends MAC binding queries to the MAC binding server.
Authentication timeout	Maximum amount of time that the device waits for portal authentication to complete after receiving the MAC binding query response.
Excluded attribute list	Numbers of attributes excluded from portal protocol packets.
Local-binding	Status of local MAC-trigger authentication: • Disabled. • Enabled.
Local-binding aging-time	Aging time for local MAC-account binding entries, in minutes.
Cloud-binding	Status of cloud MAC-trigger authentication: • Disabled. • Enabled.
Cloud server URL	URL of the cloud portal authentication server.
aaa-fail nobinding	Status of the AAA failure unbinding feature: • Disabled. • Enabled.

display portal packet statistics

Use **`display portal packet statistics`** to display packet statistics for portal authentication servers and MAC binding servers.

Syntax

display portal packet statistics [**extend-auth-server** { **cloud** | **facebook** | **mail** | **qq** | **wechat** } | **mac-trigger-server** *server-name* | **server** *server-name*] *

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

extend-auth-server: Specifies a third-party authentication server.

cloud: Specifies the cloud authentication server.

facebook: Specifies the Facebook authentication server.

mail: Specifies the email authentication server.

qq: Specifies the QQ authentication server.

wechat: Specifies the WeChat authentication server.

mac-trigger-server *server-name*: Specifies a MAC binding server by its name, a case-sensitive string of 1 to 32 characters.

server *server-name*: Specifies a portal authentication server by its name, a case-sensitive string of 1 to 32 characters.

Usage guidelines

If you do not specify any parameters, this command displays packet statistics for all third-party authentication servers, portal authentication servers, and MAC binding servers.

Examples

Display packet statistics for portal authentication server **pts**.

```
<Sysname> display portal packet statistics server pts
 Portal server :  pts
 Invalid packets: 0
 Pkt-Type                          Total    Drops    Errors
 REQ_CHALLENGE                     3        0        0
 ACK_CHALLENGE                     3        0        0
 REQ_AUTH                          3        0        0
 ACK_AUTH                          3        0        0
 REQ_LOGOUT                        1        0        0
 ACK_LOGOUT                        1        0        0
 AFF_ACK_AUTH                      3        0        0
 NTF_LOGOUT                        1        0        0
 REQ_INFO                          6        0        0
 ACK_INFO                          6        0        0
 NTF_USERDISCOVER                  0        0        0
 NTF_USERIPCHANGE                  0        0        0
```

```
 AFF_NTF_USERIPCHAN                  0        0        0
 ACK_NTF_LOGOUT                      1        0        0
 NTF_HEARTBEAT                       0        0        0
 NTF_USER_HEARTBEAT                  2        0        0
 ACK_NTF_USER_HEARTBEAT              0        0        0
 NTF_CHALLENGE                       0        0        0
 NTF_USER_NOTIFY                     0        0        0
 AFF_NTF_USER_NOTIFY                 0        0        0
```

Display packet statistics for MAC binding server **newpt**.

```
<Sysname> display portal packet statistics mac-trigger-server newpt
 MAC-trigger server: newpt
 Invalid packets: 0
 Pkt-Type                            Total    Drops    Errors
 REQ_MACBIND                         1        0        0
 ACK_MACBIND                         1        0        0
 NTF_MTUSER_LOGON                    1        0        0
 NTF_MTUSER_LOGOUT                   0        0        0
 REQ_MTUSER_OFFLINE                  0        0        0
```

Display packet statistics for the Oasis cloud authentication server.

```
<Sysname> display portal packet statistics extend-auth-server cloud
Extend-auth server:  cloud
 Update interval:  60
  Pkt-Type               Success    Error      Timeout    Conn-failure
  REQ_ACCESSTOKEN        1          0          0          0
  REQ_USERINFO           1          0          0          0
  RESP_ACCESSTOKEN       1          0          0          0
  RESP_USERINFO          1          0          0          0
  POST_ONLINEDATA        0          0          0          0
  RESP_ONLINEDATA        0          0          0          0
  POST_OFFLINEUSER       1          0          0          0
  REPORT_ONLINEUSER      1          0          0          0
  REQ_CLOUDBIND          1          0          0          0
  RESP_CLOUDBIND         1          0          0          0
  REQ_BINDUSERINFO       0          0          0          0
  RESP_BINDUSERINFO      0          0          0          0
  AUTHENTICATION         0          1          0          0
```

Table 13 Command output

Field	Description
Portal server	Name of the portal authentication server.
Invalid packets	Number of invalid packets.
Pkt-Type	Packet type.
Total	Total number of packets.
Drops	Number of dropped packets.
Errors	Number of packets that carry error information.
REQ_CHALLENGE	Challenge request packet the portal authentication server sent to the

Field	Description
	access device.
ACK_CHALLENGE	Challenge acknowledgment packet the access device sent to the portal authentication server.
REQ_AUTH	Authentication request packet the portal authentication server sent to the access device.
ACK_AUTH	Authentication acknowledgment packet the access device sent to the portal authentication server.
REQ_LOGOUT	Logout request packet the portal authentication server sent to the access device.
ACK_LOGOUT	Logout acknowledgment packet the access device sent to the portal authentication server.
AFF_ACK_AUTH	Affirmation packet the portal authentication server sent to the access device after receiving an authentication acknowledgment packet.
NTF_LOGOUT	Forced logout notification packet the access device sent to the portal authentication server.
REQ_INFO	Information request packet.
ACK_INFO	Information acknowledgment packet.
NTF_USERDISCOVER	User discovery notification packet the portal authentication server sent to the access device.
NTF_USERIPCHANGE	User IP change notification packet the access device sent to the portal authentication server.
AFF_NTF_USERIPCHAN	User IP change success notification packet the portal authentication server sent to the access device.
ACK_NTF_LOGOUT	Forced logout acknowledgment packet the portal authentication server sent to the access device.
NTF_HEARTBEAT	Server heartbeat packet the portal authentication server periodically sent to the access device.
NTF_USER_HEARTBEAT	User synchronization packet the portal authentication server sent to the access device.
ACK_NTF_USER_HEARTBEAT	User synchronization acknowledgment packet the access device sent to the portal authentication server.
NTF_CHALLENGE	Challenge request packet the access device sent to the portal authentication server.
NTF_USER_NOTIFY	User information notification packet the access device sent to the portal authentication server.
AFF_NTF_USER_NOTIFY	NTF_USER_NOTIFY acknowledgment packet the portal authentication server sent to the access device.
MAC-trigger server	Name of the MAC binding server.
REQ MACBIND	MAC binding request packet the access device sent to the MAC binding server.
ACK_MACBIND	MAC binding acknowledgment packet the MAC binding server sent to the access device.
NTF_MTUSER_LOGON	User logon notification packet the access device sent to the MAC binding server.
NTF_MTUSER_LOGOUT	User logout notification packet the access device sent to the MAC

Field	Description
	binding server.
REQ_MTUSER_OFFLINE	Forced offline request packet the MAC binding server sent to the access device.
Extend-auth server	Type of the third-party authentication server: • **qq**—QQ authentication server. • **mail**—Email authentication server. • **wechat**—WeChat authentication server. • **cloud**—Cloud authentication server. • **facebook**—Facebook authentication server.
Update interval	Interval at which the device sends online user information to the Oasis cloud server, in seconds. This field is displayed only if the third-party authentication server is the Oasis cloud authentication server.
Success	Number of packets that have been successfully sent or received.
Timeout	Number of packets that timed out of establishing a connection to the third-party authentication server.
Conn-failure	Number of packets that failed to establish a connection to the third-party authentication server.
Deny	Number of packets denied access to the third-party authentication server. This field is displayed only if the third-party authentication server is the email authentication server.
REQ_ACCESSTOKEN	Access token request packet the access device sent to the third-party authentication server. This field is displayed only if the third-party authentication server is QQ, Facebook, Oasis cloud, or WeChat authentication server.
REQ_OPENID	Open ID request packet the access device sent to the third-party authentication server. This field is displayed only if the third-party authentication server is the QQ authentication server.
REQ_USERINFO	User information request packet the access device sent to the third-party authentication server. This field is displayed only if the third-party authentication server is the QQ, Facebook, Oasis cloud, or WeChat authentication server.
RESP_ACCESSTOKEN	Access token response packet the access device received from the third-party authentication server. This field is displayed only if the third-party authentication server is the QQ, Facebook, Oasis cloud, or WeChat authentication server.
RESP_OPNEID	Open ID response packet the access device received from the third-party authentication server. This field is displayed only if the third-party authentication server is the QQ authentication server.
RESP_USERINFO	User information response packet the access device received from the third-party authentication server. This field is displayed only if the third-party authentication server is the QQ, Facebook, Oasis cloud, or WeChat authentication server.
REQ_POP3	POP3 authentication request packet the access device sent to the third-party authentication server.

Field	Description
	This field is displayed only if the third-party authentication server is the email authentication server.
REQ_IMAP	IMAP authentication request packet the access device sent to the third-party authentication server. This field is displayed only if the third-party authentication server is the email authentication server.
POST_ONLINEDATA	Cloud user information request packet the access device sent to the third-party authentication server. This field is displayed only if the third-party authentication server is the Oasis cloud authentication server.
RESP_ONLINEDATA	Cloud user information response packet the access device received from the third-party authentication server. This field is displayed only if the third-party authentication server is the Oasis cloud authentication server.
POST_OFFLINEUSER	Cloud user offline packet the access device sent to the third-party authentication server. This field is displayed only if the third-party authentication server is the Oasis cloud or WeChat authentication server.
REPORT_ONLINEUSER	Cloud user online packet the access device sent to the third-party authentication server. This field is displayed only if the third-party authentication server is Oasis cloud or WeChat authentication server.
REQ_CLOUDBIND	Cloud user binding status query request that the access device sent to the third-party authentication server. This field is displayed only if the third-party authentication server is Oasis cloud authentication server.
RESP_CLOUDBIND	Cloud user binding status query response that the access device received from the third-party authentication server. This field is displayed only if the third-party authentication server is Oasis cloud authentication server.
REQ_BINDUSERINFO	Cloud user information request packet that the access device sent to the third-party authentication server. This field is displayed only if the third-party authentication server is the Oasis cloud authentication server.
RESP_BINDUSERINFO	Cloud user information response packet that the access device received from the third-party authentication server. This field is displayed only if the third-party authentication server is the Oasis cloud authentication server.
AUTHENTICATION	Result of third-party authentication.

Related commands

`reset portal packet statistics`

display portal permit-rule statistics

Use **`display portal permit-rule statistics`** to display statistics for portal permit rules.

Syntax

`display portal permit-rule statistics`

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Usage guidelines

Portal permit rules refer to category-1 and category-2 portal filtering rules, which permit user packets to pass.

Examples

Display statistics for portal permit rules.

```
<Sysname> display portal permit-rule statistics
Interface            Free rules          Fuzzy rules           User rules
Vlan-interface30     2                   5                     10
Vlan-interface30     2                   3                     6
```

Table 14 Command output

Field	Description
Interface	Interface on which portal permit rules are used.
Free rules	Number of permit rules generated based on configured portal-free rules, excluding permit rules generated based on fuzzy matches of destination-based portal-free rules.
Fuzzy rules	Number of permit rules generated based on fuzzy matches of destination-based portal-free rules.
User rules	Number of permit rules generated after portal users pass authentication.

display portal redirect session

Use **display portal redirect session** to display redirect session statistics for online portal users.

Syntax

display portal redirect session [**ip** *ipv4-address* | **ipv6** *ipv6-address*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ip *ipv4-address*: Specifies a portal user by its IPv4 address.

ipv6 *ipv6-address*: Specifies a portal user by its IPv6 address.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays redirect session statistics for online portal users on all member devices.

Usage guidelines

If you do not specify a user IPv4 or IPv6 address, this command displays redirect session statistics for all online portal users.

Examples

Display redirect session statistics for all online portal users on the specified slot.

```
<Sysname> display portal redirect session slot 0
Total HTTP sessions: 40
Total HTTP rejected: 2542
Total HTTPS sessions: 40
Total HTTPS rejected: 0
IP: 192.168.0.1
  HTTP sessions: 20
  HTTP rejected: 10
  HTTPS sessions: 20
  HTTPS rejected: 40
IP: 192.168.0.2
  HTTP sessions: 20
  HTTP rejected: 8
  HTTPS sessions: 20
  HTTPS rejected: 40
```

Display redirect session statistics for online portal user at 192.168.0.2 on the specified slot.

```
<Sysname> display portal redirect session ip 192.168.0.2 slot 0
IP: 192.168.0.2
  HTTP sessions: 128
  HTTP rejected: 10
  HTTPS sessions: 0
  HTTPS rejected: 0
```

Table 15 Command output

Field	Description
Total HTTP sessions	Total number of HTTP redirect sessions.
Total HTTP rejected	Total number of discarded HTTP redirect session requests.
Total HTTPS sessions	Total number of HTTPS redirect sessions.
Total HTTPS rejected	Total number of discarded HTTPS redirect session requests.
IP	IP address of the online portal user.
HTTP sessions	Number of HTTP redirect sessions for the user.
HTTP rejected	Number of discarded HTTP redirect requests for the user.
HTTPS sessions	Number of HTTPS redirect sessions for the user.

Field	Description
HTTPS rejected	Number of discarded HTTPS redirect requests for the user.

Related commands

portal redirect max-session

portal redirect max-session per-user

display portal redirect session-record

Use **display portal redirect session-record** to display history records about portal redirect sessions.

Syntax

display portal redirect session-record [**start-time** *start-date start-time*] [**end-time** *end-date end-time*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

start-time *start-date start-time*: Specifies the start time of a time range. The start date must be in the format of MM/DD/YYYY or YYYY/MM/DD. The value range for MM is 1 to 12. The value range for DD varies with the specified month. The value range for YYYY is 1970 to 2037. The start time must be in the format of hh:mm. The value range for the start time is 00:00 to 23:59. If you do not specify a start time, the time range starts when portal authentication was enabled.

end-time *end-date end-time*: Specifies the end time of a time range. The end date must be in the format of MM/DD/YYYY or YYYY/MM/DD. The value range for MM is 1 to 12. The value range for DD varies with the specified month. The value range for YYYY is 1970 to 2037. The end time must be in the format of hh:mm. The value range for the end time is 00:00 to 23:59. If you do not specify an end time, the time range ends with the current time.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays history records about portal redirect sessions on all member devices.

Usage guidelines

The device records statistics about portal redirect sessions on a per minute basis since portal authentication is enabled. The device only keeps records generated within the most recent 24 hours. Twenty-four hours later, a new record will override the oldest record.

Examples

Display history records about portal redirect sessions in the time range from 2019/3/20 14:40 to now.

```
<Sysname> display portal redirect session-record start-time 2019/3/20 14:40 slot 0

Time              HTTP sessions  HTTP rejected  HTTPS sessions  HTTPS rejected
```

```
2019/03/20 14:40   1             0             21            1
2019/03/20 14:41   2             0             21            1
2019/03/20 14:42   13            1             31            1
2019/03/20 14:43   14            1             0             0
```

Table 16 Command output

Field	Description
Time	Time when the record was generated.
HTTP sessions	Number of HTTP redirect sessions for all portal users.
HTTP rejected	Number of discarded HTTP redirect session requests for all portal users.
HTTPS sessions	Number of HTTPS redirect sessions for all portal users.
HTTPS rejected	Number of discarded HTTPS redirect session requests for all portal users.

Related commands

reset portal redirect session-record

display portal redirect session-statistics

Use **display portal redirect session-statistics** to display summary statistics about portal redirect sessions.

Syntax

display portal redirect session-statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays summary statistics about portal redirect sessions on all member devices.

Examples

Display summary statistics about portal redirect sessions on the specified slot.

```
<Sysname> display portal redirect session-statistics slot 0
  HTTP sessions  HTTP rejected  HTTPS sessions  HTTPS rejected
  30             2              73              3
```

Table 17 Command output

Field	Description
HTTP sessions	Number of HTTP redirect sessions for all portal users.
HTTP rejected	Number of rejected HTTP redirect session requests for all portal users.

HTTPS sessions	Number of HTTPS redirect sessions for all portal users.
HTTPS rejected	Number of rejected HTTPS redirect session requests for all portal users.

Related commands

reset portal redirect session-statistics

display portal redirect statistics

Use **display portal redirect statistics** to display portal redirect packet statistics.

Syntax

display portal redirect statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays portal redirect packet statistics on all member devices.

Examples

Display portal redirect packet statistics on the specified slot.

```
<Sysname> display portal redirect statistics slot 1
 HTTP requests  HTTP responses  HTTPS requests  HTTPS responses
 1              1               1               1
```

Table 18 Command output

Field	Description
HTTP requests	Total number of HTTP redirect requests.
HTTP responses	Total number of HTTP redirect responses.
HTTPS requests	Total number of HTTPS redirect requests.
HTTPS responses	Total number of HTTPS redirect responses.

Related commands

reset portal redirect statistics

display portal rule

Use **display portal rule** to display portal filtering rules.

Syntax

display portal rule { **all** | **dynamic** | **static** } **interface** *interface-type interface-number* [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

all: Displays all portal filtering rules, including dynamic and static portal filtering rules.

dynamic: Displays dynamic portal filtering rules, which are generated after users pass portal authentication. These rules allow packets with specific source IP addresses to pass the interface.

static: Displays static portal filtering rules, which are generated after portal authentication is enabled. The interface filters packets by these rules when portal authentication is enabled.

interface *interface-type interface-number*: Specifies an interface by its type and number.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays portal filtering rules on all member devices.

Examples

Table 19 Command output

Field	Description
Rule	Number of the portal rule. IPv4 portal filtering rules and IPv6 portal filtering rules are numbered separately.
Type	Type of the portal filtering rule: • **Static**—Static portal rule. • **Dynamic**—Dynamic portal rule.
Action	Action triggered by the portal filtering rule: • **Permit**—The interface allows packets to pass. • **Forbid**—The interface forbids packets to pass. • **Redirect**—The interface redirects packets. • **Deny**—The interface denies packets. • **Match pre-auth ACL**—The interface matches packets against the authorized ACL rules in the preauthentication domain.
Protocol	Transport layer protocol permitted by the portal filtering rule: • **Any**—Permits any transport layer protocol. • **TCP**—Permits TCP. • **UDP**—Permits UDP.
Status	Status of the portal filtering rule: • **Active**—The portal rule is effective. • **Unactuated**—The portal rule is not activated.
Source	Source information of the portal filtering rule.

Field	Description
IP	Source IPv4 or IPv6 address. If the IPv6 address of a portal user changes after the user has come online, this field displays colons (**::**). This value indicates that no IP address is specified in the portal filtering rule.
Mask	Subnet mask of the source IPv4 address.
Prefix length	Prefix length of the source IPv6 address.
Port	Source transport layer port number.
MAC	Source MAC address.
Interface	Layer 2 or Layer 3 interface on which the portal rule is implemented.
VLAN	Source VLAN ID.
Protocol	Transport layer protocol of the portal redirect rule. This field always displays **TCP**.
Destination	Destination information of the portal filtering rule.
IP	Destination IP address.
Port	Destination transport layer port number.
Mask	Subnet mask of the destination IPv4 address.
Prefix length	Prefix length of the destination IPv6 address.
Author ACL	Authorized ACL assigned to authenticated portal users. This field is displayed only for a dynamic portal filtering rule.
Pre-auth ACL	Authorized ACL assigned to preauthentication portal users. This field is displayed only for the **Match pre-auth ACL** action.
Number	Number of the authorized ACL. This field displays **N/A** if the AAA server does not assign an ACL.

display portal safe-redirect statistics

Use **display portal safe-redirect statistics** to display portal safe-redirect packet statistics.

Syntax

display portal safe-redirect statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays statistics on all member devices.

Examples

Display portal safe-redirect packet statistics on the specified slot.

```
<Sysname> display portal safe-redirect statistics slot 1
Slot 1:
Redirect statistics:
  Success: 7
  Failure: 8
  Total  : 15

Method statistics:
  Get    : 11
  Post   : 1
  Others : 3

Default-action statistics:
  Permit: 1
  Forbid: 0

User agent statistics:
  Safari: 3
  Chrome: 2

Forbidden User URL statistics:
  www.qq.com: 4

Forbidden filename extension statistics:
  .jpg: 0
```

Table 20 Command output

Field	Description
Success	Number of packets redirected successfully.
Failure	Number of packets failed redirection.
Total	Total number of packets.
Method statistics	Statistics of HTTP request methods.
Get	Number of packets with the **GET** request method.
Post	Number of packets with the **POST** request method.
Other	Number of packets with other request methods.
User agent statistics	Browser types (in HTTP User Agent) allowed by portal safe-redirect, and packet statistics for the browsers.
Forbidden URL statistics	URLs forbidden by portal safe-redirect, and statistics for packets dropped by forbidden URL filtering.
Forbidden filename extension statistics	Filename extension forbidden by portal safe-redirect, and statistics for packets dropped by forbidden filename extension filtering.
Permit user URL statistics	URLs permitted by portal safe-redirect, and packet statistics for the URLs.
Default-action statistics	Statistics on packets processed by the default actions of portal

Field	Description
	safe-redirect.

Related commands

reset portal safe-redirect statistics

display portal server

Use **display portal server** to display information about portal authentication servers.

Syntax

display portal server [*server-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

server-name: Specifies a portal authentication server by its name, a case-sensitive string of 1 to 32 characters. If you do not specify the *server-name* argument, this command displays information about all portal authentication servers.

Examples

Display information about portal authentication server **pts**.

```
<Sysname> display portal server pts
Portal server: pts
  Type                  : IMC
  IP                    : 192.168.0.111
  VPN instance          : Not configured
  Port                  : 50100
  Server detection      : Timeout 60s  Action: log, trap
  User synchronization  : Timeout 200s
  Status                : Up
  Exclude-attribute     : Not configured
  Logout notification   : Retry 3 interval 5s
```

Table 21 Command output

Field	Description
Type	Portal authentication server type: • **CMCC**—CMCC server. • **IMC**—IMC server.
Portal server	Name of the portal authentication server.
IP	IP address of the portal authentication server.

Field	Description
VPN instance	MPLS L3VPN where the portal authentication server resides.
Port	Listening port on the portal authentication server.
Server detection	Parameters for portal authentication server detection: • Detection timeout in seconds. • Actions (**log** and **trap**) triggered by the reachability status change of the portal authentication server.
User synchronization	User idle timeout in seconds for portal user synchronization.

Status	Reachability status of the portal authentication server:
	• **Up**—This value indicates one of the following conditions:
	  ◦ Portal authentication server detection is disabled.
	  ◦ Portal authentication server detection is enabled and the server is reachable.
	• **Down**—Portal authentication server detection is enabled and the server is unreachable.

Exclude-attribute	Attributes that are not carried in portal protocol packets sent to the portal authentication server.
Logout notification	Maximum number of times and the interval (in seconds) for retransmitting a logout notification packet.

Related commands

`portal enable`

`portal server`

`server-detect` (portal authentication server view)

`user-sync`

display portal user

Use **`display portal user`** to display information about portal users.

Syntax

`display portal user` { **`all`** | **`auth-type`** { **`cloud`** | **`email`** | **`facebook`** | **`local`** | **`mac-trigger`** | **`normal`** | **`qq`** | **`wechat`** } | **`interface`** *`interface-type interface-number`* | **`ip`** *`ipv4-address`* | **`ipv6`** *`ipv6-address`* | **`mac`** *`mac-address`* | **`pre-auth`** [**`interface`** *`interface-type interface-number`* | **`ip`** *`ipv4-address`* | **`ipv6`** *`ipv6-address`*] | **`username`** *`username`* } [**`brief`** | **`verbose`**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

`all`: Displays information about all portal users.

auth-type: Specifies an authentication type.

cloud: Specifies the cloud authentication (a cloud portal authentication server performs portal authentication on portal users).

email: Specifies the email authentication.

facebook: Specifies the Facebook authentication.

local: Specifies the local authentication (a local portal authentication server performs portal authentication on portal users).

mac-trigger: Specifies the MAC-trigger authentication.

normal: Specifies the normal authentication (a remote portal authentication server performs portal authentication on portal users).

qq: Specifies QQ authentication.

wechat: Specifies WeChat authentication.

interface *interface-type interface-number*: Displays information about portal users on the specified interface.

ip *ipv4-address*: Specifies the IPv4 address of a portal user.

ipv6 *ipv6-address*: Specifies the IPv6 address of a portal user.

mac *mac-address*: Specifies the MAC address of a portal user, in the format of H-H-H.

username *username*: Specifies the username of a portal user, a case-sensitive string of 1 to 253 characters. The username cannot contain the domain name.

pre-auth: Displays information about preauthentication portal users. A preauthentication user is a user who is authorized with the authorization attributes in a preauthentication domain before portal authentication. If you do not specify the **pre-auth** keyword, this command displays information about authenticated portal users.

brief: Displays brief information about portal users.

verbose: Displays detailed information about portal users.

Usage guidelines

If you specify neither the **brief** nor the **verbose** keyword, this command displays portal authentication-related information for portal users.

Examples

Display information about all portal users.

```
<Sysname> display portal user all
Total portal users: 2
Username: abc
  Portal server: pts
  State: Online
  VPN instance: N/A
  MAC               IP                VLAN   Interface
  000d-88f8-0eab    2.2.2.2           --     GigabitEthernet1/0/1
  Authorization information:
    DHCP IP pool: N/A
    User profile: N/A
    Session group profile: N/A
    ACL number/name: N/A
    Inbound CAR: N/A
```

```
    Outbound CAR: N/A

Username: def
  Portal server: pts
  VPN instance: N/A
  MAC               IP                VLAN   Interface
  000d-88f8-0eac    3.3.3.3           --     GigabitEthernet1/0/2
  Authorization information:
    DHCP IP pool: N/A
    User profile: N/A
    Session group profile: N/A
    ACL number/name: 3000
    Inbound CAR: CIR 9000       bps PIR 20500      bps
                 CBS 20500      bit (active)
    Outbound CAR: CIR 9000       bps PIR 20400      bps
                  CBS 20400      bit (active)
```

Display information about portal users whose authentication type is normal portal authentication.

```
<Sysname> display portal user auth-type normal
Total normal users: 1
Username: abc
  Portal server: pts
  State: Online
  VPN instance: N/A
  MAC               IP                VLAN   Interface
  000d-88f8-0eab    2.2.2.2           --     GigabitEthernet1/0/1
  Authorization information:
    DHCP IP pool: N/A
    User profile: N/A
    Session group profile: N/A
    ACL number/name: N/A
    Inbound CAR: N/A
    Outbound CAR: N/A
```

Display information about the portal user whose MAC address is **000d-88f8-0eab**.

```
<Sysname> display portal user mac 000d-88f8-0eab
Username: abc
  Portal server: pts
  State: Online
  VPN instance: N/A
  MAC               IP                VLAN   Interface
  000d-88f8-0eab    2.2.2.2           --     GigabitEthernet1/0/1
  Authorization information:
    DHCP IP pool: N/A
    User profile: N/A
    Session group profile: N/A
    ACL number/name: N/A
    Inbound CAR: N/A
    Outbound CAR: N/A
```

Display information about the portal user whose username is **abc**.

```
<Sysname> display portal user username abc
Username: abc
  Portal server: pts
  State: Online
  VPN instance: N/A
  MAC               IP                VLAN   Interface
  000d-88f8-0eab    2.2.2.2           --     GigabitEthernet1/0/1
  Authorization information:
    DHCP IP pool: N/A
    User profile: N/A
    Session group profile: N/A
    ACL number/name: N/A
    Inbound CAR: N/A
    Outbound CAR: N/A
```

Table 22 Command output

Field	Description
Total portal users	Total number of portal users.
Total normal users	Total number of portal users whose authentication type is normal authentication.
Total local users	Total number of portal users whose authentication type is local authentication.
Total email users	Total number of portal users whose authentication type is email authentication.
Total cloud users	Total number of portal users whose authentication type is cloud authentication.
Total QQ users	Total number of portal users whose authentication type is QQ authentication.
Total WeChat users	Total number of portal users whose authentication type is WeChat authentication.
Total facebook users	Total number of portal users whose authentication type is Facebook authentication.
Total MAC-trigger users	Total number of portal users whose authentication type is MAC-trigger authentication.
Username	Name of the user.
Portal server	Name of the portal authentication server.
State	Current state of the portal user: • **Initialized**—The user is initialized and ready for authentication. • **Authenticating**—The user is being authenticated. • **Waiting SetRule**—Deploying portal rules to the user. • **Authorizing**—The user is being authorized. • **Online**—The user is online. • **Waiting Traffic**—Waiting for traffic from the user. • **Stop Accounting**—Stopping accounting for the user. • **Done**—The user is offline.
VPN instance	Name of the authorization VPN instance. If no VPN instance is authorized for the portal user, this field displays the MPLS L3VPN that the portal user belongs to. If the portal user is on a public network, this field displays **N/A**.

Field	Description
MAC	MAC address of the portal user.
IP	IP address of the portal user.
VLAN	VLAN where the portal user resides.
Interface	Access interface of the portal user.
Authorization information	Authorization information for the portal user.
DHCP IP pool	Name of the authorized IP address pool. If no IP address pool is authorized for the portal user, this field displays **N/A**.
User profile	This field is not supported in the current software version. Authorized user profile: • **N/A**—The AAA server authorizes no user profile. • **active**—The AAA server has authorized the user profile successfully. • **inactive**—The AAA server failed to authorize the user profile or the user profile does not exist on the device.
Session group profile	This field is not supported in the current software version. Authorized session group profile: • **N/A**—The AAA server authorizes no session group profile. • **active**—The AAA server has authorized the session group profile successfully. • **inactive**—The AAA server failed to authorize the session group profile or the session group profile does not exist on the device.
ACL number/name	Number or name of the authorized ACL: • **N/A**—The AAA server authorizes no ACL. • **active**—The AAA server has authorized the ACL successfully. • **inactive**—The AAA server failed to authorize the ACL or the ACL does not exist on the device.
Inbound CAR	Authorized inbound CAR information: • **CIR**—Committed information rate in bps. • **PIR**—Peak information rate in bps. • **CBS**—Committed burst size in bits. • **active**—The AAA server has authorized the inbound CAR successfully. • **inactive**—The AAA server failed to authorize the inbound CAR. If no inbound CAR is authorized, this field displays **N/A**.
Outbound CAR	Authorized outbound CAR information: • **CIR**—Committed information rate in bps. • **PIR**—Peak information rate in bps. • **CBS**—Committed burst size in bits. • **active**—The AAA server has authorized the outbound CAR successfully. • **inactive**—The AAA server failed to authorize the outbound CAR. If no outbound CAR is authorized, this field displays **N/A**.

Display detailed information about the portal user with IP address 50.50.50.3.

```
<Sysname> display portal user ip 50.50.50.3 verbose
Basic:
  Current IP address: 50.50.50.3
  Original IP address: 30.30.30.2
```

```
  Username: user1@hrss
  User ID: 0x18000002
  Access interface: GE1/0/2
  Service-VLAN/Customer-VLAN: -/-
  MAC address: 0000-0000-0001
  Authentication type: Normal
  Domain: hrss
  VPN instance: 123
  Status: Online
  Portal server: test
  Vendor: Apple
  Portal authentication method: Direct
AAA:
 Realtime accounting interval: 60s, retry times: 3
  Idle-cut:180 sec, 10240 bytes
  Session duration: 500 sec, remaining: 300 sec
  Remaining traffic: 10240000 bytes
  Login time: 2014-01-19  2:42:3 UTC
  ITA policy name: test
  DHCP IP pool: abc
ACL&QoS&Multicast:
    Inbound CAR: CIR 9000 bps PIR 20500 bps
                 CBS 20500 bit (active)
    Outbound CAR: CIR 9000 bps PIR 20400 bps
                  CBS 20400 bit (active)
  ACL number/name:3000(inactive)
    User profile: N/A
  Session group profile: N/A
  Max multicast addresses: 4
  Multicast address list: 1.2.3.1, 1.34.33.1, 3.123.123.3, 4.5.6.7
                          2.2.2.2, 3.3.3.3, 4.4.4.4
NAT444:
  Global IP address: 111.8.0.234
  Port block: 1024-1033
Traffic statistic:
  Uplink   packets/bytes: 7/546
  Downlink packets/bytes: 0/0
ITA:
  level-1 uplink   packets/bytes: 4/32
          downlink packets/bytes: 2/12
  level-2 uplink   packets/bytes: 0/0
          downlink packets/bytes: 0/0
Dual-stack traffic statistics:
  IPv4 address: 50.50.50.3
            Uplink   packets/bytes: 3/200
            Downlink packets/bytes: 0/0
  IPv6 address: 2001::2
            Uplink   packets/bytes: 4/346
```

```
            Downlink packets/bytes: 0/0
```

Table 23 Command output

Field	Description
Current IP address	IP address of the portal user after passing authentication.
Original IP address	IP address of the portal user during authentication.
Username	Name of the portal user.
User ID	Portal user ID.
Access interface	Access interface of the portal user.
Service-VLAN/Customer-VLAN	Public VLAN/Private VLAN to which the portal user belongs. If no VLAN is configured for the portal user, this field displays **-/-**.
MAC address	MAC address of the portal user.
Authentication type	Type of portal authentication: • **Normal**—Normal authentication. • **Local**—Local authentication. • **Email**—Email authentication. • **Cloud**—Cloud authentication. • **QQ**—QQ authentication. • **WeChat**—WeChat authentication. • **Facebook**—Facebook authentication. • **MAC-trigger**—MAC-trigger authentication.
Domain	ISP domain name for portal authentication.
VPN instance	Name of the authorized VPN instance. If no VPN instance is authorized, this field displays the MPLS L3VPN to which the portal user belongs. If the portal user is on a public network, this field displays **N/A**.
Status	Status of the portal user: • **Authenticating**—The user is being authenticated. • **Authorizing**—The user is being authorized. • **Waiting SetRule**—Deploying portal rules to the user. • **Online**—The user is online. • **Waiting Traffic**—Waiting for traffic from the user. • **Stop Accounting**—Stopping accounting for the user. • **Done**—The user is offline.
Portal server	Name of the portal server.
Vendor	Vendor name of the endpoint.
Portal authentication method	Portal authentication method on the access interface: • **Direct**—Direct authentication. • **Re-Dhcp**—Re-DHCP authentication. • **Layer3**—Cross-subnet authentication.
AAA	AAA information about the portal user.
Realtime accounting interval	Interval for sending real-time accounting updates, and the maximum number of accounting attempts. If the real-time accounting is not authorized, this field displays **N/A**.
Idle-cut	Idle timeout period and the minimum traffic threshold. If idle-cut is not authorized, this field displays **N/A**.
Session duration	Session duration and the remaining session time. If the session duration is

Field	Description
	not authorized, this field displays **N/A**.
Remaining traffic	Remaining traffic for the portal user. If the remaining traffic is not authorized, this field displays **N/A**.
Login time	Time when the user logged in. The field uses the device time format, for example, 2023-1-19 2:42:30 UTC.
ITA policy name	Name of the intelligent target accounting policy.
DHCP IP pool	Authorized DHCP IP address pool. If no DHCP IP address pool is authorized for the portal user, this field displays **N/A**.
Inbound CAR	Authorized inbound CAR information: • **CIR**—Committed information rate in bps. • **PIR**—Peak information rate in bps. • **CBS**—Committed burst size in bits. • **active**—The AAA server has authorized the inbound CAR successfully. • **inactive**—The AAA server failed to authorize the inbound CAR. If no inbound CAR is authorized, this field displays **N/A**.
Outbound CAR	Authorized outbound CAR information: • **CIR**—Committed information rate in bps. • **PIR**—Peak information rate in bps. • **CBS**—Committed burst size in bits. • **active**—The AAA server has authorized the outbound CAR successfully. • **inactive**—The AAA server failed to authorize the outbound CAR. If no outbound CAR is authorized, this field displays **N/A**.
ACL number/name	Number or name of the authorized ACL: • **N/A**—The AAA server authorizes no ACL. • **active**—The AAA server has authorized the ACL successfully. • **inactive**—The AAA server failed to authorize the ACL or the ACL does not exist on the device.
User profile	This field is not supported in the current software version. Authorized user profile: • **N/A**—The AAA server authorizes no user profile. • **active**—The AAA server has authorized the user profile successfully. • **inactive**—The AAA server failed to authorize the user profile or the user profile does not exist on the device.
Session group profile	This field is not supported in the current software version. Authorized session group profile: • **N/A**—The AAA server authorizes no session group profile. • **active**—The AAA server has authorized the session group profile successfully. • **inactive**—The AAA server failed to authorize the session group profile or the session group profile does not exist on the device.
Max multicast addresses	Maximum number of multicast groups the portal user can join.
NAT444	NAT444 mapping information for the portal user. This field is displayed only when portal is used in conjunction with NAT444.
Global IP address	Public IP address.
Port block	Port block: start port-end port.

Field	Description
Multicast address list	Multicast group list the portal user can join. If no multicast group is authorized, this field displays **N/A**.
Traffic statistic	Traffic statistics for the portal user.
Uplink packets/bytes	Packet and byte statistics of the upstream traffic.
Downlink packets/bytes	Packet and byte statistics of the downstream traffic.
ITA	ITA statistics for the portal user.
level-*n* uplink packets/bytes	Packet and byte statistics of the upstream traffic in accounting level n. Number *n* is in the range of 1 to 8.
level-*n* downlink packets/bytes	Packet and byte statistics of the downstream traffic in accounting level n. Number *n* is in the range of 1 to 8.
Dual-stack traffic statistic	IPv4 and IPv6 traffic statistics for the dual-stack user.
IPv4 address	IPv4 address of the portal user.
IPv6 address	IPv6 address of the portal user.
Uplink packets/bytes	Packet and byte statistics of the upstream traffic.
Downlink packets/bytes	Packet and byte statistics of the downstream traffic.

Display brief information about all portal users.

```
<Sysname> display portal user all brief
IP address       MAC address       Online duration       Username
2.2.2.2          000d-88f8-0eab    1:53:7                abc
3.3.3.3          000d-88f8-0eac    1:53:7                def
```

Table 24 Command output

Field	Description
IP address	IP address of the portal user.
MAC address	MAC address of the portal user.
Online duration	Online duration of the portal user, in hh:ss:mm.
Username	Username of the portal user.

Related commands

portal enable

display portal user-block

Use **display portal user-block** to display information about portal users blocked for portal authentication failure.

Syntax

display portal user-block [**ip** *ipv4-address* | **ipv6** *ipv6-address* | **mac** *mac-address* | **username** *username*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ip *ipv4-address*: Specifies a blocked portal user by its IPv4 address.

ipv6 *ipv6-address*: Specifies a blocked portal user by its IPv6 address.

mac *mac-address*: Specifies a blocked portal user by its MAC address in the format of H-H-H.

username *username*: Specifies a blocked portal user by its username, a case-insensitive string of 1 to 253 characters.

Usage guidelines

If you do not specify any parameters, this command displays information about all blocked portal users.

Examples

Display information about all blocked portal users.

```
<Sysname> display portal user-block
Total blocked users: 2

IP address: 10.2.33.2
MAC address: E0A5-66BB-B2AA
Remaining block time: 01h:38m:44s
Username: test

IP address: 19.19.0.4
MAC address: B577-CDCB-D49C
Remaining block time: 01h:26m:44s
Username: school
```

Display information about the blocked portal user at IPv4 address 10.2.33.2.

```
<Sysname> display portal user-block ip 10.2.33.2
IP address: 10.2.33.2
MAC address: E0A5-66BB-B2AA
Remaining block time: 01h:38m:44s
Username: test
```

Display information about the blocked portal user at IPv6 address 20::0:2.

```
<Sysname> display portal user-block ipv6 20::0:2
IP address: 20::0:2
MAC address: E0A5-66BB-B2AA
Remaining blocking time: 01h:38m:44s
Username: test
```

Display information about the blocked portal user at MAC address E0-A5-66-BH.

```
<Sysname> display portal user-block mac E0-A5-66-BH
IP address: 10.2.33.2
MAC address: E0A5-66BB-B2AA
```

```
Remaining block time: 01h:38m:44s
Username: test
```

Display information about the blocked portal user whose username is **test**.

```
<Sysname> display portal user-block username test
IP address: 10.2.33.2
MAC address: E0A5-66BB-B2AA
Remaining block time: 01h:38m:44s
Username: test
```

Table 25 Command output

Field	Description
IP address	IP address of the blocked portal user.
MAC address	MAC address of the blocked portal user.
Username	Username of the blocked portal user.
Remaining block time(hh:mm:ss)	Remaining blocking timeout time, in the format of hh:mm:ss.

Related commands

`portal user-block failed-times`

`portal user-block reactive`

display portal user count

Use **`display portal user count`** to display the number of portal users.

Syntax

`display portal user count`

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display the number of portal users.

```
<Sysname> display portal user count
Total number of users: 1
```

Related commands

`portal enable`

`portal delete-user`

display portal user dhcp-lease

Use **display portal user dhcp-lease** to display DHCP lease information for IPv4 portal users.

Syntax

display portal user dhcp-lease [**ipv4** *ipv4-address*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ipv4 *ipv4-address*: Specify an IPv4 portal user by its IPv4 address. If you do not specify an IPv4 portal user, this command displays DHCP lease information about all IPv4 portal users.

Usage guidelines

Use this command only when DHCP packet capture is enabled to detect online status of portal users. To enable the DHCP packet capture feature, use the **portal idle-cut dhcp-capture enable** command.

Examples

Display DHCP lease information for all IPv4 portal users.

```
<Sysname> display portal user dhcp-lease
Total DHCP lease entries: 2
IPv4 address      MAC address           Lease time          Remaining time
1.1.1.1           AABB-CCDD-1122        02h 00m 00s         01h 10m 46s
1.1.1.2           AABB-CCDD-1133        01h 00m 00s         00h 08m 46s
```

Display DHCP lease information for an IPv4 portal user.

```
<Sysname> display portal user dhcp-lease ip 1.1.1.1
IPv4 address      MAC address           Lease time          Remaining time
1.1.1.1           AABB-CCDD-1122        02h 00m 00s         01h 10m 46s
```

Table 26 Command output

Field	Description
Total DHCP lease entries	Total number of DHCP lease entries of IPv4 portal users.
IPv4 address	IPv4 address of an IPv4 portal user.
MAC	MAC address of the IPv4 portal user.
Lease time	Lease time period for the IPv4 address. • If the time period is less than one day, this field is displayed in the *xx*h *xx*m *xx*s format. • If the time period is less than one week, this field is displayed in the *x*d *xx*h format.

Field	Description
	• If the time period is greater than one week, this field is displayed in the *x*w *x*d *xx*h format. The **w**, **d**, **h**, **m**, and **s** represent weeks, days, hours, minutes, and seconds, respectively.
Remaining time	Remaining lease time period for the IPv4 address. • If the time period is less than one day, this field is displayed in the *xx*h *xx*m *xx*s format. • If the time period is less than one week, this field is displayed in the *x*d *xx*h format. • If the time period is greater than one week, this field is displayed in the *x*w *x*d *xx*h format. The **w**, **d**, **h**, **m**, and **s** represent weeks, days, hours, minutes, and seconds, respectively.

Related commands

`portal idle-cut dhcp-capture enable`

display portal user dhcpv6-lease

`display portal user dhcpv6-lease` to display DHCPv6 lease information for IPv6 portal users.

Syntax

`display portal user dhcpv6-lease` [**`ipv6`** *`ipv6-address`*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

`ipv6` *`ipv6-address`*: Specify an IPv6 portal user by its IPv6 address. If you do not specify an IPv6 portal user, this command displays DHCPv6 lease information about all IPv6 portal users.

Usage guidelines

Use this command only when DHCP packet capture is enabled to detect online status of portal users. To enable the DHCP packet capture feature, use the **`portal idle-cut dhcp-capture enable`** command.

Examples

Display DHCPv6 lease information for all IPv6 portal users.

```
<Sysname> display portal user dhcpv6-lease
Total DHCPv6 lease entries: 2
IPv6 address            MAC address       Lease time     Remaining time
2000::1                 AABB-CCDD-1144    02h 00m 00s    01h 10m 46s
2000::2                 AABB-CCDD-1155    01h 00m 00s    00h 08m 46s
```

Display DHCPv6 lease information for an IPv6 portal user.

```
<Sysname> display portal user dhcpv6-lease ipv6 2000::1
IPv6 address            MAC address       Lease time     Remaining time
2000::1                 AABB-CCDD-1144    02h 00m 00s    01h 10m 46s
```

Table 27 Command output

Field	Description
Total DHCP lease entries	Total number of DHCPv6 lease entries of IPv6 portal users.
IPv4 address	IPv4 address of an IPv6 portal user.
MAC	MAC address of the IPv6 portal user.
Lease time	Lease time period for the IPv4 address. • If the time period is less than one day, this field is displayed in the *xx*h *xx*m *xx*s format. • If the time period is less than one week, this field is displayed in the *x*d *xx*h format. • If the time period is greater than one week, this field is displayed in the *x*w *x*d *xx*h format. The **w**, **d**, **h**, **m**, and **s** represent weeks, days, hours, minutes, and seconds, respectively.
Remaining time	Remaining lease time period for the IPv4 address. • If the time period is less than one day, this field is displayed in the *xx*h *xx*m *xx*s format. • If the time period is less than one week, this field is displayed in the *x*d *xx*h format. • If the time period is greater than one week, this field is displayed in the *x*w *x*d *xx*h format. The **w**, **d**, **h**, **m**, and **s** represent weeks, days, hours, minutes, and seconds, respectively.

Related commands

`portal idle-cut dhcp-capture enable`

display portal web-server

Use **`display portal web-server`** to display information about portal Web servers.

Syntax

`display portal web-server` [*`server-name`*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

server-name: Specifies a portal Web server by its name, a case-sensitive string of 1 to 32 characters. If you do not specify a portal Web server, this command displays information about all portal Web servers.

Examples

Display information about portal Web server **wbs**.

```
<Sysname> display portal web-server wbs
Portal Web server: wbs
    Type IMC
    URL: http://www.test.com/portal
    URL parameters:
       userurl=http://www.test.com/welcome
       userip=source-address
    VPN instance: Not configured
    Server detection:
      Interval: 120s
      Attempts: 5
      Action: log, trap
      Detection URL: http://www.test.com/portal
      Detection type: TCP
    IPv4 status: Up
    IPv6 status: Up
    Captive-bypass: Disabled
    If-match: original-url:  http://2.2.2.2, redirect-url:  http://192.168.56.2
              original-url:   http://1.1.1.1, temp-pass redirect-url:
              http://192.168.1.1
```

Table 28 Command output

Field	Description
Type	Portal Web server type: • **CMCC**—CMCC server. • **IMC**—IMC server. • **ISE**—ISE sever. • **OAuth**—Cloud server. • **WiFiDog**—WiFiDog server.
Portal Web server	Name of the portal Web server.
URL	URL of the portal Web server.
URL parameters	URL parameters for the portal Web server.
VPN instance	Name of the MPLS L3VPN where the portal Web server resides.
Server detection	Parameters for portal Web server detection.
Interval	Detection interval in seconds.
Attempts	Maximum number of detection attempts.
Action	Actions (**log** and **trap**) to take when a reachability status change of the portal Web server is detected.
Detection URL	Portal Web server detection URL.

Field	Description
Detection type	Type of portal Web server detection: • TCP. • HTTP.

IPv4 status	Current state of the IPv4 portal Web server:
	• **Up**—This value indicates one of the following conditions:
	  ◦ Portal Web server detection is disabled.
	  ◦ Portal Web server detection is enabled and the server is reachable.
	• **Down**—Portal Web server detection is enabled and the server is unreachable.

IPv6 status	Current state of the IPv6 portal Web server:
	• **Up**—This value indicates one of the following conditions:
	  ◦ Portal Web server detection is disabled.
	  ◦ Portal Web server detection is enabled and the server is reachable.
	• **Down**—Portal Web server detection is enabled and the server is unreachable.

Captive-bypass	Status of the captive-bypass feature: • **Disabled**—Captive-bypass is disabled. • **Enabled**—Captive-bypass is enabled. • **Optimize Enabled**—Optimized captive-bypass is enabled.
If-match	Match rules configured for URL redirection. This field displays **Not configured** if no match rules for URL redirection are configured.

Related commands

portal enable

portal web-server

server-detect (portal Web server view)

server-detect url

display web-redirect rule

Use **display web-redirect rule** to display information about Web redirect rules.

Syntax

display web-redirect rule interface *interface-type interface-number* [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays Web redirect rules for the master device.

Examples

Display all Web redirect rules on GigabitEthernet 1/0/1.

```
<Sysname> display web-redirect rule interface gigabitethernet 1/0/1
IPv4 web-redirect rules on GigabitEthernet1/0/1:
Rule 1:
 Type                : Dynamic
 Action              : Permit
 Status              : Active
 Source:
    IP             : 192.168.2.114
    VLAN           : Any

Rule 2:
 Type                : Static
 Action              : Redirect
 Status              : Active
 Source:
    VLAN           : Any
    Protocol       : TCP
 Destination:
    Port           : 80

IPv6 web-redirect rules on GigabitEthernet1/0/1:
Rule 1:
 Type                : Static
 Action              : Redirect
 Status              : Active
 Source:
    VLAN           : Any
    Protocol       : TCP
 Destination:
    Port           : 80
```

Table 29 Command output

Field	Description
Rule	Number of the Web redirect rule.
Type	Type of the Web redirect rule: • **Static**—Static Web redirect rule, generated when the Web redirect feature takes effect. • **Dynamic**—Dynamic Web redirect rule, generated when a user visits a redirect webpage.
Action	Action in the Web redirect rule: • **Permit**—Allows packets to pass. • **Redirect**—Redirects the packets.
Status	Status of the Web redirect rule:

Field	Description
	• **Active**—The Web redirect rule is effective. • **Inactive**—The Web redirect rule is not effective.
Source	Source information in the Web redirect rule.
IP	Source IP address.
Mask	Subnet mask of the source IPv4 address.
Prefix length	Prefix length of the source IPv6 address.
VLAN	Source VLAN. If not specified, this field displays **Any**.
Protocol	Transport layer protocol in the Web redirect rule: • **Any**—No transport layer protocol is limited. • **TCP**—Transmission Control Protocol.
Destination	Destination information in the Web redirect rule.
Port	Destination transport layer port number. The default port number is 80.

exclude-attribute (MAC binding server view)

Use **exclude-attribute** to exclude an attribute from portal protocol packets.

Use **undo exclude-attribute** to not exclude an attribute from portal protocol packets.

Syntax

exclude-attribute *attribute-number*

undo exclude-attribute *attribute-number*

Default

No attributes are excluded from portal protocol packets.

Views

MAC binding server view

Predefined user roles

network-admin

context-admin

Parameters

attribute-number: Specifies an attribute by its number in the range of 1 to 255.

Usage guidelines

Support of the portal authentication server for portal protocol attributes varies by the server type. During MAC-trigger authentication, the device and the server cannot communicate if the device sends the portal authentication server a packet that contains an attribute unsupported by the server.

To address this issue, you can configure this command to exclude the unsupported attributes from portal protocol packets sent to the portal authentication server.

You can specify multiple excluded attributes.

Table 30 describes all attributes of the portal protocol.

Table 30 Portal attributes

Name	Number	Description
UserName	1	Name of the user to be authenticated.
PassWord	2	User password in plaintext form.
Challenge	3	Random challenge for CHAP authentication.
ChapPassWord	4	CHAP password encrypted by MD5.
TextInfo	5	The device uses this attribute to transparently transport prompt information of a RADIUS server or packet error information to the portal authentication server. The attribute value can be any string excluding the end character '\0'. This attribute can exist in any packet from the device to the portal server. A packet can contain multiple TextInfo attributes. As a best practice, carry only one TextInfo attribute in a packet.
UpLinkFlux	6	Uplink (output) traffic of the user, an 8-byte unsigned integer, in KB.
DownLinkFlux	7	Downlink (input) traffic of the user, an 8-byte unsigned integer, in KB.
Port	8	Port information, a string excluding the end character '\0'.
IP-Config	9	This attribute has different meanings in different types of packets. • The device uses this attribute in ACK _AUTH (Type=0x04) packets to notify the portal server that the user requires re-DHCP. • The device uses this attribute in ACK_LOGOUT (Type=0x06) and NTF_LOGOUT (Type=0x08) packets to indicate that the current user IP address must be released. The portal server must notify the user to release the public IP address through DHCP. The device will reallocate a private IP address to the user.
BAS-IP	10	IP address of the access device. For re-DHCP portal authentication, the value of this attribute is the public IP address of the access device.
Session-ID	11	Identification of a portal user. Generally, the value of this attribute is the MAC address of the portal user.
Delay-Time	12	Delay time for sending a packet. This attributes exists in NTF_LOGOUT (Type=0x08) packets.
User-List	13	List of IP addresses of an IPv4 portal user.
EAP-Message	14	An EAP attribute that needs to be transported transparently. This attribute is applicable to EAP TLS authentication. Multiple EAP-Message attributes can exist in a portal authentication packet.
User-Notify	15	Value of the hw_User_Notify attribute in a RADIUS accounting response. This attribute needs to be transported transparently.
BAS-IPv6	100	IPv6 address of the access device.
UserIPv6-List	101	List of IPv6 addresses of an IPv6 portal user.

Examples

Exclude the BAS-IP attribute (number 10) from portal packets sent to MAC binding server 123.

```
<Sysname> system-view
[Sysname] portal mac-trigger-server 123
[Sysname-portal-mac-trigger-server-123] exclude-attribute 10
```

exclude-attribute (portal authentication server view)

Use **exclude-attribute** to exclude an attribute from portal protocol packets.

Use **undo exclude-attribute** to not exclude an attribute from portal protocol packets.

Syntax

exclude-attribute *number* { **ack-auth** | **ack-logout** | **ntf-logout** }

undo exclude-attribute *number* { **ack-auth** | **ack-logout** | **ntf-logout** }

Default

No attributes are excluded from portal protocol packets.

Views

Portal authentication server view

Predefined user roles

network-admin

context-admin

Parameters

number: Specifies an attribute by its number in the range of 1 to 255.

ack-auth: Excludes the attribute from ACK_AUTH packets.

ack-logout: Excludes the attribute from ACK_LOGOUT packets.

ntf-logout: Excludes the attribute from NTF_LOGOUT packets.

Usage guidelines

Support of the portal authentication server for portal protocol attributes varies by the server type. If the device sends the portal authentication server a packet that contains an attribute unsupported by the server, the device and the server cannot communicate.

To address this issue, you can configure this command to exclude the unsupported attributes from specific portal protocol packets sent to the portal authentication server.

You can specify multiple excluded attributes. For an excluded attribute, you can specify multiple types of portal protocol packets (**ack-auth**, **ntf-logout**, and **ack-logout**).

Table 31 describes all attributes of the portal protocol.

Table 31 Portal attributes

Name	Number	Description
UserName	1	Name of the user to be authenticated.
PassWord	2	User password in plaintext form.
Challenge	3	Random challenge for CHAP authentication.
ChapPassWord	4	CHAP password encrypted by MD5.
TextInfo	5	The device uses this attribute to transparently transport prompt information of a RADIUS server or packet error information to the portal authentication server. The attribute value can be any string excluding the end character '\0'. This attribute can exist in any packet from the device to the portal server. A packet can contain multiple TextInfo attributes. As a best practice, carry only one TextInfo attribute in a packet.

Name	Number	Description
UpLinkFlux	6	Uplink (output) traffic of the user, an 8-byte unsigned integer, in KB.
DownLinkFlux	7	Downlink (input) traffic of the user, an 8-byte unsigned integer, in KB.
Port	8	Port information, a string excluding the end character '\0'.
IP-Config	9	This attribute has different meanings in different types of packets. • The device uses this attribute in ACK _AUTH (Type=0x04) packets to notify the portal server that the user requires re-DHCP. • The device uses this attribute in ACK_LOGOUT (Type=0x06) and NTF_LOGOUT (Type=0x08) packets to indicate that the current user IP address must be released. The portal server must notify the user to release the public IP address through DHCP. The device will reallocate a private IP address to the user.
BAS-IP	10	IP address of the access device. For re-DHCP portal authentication, the value of this attribute is the public IP address of the access device.
Session-ID	11	Identification of a portal user. Generally, the value of this attribute is the MAC address of the portal user.
Delay-Time	12	Delay time for sending a packet. This attributes exists in NTF_LOGOUT (Type=0x08) packets.
User-List	13	List of IP addresses of an IPv4 portal user.
EAP-Message	14	An EAP attribute that needs to be transported transparently. This attribute is applicable to EAP TLS authentication. Multiple EAP-Message attributes can exist in a portal authentication packet.
User-Notify	15	Value of the hw_User_Notify attribute in a RADIUS accounting response. This attribute needs to be transported transparently.
BAS-IPv6	100	IPv6 address of the access device.
UserIPv6-List	101	List of IPv6 addresses of an IPv6 portal user.

Examples

Exclude the UpLinkFlux attribute (number 6) from portal ACK_AUTH packets.

```
<Sysname> system-view
[Sysname] portal server pts
[Sysname-portal-server-pts] exclude-attribute 6 ack-auth
```

Related commands

display portal server

free-traffic threshold

Use **free-traffic threshold** to set the free-traffic threshold for portal users.

Use **undo free-traffic threshold** to restore the default.

Syntax

free-traffic threshold *value*

undo free-traffic threshold

Default

The free-traffic threshold is 0 bytes.

Views

MAC binding server view

Predefined user roles

network-admin

context-admin

Parameters

value: Specifies the free-traffic threshold in the range of 0 to 10240000 bytes. If the free-traffic threshold is set to 0, the device immediately triggers MAC-based quick portal authentication for a user once the user's traffic is detected.

Usage guidelines

After MAC-based quick portal authentication is configured, the device monitors a user's network traffic (sent and received) in real time before the MAC-trigger entry for the user ages out. A user can access the network without authentication if the user's network traffic is below the free-traffic threshold. When the user's network traffic reaches the threshold, the device triggers MAC-based quick portal authentication for the user.

If the user passes portal authentication, the device deletes the MAC-trigger entry and clears the user traffic statistics. If the user fails authentication, the device does not trigger MAC-based quick authentication for the user before the MAC-trigger entry ages out. When the MAC-trigger entry ages out, the device clears the user traffic statistics.

When traffic is detected from the user again, the device re-creates a MAC-trigger entry for the user and repeats the previous procedure.

Examples

Set the free-traffic threshold for portal users to 10240 bytes.

```
<Sysname> system-view
[Sysname] portal mac-trigger-server mts
[Sysname-portal-mac-trigger-server-mts] free-traffic threshold 10240
```

Related commands

display portal mac-trigger-server

if-match

Use **if-match** to configure a match rule for URL redirection.

Use **undo if-match** to delete a URL redirection match rule.

Syntax

if-match { **original-url** *url-string* **redirect-url** *url-string* [**url-param-encryption** { **aes** | **des** } **key** { **cipher** | **simple** } *string*] | **user-agent** *string* **redirect-url** *url-string* }

undo if-match { **original-url** *url-string* | **user-agent** *user-agent* }

Default

No URL redirection match rules exist.

Views

Portal Web server view

Predefined user roles

network-admin

context-admin

Parameters

original-url *url-string*: Specifies the user-requested URL to be matched. The specified URL must be a complete URL starting with **http://** or **https://**, a case-sensitive string of 1 to 256 characters. The URL string can include question marks (?). If you enter a question mark (?) in the place of the *url-string* argument, the CLI does not display help information for this argument.

redirect-url *url-string*: Specifies the URL to which the user is redirected. The specified URL must be a complete URL starting with **http://** or **https://**, a case-sensitive string of 1 to 256 characters. The URL string can include question marks (?). If you enter a question mark (?) in the place of the *url-string* argument, the CLI does not display help information for this argument.

url-param-encryption: Specifies an encryption algorithm to encrypt the parameters carried in the redirection URL. If you do not specify an encryption algorithm, the parameters carried in the redirection URL are not encrypted.

aes: Specifies the AES algorithm.

des: Specifies the DES algorithm.

key: Specifies a key for encryption.

cipher: Specifies a key in encrypted form.

simple: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the case-sensitive key string. The string length varies by the selected encryption method:

- If **des cipher** is specified, the string length is 41 characters.
- If **des simple** is specified, the string length is 8 characters.
- If **aes cipher** is specified, the string length is 1 to 73 characters.
- If **aes simple** is specified, the string length is 1 to 31 characters.

user-agent *user-agent*: Specifies a user agent string to match the User-Agent string in HTTP/HTTPS requests. The user agent string is a case-sensitive string of 1 to 255 characters. The User-Agent string in HTTP or HTTPS requests includes information about hardware manufacturer, operating system, browser, and search engine.

Usage guidelines

A URL redirection match rule matches Web requests (HTTP or HTTPS requests) by user-requested URL or User-Agent information, and redirects the matching Web requests to the specified redirection URL.

For a user to successfully access a redirection URL, configure a portal-free rule to allow HTTP or HTTPS requests destined for the redirection URL to pass. For information about configuring portal-free rules, see the **portal free-rule** command.

For a portal Web server, you can configure the **url** command and the **if-match** command for URL redirection. The **url** command redirects all Web requests from unauthenticated users to the portal Web server for authentication. The **if-match** command allows for flexible URL redirection by redirecting specific Web requests to specific redirection URLs. If both commands are executed, the **if-match** command takes priority to perform URL redirection.

If both portal safe-redirect and URL redirection match rules are configured, the device preferentially uses URL redirection match rules to perform URL redirection.

If you configure encryption for parameters in the redirection URL, you must add an encryption prompt field after the redirection URL address. For example, to redirect HTTP requests to URL 10.1.1.1 with encrypted URL parameters, specify the redirection URL as **http://10.1.1.1?yyyy=**. The

value of yyyy depends on the portal Web server configuration. For more information, see the portal Web server configuration guide.

You can configure a URL in a URL redirection match rule in one of the following ways:

- **For exact match**—Specify a complete URL. For example, if you configure the URL as **abc.com.cn**, only Web requests that contain URL **abc.com.cn** match the rule.
- **For fuzzy match**—Specify a URL by placing the asterisk (*) wildcard character at the beginning or end of the URL string. For example, if you configure the URL as ***abc.com.cn**, **abc***, or ***abc***, Web requests that carry the URL ending with **abc.com.cn**, starting with **abc**, or including **abc** match the rule.
  - The asterisk (*) wildcard character represents any characters. The device treats multiple consecutive asterisks as one.
  - The configured URL cannot contain only asterisks (*).

You cannot configure two URL redirection match rules with the same user-requested URL.

Examples

Configure a match rule to redirect HTTP requests destined for the URL **http://www.abc.com.cn** to the URL **http://192.168.0.1**.

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] if-match original-url http://www.abc.com.cn redirect-url
http://192.168.0.1
```

Configure a match rule to redirect HTTP requests that carry the user agent string **5.0(WindowsNT6.1)AppleWebKit/537.36(KHTML,likeGecko)Chrome/36.0.1985.125Safari/537.36** to the URL **http://192.168.0.1.**

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] if-match user-agent
5.0(WindowsNT6.1)AppleWebKit/537.36(KHTML,likeGecko)Chrome/36.0.1985.125Safari/537.36
redirect-url http://192.168.0.1
```

Related commands

display portal web-server

portal free-rule

url

url-parameter

if-match temp-pass

Use **if-match temp-pass** to configure a match rule for temporary pass.

Use **undo if-match temp-pass** to restore the default.

Syntax

if-match { **original-url** *url-string* | **user-agent** *user-agent* } * **temp-pass** [**redirect-url** *url-string* | **original**]

undo if-match { **original-url** *url-string* | **user-agent** *user-agent* } * **temp-pass**

Default

No match rules for temporary pass are configured.

Views

Portal Web server view

Predefined user roles

network-admin

context-admin

Parameters

original-url *url-string*: Specifies a URL string to match the URL in HTTP/HTTPS requests of portal users. The specified URL must be a complete URL starting with **http://** or **https://**, a case-sensitive string of 1 to 256 characters. The URL string can include question marks (?). If you enter a question mark (?) in the place of the *url-string* argument, the CLI does not display help information for this argument.

user-agent *user-agent*: Specifies a user agent string to match the User-Agent string in HTTP/HTTPS requests. The user agent string is a case-sensitive string of 1 to 255 characters. The User-Agent string in HTTP or HTTPS requests includes information about hardware manufacturer, operating system, browser, and search engine.

redirect-url *url-string*: Redirects the matching Web requests to the specified URL. The specified URL must be a complete URL starting with **http://** or **https://**, a case-sensitive string of 1 to 256 characters. The URL string can include question marks (?). If you enter a question mark (?) in the place of the *url-string* argument, the CLI does not display help information for this argument.

original: Redirects the matching Web requests to the originally requested URLs.

Usage guidelines

A match rule for temporary pass matches Web requests by URL or User-Agent information. Only the matching Web requests are temporarily permitted to pass.

A permitted request can be redirected to the specified redirection URL or to the originally requested URL, depending on the redirection action in the match rule. If you do not configure a redirection action (by using the **redirect-url** *url-string* option or the **original** keyword), the device permits the matching requests to pass without redirection.

For the match rules to take effect, make sure the portal temporary pass feature is enabled.

If you configure the same match criteria but different redirection actions in two match rules, the new configuration overwrites the existing one.

If both portal safe-redirect and portal temporary pass match rules are configured, portal temporary pass match rules take precedence.

Examples

Configure a temporary pass match rule to temporarily allow user packets that access URL **http://www.abc.com.cn** to pass.

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] if-match original-url http://www.abc.com.cn temp-pass
```

Configure a temporary pass match rule to temporarily allow user packets that access the URL **http://www.abc.com.cn/** to pass and then redirect the packets to the originally requested URL.

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] if-match original-url http://www.abc.com.cn temp-pass
original
```

Configure a temporary pass match rule to allow user packets that contain user agent information **5.0(WindowsNT6.1)AppleWebKit/537.36(KHTML,likeGecko)Chrome/36.0.1985.125Safari/537.36** to pass and then redirect the packets to URL **http://192.168.0.1**.

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] if-match user-agent
5.0(WindowsNT6.1)AppleWebKit/537.36(KHTML,likeGecko)Chrome/36.0.1985.125Safari/537.36
temp-pass redirect-url http://192.168.0.1
```

Configure a temporary pass match rule. This rule allows user packets that access the URL **http://www.abc.com.cn/** and contain user agent information **5.0(WindowsNT6.1)AppleWebKit/537.36(KHTML,likeGecko)Chrome/36.0.1985.125Safari/537.36** to pass and then redirects the packets to URL **http://192.168.0.1**.

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] if-match original-url http://www.123.com.cn user-agent
5.0(WindowsNT6.1)AppleWebKit/537.36(KHTML,likeGecko)Chrome/36.0.1985.125Safari/537.36
temp-pass redirect-url http://192.168.0.1
```

Related commands

display portal web-server

portal free-rule

portal temp-pass enable

url

url-parameter

ip (MAC binding server view)

Use **ip** to specify the IP address of a MAC binding server.

Use **undo ip** to restore the default.

Syntax

ip *ipv4-address* [**vpn-instance** *vpn-instance-name*] [**key** { **cipher** | **simple** } *string*]

undo ip

Default

The IP address of the MAC binding server is not specified.

Views

MAC binding server view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-address: Specifies the IP address of a MAC binding server.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the MAC binding server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the MAC binding server belongs to the public network, do not specify this option.

key: Specifies a shared key to be used to authenticate packets between the device and the MAC binding server. Portal packets exchanged between the device and MAC binding server carry an authenticator that is generated with the shared key. The receiver uses the authenticator to verify the correctness of the received portal packets. If you do not specify a shared key, the device and MAC binding server do not authenticate the packets between them.

cipher: Specifies a shared key in encrypted form.

simple: Specifies a shared key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the shared key. Its plaintext form is a case-sensitive string of 1 to 64 characters. Its encrypted form is a case-sensitive string of 33 to 117 characters.

Usage guidelines

If you execute this command multiple times in the same MAC binding server view, the most recent configuration takes effect.

Examples

Specify the IP address of the MAC binding server as **192.168.0.111** and the plaintext key as **portal**.

```
<Sysname> system-view
[Sysname] portal mac-trigger-server mts
[Sysname-portal-mac-trigger-server-mts] ip 192.168.0.111 key simple portal
```

Related commands

display portal mac-trigger-server

ip (portal authentication server view)

Use **ip** to specify the IPv4 address of a portal authentication server.

Use **undo ip** to restore the default.

Syntax

ip *ipv4-address* [**vpn-instance** *vpn-instance-name*] [**key** { **cipher** | **simple** } *string*]

undo ip

Default

The IPv4 address of the portal authentication server is not specified.

Views

Portal authentication server view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-address: Specifies the IPv4 address of the portal authentication server.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN where the portal authentication server resides by the VPN instance name, a case-sensitive string of 1 to 31 characters. If the portal authentication server is on the public network, do not specify this option.

key: Specifies a shared key for communication with the portal authentication server. Portal packets exchanged between the access device and the portal authentication server carry an authenticator

that is generated with the shared key. The receiver uses the authenticator to check the correctness of the received portal packets.

cipher: Specifies a key in encrypted form.

simple: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. Its plaintext form is a case-sensitive string of 1 to 64 characters. Its encrypted form is a case-sensitive string of 33 to 117 characters.

Usage guidelines

A portal authentication server has only one IPv4 address. Therefore, in portal authentication server view, only one IPv4 address exists. If you execute this command multiple times, the most recent configuration takes effect.

Do not configure the same IPv4 address and VPN instance for different portal authentication servers.

Examples

Specify **192.168.0.111** as the IPv4 address of portal authentication server **pts** and plaintext key **portal** as the shared key for communication with the portal authentication server.

```
<Sysname> system-view
[Sysname] portal server pts
[Sysname-portal-server-pts] ip 192.168.0.111 key simple portal
```

Related commands

display portal server

portal server

ipv6 (portal authentication server view)

Use **ipv6** to specify the IPv6 address of a portal authentication server.

Use **undo ipv6** to restore the default.

Syntax

ipv6 *ipv6-address* [**vpn-instance** *vpn-instance-name*] [**key** { **cipher** | **simple** } *string*]

undo ipv6

Default

The IPv6 address of the portal authentication server is not specified.

Views

Portal authentication server view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address: Specifies the IPv6 address of the portal authentication server.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN where the portal authentication server resides by the VPN instance name, a case-sensitive string of 1 to 31 characters. If the portal authentication server is on the public network, do not specify this option.

key: Specifies a shared key for communication with the portal authentication server. Portal packets exchanged between the access device and the portal authentication server carry an authenticator that is generated with the shared key. The receiver uses the authenticator to check the correctness of the received portal packets.

cipher: Specifies a key in encrypted form.

simple: Specifies a key in plaintext form. For security purposes, the key in plaintext form will be stored in encrypted form.

string: Specifies the key. Its plaintext form is a case-sensitive string of 1 to 64 characters. Its encrypted form is a case-sensitive string of 33 to 117 characters.

Usage guidelines

A portal authentication server has only one IPv6 address. Therefore in portal authentication server view, only one IPv6 address exists. If you execute this command multiple times, the most recent configuration takes effect.

Do not configure the same IPv6 address and VPN instance for different portal authentication servers.

Examples

Specify **2000::1** as the IPv6 address of portal authentication server **pts** and plaintext key **portal** as the shared key for communication with the portal authentication server.

```
<Sysname> system-view
[Sysname] portal server pts
[Sysname-portal-server-pts] ipv6 2000::1 key simple portal
```

Related commands

display portal server

portal server

local-binding aging-time

Use **local-binding aging-time** to set the aging time for local MAC-account binding entries.

Use **undo local-binding aging-time** to restore the default.

Syntax

local-binding aging-time *minutes*

undo local-binding aging-time

Default

The aging time for local MAC-account binding entries is 720 minutes.

Views

MAC binding server view

Predefined user roles

network-admin

context-admin

Parameters

minutes: Specifies the aging time for local MAC-account binding entries. The value range for this argument is 1 to 129600 minutes.

Usage guidelines

The local MAC binding server uses a local MAC-account binding entry to record the MAC address and portal account information (username and password) of a portal user.

The local MAC-account binding entry of a portal user is deleted when the entry ages out. The device creates a local MAC-account binding entry for the user again when the user triggers and passes a new portal authentication.

If you disable local MAC-trigger authentication, the device does not delete existing local MAC-account binding entries. These entries are automatically deleted when they age out.

Examples

Set the aging time for local MAC-account binding entries to 240 minutes in the view of MAC binding server **mts**.

```
<Sysname> system-view
[Sysname] portal mac-trigger-server mts
[Sysname-portal-mac-trigger-server-mts] local-binding aging-time 240
```

Related commands

`display portal mac-trigger-server`

`local-binding enable`

local-binding enable

Use **`local-binding enable`** to enable local MAC-trigger authentication.

Use **`undo local-binding enable`** to disable local MAC-trigger authentication.

Syntax

`local-binding enable`

`undo local-binding enable`

Default

Local MAC-trigger authentication is disabled.

Views

MAC binding server view

Predefined user roles

network-admin

context-admin

Usage guidelines

This feature enables the device to act as a local MAC binding server to provide MAC-trigger authentication for local portal authentication users.

After a user passes portal authentication for the first time, the access device (local MAC binding server) generates a local MAC-account binding entry for the user. The local MAC binding-account entry records the MAC address and portal account information (username and password) of the user. Then, the user can automatically connect to the network without manual authentication for subsequent network access attempts.

Examples

Enable local MAC-trigger authentication in the view of MAC binding server **mts**.

```
<Sysname> system-view
[Sysname] portal mac-trigger-server mts
```

```
[Sysname-portal-mac-trigger-server-mts] local-binding enable
```

Related commands

display portal mac-trigger-server

local-binding aging-time

login failed-url

Use **login failed-url** to configure the redirect URL for authentication failure.

Use **undo login failed-url** to restore the default.

Syntax

login failed-url *url-string*

undo login failed-url

Default

No redirection URL for authentication failure is configured.

Views

Local portal Web service view

Predefined user roles

network-admin

context-admin

Parameters

url-string: Specifies the redirect URL for authentication failure, a case-sensitive string of 1 to 256 characters.

Usage guidelines

The device redirects portal users to the specified URL after they fail authentication.

Examples

Configure the redirect URL for authentication failure as **https://1.1.1.1/portal/iselogin.html**.

```
<Sysname> system-view
[Sysname] portal local-web-server https
[Sysname-portal-local-websvr-https] login failure-url
https://1.1.1.1/portal/iselogin.html
```

login success-url

Use **login success-url** to configure the redirect URL for authentication success.

Use **undo login success-url** to restore the default.

Syntax

login success-url *url-string*

undo login success-url

Default

No redirection URL for authentication success is configured.

Views

Local portal Web service view

Predefined user roles

network-admin

context-admin

Parameters

url-string: Specifies the redirect URL for authentication success, a case-sensitive string of 1 to 256 characters.

Usage guidelines

The device redirects portal users to the specified URL after they pass authentication.

Examples

Configure the redirect URL for authentication success as **https://1.1.1.1/portal/islogin.html**.

```
<Sysname> system-view
[Sysname] portal local-web-server https
[Sysname-portal-local-websvr-https] login success-url
https://1.1.1.1/portal/islogin.html
```

logon-page bind

Use **logon-page bind** to bind an endpoint name or endpoint type to an authentication page file.

Use **undo logon-page bind** to unbind the endpoint name or endpoint type from the authentication page file.

Syntax

logon-page bind { **device-type** { **computer** | **pad** | **phone** } | **device-name** *device-name* } * **file** *file-name*

undo logon-page bind { **all** | **device-type** { **computer** | **pad** | **phone** } | **device-name** *device-name* } *

Default

No endpoint name or endpoint type is bound to an authentication page file.

Views

Local portal Web service view

Predefined user roles

network-admin

context-admin

Parameters

all: Specifies all endpoint names and endpoint types.

device-type *type-name*: Specifies an endpoint type.

computer: Specifies the endpoint type as computer.

pad: Specifies the endpoint type as tablet.

phone: Specifies the endpoint type as mobile phone.

device-name *device-name*: Specify an endpoint by its name, a case-sensitive string of 1 to 127 characters. The specified endpoint name must have been predefined on the device. Otherwise, the bound authentication page file does not take effect.

file *file-name*: Specifies an authentication page file by the file name (without the file storage directory). A file name is a string of 1 to 91 characters, and can contain letters, digits, and underscores (_). You must edit the authentication pages, compress them to a .zip file, and then upload the file to the root directory of the storage medium of the device.

Usage guidelines

This command implements customized authentication page pushing for portal users. After you configure this command, the device pushes authentication pages to users according to the user's, endpoint name and endpoint type.

When a Web user triggers local portal authentication, the device searches for a binding that matches the user's endpoint name and endpoint type.

- If the binding exists, the device pushes the bound authentication pages to the user.
- If multiple matching binding entries are found, the device selects an entry in the following order:
  a. The entry that specifies the endpoint name and endpoint type.
  b. The entry that specifies only the endpoint name.
  c. The entry that specifies only the endpoint type.
- If the binding does not exist, the device pushes the default authentication pages to the user.

When you configure this command, follow these restrictions and guidelines:

- If the name or content of the file in a binding entry is changed, you must reconfigure the binding.
- To reconfigure or modify a binding, you can simply re-execute this command without canceling the existing binding.
- If you execute this command multiple times to bind an endpoint name or endpoint type to different authentication page files, the most recent configuration takes effect.
- You can configure multiple binding entries on the device.

Examples

Create an HTTP-based local portal Web service.

```
<Sysname> system-view
[Sysname] portal local-web-server http
```

Bind endpoint type **phone** to authentication page file **file2.zip**.

```
[Sysname-portal-local-websvr-http] logon-page bind device-type phone file file2.zip
```

Related commands

default-logon-page

portal local-web-server

logout-notify

Use **logout-notify** to set the maximum number of times and the interval for retransmitting a logout notification packet.

Use **undo logout-notify** to restore the default.

Syntax

logout-notify retry *retries* **interval** *interval*

undo logout-notify

Default

The device does not retransmit a logout notification packet.

Views

Portal authentication server view

Predefined user roles

network-admin

context-admin

Parameters

retry *retries*: Specifies the maximum number of retries, in the range of 1 to 5.

interval *interval*: Specifies the retry interval, in the range of 1 to 10 seconds.

Usage guidelines

A logout notification packet is a UDP packet that the device sends to the portal authentication server for forcibly logging out a portal user. To increase the delivery reliability, you can set the maximum number of times and the interval for retransmitting a logout notification packet.

After the device sends a logout notification packet for logging out a portal user, it waits for a response from the portal authentication server. If the device receives a response within the specified period of time (maximum number of retries × retry interval), it logs out and deletes the user immediately. If the device does not receive a response within the period of time, the device logs out and deletes the user when the period of time elapses.

Examples

Set the maximum number of times for retransmitting a logout notification packet to 3 and the retry interval to 5 seconds.

```
<Sysname> system-view
[Sysname] portal server pt
[Sysname-portal-server-pt] logout-notify retry 3 interval 5
```

Related commands

display portal server

mail-domain-name

Use **mail-domain-name** to specify an email domain name for email authentication.

Use **undo mail-address** to remove an email domain name for email authentication.

Syntax

mail-domain-name *string*

undo mail-domain-name [*string*]

Default

No email domain names are specified for email authentication.

Views

Email authentication server view

Predefined user roles

network-admin

context-admin

Parameters

string: Specifies an email domain name for email authentication, a case-sensitive string of 1 to 255 characters, in the format of @XXX.XXX.

Usage guidelines

If you do not specify an email domain name in the **undo** form of this command, this command removes all email domain names for email authentication.

After you configure this command, the device performs email authentication only on portal users that use the specified email domain names.

You can specify a maximum of 16 email domain names for email authentication.

Examples

Specify **@qq.com** and **@sina.com** email domain names for email authentication.

```
<Sysname> system-view
[Sysname] portal extend-auth-server mail
[Sysname-portal-extend-auth-server-mail] mail-domain-name @qq.com
[Sysname-portal-extend-auth-server-mail] mail-domain-name @Sina.com
```

Related commands

display portal extend-auth-server

mail-protocol

Use **mail-protocol** to specify protocols for email authentication.

Use **undo mail-protocol** to restore the default.

Syntax

mail-protocol { **imap** | **pop3** } *

undo mail-protocol

Default

No protocols are specified for email authentication.

Views

Email authentication server view

Predefined user roles

network-admin

context-admin

Parameters

imap: Specifies the Internet Message Access Protocol (IMAP).

pop3: Specifies the Post Office Protocol 3 (POP3).

Usage guidelines

This command specifies email protocols that the device uses to interact with the email server to perform authentication and authorization on portal users who uses email authentication.

Examples

Specify POP3 as the protocol for email authentication.

```
<Sysname> system-view
[Sysname] portal extend-auth-server mail
```

```
[Sysname-portal-extend-auth-server-mail] mail-protocol pop3
```

Related commands

display portal extend-auth-server

nas-port-type

Use **nas-port-type** to specify the NAS-Port-Type value carried in RADIUS requests sent to the RADIUS server.

Use **undo nas-port-type** to restore the default.

Syntax

nas-port-type *value*

undo nas-port-type

Default

The NAS-Port-Type value carried in RADIUS requests is 15.

Views

MAC binding server view

Predefined user roles

network-admin

context-admin

Parameters

value: Specifies the NAS-Port-Type value in the range of 1 to 255.

Usage guidelines

Some MAC binding servers identify MAC-based quick portal authentication by a specific NAS-Port-Type value in received RADIUS requests. To communicate with such a MAC binding server, you must configure the device to use the NAS-Port-Type value required by the MAC binding server.

Examples

Set the NAS-Port-Type value in RADIUS requests sent to the MAC binding server **mts** to 30.

```
<Sysname> system-view
[Sysname] portal mac-trigger-server mts
[Sysname-portal-mac-trigger-server-mts] nas-port-type 30
```

Related commands

display portal mac-trigger-server

port (MAC binding server view)

Use **port** to set the UDP port number the MAC binding server uses to listen for MAC binding query packets.

Use **undo port** to restore the default.

Syntax

port *port-number*

undo port

Default

The MAC binding server listens for MAC binding query packets on UDP port 50100.

Views

MAC binding server view

Predefined user roles

network-admin

context-admin

Parameters

port-number: Specifies the listening UDP port number in the range of 1 to 65534.

Usage guidelines

The specified port number must be the same as the query listening port number configured on the MAC binding server.

Examples

Set the UDP port number to **1000** for the MAC binding server **pts** to listen for MAC binding query packets.

```
<sysname> system-view
[sysname] portal mac-trigger-server mts
[sysname-portal-mac-trigger-server-mts] port 1000
```

Related commands

display portal mac-trigger-server

port (portal authentication server view)

Use **port** to set the destination UDP port number used by the device to send unsolicited portal packets to the portal authentication server.

Use **undo port** to restore the default.

Syntax

port *port-number*

undo port

Default

The device uses 50100 as the destination UDP port number for unsolicited portal packets.

Views

Portal authentication server view

Predefined user roles

network-admin

context-admin

Parameters

port-number: Specifies a destination UDP port number the device uses to send unsolicited portal packets to the portal authentication server. The value range for this argument is 1 to 65534.

Usage guidelines

The specified port must be the port that listens to portal packets on the portal authentication server.

Examples

Set the destination UDP port number to **50000** for the device to send unsolicited portal packets to the portal authentication server **pts**.

```
<Sysname> system-view
[Sysname] portal server pts
[Sysname-portal-server-pts] port 50000
```

Related commands

portal server

portal ad-push

Use **portal ad-push** to specify an advertisement URL or advertisement group for portal advertisement push.

Use **undo portal ad-push** to restore the default.

Syntax

portal [**ipv6**] **ad-push** { **url** *url-string* [**interval** *interval* | **time-range** *time-range-name* | **traffic-threshold** *traffic-threshold*] | **url-group** *group-name* }

undo portal [**ipv6**] **ad-push** { **url** | **url-group** }

Default

No advertisement URL or advertisement group is specified for portal advertisement push.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ipv6: Specifies IPv6 URLs. To specify IPv4 URLs, do not specify this keyword.

url *url-string*: Specifies the URL of an advertisement to be pushed to portal users. The URL is a case-sensitive string of 1 to 256 characters and must begin with **http://**. If you specify the **ipv6** keyword, the URL of the advertisement must be an IPv6 URL.

url-group *group-name*: Specifies an advertisement group by its name, a case-sensitive string of 1 to 32 characters. The device will push advertisements in this group to portal users. If you specify the **ipv6** keyword, the URLs of advertisements in this group must be IPv6 URLs.

interval *interval*: Specifies the advertisement push interval, in the range of 5 to 1440 minutes. The interval begins when a portal user comes online.

time-range *time-range-name*: Specifies a time range for portal advertisement push. The *time-range-name* argument represents the name of the time range, a case-insensitive string of 1 to 32 characters. The time range name must begin with a letter and cannot be **all**. For more information about time ranges, see time range configuration in *ACL and QoS Configuration Guide*.

traffic-threshold *traffic-threshold*: Specifies the traffic threshold for portal advertisement push. The value range for the argument is 1 to 1024, in MB.

Usage guidelines

If you specify an advertisement group for portal advertisement push, the device uses the group advertisement push method specified by using the **portal ad-url-group** command.

If you specify an advertisement URL without configuring a push method, the device only pushes the advertisement to the portal user five seconds after the user comes online.

Examples

Configure the device to push the advertisement on URL **http://192.168.56.1/welcome** every 60 minutes to portal users on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] portal ad-push url http://192.168.56.1/welcome interval
60
```

Configure the device to push advertisements in advertisement group **test** to portal users on GigabitEthernet 1/0/2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] portal ad-push url-group test
```

Related commands

portal ad-push enable

portal ad-url-group

portal ad-push embedded

Use **portal ad-push embedded** to enable embedded portal advertisement push.

Use **undo portal ad-push embedded** to disable embedded portal advertisement push.

Syntax

portal ad-push embedded

undo portal ad-push embedded

Default

Embedded portal advertisement push is disabled. The advertisements that the device pushes to portal users are independent of the user visited webpages.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

This feature enables the device to embed advertisements in webpages that portal users visit.

Examples

Enable embedded portal advertisement push on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] portal ad-push embedded
```

Related commands

portal ad-push enable

portal ad-push enable

Use **portal ad-push enable** to enable portal advertisement push.

Use **undo portal ad-push enable** to disable portal advertisement push.

Syntax

portal ad-push enable

undo portal ad-push enable

Default

Portal advertisement push is disabled.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

This feature enables the device to push advertisements to portal users after they pass portal authentication.

Examples

Enable portal advertisement push on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] portal ad-push enable
```

Related commands

portal ad-push url

portal ad-push whitelist

Use **portal ad-push whitelist** to add a portal user to a portal advertisement whitelist.

Use **undo ad-push whitelist** to remove portal users from the portal advertisement whitelist.

Syntax

portal ad-push whitelist { **ip** *ipv4-address* | **ipv6** *ipv6-address* | **mac-address** *mac-address* }

undo portal ad-push whitelist { **all** | **ip** *ipv4-address* | **ipv6** *ipv6-address* | **mac-address** *mac-address* }

Default

No portal advertisement whitelist exists.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

all: Specifies all portal users.

ip *ipv4-address*: Specifies a portal user by its IPv4 address.

ipv6 *ipv6-address*: Specifies a portal user by its IPv6 address.

mac-address *mac-address*: Specifies a portal user by its MAC address in the format of H-H-H.

Usage guidelines

If a portal user has been added to the portal advertisement whitelist, the device does not push advertisements to the portal user.

You can execute this command multiple times to add multiple portal users to the portal advertisement whitelist. A maximum of 1024 portal users can be added to the whitelist.

Examples

Add portal user at IPv4 address 20.20.20.3 to the portal advertisement whitelist.

```
<Sysname> system-view
[Sysname] portal ad-push whitelist ip 20.20.20.3
```

Add portal user at IPv6 address 2000::0:3 to the portal advertisement whitelist.

```
<Sysname> system-view
[Sysname] portal ad-push whitelist ipv6 2000::0:3
```

Related commands

portal ad-push enable

portal ad-push url

portal ad-url-group

Use **portal ad-url-group** to create an advertisement group and enter its view, or enter the view of an existing advertisement group.

Use **undo portal ad-url-group** to delete an advertisement group.

Syntax

portal ad-url-group *group-name* [**method** { **interval** | **time-range** | **traffic** }]

undo portal ad-url-group *group-name*

Default

No advertisement groups exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies an advertisement group name, a case-sensitive string of 1 to 32 characters.

method: Specifies the advertisement push method. If you do not specify a method, the device uses the time-based advertisement push method.

interval: Specifies the time-based advertisement push method.

time-range: Specifies the time range-based advertisement push method. For more information about time ranges, see time range configuration in *ACL and QoS Configuration Guide*.

traffic: Specifies the traffic-based advertisement push method.

Usage guidelines

If you have specified an advertisement push method for an advertisement group, you cannot directly change the method. To change the method, use the **undo** form of this command to delete the advertisement group and then recreate it with the new method specified.

Examples

Create an advertisement group named **test** and specify the time-based advertisement push method.

```
<Sysname> system-view
[Sysname] portal ad-url-group test method interval
[Sysname-portal-ad-url-group-test]
```

Related commands

portal ad-push

portal apply mac-trigger-server

Use **portal apply mac-trigger-server** to specify a MAC binding server.

Use **undo portal apply mac-trigger-server** to restore the default.

Syntax

portal apply mac-trigger-server *server-name*

undo portal apply mac-trigger-server

Default

No MAC binding server is specified.

Views

VLAN interface view

Predefined user roles

network-admin

context-admin

Parameters

server-name: Specifies a MAC binding server by its name, a case-sensitive string of 1 to 32 characters.

Usage guidelines

Only direct IPv4 portal authentication supports MAC-based quick portal authentication.

For MAC-based quick portal authentication to take effect, perform the following tasks:

- Configure normal portal authentication.
- Configure a MAC binding server.
- Specify the MAC binding server on a portal-enabled VLAN interface.

Examples

Specify the MAC binding server **mts** on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] portal apply mac-trigger-server mts
```

Related commands

portal mac-trigger-server

portal apply web-server

Use **portal apply web-server** to specify a portal Web server. The device redirects the HTTP or HTTPS requests sent by unauthenticated portal users to the portal Web server.

Use **undo portal apply web-server** to delete a portal Web server.

Syntax

portal [**ipv6**] **apply web-server** *server-name* [**secondary**]

undo portal [**ipv6**] **apply web-server** [*server-name*]

Default

No portal Web servers are specified.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ipv6: Specifies an IPv6 portal Web server. If the server is an IPv4 portal Web server, do not specify this keyword.

secondary: Specifies the backup portal Web server. If you do not specify this keyword, the specified server is the primary portal Web server.

server-name: Specifies a portal Web server to be specified on the interface by its name, a case-sensitive string of 1 to 32 characters. The name must already exist. If you do not specify a server name in the **undo** form of this command, all portal Web servers on the interface are removed.

Usage guidelines

IPv4 and IPv6 portal authentication can both be enabled on an interface.

You can specify both a primary portal Web server and a backup portal Web server after enabling each type (IPv4 or IPv6) of portal authentication.

The device first uses the primary portal Web server for portal authentication. When the primary portal Web server is unreachable but the backup portal Web server is reachable, the device uses the backup portal Web server. When the primary portal Web server becomes reachable, the device switches back to the primary portal Web server for portal authentication.

To automatically switch between the primary portal Web server and the backup portal Web server, configure portal Web server detection on both servers.

Examples

Specify portal Web server **wbs** as the backup portal Web server on GigabitEthernet 1/0/1 for portal authentication.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] portal apply web-server wbs secondary
```

Related commands

display portal

portal fail-permit server

portal web-server

server-detect (portal Web server view)

portal auth-error-record enable

Use **portal auth-error-record enable** to enable portal authentication error recording.

Use **undo portal auth-error-record enable** to disable portal authentication error recording.

Syntax

portal auth-error-record enable

undo portal auth-error-record enable

Default

Portal authentication error recording is enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This feature enables the device to save all portal authentication error records and to periodically send the records to the authentication server.

Examples

Enable portal authentication error recording.

```
<Sysname> system-view
[Sysname] portal auth-error-record enable
```

Related commands

display portal auth-error-record

portal auth-error-record export

Use **portal auth-error-record export** to export portal authentication error records to a path.

Syntax

portal auth-error-record export url *url-string* [**start-time** *start-date start-time* **end-time** *end-date end-time*]

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

url *url-string*: Specifies the URL to which portal authentication error records are exported. The URL is a case-insensitive string of 1 to 255 characters. The URL string can include question marks (?). If you enter a question mark (?) in the place of the *url-string* argument, the CLI does not display help information for this argument.

start-time *start-date start-time* **end-time** *end-date end-time*: Specifies a time range. The start date and end date must be in the format of MM/DD/YYYY or YYYY/MM/DD. The value range for MM is 1 to 12. The value range for DD varies with the specified month. The value range for YYYY is 1970 to 2037. The start time and end time must be in the format of hh:mm. The value range for the start time and end time is 00:00 to 23:59.

Usage guidelines

The device supports FTP, TFTP, and HTTP file transfer methods. Table 32 describes the valid URL format for each method.

Table 32 URL formats

Protocol	URL format	Remarks
FTP	ftp://*username*[:*password*]@*server-address*[:*port-number*]/*file-path* Example: **ftp://a:1@1.1.1.1/authfail/**	The username and password must be the same as those on the server. If the server authenticates only the username, no password is required.
TFTP	tftp://*server-address*[:*port-number*]/*file-path* Example: **tftp://1.1.1.1/ autherror/**	N/A
HTTP	http://*username*[:*password*]@*server-address*[:*port-number*]/*file-path* Example: **http://1.1.1.1/autherror/**	The username and password must be the same as those on the server. If the server authenticates only the username, no password is required.

If the server address is an IPv6 address, bracket the IPv6 address to distinguish the IPv6 address from the port number. For example, if the server address is **2001::1** and the port number is 21, the URL is **ftp://test:test@[2001::1]/test/**.

Examples

Export all portal authentication error records to path **tftp://1.1.1.1/record/autherror/**.

```
<Sysname> system-view
[Sysname] portal auth-error-record export url tftp://1.1.1.1/record/autherror/
```

Export portal authentication error records in the time range from 2016/3/4 14:20 to 2016/3/4 15:00 to path **tftp://1.1.1.1/record/autherror/**.

```
<Sysname> system-view
```

```
[Sysname] portal auth-error-record export url tftp://1.1.1.1/record/autherror/
start-time 2016/3/4 14:20 end-time 2016/3/4 15:00
```

Related commands

display portal auth-error-record

portal auth-error-record enable

reset portal auth-error-record

portal auth-error-record max

Use **portal auth-error-record max** to set the maximum number of portal authentication error records.

Use **undo portal auth-error-record max** to restore the default.

Syntax

portal auth-error-record max *number*

undo portal auth-error-record max

Default

Models	Default
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280	The device supports a maximum of 60000 portal authentication error records.
NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	The device supports a maximum of 24000 portal authentication error records.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

number: Specifies the maximum number of portal authentication error records.

The following compatibility matrixes show the value ranges for this argument:

Models	Value range
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280	1 to 60000
NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	1 to 24000

Usage guidelines

When the maximum number of portal authentication error records is reached, a new record overwrites the oldest one.

Examples

Set the maximum number of portal authentication error records to 50.

```
<Sysname> system-view
[Sysname] portal auth-error-record max 50
```

Related commands

display portal auth-error-record

portal auth-fail-record enable

Use **portal auth-fail-record enable** to enable portal authentication failure recording.

Use **undo portal auth-fail-record enable** to disable portal authentication failure recording.

Syntax

portal auth-fail-record enable

undo portal auth-fail-record enable

Default

Portal authentication failure recording is enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This feature enables the device to save portal authentication failure records and to periodically send the records to the authentication server.

Examples

Enable portal authentication failure recording.

```
<Sysname> system-view
[Sysname] portal auth-fail-record enable
```

Related commands

display portal auth-fail-record

portal auth-fail-record export

Use **portal auth-fail-record export** to export portal authentication failure records to a path.

Syntax

portal auth-fail-record export url *url-string* [**start-time** *start-date start-time* **end-time** *end-date end-time*]

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

url *url-string*: Specifies the URL to which portal authentication failure records are exported. The URL is a case-insensitive string of 1 to 255 characters. The URL string can include question marks (?). If you enter a question mark (?) in the place of the *url-string* argument, the CLI does not display help information for this argument.

start-time *start-date start-time* **end-time** *end-date end-time*: Specifies a time range. The start date and end date must be in the format of MM/DD/YYYY or YYYY/MM/DD. The value range for MM is 1 to 12. The value range for DD varies with the specified month. The value range for YYYY is 1970 to 2037. The start time and end time must be in the format of hh:mm. The value range for the start time and end time is 00:00 to 23:59.

Usage guidelines

The device supports FTP, TFTP, and HTTP file transfer methods. Table 33 describes the valid URL format for each method.

Table 33 URL formats

Protocol	URL format	Remarks
FTP	ftp://*username*[:*password*]@*server-address*[:*port-number*]/*file-path* Example: **ftp://a:1@1.1.1.1/authfail/**	The username and password must be the same as those on the server. If the server authenticates only the username, no password is required.
TFTP	tftp://*server-address*[:*port-number*]/*file-path* Example: **tftp://1.1.1.1/ autherror/**	N/A
HTTP	http://*username*[:*password*]@*server-address*[:*port-number*]/*file-path* Example: **http://1.1.1.1/autherror/**	The username and password must be the same as those on the server. If the server authenticates only the username, no password is required.

If the server address is an IPv6 address, bracket the IPv6 address to distinguish the IPv6 address from the port number. For example, if the server address is **2001::1** and the port number is 21, the URL is **ftp://test:test@[2001::1]/test/**.

Examples

Export all portal authentication failure records to path **tftp://1.1.1.1/record/authfail/**.

```
<Sysname> system-view
[Sysname] portal auth-fail-record export url tftp://1.1.1.1/record/authfail/
```

Export portal authentication failure records in the time range from 2016/3/4 14:20 to 2016/3/4 15:00 to path **tftp://1.1.1.1/record/authfail/**.

```
<Sysname> system-view
[Sysname] portal auth-fail-record export url tftp://1.1.1.1/record/authfail/ start-time
2016/3/4 14:20 end-time 2016/3/4 15:00
```

Related commands

display portal auth-fail-record

portal auth-fail-record enable

reset portal auth-fail-record

portal auth-fail-record max

Use **portal auth-fail-record max** to set the maximum number of portal authentication failure records.

Use **undo portal auth-fail-record max** to restore the default.

Syntax

portal auth-fail-record max *number*

undo portal auth-fail-record max

Default

Models	Default
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280	The maximum number of portal authentication failure records is 60000.
NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	The maximum number of portal authentication failure records is 24000.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

number: Specifies the maximum number of portal authentication failure records.

The following compatibility matrixes show the value ranges for this argument:

Models	Value range
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280	1 to 60000
NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	1 to 24000

Usage guidelines

When the maximum number of portal authentication failure records is reached, a new record overwrites the oldest one.

Examples

Set the maximum number of portal authentication failure records to 50.

```
<Sysname> system-view
[Sysname] portal auth-fail-record max 50
```

Related commands

display portal auth-fail-record

portal authorization strict-checking

Use **portal authorization strict-checking** to enable strict checking on portal authorization information.

Use **undo portal authorization strict-checking** to disable strict checking on portal authorization information.

Syntax

portal authorization acl strict-checking

undo portal authorization acl strict-checking

Default

Strict checking mode on portal authentication information is disabled. If an authorized ACL does not exist on the device or the ACL fails to be deployed, the user will not be logged out.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

CAUTION:

- The strict checking feature on an interface allows a portal user to stay online only when the authorization information for the user is successfully deployed. The strict checking fails if the authorized ACL does not exist on the device or the device fails to deploy the authorized ACL.

Examples

Enable strict checking on authorized ACLs on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname–GigabitEthernet1/0/1] portal authorization acl strict-checking
```

Related commands

display portal

portal captive-bypass optimize delay

Use **portal captive-bypass optimize delay** to set the captive-bypass detection timeout time.

Use **undo portal captive-bypass optimize delay** to restore the default.

Syntax

portal captive-bypass optimize delay *seconds*

undo portal captive-bypass optimize delay

Default

The captive-bypass detection timeout time is 6 seconds.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies the captive-bypass detection timeout time, in the range of 1 to 120 seconds.

Usage guidelines

This command applies only to iOS mobile clients.

With optimized captive-bypass enabled, the device automatically pushes the portal authentication page to iOS mobile devices when they are connected to the network. Users can perform authentication on the page or press the home button to return to the desktop without performing authentication, and the Wi-Fi connection is not terminated.

Optimized captive-bypass might fail when the network condition is poor. The device cannot detect a server reachability detection packet from an iOS mobile device within the captive-bypass detection timeout time. Therefore, the Wi-Fi connection will be terminated on the iOS mobile device. To avoid Wi-Fi disconnections caused by server reachability detection failure, you can set a longer captive-bypass detection timeout time when the network condition is poor.

Examples

Set the captive-bypass detection timeout time to 20 seconds.

```
<Sysname> system-view
[Sysname] portal captive-bypass optimize delay 20
```

Related commands

captive-bypass enable

portal cloud report interval

Use **portal cloud report interval** to configure the time interval at which portal authentication information is reported to the cloud server.

Use **undo portal cloud report interval** to restore the default.

Syntax

portal cloud report interval *minutes*

undo portal cloud report interval

Default

The portal authentication information is reported to the cloud server at intervals of 5 minutes.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

minutes: Specifies the time interval at which portal authentication information is reported to the cloud server. The value range for the time interval is 0 to 60 minutes. If you set the interval to 0 minutes, the device does not report portal authentication information to the cloud server.

Usage guidelines

After you configure this command, the device reports portal authentication failure and error information to the cloud server. The first report is sent to the cloud server 30 seconds after the device is connected to the server. The subsequent reports are sent at regularly intervals as configured by the command.

If you modify the report interval, the modified interval takes effect for the next report.

Examples

Configure the device to report portal authentication failure and error information to the cloud server at intervals of 60 minutes.

```
<Sysname> system-view
[Sysname] portal cloud report interval 60
```

portal delete-user

Use **portal delete-user** to log out online portal users.

Syntax

portal delete-user { *ipv4-address* | **all** | **auth-type** { **cloud** | **email** | **facebook** | **local** | **normal** | **qq** | **wechat** } | **interface** *interface-type interface-number* | **ipv6** *ipv6-address* | **mac** *mac-address* | **username** *username* }

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-address: Specifies the IP address of an IPv4 online portal user.

all: Specifies IPv4 and IPv6 online portal users on all interfaces.

auth-type: Specifies online portal users by the authentication type.

cloud: Specifies the cloud authentication.

email: Specifies the email authentication.

facebook: Specifies the Facebook authentication.

local: Specifies the local authentication.

normal: Specifies the normal authentication.

qq: Specifies the QQ authentication.

wechat: Specifies the WeChat authentication.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you specify this option, this command logs out all IPv4 and IPv6 online portal users on the interface.

ipv6 *ipv6-address*: Specifies the IP address of an IPv6 online portal user.

mac *mac-address*: Specifies the MAC address of an online portal user, in the format of H-H-H.

username *username*: Specifies the username of an online portal user, a case-sensitive string of 1 to 253 characters. The username cannot contain the domain name.

Examples

Log out the portal user whose IP address is **1.1.1.1**.

```
<Sysname> system-view
[Sysname] portal delete-user 1.1.1.1
```

Log out the portal user whose MAC address is **000d-88f8-0eab**.

```
<Sysname> system-view
[Sysname] portal delete-user mac 000d-88f8-0eab
```

Log out all portal users that come online through email authentication.

```
<Sysname> system-view
[Sysname] portal delete-user auth-type email
```

Log out the portal user whose username is **abc**.

```
<Sysname> system-view
[Sysname] portal delete-user username abc
```

Related commands

display portal user

portal device-id

Use **portal device-id** to specify the device ID.

Use **undo portal device-id** to restore the default.

Syntax

portal device-id *device-id*

undo portal device-id

Default

A device is not configured with a device ID.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

device-id: Specifies a device ID for the device, a case-sensitive string of 1 to 63 characters.

Usage guidelines

The portal authentication server uses device IDs to identify the device that sends protocol packets to the portal server.

Make sure the configured device ID is different than any other access devices communicating with the same portal authentication server.

Examples

Set the device ID of the device to 0002.0010.100.00.

```
<Sysname> system-view
[Sysname] portal device-id 0002.0010.100.00
```

portal domain

Use **portal domain** to configure a portal authentication domain. All portal users accessing through the interface must use the authentication domain.

Use **undo portal domain** to delete the configured portal authentication domain.

Syntax

portal [**ipv6**] **domain** *domain-name*

undo portal [**ipv6**] **domain**

Default

No portal authentication domain is configured.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ipv6: Specifies an authentication domain for IPv6 portal users. Do not specify this keyword for IPv4 portal users.

domain-name: Specifies an ISP authentication domain by its name, a case-insensitive string of 1 to 255 characters.

Usage guidelines

You can specify both an IPv4 portal authentication domain and an IPv6 portal authentication domain on an interface.

Do not specify the **ipv6** keyword for IPv4 portal users.

Examples

Configure the authentication domain for IPv4 portal users as **my-domain** on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname–GigabitEthernet1/0/1] portal domain my-domain
```

Related commands

display portal

portal dual-ip enable

Use **portal dual-ip enable** to enable the dual IP feature for single-stack portal users in remote portal authentication.

Use **undo portal dual-ip enable** to disable the dual IP feature for single-stack portal users in remote portal authentication.

Syntax

portal dual-ip enable

undo portal dual-ip enable

Default

The dual IP feature is disabled for single-stack portal users in remote portal authentication.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

This feature enables the device to carry both an IPv4 address and an IPv6 address for single-stack portal users in the authentication requests during remote portal authentication. For IPv4 portal users, the carried IPv6 address is 0. For IPv6 portal users, the carried IPv4 address is 0.

This feature is applicable only to RADIUS-based remote portal authentication.

Some RADIUS servers require that both IPv4 and IPv6 addresses of portal users must be carried in portal authentication requests. To avoid authentication failure, enable this feature for single-stack portal users when such a RADIUS server is used.

Examples

Enable the dual IP feature on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname–Vlan-interface100] portal dual-ip enable
```

portal dual-stack enable

Use **portal dual-stack enable** to enable the portal dual-stack feature.

Use **undo portal dual-stack enable** to disable the portal dual-stack feature.

Syntax

portal dual-stack enable

undo portal dual-stack enable

Default

The portal dual-stack feature is disabled.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

The portal dual-stack feature enables portal users to access both IPv4 and IPv6 networks after passing one type (IPv4 or IPv6) of portal authentication.

Only direct portal authentication supports this feature.

Examples

Enable the portal dual-stack feature on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] portal dual-stack enable
```

Related commands

portal dual-stack traffic-separate enable

portal dual-stack traffic-separate enable

Use **portal dual-stack traffic-separate enable** to enable separate IPv4 and IPv6 traffic statistics for dual-stack portal users.

Use **undo portal dual-stack traffic-separate enable** to disable separate IPv4 and IPv6 traffic statistics for dual-stack portal users.

Syntax

portal dual-stack traffic-separate enable

undo portal dual-stack traffic-separate enable

Default

Separate IPv4 and IPv6 traffic statistics is disabled for dual-stack portal users. The device collects IPv4 and IPv6 traffic statistics collectively.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

This feature enables the device to separately collect IPv4 traffic statistics and IPv6 traffic statistics for a dual-stack portal user. Then, the AAA server can separately perform accounting on IPv4 traffic and IPv6 traffic of the user.

For this feature to take effect, you must enable the portal dual-stack feature.

This command has a higher priority over the **accounting dual-stack** command in ISP domain view. For more information about the **accounting dual-stack** command, see "AAA commands."

Examples

Enable separate IPv4 and IPv6 traffic statistics for dual-stack portal users on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] portal dual-stack traffic-separate enable
```

Related commands

accounting dual-stack

portal dual-stack enable

portal enable (interface view)

Use **portal enable** to enable portal authentication.

Use **undo portal enable** to disable portal authentication.

Syntax

portal enable method { **direct** | **layer3** | **redhcp** }

portal ipv6 enable method { **direct** | **layer3** }

undo portal [**ipv6**] **enable**

Default

Portal authentication is disabled.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ipv6: Enables IPv6 portal authentication. Do not specify this keyword for IPv4 portal authentication.

method: Specifies an authentication mode.

direct: Specifies direct authentication.

layer3: Specifies cross-subnet authentication.

redhcp: Specifies re-DHCP authentication.

Usage guidelines

To modify the portal authentication mode, first execute the **undo** form of this command to disable portal authentication.

Make sure the device supports IPv6 ACL and IPv6 forwarding before you enable IPv6 portal authentication on the interface.

IPv6 portal authentication does not support the re-DHCP authentication mode.

You can enable both IPv4 portal authentication and IPv6 portal authentication on an interface.

Do not add a portal authentication-enabled Ethernet interface to an aggregation group. Otherwise, portal authentication cannot take effect on the interface.

Examples

Enable direct IPv4 portal authentication on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] portal enable method direct
```

Related commands

display portal

portal extend-auth domain

Use **portal extend-auth domain** to specify the authentication domain for third-party authentication.

Use **undo portal extend-auth domain** to remove the authentication domain for third-party authentication.

Syntax

portal extend-auth domain *domain-name*

undo portal extend-auth domain

Default

No authentication domain is specified for third-party authentication.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

domain-name: Specifies an ISP domain by its name, a case-insensitive string of 1 to 255 characters.

Usage guidelines

The specified ISP domain takes effect only on IPv4 portal users that use third-party authentication.

Make sure the authentication, authorization, and accounting methods in the authentication domain are **none**.

Examples

Specify authentication domain **my-domain** for third-party authentication on GigabitEthernet1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname–GigabitEthernet1/0/1] portal extend-auth domain my-domain
```

Related commands

display portal

portal extend-auth-server

Use **portal extend-auth-server** to create a third-party authentication server and enter its view, or enter the view of an existing third-party authentication server.

Use **undo portal extend-auth-server** to delete a third-party authentication server.

Syntax

portal extend-auth-server { **facebook** | **mail** | **qq** | **wechat** }

undo portal extend-auth-server { **facebook** | **mail** | **qq** | **wechat** }

Default

No third-party authentication servers exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

facebook: Specifies the Facebook authentication server.

mail: Specifies the email authentication server.

qq: Specifies the QQ authentication server.

wechat: Specifies the WeChat authentication server.

Usage guidelines

The device supports using a third-party portal authentication server for portal authentication. A portal user can use a third-party account instead of a portal account to perform portal authentication. If the user passes third-party authentication, the third-party server notifies the third-party authentication success of the user to the device. Then, the device interacts with the local portal Web service to complete the remaining process of portal authentication.

Only direct portal authentication that uses a local portal Web portal service supports third-party authentication.

Examples

Create a QQ authentication server and enter its view.

```
<Sysname> system-view
[Sysname] portal extend-auth-server qq
[Sysname-portal-extend-auth-server-qq]
```

Create an email authentication server and enter its view.

```
<Sysname> system-view
[Sysname] portal extend-auth-server mail
[Sysname-portal-extend-auth-server-mail]
```

Create a WeChat authentication server and enter its view.

```
<Sysname> system-view
[Sysname] portal extend-auth-server wechat
[Sysname-portal-extend-auth-server-wechat]
```

Create a Facebook authentication server and enter its view.

```
<Sysname> system-view
[Sysname] portal extend-auth-server facebook
[Sysname-portal-extend-auth-server-fb]
```

Related commands

display portal extend-auth-server

portal fail-permit server

Use **portal fail-permit server** to enable the portal fail-permit feature for a portal authentication server.

Use **undo portal fail-permit server** to disable the portal fail-permit feature for the portal authentication server.

Syntax

portal [**ipv6**] **fail-permit server** *server-name*

undo portal [**ipv6**] **fail-permit server**

Default

Portal fail-permit is disabled for the portal authentication server.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ipv6: Specifies an IPv6 portal authentication server. Do not specify this keyword for an IPv4 portal authentication server.

server-name: Specifies a portal authentication server by its name, a case-sensitive string of 1 to 32 characters.

Usage guidelines

On an interface, you can enable portal fail-permit for both the portal authentication server and the portal Web servers.

On an interface enabled with portal fail-permit for a portal authentication server and portal Web servers, portal authentication on the interface is disabled in either of the following conditions:

- All portal Web servers are unreachable.
- The specified portal authentication server is unreachable.

Portal authentication resumes on the interface when the specified portal authentication server and a minimum of one portal Web server becomes reachable. After portal authentication resumes, unauthenticated portal users need to pass authentication to access network resources. Portal users who have passed authentication can continue accessing network resources.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Enable portal fail-permit for portal authentication server **pts1** on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] portal fail-permit server pts1
```

Related commands

display portal

portal fail-permit web-server

Use **portal fail-permit web-server** to enable the portal fail-permit feature for portal Web servers.

Use **undo portal fail-permit web-server** to disable the portal fail-permit feature for portal Web servers.

Syntax

portal [**ipv6**] **fail-permit web-server**

undo portal [**ipv6**] **fail-permit web-server**

Default

Portal fail-permit is disabled for portal Web servers.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ipv6: Specifies IPv6 portal Web servers. To specify IPv4 portal Web servers, do not specify this keyword.

Usage guidelines

On an interface enabled with portal fail-permit for a portal authentication server and portal Web servers, portal authentication on the interface is disabled in either of the following conditions:

- All portal Web servers are unreachable.
- The specified portal authentication server is unreachable.

Portal authentication resumes on the interface when the specified portal authentication server and a minimum of one portal Web server becomes reachable. After portal authentication resumes, unauthenticated portal users need to pass authentication to access network resources. Portal users who have passed authentication can continue accessing network resources.

Examples

Enable portal fail-permit for the portal Web servers on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname–GigabitEthernet1/0/1] portal fail-permit web-server
```

Related commands

display portal

portal forbidden-rule

Use **portal forbidden-rule** to configure a portal-forbidden rule.

Use **undo portal forbidden-rule** to delete portal-forbidden rules.

Syntax

portal forbidden-rule *rule-number* [**source ip** { *ipv4-address* { *mask-length* | *mask* } | **any** } [**tcp** *tcp-port-number* | **udp** *udp-port-number*]] **destination** { *host-name* | **ip** { *ipv4-address* { *mask-length* | *mask* } | **any** } [**tcp** *tcp-port-number* | **udp** *udp-port-number*] }

portal forbidden-rule *rule-number* [**source ipv6** { *ipv6-address prefix-length* | **any** } [**tcp** *tcp-port-number* | **udp** *udp-port-number*]] **destination** { *host-name* | **ipv6** { *ipv6-address prefix-length* | **any** } [**tcp** *tcp-port-number* | **udp** *udp-port-number*] }

undo portal forbidden-rule { *rule-number* | **all** }

Default

No portal-forbidden rules are configured.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

rule-number: Specifies the number of a portal-forbidden rule. The value range for this argument is 0 to 4294967295.

source: Specifies the source information.

ip *ipv4-address*: Specifies an IPv4 address.

{ *mask-length* | *mask* }: Specifies the subnet mask of the IPv4 address. The *mask-length* argument represents the length of a subnet mask, in the range of 0 to 32. The *mask* argument represents a subnet mask in dotted decimal notation.

ip any: Specifies any IPv4 address.

tcp *tcp-port-number*: Specifies a TCP port number in the range of 0 to 65535.

udp *udp-port-number*: Specifies a UDP port number in the range of 0 to 65535.

ipv6 *ipv6-address*: Specifies an IPv6 address.

prefix-length: Specifies the prefix length of the IPv6 address, in the range of 0 to 128.

ipv6 any: Specifies any IPv6 address.

host-name: Specifies a destination host by its name, a case-insensitive string of 1 to 253 characters. Valid characters include letters, digits, hyphens (-), underscores (_), and dots (.). The host name cannot be **i**, **ip**, **ipv**, or **ipv6**.

all: Specifies all portal-forbidden rules.

Usage guidelines

Portal-forbidden rules are used to filter user packets from the specified sources or destined for the specified destinations. The device drops user packets that match the portal-forbidden rules.

Portal-forbidden rules take effect only when portal authentication is enabled.

In a portal-forbidden rule, the source and destination IP addresses must be of the same IP type, and the source and destination ports must be of the same transport protocol type.

You can configure multiple portal-forbidden rules.

If the source or destination information in a portal-free rule and that in a portal-forbidden rule overlap, the portal-forbidden rule takes effect.

If you specify a destination host name in a portal-forbidden rule, the device drops users' DNS query packets for the specified host name. In addition, if a DNS server is correctly configured on the device, the device also drops user packets destined for the IP address resolved from the specified host name. If the DNS server is not correctly configured, the rule does not take effect on user packets destined for that IP address.

Examples

Configure portal-forbidden rule 10 to prohibit portal users from accessing website **www.xyz.com**.

```
<Sysname> system-view
[Sysname] portal forbidden-rule 10 source ip any destination www.xyz.com
```

Configure portal-forbidden rule 12 to prohibit the portal user with IP address 1.1.1.1/32 from accessing IP address 2.2.2.2/32.

```
<Sysname> system-view
[Sysname] portal forbidden-rule 12 source ip 1.1.1.1 32 destination ip 2.2.2.2 32
```

Related commands

display portal rule

portal free-all except destination

Use **portal free-all except destination** to configure an IPv4 portal authentication destination subnet on an interface.

Use **undo portal free-all except destination** to delete the IPv4 portal authentication destination subnets on the interface.

Syntax

portal free-all except destination *ipv4-network-address* { *mask-length* | *mask* }

undo portal free-all except destination [*ipv4-network-address*]

Default

No IPv4 portal authentication destination subnet is configured on the interface. Portal users must pass portal authentication to access any subnet.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-network-address: Specifies an IPv4 portal authentication subnet address.

mask-length: Specifies the subnet mask length for the authentication subnet address, in the range of 0 to 32.

mask: Specifies the subnet mask in dotted decimal format.

Usage guidelines

Portal users on the interface are authenticated when accessing the specified authentication destination subnet (except IP addresses and subnets specified in portal-free rules). The users can access other subnets without portal authentication.

If you do not specify the *ipv4-network-address* argument in the **undo portal free-all except destination** command, this commands deletes all IPv4 portal authentication destination subnets on the interface.

Re-DHCP authentication does not support authentication destination subnets.

If you configure both an authentication source subnet and an authentication destination subnet on an interface, only the authentication destination subnet takes effect.

You can repeat this command to configure multiple authentication destination subnets.

Examples

Configure an IPv4 portal authentication destination subnet of **11.11.11.0**/**24** on GigabitEthernet 1/0/1. Portal users need to pass authentication to access this subnet and can access other subnets without authentication.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname–GigabitEthernet1/0/1] portal free-all except destination 11.11.11.0 24
```

Related commands

display portal

portal free-rule

Use **portal free-rule** to configure an IP-based portal-free rule.

Use **undo portal free-rule** to delete portal-free rules.

Syntax

portal free-rule *rule-number* { **destination ip** { *ipv4-address* { *mask-length* | *mask* } | **any** } [**tcp** *tcp-port-number* | **udp** *udp-port-number*] | **source ip** { *ipv4-address* { *mask-length* | *mask* } | **any** } [**tcp** *tcp-port-number* | **udp** *udp-port-number*] } * [**interface** *interface-type interface-number*]

portal free-rule *rule-number* { **destination ipv6** { *ipv6-address prefix-length* | **any** } [**tcp** *tcp-port-number* | **udp** *udp-port-number*] | **source ipv6** { *ipv6-address prefix-length* | **any** } [**tcp** *tcp-port-number* | **udp** *udp-port-number*] } * [**interface** *interface-type interface-number*]

undo portal free-rule { *rule-number* | **all** }

Default

No IP-based portal-free rule is configured.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

rule-number: Specifies a portal-free rule number. The value range for this argument is 0 to 4294967295.

destination: Specifies the destination information.

source: Specifies the source information.

ip *ipv4-address*: Specifies an IPv4 address for the portal-free rule.

{ *mask-length* | *mask* }: Specifies the subnet mask of the IPv4 address. The value range for the *mask-length* argument is 0 to 32. The *mask* argument is in dotted decimal format.

ip any: Represents any IPv4 address.

tcp *tcp-port-number*: Specifies a TCP port number for the portal-free rule, in the range of 0 to 65535.

udp *udp-port-number*: Specifies a UDP port number for the portal-free rule, in the range of 0 to 65535.

ipv6 *ipv6-address*: Specifies an IPv6 address for the portal-free rule.

prefix-length: Specifies the prefix length of the IPv6 address, in the range of 0 to 128.

ipv6 any: Represents any IPv6 address.

all: Specifies all portal-free rules.

interface *interface-type interface-number*: Specifies a Layer 3 interface on which the portal-free rule takes effect.

Usage guidelines

You can specify both the **source** and **destination** keyword for a portal-free rule. If you specify only one keyword, the other keyword does not act as a filtering criterion.

If you specify both a source port number and a destination port number for a portal-free rule, the two port numbers must belong to the same transport layer protocol.

If you do not specify a Layer 3 interface, the portal-free rule takes effect on all portal-enabled interfaces.

You cannot configure two portal-free rules with the same filtering criteria.

Examples

Configure an IPv4-based portal-free rule numbered **1** for GigabitEthernet 1/0/1. In the rule, the source IP address is 10.10.10.1/24, the destination IP address is 20.20.20.1/32, the destination TCP port number is 23.

```
<Sysname> system-view
[Sysname] portal free-rule 1 destination ip 20.20.20.1 32 tcp 23 source ip 10.10.10.1 24
interface gigabitethernet 1/0/1
```

Configure an IPv6-based portal-free rule numbered **2** for GigabitEthernet 1/0/1. In this rule, the source IPv6 address is 2000::1/64, the destination IPv6 address is 2001::1/128, the destination TCP port number is 23.

```
<Sysname> system-view
[Sysname] portal free-rule 2 destination ipv6 2001::1 128 tcp 23 source ipv6 2000::1 64
interface gigabitethernet 1/0/1
```

Related commands

display portal rule

portal free-rule acl

Use **portal free-rule acl** to configure an ACL-based portal-free rule.

Use **undo portal free-rule acl** to delete portal-free rules.

Syntax

portal free-rule *rule-number* **acl** [**ipv6**] *acl-number*

undo portal free-rule { *rule-number* | **all** }

Default

No ACL-based portal-free rules exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

rule-number: Specifies a portal-free rule number. The value range for this argument is 0 to 4294967295.

ipv6: Specifies an IPv6 ACL-based portal-free rule. To configure an IPv4 ACL-based portal-free rule, do not specify this keyword.

acl-number: Specifies an ACL number in the range of 2000 to 3999.

all: Specifies all portal-free rules.

Usage guidelines

The ACL used by a portal-free rule can contain only IP address object groups and IP quintuples (source and destination IP addresses, source and destination port numbers, and transport layer protocol).

If an ACL has already been used by a portal-free rule, you cannot configure another portal-free rule that uses the same ACL.

If the specified ACL does not exist or does not contain rules, all users are allowed to access network resources without passing portal authentication.

If the **vpn-instance** keyword is specified in an ACL rule, the rule applies only to VPN packets. If the **vpn-instance** keyword is not specified in an ACL rule, the rule applies only to public network packets.

Examples

Configure an IPv4 ACL-based portal-free rule numbered **1**. This portal-free rule allows portal user traffic that matches ACL 3001 to pass through without authentication.

```
<Sysname> system-view
[Sysname] portal free-rule 1 acl 3001
```

Configure an IPv6 ACL-based portal-free rule numbered **2**. This portal-free rule allows portal user traffic that matches ACL 3001 to pass through without authentication.

```
<Sysname> system-view
[Sysname] portal free-rule 2 acl ipv6 3001
```

portal free-rule description

Use **portal free-rule description** to configure a description for a portal-free rule.

Use **undo portal free-rule description** to delete the description of a portal-free rule.

Syntax

portal free-rule *rule-number* **description** *text*

undo portal free-rule *rule-number* **description**

Default

No description is configured for a portal-free rule.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

rule-number: Specifies a portal-free rule by its rule number. The value range for this argument is 0 to 4294967295.

text: Specifies the description, a case-sensitive string of 1 to 255 characters.

Examples

Configure a description of **This is IT department** for portal-free rule 2.

```
<Sysname> system-view
[Sysname] portal free-rule 2 description This is IT department
```

portal free-rule destination

Use **portal free-rule destination** to configure a destination-based portal-free rule.

Use **undo portal free-rule** to delete portal-free rules.

Syntax

portal free-rule *rule-number* **destination** *host-name*

undo portal free-rule { *rule-number* | **all** }

Default

No destination-based portal-free rule is configured.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

rule-number: Specifies a portal-free rule number. The value range for this argument is 0 to 4294967295.

destination: Specifies the destination host.

host-name: Specifies the destination host by its name, a case-insensitive string of 1 to 253 characters. Valid characters are letters, digits, hyphens (-), underscores (_), dots (.), and asterisks (*). The host name string cannot be **i**, **ip**, **ipv**, or **ipv6**.

all: Specifies all portal-free rules.

Usage guidelines

Before you configure destination-based portal-free rules, make sure a DNS server has been deployed in the network.

You can configure a host name in one of the following ways:

- **For exact match**—Specify a complete host name. For example, if you configure the host name as **abc.com.cn** in the portal-free rule, only packets that contain the host name **abc.com.cn** match the rule. Packets that carry any other host names (such as **dfabc.com.cn**) do not match the rule.
- **For fuzzy match**—Specify a host name by placing the asterisk (*) wildcard character at the beginning or end of the host name string. For example, if you configure the host name as ***abc.com.cn, abc***, or ***abc***, packets that carry the host name ending with **abc.com.cn**, starting with **abc**, or including **abc** match the rule.

The asterisk (*) wildcard character represents any characters. The device treats multiple consecutive asterisks as one.

The configured host name cannot contain only asterisks (*).

The fuzzy match feature takes effect only on HTTP or HTTPS requests initiated by Web browsers.

You cannot configure two destination-based portal-free rules with the same destination information. Otherwise the system prompts you that the same rule already exists.

Examples

Configure a destination-based portal-free rule: specify the rule number as **4** and host name as **www.abc.com**. This rule allows the portal user who sends the HTTP/HTTPS request that carries the host name **www.abc.com** to access network resources without authentication.

```
<Sysname> system-view
[Sysname] portal free-rule 4 destination www.abc.com
```

Related commands

display portal rule

portal free-rule source

Use **portal free-rule source** to configure a source-based portal-free rule. The filtering criteria include source MAC address, source interface, and source VLAN.

Use **undo portal free-rule** to delete a specific or all portal-free rules.

Syntax

portal free-rule *rule-number* **source** { **interface** *interface-type interface-number* | **mac** *mac-address* | **object-group** *object-group-name* | **vlan** *vlan-id* } * }

undo portal free-rule { *rule-number* | **all** }

Default

No source-based portal-free rules exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

rule-number: Specifies a portal-free rule number. The value range for this argument is 0 to 4294967295.

interface *interface-type interface-number*: Specifies a source interface by its type and number for the portal-free rule.

mac *mac-address*: Specifies a source MAC address for the portal-free rule, in the form of H-H-H.

object-group *object-group-name*: Specifies a source object group by its name, a case-insensitive string of 1 to 31 characters.

vlan *vlan-id*: Specifies a source VLAN ID for the portal-free rule. This option takes effect only on portal users that access the network through VLAN interfaces.

all: Specifies all portal-free rules.

Usage guidelines

If you specify both the source VLAN and the source Layer 2 interface, the interface must be in the VLAN.

For a source-based portal-free rule to be correctly created, make sure the object group you specified already exists. Only IPv4 address groups and IPv6 address groups are supported.

Examples

Configure a source-based portal-free rule: specify the rule number as **3**, source MAC address as **1-1-1**, and source VLAN ID as **10**. This rule allows the portal user whose source MAC address is 1-1-1 from VLAN 10 to access network resources without authentication.

```
<Sysname> system-view
[Sysname] portal free-rule 3 source mac 1-1-1 vlan 10
```

Related commands

`display portal rule`

portal idle-cut dhcp-capture enable

Use **`portal idle-cut dhcp-capture enable`** to enable DHCP packet capture to detect online status of portal users by capturing DHCP packets of the portal users.

Use **`undo portal idle-cut dhcp-capture enable`** to disable DHCP packet capture.

Syntax

`portal idle-cut dhcp-capture enable`

`undo portal idle-cut dhcp-capture enable`

Default

DHCP packet capture is enabled.

Views

System view

Predefined user roles

network-admin

context-admin

context-operator

Usage guidelines

This feature enables the AC to detect the online status of portal users by capturing DHCP packets of the portal users.

When this feature is enabled, the AC captures DHCP packets between a portal user and the DHCP server and obtains the IP address lease information of the user. The AC then detects the online status of the portal user as follows:

- If the AC captures a DHCP lease renewal packet from the portal user before the lease expires, the AC determines that the portal user is online.
- If no DHCP lease renewal packet is captured before the lease expires, the AC forcibly logs out the portal user.

For more information about DHCP packets, see DHCP configuration in *Layer 3—IP Services Configuration Guide*.

The timeout time of the DHCP packet capture timer is the same as the IP address lease time in DHCP packets. This timer resets each time a DHCP packet is captured.

Examples

Enable DHCP packet capture to detect online status of portal users.

```
<Sysname> system-view
[Sysname] portal idle-cut dhcp-capture enable
```

portal ipv6 free-all except destination

Use **portal ipv6 free-all except destination** to configure an IPv6 portal authentication destination subnet on an interface.

Use **undo portal ipv6 free-all except destination** to delete IPv6 portal authentication destination subnets on the interface.

Syntax

portal ipv6 free-all except destination *ipv6-network-address prefix-length*

undo portal ipv6 free-all except destination [*ipv6-network-address*]

Default

No IPv6 portal authentication destination subnet is configured on the interface. Portal users must pass portal authentication to access any IPv6 subnet.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-network-address: Specifies an IPv6 portal authentication destination subnet.

prefix-length: Specifies the prefix length of the IPv6 subnet, in the range of 0 to 128.

Usage guidelines

Portal users on the interface are authenticated when accessing the specified authentication destination subnet (except IP addresses and subnets specified in portal-free rules). The users can access other subnets without portal authentication.

If you do not specify the *ipv6-network-address* argument in the **undo portal ipv6 free-all except destination** command, this command deletes all IPv6 portal authentication destination subnets on the interface.

Re-DHCP authentication does not support authentication destination subnets.

If you configure both an authentication source subnet and an authentication destination subnet on an interface, only the authentication destination subnet takes effect.

You can repeat this command to configure multiple authentication destination subnets.

Examples

Configure an IPv6 portal authentication destination subnet of **1::2/16** on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname–GigabitEthernet1/0/1] portal ipv6 free-all except destination 1::2 16
```

Related commands

display portal

portal ipv6 layer3 source

Use **portal ipv6 layer3 source** to configure an IPv6 portal authentication source subnet on an interface.

Use **undo portal ipv6 layer3 source** to delete IPv6 portal authentication source subnets on an interface.

Syntax

portal ipv6 layer3 source *ipv6-network-address prefix-length*

undo portal ipv6 layer3 source [*ipv6-network-address*]

Default

No IPv6 portal authentication source subnet is configured on the interface. Portal users from any IPv6 subnet must pass portal authentication.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-network-address: Specifies an IPv6 portal authentication source subnet address.

prefix-length: Specifies the prefix length of the IPv6 address, in the range of 0 to 128.

Usage guidelines

With IPv6 authentication source subnets configured, only packets from IPv6 users on the authentication source subnets can trigger portal authentication. If an unauthenticated IPv6 user is not on any authentication source subnet, the access device discards all the user's packets that do not match any portal-free rule.

If you do not specify the *ipv6-network-address* argument in the **undo portal ipv6 layer3 source** command, this command deletes all IPv6 portal authentication source subnets on the interface.

Only cross-subnet authentication supports authentication source subnets.

If you configure both an authentication source subnet and an authentication destination subnet on an interface, only the authentication destination subnet takes effect.

Examples

Configure an IPv6 portal authentication source subnet of **1::1/16** on GigabitEthernet 1/0/1. Only portal users from subnet 1::1/16 trigger portal authentication.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname–GigabitEthernet1/0/1] portal ipv6 layer3 source 1::1 16
```

Related commands

display portal

portal ipv6 free-all except destination

portal ipv6 user-detect

Use **portal ipv6 user-detect** to enable online detection of IPv6 portal users.

Use **undo ipv6 portal user-detect** to disable online detection of IPv6 portal users.

Syntax

portal ipv6 user-detect type { **icmpv6** | **nd** } [**retry** *retries*] [**interval** *interval*] [**idle** *time*]

undo portal ipv6 user-detect

Default

Online detection of IPv6 portal users is disabled.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

type: Specifies the detection type.

icmpv6: Specifies ICMPv6 detection.

nd: Specifies ND detection.

retry *retries*: Specifies the maximum number of detection attempts, in the range of 1 to 10. The default value is 3.

interval *interval*: Specifies a detection interval in the range of 1 to 1200 seconds. The default interval is 3 seconds.

idle *time*: Specifies the user idle timeout in the range of 60 to 3600 seconds. The default idle timeout is 180 seconds. When the timeout expires, online detection of portal users is started.

Usage guidelines

If the device receives no packets from a portal user within the idle time, the device detects the user's online status as follows:

- **ICMPv6 detection**—Sends ICMPv6 requests to the user at configurable intervals to detect the user status.
  - If the device receives a reply within the maximum number of detection attempts, it considers that the user is online and stops sending detection packets. Then the device resets the idle timer and repeats the detection process when the timer expires.
  - If the device receives no reply after the maximum number of detection attempts, the device logs out the user.
- **ND detection**—Sends ND requests to the user and detects the ND entry status of the user at configurable intervals.
  - If the ND entry of the user is refreshed within the maximum number of detection attempts, the device considers that the user is online and stops detecting the user's ND entry. Then the device resets the idle timer and repeats the detection process when the timer expires.
  - If the ND entry of the user is not refreshed after the maximum number of detection attempts, the device logs out the user.

Direct authentication and re-DHCP authentication support both ND detection and ICMPv6 detection. Cross-subnet authentication only supports ICMPv6 detection.

If the access device filters out ICMPv6 packets, ICMPv6 detection might fail and result in the logout of portal users. Make sure the access device does not block ICMPv6 packets before you enable ICMPv6 detection on an interface.

Examples

Enable online detection of IPv6 portal users on GigabitEthernet 1/0/1. Configure the detection type as **ICMPv6**, the maximum number of detection attempts as **5**, the detection interval as **10** seconds, and the user idle timeout as **300** seconds.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname–GigabitEthernet1/0/1] portal ipv6 user-detect type icmpv6 retry 5 interval 10
idle 300
```

Related commands

display portal

portal layer3 source

Use **portal layer3 source** to configure an IPv4 portal authentication source subnet.

Use **undo portal layer3 source** to delete IPv4 portal authentication source subnets.

Syntax

portal layer3 source *ipv4-network-address* { *mask-length* | *mask* }

undo portal layer3 source [*ipv4-network-address*]

Default

No IPv4 portal authentication source subnet is configured. Portal users from any IPv4 subnet must pass portal authentication.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-network-address: Specifies an IPv4 portal authentication source subnet address.

mask-length: Specifies the subnet mask length of the IPv4 address, in the range of 0 to 32.

mask: Specifies the subnet mask in dotted decimal format.

Usage guidelines

With IPv4 authentication source subnets configured, only packets from IPv4 users on the authentication source subnets can trigger portal authentication. If an unauthenticated IPv4 user is not on any authentication source subnet, the access device discards all the user's packets that do not match any portal-free rule.

If you do not specify the *ipv4-network-address* argument in the **undo portal layer3 source** command, this command deletes all IPv4 portal authentication source subnets on the interface.

Only cross-subnet authentication supports authentication source subnets.

If you configure both an authentication source subnet and an authentication destination subnet on an interface, only the authentication destination subnet takes effect.

Examples

Configure an IPv4 portal authentication source subnet of **10.10.10.0/24** on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname–GigabitEthernet1/0/1] portal layer3 source 10.10.10.0 24
```

Related commands

display portal

portal free-all except destination

portal local-web-server

Use **portal local-web-server** create an HTTP- or HTTPS-based local portal Web service and enter its view, or enter the view of the existing HTTP- or HTTPS-based local portal Web service.

Use **undo portal local-web-server** to delete the HTTP- or HTTPS-based local portal Web service.

Syntax

portal local-web-server { **http** | **https** [**ssl-server-policy** *policy-name*] [**tcp-port** *port-number*] }

undo portal local-web-server { **http** | **https** }

Default

No local portal Web services exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

http: Specifies the HTTP-based local portal Web service, which uses HTTP to exchange authentication information with clients.

https: Specifies the HTTPS-based local portal Web service, which uses HTTPS to exchange authentication information with clients.

ssl-server-policy *policy-name*: Specifies an existing SSL server policy for HTTPS. The policy name is a case-insensitive string of 1 to 31 characters.

tcp-port *port-number*: Specifies the listening TCP port number for the HTTPS-based local portal Web service. The value range for the *port-number* argument is 1 to 65535. The default port number is 443.

Usage guidelines

In the local portal Web service, the access device also acts as the portal Web server and the portal authentication server. No external portal Web server and portal authentication server are needed.

For an interface to use the local portal Web service, the URL of the portal Web server specified for the interface must meet the following requirements:

- The IP address in the URL must be a local IP address on the device.
- The URL must be ended with **/portal/**. For example: **http://1.1.1.1/portal/**.

You cannot delete an SSL server policy by using the **undo ssl server-policy** command when the policy is associated with HTTPS.

To specify a new SSL server policy for HTTPS, first execute the **undo** form of this command to delete the existing HTTPS-based local portal Web service.

When you specify the listening TCP port number for the HTTPS-based local portal Web service, follow these restrictions and guidelines:

- For HTTPS-based local portal Web service and other services that use HTTPS:
  - If they use the same SSL server policy, they can use the same TCP port number to listen to HTTPS.
  - If they use different SSL server policies, they cannot use the same TCP port number to listen to HTTPS.
- Do not configure the HTTPS listening TCP port number as the port number used by a known protocol (except HTTPS) or other service.
- Do not configure the same TCP port number for HTTP-based local portal Web service and HTTPS-based local portal Web service.

Examples

Create an HTTP-based local portal Web service and enter its view.

```
<Sysname> system-view
[Sysname] portal local-web-server http
[Sysname-portal-local-websvr-http] quit
```

Create an HTTPS-based local portal Web service and associate SSL server policy **policy1** with the service.

```
<Sysname> system-view
[Sysname] portal local-web-server https ssl-server-policy policy1
[Sysname-portal-local-websvr-https] quit
```

Change the SSL server policy to **policy2**.

```
[Sysname] undo portal local-web-server https
[Sysname] portal local-web-server https ssl-server-policy policy2
[Sysname-portal-local-websvr-https] quit
```

Create an HTTPS-based local portal Web service. In the service, the associated SSL server policy is **policy1** and the listening port number is 442.

```
<Sysname> system-view
[Sysname] portal local-web-server https ssl-server-policy policy1 tcp-port 442
[Sysname-portal-local-websvr-https] quit
```

Related commands

default-logon-page

portal local-web-server

ssl server-policy

portal logout-record enable

Use **portal logout-record enable** to enable portal user offline recording.

Use **undo portal logout-record enable** to disable portal user offline recording.

Syntax

portal logout-record enable

undo portal logout-record enable

Default

Portal user offline recording is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This feature enables the device to save all portal user offline records and to periodically send the records to the authentication server.

Examples

Enable portal user offline recording.

```
<Sysname> system-view
[Sysname] portal logout-record enable
```

Related commands

display portal logout-record

portal logout-record export

Use **portal logout-record export** to export portal user offline records to a path.

Syntax

portal logout-record export url *url-string* [**start-time** *start-date start-time* **end-time** *end-date end-time*]

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

url *url-string*: Specifies the URL to which portal user offline records are exported. The URL is a case-insensitive string of 1 to 255 characters. The URL string can include question marks (?). If you enter a question mark (?) in the place of the *url-string* argument, the CLI does not display help information for this argument.

start-time *start-date start-time* **end-time** *end-date end-time*: Specifies a time range. The start date and end date must be in the format of MM/DD/YYYY or YYYY/MM/DD. The value range for MM is 1 to 12. The value range for DD varies with the specified month. The value range for YYYY is 1970 to 2037. The start time and end time must be in the format of hh:mm. The value range for the start time and end time is 00:00 to 23:59.

Usage guidelines

The device supports FTP, TFTP, and HTTP file transfer methods. Table 34 describes the valid URL format for each method.

Table 34 URL formats

Protocol	URL format	Remarks
FTP	ftp://*username*[:*password*]@*server-address*[:*port-number*]/*file-path* Example: **ftp://a:1@1.1.1.1/authfail/**	The username and password must be the same as those on the server. If the server authenticates only the username, no password is required.
TFTP	tftp://*server-address*[:*port-number*]/*file-path* Example: **tftp://1.1.1.1/ autherror/**	N/A
HTTP	http://*username*[:*password*]@*server-address*[:*port-number*]/*file-path* Example: **http://1.1.1.1/autherror/**	The username and password must be the same as those on the server. If the server authenticates only the username, no password is required.

If the server address is an IPv6 address, bracket the IPv6 address to distinguish the IPv6 address from the port number. For example, if the server address is **2001::1** and the port number is 21, the URL is **ftp://test:test@[2001::1]/test/**.

Examples

Export all portal user offline records to path **tftp://1.1.1.1/record/logout/**.

```
<Sysname> system-view
[Sysname] portal logout-record export url tftp://1.1.1.1/record/logout/
```

Export portal user offline records in the time rang of 2016/3/4 14:20 to 2016/3/4 15:00 to path **tftp://1.1.1.1/record/logout/**.

```
<Sysname> system-view
[Sysname] portal logout-record export url tftp://1.1.1.1/record/logout/ start-time
2016/3/4 14:20 end-time 2016/3/4 15:00
```

Related commands

display portal logout-record

portal logout-record enable

reset portal logout-record

portal logout-record max

Use **portal logout-record max** to set the maximum number of portal user offline records.

Use **undo portal logout-record max** to restore the default.

Syntax

portal logout-record max *number*

undo portal logout-record max

Default

Models	Default
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280	The device supports a maximum of 60000 portal user offline records.
NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480,	The device supports a maximum of 24000 portal user offline records.

Models	Default
NFNX3-HDB680, NFNX3-HDB1080	

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

number: Specifies the maximum number of portal user offline records.

The following compatibility matrixes show the value ranges for this argument:

Models	Value range
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280,	1 to 60000
NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	1 to 24000

Usage guidelines

When the maximum number of portal user offline records is reached, a new record overwrites the oldest one.

Examples

Set the maximum number of portal user offline records to 50.

```
<Sysname> system-view
[Sysname] portal logout-record max 50
```

Related commands

display portal logout-record

portal mac-trigger-server

Use **portal mac-trigger-server** to create a MAC binding server and enter its view, or enter the view of an existing MAC binding server.

Use **undo portal mac-trigger-server** to delete the MAC binding server.

Syntax

portal mac-trigger-server *server-name*

undo portal mac-trigger-server *server-name*

Default

No MAC binding servers exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

server-name: Specifies a MAC binding server name, a case-sensitive string of 1 to 32 characters.

Usage guidelines

After you create a MAC binding server, you can configure MAC binding server parameters, such as the server's IP address and port number.

Examples

Create the MAC binding server **mts** and enter its view.

```
<Sysname> system-view
[Sysname] portal mac-trigger-server mts
[Sysname-portal-mac-trigger-server-mts]
```

Related commands

display portal mac-trigger-server

portal apply mac-trigger-server

portal max-user

Use **portal max-user** to set the maximum number of total portal users allowed in the system.

Use **undo portal max-user** to restore the default.

Syntax

portal max-user *max-number*

undo portal max-user

Default

No limit is placed on the total number of portal users allowed in the system.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

max-number: Specifies the maximum number of total portal users in the system. The value range for this argument is 1 to 4294967295.

Usage guidelines

If you configure the maximum total number smaller than the number of current online portal users on the device, this command still takes effect. The online users are not affected by this command, but the system forbids new portal users to log in.

This command sets the maximum number of online IPv4 and IPv6 portal users in all.

Make sure the maximum combined number of IPv4 and IPv6 portal users specified on all interfaces does not exceed the system-allowed maximum number. Otherwise, the exceeding portal users will not be able to log in to the device.

Examples

Set the maximum number of online portal users allowed in the system to 100.

```
<Sysname> system-view
```

```
[Sysname] portal max-user 100
```

Related commands

display portal user

portal { **ipv4-max-user** | **ipv6-max-user** }

portal nas-id profile

Use **portal nas-id-profile** to specify a NAS-ID profile for an interface.

Use **undo portal nas-id-profile** to restore the default.

Syntax

portal nas-id-profile *profile-name*

undo portal nas-id-profile

Default

No NAS-ID profile is specified for an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

profile-name: Specifies the name of a NAS-ID profile, a case-insensitive string of 1 to 31 characters.

Usage guidelines

A NAS-ID profile defines the binding relationship between VLANs and NAS-IDs. To configure a NAS-ID profile, use the **aaa nas-id profile** command. For more information about the **aaa nas-id profile** command, see "AAA commands."

If an interface is specified with a NAS-ID profile, the interface prefers to use the bindings defined in the profile.

If no NAS-ID profile is specified for an interface or no matching binding is found in the specified profile, the device uses the device name as the interface NAS-ID.

Examples

Specify the NAS-ID profile **aaa** for GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname–GigabitEthernet1/0/1] portal nas-id-profile aaa
```

Related commands

aaa nas-id profile

portal nas-port-id format

Use **portal nas-port-id format** to specify the NAS-Port-Id attribute format.

Use **undo portal nas-port-id format** to restore the default.

Syntax

portal nas-port-id format { **1** | **2** | **3** | **4** }

undo portal nas-port-id format

Default

The format for the NAS-Port-Id attribute is format 2.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

1: Uses format 1 for the NAS-Port-Id attribute.

2: Uses format 2 for the NAS-Port-Id attribute.

3: Uses format 3 for the NAS-Port-Id attribute.

4: Uses format 4 for the NAS-Port-Id attribute.

Usage guidelines

The NAS-Port-Id format supported by RADIUS servers varies by vendor. Use this command to specify the format of the NAS-Port-Id attribute in the RADIUS packets sent for portal users to the RADIUS server. The device then automatically constructs a value for the NAS-Port-Id attribute in the specified format to meet the RADIUS server requirements.

Format 1 contains three space-separated strings: *interface-type port-location access-node-id*. Spaces are not allowed within a string.

- The *interface-type* string specifies the interface type of the NAS port. Available options include:
  - **eth**—Common Ethernet interface.
  - **trunk**—Ethernet trunk interface.
  - **0**—The interface type information will be reported by the access node to the BRAS.
- The *port-location* string represents the location of the access line on the BRAS. Its format is NAS_slot/NAS_subslot/NAS_port:XPI.XCI.

Field	Description
NAS_slot	Slot number of the BRAS, in the range of 0 to 31.
NAS_subslot	Subslot number of the BRAS, in the range of 0 to 31.
NAS_Port	Port number of the BRAS, in the range of 0 to 63.
XPI.XCI	For Ethernet interfaces or Ethernet trunk interfaces: • XPI is PVLAN in the range of 0 to 4095. This field is set to 4096 if there is no PVLAN. • XCI is CVLAN in the range of 0 to 4095. This field is set to 4096 if the user is not assigned to a VLAN as in the situation where the end user device is directly connected to a BRAS port.

For the access node to report its access line information to the BRAS, all fields will be set to 0s except for the XPI and XCI fields.

- The *access-node-id* string specifies the attributes the of BRAS. Its format is AccessNodeIdentifier/ANI_rack/ANI_frame/ANI_slot/ANI_subslot/ANI_port:ANI_XPI.ANI_XCI, in which the :ANI_XPI.ANI_XCI portion is optional.

AccessNodeIdentifier	Identifier description of the access node, a string not longer than 50 characters without spaces.
ANI_rack	Rack number of the access node, in the range of 0 to 15.
ANI_frame	Frame number of the access node, in the range of 0 to 31.
ANI_slot	Slot number of the access node, in the range of 0 to 127.
ANI_subslot	Subslot number of the access node, in the range of 0 to 31.
ANI_port	Port number of the access node, in the range of 0 to 255.
ANI_XPI.ANI_XCI	Optional. This field is mainly used to carry CPE-side service information, identifying the further service type requirement. For example, use this field to identify specific services in a multi-PVC scenario. For Ethernet interfaces or Ethernet trunk interfaces: • ANI_XPI is PVLAN in the range of 0 to 4095. This field is set to 4096 if there is no PVLAN. • ANI_XCI is CVLAN in the range of 0 to 4095. This field is set to 4096 if the user is not assigned to a VLAN as in the situation where the end user device is directly connected to a BRAS port.

  If the device does not have rack, frame, or subslot information, 0 is padded in the corresponding field.

- Examples of format 1:

NAS-Port-Id	Description
eth 31/31/7:1234.2345 0/0/0/0/0/0	The subscriber interface type is an Ethernet interface. The slot number is 31, the subslot number is 31, the port number is 7, the PVLAN is 1234, and the CVLAN is 2345. If there is no PVLAN, 1234 will be replaced with 4096.
eth 31/31/7:4096.2345 0/0/0/0/0/0	The subscriber interface type is Ethernet. The slot number is 31, the subslot number is 31, the port number is 7, and the VLAN ID is 2345.
eth 31/31/7:4096.2345 guangzhou001/1/31/63/31/127	The subscriber interface type is Ethernet. The slot number is 31, the subslot number is 31, the port number is 7, and the VLAN ID is 2345. The access node identifier of the DSLAM is guangzhou001, the rack number is 1, the frame number is 31, the slot number is 63, the subslot number is 31, and the port number is 127.

Format 2 is SlotID00IfNOVlanID.

- **SlotID**—Slot number, a string of 2 characters.
- **IfNO**—Slot number, a string of 3 characters.
- **VlanID**—VLAN ID, a string of 9 characters.

Format 3 is SlotID00IfNOVlanIDDHCPoption.

- **SlotID**—Slot number, a string of 2 characters.
- **IfNO**—Interface number, a string of 3 characters.
- **VlanID**—VLAN ID, a string of 9 characters.
- **DHCPoption**—DHCP option 82 is appended for IPv4 users and DHCP option 1 is appended for IPv6 users.

Format 4 is slot=**;subslot=**;port=**;vlanid=**;vlanid2=**.

- For non-VLAN interfaces, the slot=**;subslot=**;port=**;vlanid=0 format is used.
- For interfaces that terminate only the outermost VLAN tag, the slot=**;subslot=**;port=**;vlanid=** format is used.

Examples

Set the format of the NAS-Port-Id attribute to format 1.

```
<Sysname> system-view
[Sysname] portal nas-port-id format 1
```

portal oauth user-sync interval

Use **portal oauth user-sync interval** to set the user synchronization interval for portal authentication using OAuth.

Use **undo portal oauth user-sync interval** to restore the default.

Syntax

portal oauth user-sync interval *interval*

undo portal oauth user-sync interval

Default

The user synchronization interval is 60 seconds for portal authentication using OAuth.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies the user synchronization interval, in seconds. The value for this argument can be 0 or in the range of 60 to 3600.

Usage guidelines

If portal authentication uses OAuth, the device periodically reports user information to the portal authentication server for user synchronization on the server. To disable user synchronization from the device to the portal authentication server, set the user synchronization interval to 0 seconds on the device.

Examples

Set the user synchronization interval to 120 seconds for portal authentication using OAuth.

```
<Sysname> system-view
[Sysname] portal oauth user-sync interval 120
```

portal outbound-filter enable

Use **portal outbound-filter enable** to enable outgoing packets filtering.

Use **undo portal outbound-filter enable** to disable outgoing packets filtering.

Syntax

portal [**ipv6**] **outbound-filter enable**

undo portal [**ipv6**] **outbound-filter enable**

Default

Outgoing packets filtering is disabled. A portal-enabled interface can send any packets.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ipv6: Specifies outgoing IPv6 packets. If you do not specify this keyword, the command is for outgoing IPv4 packets.

Usage guidelines

When you enable this feature on a portal-enabled interface, the device permits the interface to send the following packets:

- Packets whose destination IP addresses are IP addresses of authenticated portal users.
- Packets that match portal-free rules.

Other outgoing packets on the interface are dropped.

Examples

Enable outgoing packets filtering on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] portal outbound-filter enable
```

portal packet log enable

Use **portal packet log enable** to enable logging for portal protocol packets.

Use undo **portal packet log enable** to disable logging for portal protocol packets.

Syntax

portal packet log enable

undo portal packet log enable

Default

Portal protocol packet logging is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This feature logs information about portal protocol packets, including the username, IP address, authentication type, and packet type. For portal log messages to be sent correctly, you must also configure the information center on the device. For more information about information center configuration, see *Network Management and Monitoring Configuration Guide*.

Examples

Enable logging for portal protocol packets.

```
<Sysname> system-view
[Sysname] portal packet log enable
```

Related commands

portal redirect log enable

portal user log enable

portal pre-auth domain

Use **portal pre-auth domain** to specify a preauthentication domain for portal users.

Use **undo portal pre-auth domain** to restore the default.

Syntax

portal [**ipv6**] **pre-auth domain** *domain-name*

undo portal [**ipv6**] **pre-auth domain**

Default

No preauthentication domain is specified for portal users.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ipv6: Specifies IPv6 portal users. Do not specify this keyword for IPv4 portal users.

domain-name: Specifies an existing ISP domain by its name, a case-insensitive string of 1 to 255 characters. The string cannot contain the following characters: slashes (/), backslashes (\), vertical bars (|), quotation marks ("), colons (:), asterisks (*), question marks (?), left angle brackets (<), right angle brackets (>), and at signs (@).

Usage guidelines

After you configure a preauthentication domain on a portal-enabled interface, the device authorizes users on the interface as follows:

1. After an unauthenticated user obtains an IP address, the user is assigned with authorization attributes configured for the preauthentication domain.

   The authorization attributes in a preauthentication domain include ACL and CAR.

An unauthenticated user who is authorized with the authorization attributes in a preauthentication domain is called a preauthentication user.

2. After the user passes portal authentication, the user is assigned with new authorization attributes from the AAA server.
3. After the user goes offline, the user is reassigned with the authorization attributes in the preauthentication domain.

Make sure you specify an existing ISP domain as a preauthentication domain. If the specified ISP domain does not exist, the device might operate incorrectly. You must delete a preauthentication domain (by using the **undo portal** [**ipv6**] **pre-auth domain** command) and reconfigure it in the following situations:

- You create the ISP domain after specifying it as the preauthentication domain.
- You delete the specified ISP domain and then re-create it.

The preauthentication domain takes effect only on portal users with IP addresses assigned by DHCP or DHCPv6.

If you change the preauthentication domain on an interface, the interface uses the new preauthentication domain for both new and existing preauthentication users.

If authorization attributes in the preauthentication domain are modified, the modified attributes take effect only on new preauthentication users. Existing preauthentication users use the original authorization attributes.

If both a preauthentication domain and MAC-trigger authentication are configured on the device, set the free-traffic threshold for MAC-trigger authentication to 0 bytes.

Examples

Create preauthentication domain **abc** for VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] portal pre-auth domain abc
```

Related commands

display portal

portal pre-auth ip-pool

Use **portal pre-auth ip-pool** to specify a preauthentication IP address pool for portal users.

Use **undo portal pre-auth ip-pool** to restore the default.

Syntax

portal [**ipv6**] **pre-auth ip-pool** *pool-name*

undo portal [**ipv6**] **pre-auth ip-pool**

Default

No preauthentication IP address pool is specified for portal users.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ipv6: Specifies IPv6 portal users. Do not specify this keyword for IPv4 portal users.

pool-name: Specifies an IP address pool by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

You must use this command to specify a preauthentication IP address pool on a portal-enabled Layer 3 interface in the following situation:

- Portal users access the network through a subinterface of the portal-enabled Layer 3 interface.
- The subinterface does not have an IP address.
- Portal users need to obtain IP addresses through DHCP.

DHCP assigns an IP address from the specified IP address pool to a user. Then, the user can use this IP address to perform portal authentication.

The specified IP address pool takes effect only when the direct portal authentication mode is used on the interface.

For the preauthentication IP address pool to take effect, make sure the specified IP address pool exists and has been correctly configured.

Examples

Specify IPv4 address pool **abc** as the preauthentication IP address pool for portal users on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] portal pre-auth ip-pool abc
```

Related commands

dhcp server ip-pool (*Layer 3—IP Services Command Reference*)

display portal

ipv6 dhcp pool (*Layer 3—IP Services Command Reference*)

portal redirect log enable

Use **portal redirect log enable** to enable logging for portal redirect.

Use **undo portal redirect log enable** to disable logging for portal redirect.

Syntax

portal redirect log enable

undo portal redirect log enable

Default

Portal redirect logging is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This feature logs information about portal redirect packets, including the user IP address, MAC address, BAS IP, and Web server IP address. For portal log messages to be sent correctly, you must also configure the information center on the device. For more information about information center configuration, see *Network Management and Monitoring Configuration Guide*.

Examples

Enable logging for portal redirect.

```
<Sysname> system-view
[Sysname] portal redirect log enable
```

Related commands

portal packet log enable

portal user log enable

portal redirect max-session per-user

Use **portal redirect max-session per-user** to set the maximum number of portal redirect sessions for a single user.

Use **undo portal redirect max-session per-user** to disable logging for portal redirect.

Syntax

portal redirect max-session per-user *number*

undo redirect max-session per-user

Default

No limit is set on the number of portal redirect sessions for a single user.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

number: Specifies the maximum number of portal redirect sessions for a single user, in the range of 1 to 128.

Usage guidelines

If a user client is attacked by malicious software or viruses, it might initiate a large number of portal redirect sessions. You can configure this command to limit the number of portal redirect sessions that can be established for that user.

The value set by this command applies to the HTTP redirect sessions and HTTPS redirect sessions separately. For example, assume you set the maximum value to 50. Then, a portal user can establish a maximum of 50 HTTP redirect sessions and a maximum of 50 HTTPS redirect sessions.

Examples

Set the maximum number of portal redirect sessions for a single user to 128.

```
<Sysname> system-view
[Sysname] portal redirect max-session per-user 128
```

Related commands

portal redirect max-session

display portal redirect

portal redirect-rule

Use **portal redirect-rule destination** to configure a destination-based portal redirection rule.

Use **undo portal redirect-rule destination** to delete a destination-based portal redirection rule.

Syntax

portal redirect-rule destination { **host** { *host-name* | *ip-address* } | **ipv6** *ipv6-address* } [**redirect-url** *url*]

undo portal redirect-rule destination { **host** { *host-name* | *ip-address* } | **ipv6** *ipv6-address* | **all** }

Default

No destination-based portal redirection rules are configured.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

host *host-name*: Specifies a destination host by its host name, a case-insensitive string of 1 to 253 characters. Valid characters include letters, digits, hyphens (-), underscores (_), and dots (.).

host *ip-address*: Specifies a destination IPv4 address.

ipv6 *ipv6-address*: Specifies a destination IPv6 address.

redirect-url *url*: Specifies the redirection URL. The device will redirect Web requests destined for the specified destination to the specified redirection URL. The specified URL must be a complete URL starting with http:// or https://, a case-sensitive string of 1 to 256 characters. If you do not specify a redirection URL, the device redirects the user to the redirection URL in a URL redirection match rule (**if-match** rule) that matches the user's Web request. If no matching **if-match** rule is found, the device redirects the user to the URL of the portal Web server.

all: Specifies all destination-based portal redirection rules.

Usage guidelines

The device uses destination-based portal redirection rules to perform URL redirection. If the Web request of a portal user matches the specified destination in a redirection rule, the device redirects the user to the URL specified in the redirection rule.

If the Web request of a portal user matches a destination-based portal redirection rule and a URL redirection match rule (configured by using the **if-match** command), the redirection rule takes effect.

If you specify a host name or IP address in a destination-based portal redirection rule, do not specify a URL that includes the host name or IP address as the redirection URL in another rule. A violation will cause redirect loops.

The system supports a maximum of 10 destination-based portal redirection rules. For the same host or IP address, only one destination-based portal redirection rule is supported.

Examples

Configure a destination-based portal redirection rule to redirect Web requests destined for host **http://www.abc.com.cn** to **http://192.168.0.1**.

```
<Sysname> system-view
[Sysname] portal redirect-rule destination host www.abc.com.cn redirect-url
http://192.168.0.1
```

Related commands

display portal dns redirect-rule-host

portal refresh enable

Use **portal refresh enable** to enable the Rule ARP or ND entry feature for portal clients.

Use **undo portal refresh enable** to disable the Rule ARP or ND entry feature for portal clients.

Syntax

portal refresh { **arp** | **nd** } **enable**

undo portal refresh { **arp** | **nd** } **enable**

Default

The Rule ARP or ND entry feature is disabled for portal clients.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

arp: Enables the Rule ARP entry feature.

nd: Enables the Rule ND entry feature.

Usage guidelines

When the Rule ARP or ND entry feature is enabled for portal clients, ARP or ND entries for portal clients are Rule entries after the clients come online. These entries will not age out and will be deleted immediately after the portal clients go offline. If portal clients go offline and then try to come online before these entries are relearned for them, the clients will fail the authentication. In this case, disable this feature so that ARP or ND entries are dynamic entries after the clients come online. The dynamic ARP or ND entries are deleted only when they age out.

Enabling or disabling of this feature does not affect existing Rule ARP or ND entries for portal users.

Examples

Disable the Rule ARP entry feature for portal clients.

```
<Sysname> system-view
[Sysname] undo portal refresh arp enable
```

portal roaming enable

Use **portal roaming enable** to enable intra-VLAN roaming for portal users.

Use **undo portal roaming enable** to disable intra-VLAN roaming for portal users.

Syntax

portal roaming enable

undo portal roaming enable

Default

Intra-VLAN roaming is disabled for portal users.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

If intra-VLAN roaming is enabled for portal users, an online portal user can access network resources from any Layer 2 port in its local VLAN. If intra-VLAN roaming is disabled for portal users, the portal user can access network resources only from the Layer 2 port on which it passes authentication.

For intra-VLAN roaming for portal users to take effect, you must disable the Rule ARP or ND entry feature by using the **undo portal refresh** { **arp** | **nd** } **enable** command.

Intra-VLAN roaming applies only to portal users that log in from VLAN interfaces.

This command cannot be executed when online users or preauthentication portal users are present on the device.

Examples

Enable intra-VLAN roaming for portal users.

```
<Sysname> system-view
[Sysname] portal roaming enable
```

Related commands

portal refresh enable

portal safe-redirect default-action

Use **portal safe-redirect default-action** to configure the default action for portal safe-redirect.

Use **undo portal safe-redirect default-action** to restore the default.

Syntax

portal safe-redirect default-action { **forbidden** | **permit** }

undo portal safe-redirect default-action

Default

No default action is configured for portal safe-redirect.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

`forbidden`: Sets the default action to forbid, which drops a packet.

`permit`: Sets the default action to permit, which permits a packet.

Usage guidelines

The portal safe-redirect default action rule matches URLs that are not permitted or forbidden by portal safe-redirect, and applies the default action to packets containing the matching URLs.

For this command to take effect, make sure portal safe-redirect is enabled.

Portal safe-redirect matches URL information of a Web request packet in the following order:

1. Matches the HTTP request methods specified for portal safe-redirect.
   - If the packet does not match a specified HTTP request method, the packet is dropped.
   - If the packet matches a specified method or no HTTP request methods are specified for portal safe-redirect, the next step applies.
2. Matches the browser types specified for portal safe-redirect.
   - If the packet does not match a specified browser type, the packet is dropped.
   - If the packet matches a specified browser type or no browser types are specified for portal sate-redirect, the next step applies.
3. Matches the forbidden URLs configured for portal safe-redirect.
   - If the packet matches a forbidden URL, the packet is dropped.
   - If the packet does not match a forbidden URL or no forbidden URLs are configured, the next step applies.
4. Matches the forbidden filename extensions configured for portal safe-redirect.
   - If the packet matches a forbidden filename extension, the packet is dropped.
   - If the packet does not match a forbidden filename extension or no forbidden filename extensions are configured for portal safe-redirect, the next step applies.
5. Matches the permitted URLs configured for portal safe-redirect.
   - If the packet matches a permitted URL, the packet is permitted.
   - If the packet does not match a permitted URL or no permitted URLs are configured for portal safe-redirect, the packet is dropped.
6. Matches the default HTTP request method of portal safe-redirect.
   - If the packet does not match the default HTTP request method, the packet is dropped.
   - If the packet matches the default HTTP request method, the next step applies.
7. Identifies whether browser types are specified portal safe-redirect.
   - If browser types are specified for portal safe-redirect, the packet is permitted.
   - If no browser types are specified for portal safe-redirect, the next step applies.
8. Matches the portal safe-redirect default action rule.
   - If the packet matches the default action rule, the packet is processed according to the default action.
   - If the packet does not match the default action rule or the default action is not configured, the next step applies.

9. Matches the default browser types of portal safe-redirect.
    - If the packet matches a default browser type, the packet is permitted.
    - If the packet does not match a default browser type, the packet is dropped.

Examples

Configure the default action as permit for portal safe-redirect.

```
<Sysname> system-view
[Sysname] portal safe-redirect default-action permit
```

Related commands

portal safe-redirect enable

portal safe-redirect forbidden-file

portal safe-redirect forbidden-url

portal safe-redirect method

portal safe-redirect permit-url

portal safe-redirect user-agent

portal safe-redirect enable

Use **portal safe-redirect enable** to enable the portal safe-redirect feature.

Use **undo portal safe-redirect enable** to restore the default.

Syntax

portal safe-redirect enable

undo portal safe-redirect enable

Default

The portal safe-redirect feature is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

Portal redirects all HTTP requests except HTTP requests that match portal-free rules to the portal Web server, which might overload the server.

Portal safe-redirect filters HTTP requests by HTTP request method, browser type (in HTTP User Agent), and destination URL, and redirects only the permitted HTTP requests.

As a best practice to avoid server overload and improve security, enable portal safe-redirect on the device.

Examples

Enable the portal safe-redirect feature.

```
<Sysname> system-view
[Sysname] portal safe-redirect enable
```

Related commands

portal safe-redirect forbidden-url

portal safe-redirect method

portal safe-redirect user-agent

portal safe-redirect forbidden-keyword

Use **portal safe-redirect forbidden-keyword** to configure a URL keyword forbidden by portal safe-redirect.

Use **undo portal safe-redirect forbidden-keyword** to delete a portal safe-redirect forbidden URL keyword.

Syntax

portal safe-redirect forbidden-keyword *keyword*

undo portal safe-redirect forbidden-keyword *keyword*

Default

No forbidden URL keywords are configured. The device redirects HTTP requests regardless of the keywords in the URL.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

keyword: Specifies a URL keyword forbidden by portal safe-redirect, a case-insensitive string of 1 to 16 characters.

Usage guidelines

If the URL in an HTTP request of a portal user contains a specified forbidden URL keyword, the device drops the HTTP request.

- If the HTTP request comes from an unauthenticated user, the device does not redirect the user to the portal Web server for authentication.
- If the HTTP request comes from an authenticated user, the device does not redirect the user to the specified redirection webpages (such as an advertisement webpage configured by using the **ad-url** command).

For this command to take effect, make sure portal safe-redirect is enabled.

You can configure multiple portal safe-redirect forbidden URL keywords.

Examples

Specify **.jpg** as a portal safe-redirect forbidden URL keywords.

```
<Sysname> system-view
[Sysname] portal safe-redirect forbidden-keyword .jpg
```

Related commands

display portal safe-redirect statistics

portal safe-redirect enable

portal safe-redirect forbidden-url

Use **portal safe-redirect forbidden-url** to configure a URL forbidden by portal safe-redirect.

Use **undo portal safe-redirect forbidden-url** to delete a portal safe-redirect forbidden URL.

Syntax

portal safe-redirect forbidden-url *user-url-string*

undo portal safe-redirect forbidden-url *user-url-string*

Default

No forbidden URLs are configured. The device can redirect HTTP requests with any URLs.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

user-url-string: Specifies a URL forbidden by portal safe-redirect, a case sensitive string of 1 to 256 characters. Valid characters are letters, digits, hyphens (-), underscores (_), and wildcards (asterisks *). The URL string can include question marks (?). If you enter a question mark (?) in the place of this argument, the CLI does not display help information for this argument.

Usage guidelines

For this command to take effect, make sure portal safe-redirect is enabled.

You can repeat this command to configure multiple portal safe-redirect forbidden URLs. The device does not redirect HTTP requests destined for the specified URLs to the portal Web server.

You can configure a forbidden URL in one of the following ways:

- **For exact match**—Specify a complete URL. For example, if you configure the URL as **abc.com.cn**, only Web requests that contain URL **abc.com.cn** match the rule.
- **For fuzzy match**—Specify a URL by placing the asterisk (*) wildcard character at the beginning or end of the URL string. For example, if you configure the URL as ***abc.com.cn**, **abc***, or ***abc***, Web requests that carry the URL ending with **abc.com.cn**, starting with **abc**, or including **abc** match the rule.
  - The asterisk (*) wildcard character represents any characters. The device treats multiple consecutive asterisks as one.
  - The configured URL cannot contain only asterisks (*).

Examples

Specify **http://www.abc.com** as a portal safe-redirect forbidden URL.

```
<Sysname> system-view
[Sysname] portal safe-redirect forbidden-url http://www.abc.com
```

Related commands

portal safe-redirect enable

portal safe-redirect method

Use **portal safe-redirect method** to specify HTTP request methods permitted by portal safe-redirect.

Use **undo portal safe-redirect method** to delete HTTP request methods permitted by portal safe-redirect.

Syntax

portal safe-redirect method { **get** | **post** }*

undo portal safe-redirect method { **get** | **post** }*

Default

After portal safe-redirect is enabled, the device redirects only HTTP requests with the GET method.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

get: Specifies the GET request method.

post: Specifies the POST request method.

Usage guidelines

After you specify HTTP request methods for portal safe-redirect, the device redirects only the HTTP requests with the specified methods to the portal Web server.

For this command to take effect, make sure portal safe-redirect is enabled.

If you configure this command multiple times, the most recent configuration takes effect.

Examples

Specify the GET request method for portal safe-redirect.

```
<Sysname> system-view
[Sysname] portal safe-redirect method get
```

Related commands

portal safe-redirect enable

portal safe-redirect permit-url

Use **portal safe-redirect permit-url** to configure a URL permitted by portal safe-redirect.

Use **undo portal safe-redirect permit-url** to delete a portal safe-redirect permitted URL.

Syntax

portal safe-redirect permit-url *user-url-string*

undo portal safe-redirect permit-url *user-url-string*

Default

The device can redirect Web requests with any URLs.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

user-url-string: Specifies a URL permitted by portal safe-redirect, a case sensitive string of 1 to 256 characters. Valid characters are letters, digits, hyphens (-), underscores (_), and wildcards (asterisks *). The URL string can include question marks (?). If you enter a question mark (?) in the place of this argument, the CLI does not display help information for this argument.

Usage guidelines

For this command to take effect, make sure portal safe-redirect is enabled.

You can repeat this command to configure multiple portal safe-redirect permitted URLs.

You can configure a permitted URL in one of the following ways:

- **For exact match**—Specify a complete URL. For example, if you configure the URL as **abc.com.cn**, only Web requests that contain URL **abc.com.cn** match the rule.
- **For fuzzy match**—Specify a URL by placing the asterisk (*) wildcard character at the beginning or end of the URL string. For example, if you configure the URL as ***abc.com.cn**, **abc***, or ***abc***, Web requests that carry the URL ending with **abc.com.cn**, starting with **abc**, or including **abc** match the rule.
  - The asterisk (*) wildcard character represents any characters. The device treats multiple consecutive asterisks as one.
  - The configured URL cannot contain only asterisks (*).

Examples

Specify **http://www.abc.com** as a portal safe-redirect permitted URL.

```
<Sysname> system-view
[Sysname] portal safe-redirect permit-url http://www.abc.com
```

Related commands

portal safe-redirect enable

portal safe-redirect action

portal safe-redirect user-agent

Use **portal safe-redirect user-agent** to specify a browser type for portal safe-redirect.

Use **undo portal safe-redirect user-agent** to delete a browser type for portal safe-redirect.

Syntax

portal safe-redirect user-agent *user-agent-string*

undo portal safe-redirect user-agent *user-agent-string*

Default

After portal safe-redirect is enabled, the device redirects the HTTP packets matching any browser types in Table 35.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

user-agent-string: Specifies a browser type in HTTP User Agent, a case-sensitive string of 1 to 255 characters. You can specify the browser types as shown in Table 35.

Table 35 Browser type and description

Browser type	Description
Safari	Apple browser
Chrome	Google browser
Firefox	Firefox browser
UC	UC browser
QQBrowser	QQ browser
LBBROWSER	Cheetah browser
TaoBrowser	Taobao browser
Maxthon	Maxthon browser
BIDUBrowser	Baidu browser
MSIE 10.0	Microsoft IE 10.0 browser
MSIE 9.0	Microsoft IE 9.0 browser
MSIE 8.0	Microsoft IE 8.0 browser
MSIE 7.0	Microsoft IE 7.0 browser
MSIE 6.0	Microsoft IE 6.0 browser
MetaSr	Sogou browser

Usage guidelines

You can execute this command for multiple times to specify multiple browser types. The device redirects an HTTP request only when its User-Agent string contains a specified browser type.

For this command to take effect, make sure portal safe-redirect is enabled.

Examples

Specify browser types **Chrome** and **Safari** for portal safe-redirect.

```
<Sysname> system-view
[Sysname] portal safe-redirect user-agent Chrome
[Sysname] portal safe-redirect user-agent Safari
```

Related commands

portal safe-redirect enable

portal server

Use **portal server** to create a portal authentication server and enter its view, or enter the view of an existing portal authentication server.

Use **undo portal server** to delete the specified portal authentication server.

Syntax

portal server *server-name*

undo portal server *server-name*

Default

No portal authentication servers exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

server-name: Specifies a portal authentication server by its name, a case-sensitive string of 1 to 32 characters.

Usage guidelines

In portal authentication server view, you can configure the following parameters and features for the portal authentication server:

- IP address of the server.
- Destination UDP port number used by the device to send unsolicited portal packets to the portal authentication server.
- Pre-shared key for communication between the access device and the server.
- Server detection feature.

You can configure multiple portal authentication servers for an access device.

Examples

Create the portal authentication server **pts** and enter its view.

```
<Sysname> system-view
[Sysname] portal server pts
[Sysname-portal-server-pts]
```

Related commands

display portal server

portal temp-pass enable

Use **portal temp-pass enable** to enable portal temporary pass and set the temporary pass period.

Use **undo portal temp-pass enable** to disable portal temporary pass.

Syntax

portal temp-pass [**period** *period-value*] **enable**

undo portal temp-pass enable

Default

Portal temporary pass is disabled.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

period *period-value*: Specifies the temporary pass period. The value range for the *period-value* argument is 10 to 3600 seconds, and the default is 30 seconds.

Usage guidelines

This command is available only for direct portal authentication mode.

Typically, a portal user cannot access the network before passing portal authentication. This feature allows a user to access the Internet temporarily if the user uses a WeChat account to perform portal authentication. During the temporary pass period, the user provides WeChat authentication information to the WeChat server for the server to interact with the access device to finish portal authentication.

Examples

On GigabitEthernet1/0/1, enable portal temporary pass and set the temporary pass period to 25 seconds.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] portal temp-pass period 25 enable
```

Related commands

display portal

portal traffic-accounting disable

Use **portal traffic-accounting disable** to disable traffic accounting for portal users.

Use **undo portal traffic-accounting disable** to restore the default.

Syntax

portal traffic-accounting disable

undo portal traffic-accounting disable

Default

Traffic accounting for portal users is enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

The accounting server might perform time-based or traffic-based accounting, or it might not perform accounting. If the accounting server does not perform traffic-based accounting, disable traffic accounting for portal users on the device. The device will provide quick accounting for portal users, and the traffic statistics will be imprecise. If the accounting server performs traffic-based accounting, enable traffic accounting for portal users. The device will provide precise traffic statistics for portal users.

Examples

Disable traffic accounting for portal users.

```
<Sysname> system-view
[Sysname] portal traffic-accounting disable
```

portal traffic-backup threshold

Use **portal traffic-backup threshold** to set the user traffic backup threshold.

Use **undo portal traffic-backup threshold** to restore the default.

Syntax

portal traffic-backup threshold *value*

undo portal traffic-backup threshold

Default

The user traffic backup threshold is 10 MB.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

value: Specifies the user traffic backup threshold, in MB. The value range for this argument is 0 to 100000. If you set the threshold to 0 MB, the device backs up user traffic in real time.

Usage guidelines

The device backs up traffic for a user when the user's traffic reaches the user traffic backup threshold. A smaller threshold provides more accurate backup for user traffic. However, when a large number of users exist, a small threshold results in frequent user traffic backups, affecting the user online, offline, and accounting processes. Set a proper threshold to balance between service performance and traffic backup accuracy.

Examples

Set the user traffic backup threshold to 10240 MB.

```
<Sysname> system-view
[Sysname] portal traffic-backup threshold 10240
```

portal user log enable

Use **portal user log enable** to enable logging for portal user logins and logouts.

Use **undo portal user log enable** to disable logging for portal user logins and logouts.

Syntax

portal user log enable

undo portal user log enable

Default

Portal user login and logout logging is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This feature logs information about portal user login and logout events, including the username, IP address, user's MAC address, interface name, VLAN, and reason for login failure. For portal log messages to be sent correctly, you must also configure the information center on the device. For more information about information center configuration, see *Network Management and Monitoring Configuration Guide*.

Examples

Enable logging for portal user logins and logouts.

```
<Sysname> system-view
[Sysname] portal user log enable
```

Related commands

portal packet log enable

portal redirect log enable

portal user-block failed-times

Use **portal user-block failed-times** to configure the device to block portal users that fail portal authentication.

Use **undo portal user-block failed-times** to configure the device not to block portal users that fail portal authentication.

Syntax

portal user-block failed-times *failed-times* **period** *period* [**method** { **ip** | **mac** | **username** }]

undo portal user-block failed-times

Default

The device does not block portal users that fail portal authentication.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

failed-times: Specifies the maximum number of consecutive authentication failures allowed for a portal user in the specified failure detection period. The value range for this argument is 0 to 10. If you specify value 0 for this argument, the device does not block portal users that fail portal authentication.

period *period*: Specifies the authentication failure detection period, in the range of 1 to 120 minutes.

method: Specifies the method to block portal users that fail portal authentication. If you do not specify this keyword, the device blockes portal users that fail portal authentication by IP address.

ip: Blocks portal users by IP address. If portal users at the same IP address consecutively fail portal authentication for the specified times within the failure detection period, the device blocks the IP address.

mac: Blocks portal users by MAC address. If portal users at the same MAC address consecutively fail portal authentication for the specified times within the failure detection period, the device blocks the MAC address.

username: Blocks portal users by username. If portal users using the same username consecutively fail portal authentication for the specified times within the failure detection period, the device blocks the username.

Usage guidelines

This feature prevents exhaustive password cracking. It blocks a portal user if the user consecutively fails authentication for the specified times within the failure detection period. All authentication requests from the user are dropped by the device till the blocking times out. To set the blocking timeout time, use the **portal user-block reactive** command.

This feature does not block preauthentication portal users.

Examples

Configure the device to block portal users at a MAC address if the users consecutively fail portal authentication twice within 100 minutes.

```
<Sysname> system-view
[Sysname] portal user-block failed-times 2 period 100 method mac
```

Related commands

portal user-block reactive

portal user-block reactive

Use **portal user-block reactive** to set the portal user blocking timeout time.

Use **undo portal user-block reactive** to restore the default.

Syntax

portal user-block reactive *period*

undo portal user-block reactive

Default

The portal user blocking timeout time is 30 minutes.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

period: Specifies the blocking timeout time, in the range of 0 to 1000 minutes. If you specify value 0 for this argument, blocked portal users cannot perform portal authentication again.

Usage guidelines

A portal user is blocked after the user consecutively fails portal authentication for the specified times within the specified failure detection period (set by using the **portal user-block failed-times** command). This user can perform portal authentication again only after the portal user blocking timeout time expires.

Examples

Set the portal user blocking timeout time to 20 minutes.

```
<Sysname> system-view
[Sysname] portal user-block reactive 20
```

Related commands

portal user-block failed-times

portal user-detect

Use **portal user-detect** to enable online detection of IPv4 portal users.

Use **undo portal user-detect** to disable online detection of IPv4 portal users.

Syntax

portal user-detect type { **arp** | **icmp** } [**retry** *retries*] [**interval** *interval*] [**idle** *time*]

undo portal user-detect

Default

Online detection of IPv4 portal users is disabled.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

type: Specifies the detection type.

arp: Specifies ARP detection.

icmp: Specifies ICMP detection.

retry *retries*: Specifies the maximum number of detection attempts, in the range of 1 to 10. The default value is 3.

interval *interval*: Specifies a detection interval in the range of 1 to 1200 seconds. The default interval is 3 seconds.

idle *time*: Specifies a user idle timeout in the range of 60 to 3600 seconds. The default idle timeout is 180 seconds. When the timeout expires, online detection of IPv4 portal users is started.

Usage guidelines

If the device receives no packets from a portal user within the configured idle time, the device detects the user's online status as follows:

- **ICMP detection**—Sends ICMP requests to the user at configurable intervals to detect the user status.
  - If the device receives a reply within the maximum number of detection attempts, it considers that the user is online and stops sending detection packets. Then the device resets the idle timer and repeats the detection process when the timer expires.
  - If the device receives no reply after the maximum number of detection attempts, the device logs out the user.
- **ARP detection**—Sends ARP requests to the user and detects the ARP entry status of the user at configurable intervals.
  - If the ARP entry of the user is refreshed within the maximum number of detection attempts, the device considers that the user is online and stops detecting the user's ARP entry. Then the device resets the idle timer and repeats the detection process when the timer expires.
  - If the ARP entry of the user is not refreshed after the maximum number of detection attempts, the device logs out the user.

Direct authentication and re-DHCP authentication support both ARP detection and ICMP detection. Cross-subnet authentication only supports ICMP detection.

If the access device filters out ICMP packets, ICMP detection might fail and result in the logout of portal users. Make sure the access device does not block ICMP packets before you enable ICMP detection on an interface.

Examples

Enable online detection of IPv4 portal users on GigabitEthernet 1/0/1. Configure the detection type as **ICMP**, the maximum number of detection attempts as **5**, the detection interval as **10** seconds, and the user idle timeout as **300** seconds.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname–GigabitEthernet1/0/1] portal user-detect type icmp retry 5 interval 10 idle 300
```

Related commands

display portal

portal user-dhcp-only

Use **portal user-dhcp-only** to allow only users with DHCP-assigned IP addresses to pass portal authentication.

Use **undo portal user-dhcp-only** to restore the default.

Syntax

portal [**ipv6**] **user-dhcp-only**

undo portal [**ipv6**] **user-dhcp-only**

Default

Both users with DHCP-assigned IP addresses and users with static IP addresses can pass portal authentication to come online.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ipv6: Specifies IPv6 portal users. Do not specify this keyword for IPv4 portal users.

Usage guidelines

CAUTION:

- With this feature enabled, users with static IP addresses cannot pass portal authentication to come online.

Examples

Allow only users with DHCP-assigned IP addresses on GigabitEthernet 1/0/1 to pass portal authentication.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] portal user-dhcp-only
```

Related commands

display portal

portal user-log traffic-separate

Use **portal user-log traffic-separate** to enable separate IPv4 and IPv6 traffic statistics in portal user offline logs.

Use **undo portal user-log traffic-separate** to restore the default.

Syntax

portal user-log traffic-separate

undo portal user-log traffic-separate

Default

IPv4 and IPv6 traffic statistics of portal users are collectively counted as IPv4 traffic statistics in portal user offline logs. No IPv6 traffic statistics is displayed in portal user offline logs.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

For single-stack users:

- If this feature is enabled, both IPv4 and IPv6 traffic statistics are displayed in user offline logs. For IPv4 users, the IPv6 traffic statistics is displayed as 0. For IPv6 users, the IPv4 traffic statistics is displayed as 0.

- If this feature is disabled, traffic statistics of both IPv4 users and IPv6 users are displayed as IPv4 traffic statistics in portal user offline logs.

For dual-stack users:

- If this feature is enabled, IPv4 and IPv6 traffic statistics of a user are displayed separately in the user offline logs.
- If this feature is disabled, IPv4 and IPv6 traffic statistics of a user are collectively counted as IPv4 traffic statistics in portal user offline logs.

Examples

Enable separate IPv4 and IPv6 traffic statistics in portal user offline logs.

```
<Sysname> system-view
[Sysname] portal user-log traffic-separate
```

portal web-proxy port

Use **portal web-proxy port** to specify the port number of a Web proxy server.

Use **undo portal web-proxy port** to delete port numbers of Web proxy servers.

Syntax

portal web-proxy { **http** | **https** } **port** *port-number*

undo portal web-proxy { { **http** | **https** } **port** *port-number* | **all-port** }

Default

No port numbers of Web proxy servers are specified. Proxied HTTP and HTTPS requests are dropped.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

http: Specifies the HTTP service.

https: Specifies the HTTPS service.

port-number: Specifies the TCP port number of a Web proxy server. The value range for this argument is 1 to 65535. Do not specify TCP port number 80 or 443 because 80 and 443 are port numbers reserved for portal.

all-port: Specifies all port numbers of Web proxy servers.

Usage guidelines

To allow HTTP or HTTPS requests proxied by Web proxy servers to trigger portal authentication, specify the port numbers of the Web proxy servers on the device. If a Web proxy server port is not specified on the device, HTTP or HTTPS requests proxied by the Web proxy server are dropped, and portal authentication cannot be triggered.

You can configure this command multiple times to specify a maximum of 64 Web proxy server ports for HTTP and HTTPS.

Do not specify the same Web proxy server port for HTTP and HTTPS.

If a user's browser uses the Web Proxy Auto-Discovery (WPAD) protocol to discover Web proxy servers, you must perform the following tasks on the device:

- Specify the port numbers of the Web proxy servers on the device.
- Configure portal-free rules to allow user packets destined for the IP address of the WPAD server to pass without authentication.

If portal users enable Web proxy in their browsers, the users must add the IP address of the portal authentication server as a proxy exception in their browsers. Then, HTTP or HTTPS packets that the users send to the portal authentication server will not be sent to Web proxy servers.

Examples

Specify TCP port number 8080 as a Web proxy server port that allows HTTP requests to trigger portal authentication.

```
<Sysname> system-view
[Sysname] portal web-proxy http port 8080
```

Related commands

portal enable method

portal web-server

Use **portal web-server** to create a portal Web server and enter its view, or enter the view of an existing portal Web server.

Use **undo portal web-server** to delete a portal Web server.

Syntax

portal web-server *server-name*

undo portal web-server *server-name*

Default

No portal Web servers exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

server-name: Specifies a portal Web server by its name, a case-sensitive string of 1 to 32 characters.

Usage guidelines

The portal Web server pushes portal authentication pages to portal users during authentication. The access device redirects HTTP requests of unauthenticated portal users to the portal Web server. In portal Web server view, you can configure the URL and URL parameters for the portal Web server and the portal Web server detection feature.

Examples

Create the portal Web server **wbs** and enter its view.

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs]
```

Related commands

display portal web-server

portal apply web-server

portal wifidog user-sync interval

Use **portal wifidog user-sync interval** to enable user information synchronization and set the synchronization interval for portal authentication using WiFiDog.

Use **undo portal wifidog user-sync interval** to disable user information synchronization and cancel the synchronization interval setting for portal authentication using WiFiDog.

Syntax

portal wifidog user-sync interval *interval*

undo portal wifidog user-sync interval

Default

User information synchronization is disabled for portal authentication using WiFiDog.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies the user information synchronization interval, in the range of 60 to 1440 minutes.

Usage guidelines

Use this feature when users perform portal authentication using the WiFiDog protocol. This feature enables the device to periodically synchronize user information with the portal server to ensure user information consistency between the device and the portal server.

For this feature to take effect, make sure the type of the portal Web server is Wifidog before you perform this task. To specify the type of the portal Web server, use the **server-type** command.

Examples

Enable user information synchronization and set the synchronization interval to 61 minutes for portal authentication using WiFiDog.

```
<Sysname> system-view
[Sysname] portal wifidog user-sync interval 61
```

Related commands

server-type

portal { bas-ip | bas-ipv6 }

Use **portal** { **bas-ip** | **bas-ipv6** } to configure the BAS-IP or BAS-IPv6 attribute carried in the portal packets sent to the portal authentication server.

Use **undo portal** { **bas-ip** | **bas-ipv6** } to delete the BAS-IP or BAS-IPv6 attribute setting.

Syntax

portal { **bas-ip** *ipv4-address* | **bas-ipv6** *ipv6-address* }

undo portal { **bas-ip** | **bas-ipv6** }

Default

The BAS-IP attribute of an IPv4 portal reply packet sent to the portal authentication server is the source IPv4 address of the packet. The BAS-IPv6 attribute of an IPv6 portal reply packet sent to the portal authentication server is the source IPv6 address of the packet.

The BAS-IP attribute of an IPv4 portal notification packet sent to the portal authentication server is the IPv4 address of the packet's outgoing interface. The BAS-IPv6 attribute of an IPv6 portal notification packet sent to the portal authentication server is the IPv6 address of the packet's outgoing interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

bas-ip *ipv4-address*: Specifies BAS-IP for portal packets sent to the portal authentication server. The *ipv4-address* argument must be the IPv4 address of an interface on the device. It cannot be 0.0.0.0, 1.1.1.1, a class D address, a class E address, or a loopback address.

bas-ipv6 *ipv6-address*: Specifies BAS-IPv6 for portal packets sent to the portal authentication server. The *ipv6-address* argument must be the IPv6 address of an interface on the device. It cannot be a multicast address, an all 0 address, or a link-local address.

Usage guidelines

If the device runs Portal 2.0, unsolicited portal packets (such as a logout notification packet) sent to the portal authentication server must carry the BAS-IP attribute. If the device runs Portal 3.0, unsolicited portal packets sent to the portal authentication server must carry the BAS-IP or BAS-IPv6 attribute.

After this command takes effect, the source IP address for unsolicited notification portal packets the device sends to the portal authentication server is the configured BAS-IP or BAS-IPv6. If the BAS IP address is not configured, the source IP address of the packets is the IP address of the packet output interface.

You must configure the BAS-IP or BAS-IPv6 attribute on a portal authentication-enabled interface if the following conditions are met:

- The portal authentication server is an IMC server or the portal authentication mode on the interface is re-DHCP.
- The portal device IP address specified on the portal authentication server is not the IP address of the portal packet output interface.

Examples

On GigabitEthernet 1/0/1, configure the BAS-IP attribute as **2.2.2.2** for portal packets sent to the portal authentication server.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] portal bas-ip 2.2.2.2
```

Related commands

display portal

portal { ipv4-max-user | ipv6-max-user }

Use **portal** { **ipv4-max-user** | **ipv6-max-user** } to set the maximum number of portal users allowed on an interface.

Use **undo portal** { **ipv4-max-user** | **ipv6-max-user** } to restore the default.

Syntax

portal { **ipv4-max-user** | **ipv6-max-user** } *max-number*

undo portal { **ipv4-max-user** | **ipv6-max-user** }

Default

No limit is placed on the maximum number of portal users allowed.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

max-number: Specifies the maximum number of IPv4 or IPv6 portal users allowed on an interface. The value range for this argument is 1 to 4294967295.

Usage guidelines

If the specified maximum number is smaller than the number of current online portal users on the interface, the limit can be set successfully. The limit does not impact the online portal users. However, the device does not allow new portal users to log in from the interface until the number drops down below the limit.

Make sure the maximum combined number of IPv4 and IPv6 portal users specified on all interfaces does not exceed the system-allowed maximum number. Otherwise, the exceeding portal users will not be able to log in to the device.

Examples

Set the maximum number of IPv4 portal users to 100 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] portal ipv4-max-user 100
```

Related commands

display portal user

portal max-user

redirect-url

Use **redirect-url** to specify the URL to which portal users are redirected after they pass QQ or Facebook authentication.

Use **undo redirect-url** to restore the default.

Syntax

redirect-url *url-string*

undo redirect-url

Default

Portal users are redirected to URLs **http://lvzhou.nsfocus.com.cn/portal/qqlogin.html** and **http://oauthindev.nsfocus.com.cn/portal/fblogin.html** after they pass QQ authentication and Facebook authentication, respectively.

Views

QQ authentication server view

Facebook authentication server view

Predefined user roles

network-admin

context-admin

Parameters

url-string: Specifies the URL to which portal users are redirected after they pass QQ or Facebook authentication. The URL is a case-sensitive string of 1 to 256 characters. The URL string can include question marks (?). If you enter a question mark (?) in the place of this argument, the CLI does not display help information for this argument.

Usage guidelines

After a portal user passes QQ or Facebook authentication, the user is redirected to the specified webpage to complete portal authentication.

You must enable DNS proxy and specify the IP address of an interface on the device as the DNS server.

Examples

Configure the device to redirect portal users to URL **http://www.abc.com/portal/qqlogin.html** after they pass QQ authentication.

```
<Sysname> system-view
[Sysname] portal extend-auth-server qq
[Sysname-portal-extend-auth-server-qq] redirect-url
http://www.abc.com/portal/qqlogin.html
```

Configure the device to redirect portal users to URL **http://www.abc.com/portal/qqlogin.html** after they pass Facebook authentication.

```
<Sysname> system-view
[Sysname] portal extend-auth-server qq
[Sysname-portal-extend-auth-server-qq] redirect-url
http://www.abc.com/portal/qqlogin.html
```

Related commands

display portal extend-auth-server

reset portal ad-push statistics

Use **reset portal ad-push statistics** to clear statistics about portal advertisement push.

Syntax

reset portal ad-push statistics { **ad-url-group** | **url** }

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

ad-url-group: Clears advertisement group-based statistics about portal advertisement push.

url: Clears URL-based statistics about portal advertisement push.

Examples

Clear advertisement group-based statistics about portal advertisement push.

```
<Sysname> reset portal ad-push statistics url
```

Clear URL-based statistics about portal advertisement push.

```
<Sysname> reset portal ad-push statistics ad-url-group
```

Related commands

display portal ad-push statistics

reset portal auth-error-record

Use **reset portal auth-error-record** to clear portal authentication error records.

Syntax

reset portal auth-error-record { **all** | **ipv4** *ipv4-address* | **ipv6** *ipv6-address* | **start-time** *start-date start-time* **end-time** *end-date end-time* }

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

all: Specifies all portal authentication error records.

ipv4 *ipv4-address*: Specifies the IPv4 address of a portal user.

ipv6 *ipv6-address*: Specifies the IPv6 address of a portal user.

start-time *start-date start-time* **end-time** *end-date end-time*: Specifies a time range. The start date and end date must be in the format of MM/DD/YYYY or YYYY/MM/DD. The value range for MM is 1 to 12. The value range for DD varies with the specified month. The value range for YYYY is 1970 to 2037. The start time and end time must be in the format of hh:mm. The value range for the start time and end time is 00:00 to 23:59.

Examples

Clear all portal authentication error records.

```
<Sysname> reset portal auth-error-record all
```

Clear portal authentication error records of the portal user whose IPv4 address is **11.1.0.1**.

```
<Sysname> reset portal auth-error-record ipv4 11.1.0.1
```

Clear portal authentication error records of the portal user whose IPv6 address is **2000::2**.

```
<Sysname> reset portal auth-error-record ipv6 2000::2
```

Clear portal authentication error records with the error time in the range of 2016/3/4 14:20 to 2016/3/4 16:23.

```
<Sysname> reset portal auth-error-record start-time 2016/3/4 14:20 end-time 2016/3/4 16:23
```

Related commands

display portal auth-error-record

reset portal auth-fail-record

Use **reset portal auth-fail-record** to clear portal authentication failure records.

Syntax

reset portal auth-fail-record { **all** | **ipv4** *ipv4-address* | **ipv6** *ipv6-address* | **start-time** *start-date start-time* **end-time** *end-date end-time* | **username** *username* }

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

all: Specifies all portal authentication failure records.

ipv4 *ipv4-address*: Specifies the IPv4 address of a portal user.

ipv6 *ipv6-address*: Specifies the IPv6 address of a portal user.

start-time *start-date start-time* **end-time** *end-date end-time*: Specifies a time range. The start date and end date must be in the format of MM/DD/YYYY or YYYY/MM/DD. The value range for MM is 1 to 12. The value range for DD varies with the specified month. The value range for YYYY is 1970 to 2037. The start time and end time must be in the format of hh:mm. The value range for the start time and end time is 00:00 to 23:59.

username *username*: Specifies the username of a portal user, a case-sensitive string of 1 to 253 characters. The username cannot contain the domain name.

Examples

Clear all portal authentication failure records.

```
<Sysname> reset portal auth-fail-record all
```

Clear portal authentication failure records of the portal user whose IPv4 address is **11.1.0.1**.

```
<Sysname> reset portal auth-fail-record ipv4 11.1.0.1
```

Clear portal authentication failure records of the portal user whose IPv6 address is **2000::2**.

```
<Sysname> reset portal auth-fail-record ipv6 2000::2
```

Clear portal authentication failure records of the portal user whose username is **abc**.

```
<Sysname> reset portal auth-fail-record username abc
```

Clear portal authentication failure records with the failure time in the range of 2016/3/4 14:20 to 2016/3/4 16:23.

```
<Sysname> reset portal auth-fail-record start-time 2016/3/4 14:20 end-time 2016/3/4 16:23
```

Related commands

display portal auth-fail-record

reset portal captive-bypass statistics

Use **reset portal captive-bypass statistics** to clear portal captive-bypass packet statistics.

Syntax

reset portal captive-bypass statistics [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears portal captive-bypass packet statistics on all member devices.

Examples

Clear portal captive-bypass packet statistics on the specified slot.

```
<Sysname> reset portal captive-bypass statistics slot 0
```

Related commands

display portal captive-bypass statistics

reset portal local-binding mac-address

Use **reset portal local-binding mac-address** to clear local MAC-account binding entries.

Syntax

reset portal local-binding mac-address { *mac-address* | **all** }

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

mac-address: Specifies the MAC address of a portal user, in the format of H-H-H.

all: Specifies all local MAC-account binding entries.

Examples

Clear all local MAC-account binding entries.

```
<Sysname> reset portal local-binding mac-address all
```

Related commands

display portal local-binding mac-address

local-binding aging-time

reset portal logout-record

Use **reset portal logout-record** to clear portal user offline records.

Syntax

reset portal logout-record { **all** | **ipv4** *ipv4-address* | **ipv6** *ipv6-address* | **start-time** *start-date start-time* **end-time** *end-date end-time* | **username** *username* }

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

all: Specifies all portal user offline records.

ipv4 *ipv4-address*: Specifies the IPv4 address of a portal user.

ipv6 *ipv6-address*: Specifies the IPv6 address of a portal user.

start-time *start-date start-time* **end-time** *end-date end-time*: Specifies a time range. The start date and end date must be in the format of MM/DD/YYYY or YYYY/MM/DD. The value range for MM is 1 to 12. The value range for DD varies with the specified month. The value range for YYYY is 1970 to 2037. The start time and end time must be in the format of hh:mm. The value range for the start time and end time is 00:00 to 23:59.

username *username*: Specifies the username of a portal user, a case-sensitive string of 1 to 253 characters. The username cannot contain the domain name.

Examples

Clear all portal user offline records.

```
<Sysname> reset portal logout-record all
```

Clear offline records of the portal user whose IPv4 address is **11.1.0.1**.

```
<Sysname> reset portal logout-record ipv4 11.1.0.1
```

Clear offline records of the portal user whose IPv6 address is **2000::2**.

```
<Sysname> reset portal logout-record ipv6 2000::2
```

Clear offline records of the portal user whose username is **abc**.

```
<Sysname> reset portal logout-record username abc
```

Clear portal user offline records with the logout time in the range of 2016/3/4 14:20 to 2016/3/4 16:23.

```
<Sysname> reset portal logout-record start-time 2016/3/4 14:20 end-time 2016/3/4 16:23
```

Related commands

display portal logout-record

reset portal packet statistics

Use **reset portal packet statistics** to clear packet statistics for portal authentication servers.

Syntax

reset portal packet statistics [**extend-auth-server** { **cloud** | **facebook** | **mail** | **qq** | **wechat** } | **mac-trigger-server** *server-name* | **server** *server-name*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

extend-auth-server: Specifies a third-party authentication server by its type.

facebook: Specifies the Facebook authentication server.

cloud: Specifies the cloud authentication server.

mail: Specifies the email authentication server.

qq: Specifies the QQ authentication server.

wechat: Specifies the WeChat authentication server.

mac-trigger-server: Specify a MAC binding server by its name, a case-sensitive string of 1 to 32 characters. If you do not specify a MAC binding server, this command clears packet statistics for the specified portal authentication server.

server *server-name*: Specifies a normal portal authentication server by its name, a case-sensitive string of 1 to 32 characters. If you do not specify this parameter, this command clears packet statistics for the specified MAC binding server.

Usage guidelines

If you do not specify any parameters, this command clears packet statistics for all portal authentication servers and MAC binding servers.

Examples

Clear packet statistics for portal authentication server **pts**.

```
<Sysname> reset portal packet statistics server pts
```

Clear packet statistics for MAC binding server **newps**.

```
<Sysname> reset portal packet statistics mac-trigger-server newpt
```

Clear packet statistics for the Oasis cloud authentication server.

```
<Sysname> reset portal packet statistics extend-auth-server cloud
```

Related commands

display portal packet statistics

reset portal redirect session-record

Use **reset portal redirect session-record** to clear history records about portal redirect sessions.

Syntax

reset portal redirect session-record [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears history records about portal redirect sessions on all member devices.

Examples

Clear history records about portal redirect sessions on the specified slot.

```
<Sysname> reset portal redirect session-record slot 0
```

Related commands

display portal redirect session-record

reset portal redirect session-statistics

Use **reset portal redirect session-statistics** to clear summary statistics for portal redirect sessions.

Syntax

reset portal redirect session-statistics [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears summary statistics for portal redirect sessions on all member devices.

Examples

Clear summary statistics for portal redirect sessions on the specified slot.

```
<Sysname> reset portal redirect session-statistics slot 0
```

Related commands

display portal redirect session-statistics

reset portal redirect statistics

Use **reset portal redirect statistics** to reset portal redirect packet statistics.

Syntax

reset portal redirect statistics [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears portal redirect packet statistics on all member devices.

Examples

Clear redirect packet statistics on the specified slot.

```
<Sysname> reset portal redirect statistics slot 0
```

Related commands

display portal safe-redirect statistics

reset portal safe-redirect statistics

Use **reset portal safe-redirect statistics** to clear portal safe-redirect packet statistics.

Syntax

reset portal safe-redirect statistics [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears portal safe-redirect packet statistics on all member devices.

Examples

Clear portal safe-redirect packet statistics on the specified slot.

```
<Sysname> reset portal safe-redirect statistics slot 0
```

Related commands

display portal safe-redirect statistics

server-detect (portal authentication server view)

Use **server-detect** to enable portal authentication server detection. After server detection is enabled for a portal authentication server, the device periodically detects portal packets from the server to identify its reachability status.

Use **undo server-detect** to disable portal authentication server detection.

Syntax

server-detect [**timeout** *timeout*] { **log** | **trap** } *

undo server-detect

Default

Portal authentication server detection is disabled.

Views

Portal authentication server view

Predefined user roles

network-admin

context-admin

Parameters

timeout *timeout*: Specifies the detection timeout in the range of 10 to 3600 seconds. The default is 60 seconds.

log: Enables the device to send a log message when reachability status of the portal authentication server changes. The log message contains the name, the original state, and the current state of the portal authentication server.

trap: Enables the device to send a trap message to the NMS when reachability status of the portal authentication server changes. The trap message contains the name and the current state of the portal authentication server.

Usage guidelines

The portal authentication server detection feature takes effect only when the device has a portal-enabled interface.

To test server reachability by detecting heartbeat packets, you must enable the server heartbeat feature on the portal authentication server. Only the IMC portal authentication server supports sending heartbeat packets.

The detection timeout configured on the device must be greater than the server heartbeat interval configured on the portal authentication server.

If the device receives portal packets from the portal authentication server before the detection timeout expires and verifies the correctness of the packets, the device considers the portal authentication server is reachable. Otherwise, the device considers the portal authentication server is unreachable.

Examples

Enable server detection for the portal authentication server **pts**:

- Set the detection timeout to **600** seconds.
- Configure the device to send a log message if the server reachability status changes.

```
<Sysname> system-view
[Sysname] portal server pts
[Sysname-portal-server-pts] server-detect timeout 600 log
```

Related commands

portal server

server-detect (portal Web server view)

Use **server-detect** to enable portal Web server detection.

Use **undo server-detect** to disable portal Web server detection.

Syntax

server-detect [**interval** *interval*] [**retry** *retries*] { **log** | **trap** } *

undo server-detect

Default

Portal Web server detection is disabled.

Views

Portal Web server view

Predefined user roles

network-admin

context-admin

Parameters

interval *interval*: Specifies a detection interval in the range of 1 to 1200 seconds. The default is 5 seconds. As a best practice, set the detection interval to a value no less than 5.

retry *retries*: Specifies the maximum number of consecutive detection failures, in the range of 1 to 10. The default is 3. If the number of consecutive failed detections reaches this threshold, the device considers the server as unreachable.

log: Enables the device to send a log message when reachability status of the portal Web server changes. The log message contains the name, the original state, and the current state of the portal Web server.

trap: Enables the device to send a trap message to the NMS when reachability status of the portal Web server changes. The trap message contains the name and the current state of the portal Web server.

Usage guidelines

The access device performs server detection independently. No configuration on the portal Web server is required for the detection.

The portal Web server detection feature takes effect only when the URL of the portal Web server is specified and the device has a portal-enabled interface.

Examples

Enable server detection for the portal Web server **wbs**:

- Set the detection interval to **600** seconds.
- Set the maximum number of consecutive detection failures to 2.
- Configure the device to send a log message and a trap massage after server reachability status changes.

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] server-detect interval 600 retry 2 log trap
```

Related commands

portal web-server

server-detect url

Use **server-detect url** to configure the URL and the type for portal Web server detection.

Use **undo server-detect url** to restore the default.

Syntax

server-detect url *string* [**detect-type** { http | tcp }]

undo server-detect url

Default

The URL for portal Web server detection is the URL of the portal Web server. The type of portal Web server detection is TCP detection.

Views

Portal Web server view

Predefined user roles

network-admin

context-admin

Parameters

string: Specifies a URL to detect the reachability of the portal Web server. The URL is a case-sensitive string of 1 to 256 characters. The URL string can include question marks (?). If you enter a question mark (?) in the place of this argument, the CLI does not display help information for this argument.

detect-type: Specifies the type of portal Web server detection. If this keyword is not specified, TCP detection is used.

tcp: Specifies the TCP detection.

http: Specifies the HTTP detection.

Usage guidelines

This configuration takes effect only when portal Web server detection is enabled.

Examples

Configure **http://www.test.com/portal** as the portal Web server detection URL.

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] server-detect url http://www.test.com/portal
```

Configure **http://www.test.com/portal** as the portal Web server detection URL and specify TCP as the detection type.

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] server-detect url http://www.test.com/portal detect-type tcp
```

Configure **http://www.test.com/portal** as the portal Web server detection URL and specify HTTP as the detection type.

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] server-detect url http://www.test.com/portal detect-type
http
```

Related commands

server-detect (portal Web server view)

server-register

Use **server-register** to configure the device to periodically send register packets to the portal authentication server.

Use **undo server-register** to restore the default.

Syntax

server-register [**interval** *interval*]

undo server-register

Default

The device does not send register packets to a portal authentication server.

Views

Portal authentication server view

Predefined user roles

network-admin

context-admin

Parameters

interval *interval*: Specifies the interval at which the device sends register packets to the portal authentication server, in seconds. The value range for the *interval* argument is 1 to 3600, and the default value is 600.

Usage guidelines

This feature is typically used in scenarios where a NAT device exists between a portal authentication server and a large number of access devices.

Before this feature is used, you must configure a static NAT mapping for each access device on the NAT device, causing much workload. After this feature is enabled on an access device, the access device automatically sends a register packet to the portal authentication server. When the server receives the register packet, it records register information for the access device, including the device name, and the IP address and port number after NAT. The register information is used for subsequent authentication information exchanges between the server and the access device. The access device updates its register information on the server by sending register packets at regular intervals.

Only CMCC portal authentication servers support this feature.

Examples

Configure the device to send register packets to portal authentication server **pts** at intervals of 120 seconds.

```
<Sysname> system-view
[Sysname] portal server pts
[Sysname-portal-server-pts] server-register interval 120
```

Related commands

server-type (portal authentication server view/portal Web server view)

server-type (MAC binding server view)

Use **server-type** to specify the type of a MAC binding server.

Use **undo server-type** to restore the default.

Syntax

server-type { **cmcc** | **imc** }

undo server-type

Default

The type of the MAC binding server is IMC.

Views

MAC binding server view

Predefined user roles

network-admin

context-admin

Parameters

cmcc: Specifies the MAC binding server type as CMCC.

imc: Specifies the MAC binding server type as IMC.

Examples

Specify the type of the MAC binding server as **cmcc**.

```
<Sysname> system-view
[Sysname] portal mac-trigger-server mts
[Sysname-portal-mac-trigger-server-mts] server-type cmcc
```

server-type (portal authentication server view/portal Web server view)

Use **server-type** to specify the type of a portal authentication server or portal Web server.

Use **undo server-type** to restore the default.

Syntax

server-type { **cmcc** | **imc** | **ise** | **oauth** | **wifidog** }

undo server-type

Default

The type of the portal authentication server and portal Web server is IMC.

Views

Portal authentication server view

Portal Web server view

Predefined user roles

network-admin

context-admin

Parameters

cmcc: Specifies the portal server type as CMCC.

imc: Specifies the portal server type as IMC.

ise: Specifies the portal server type as ISE. This keyword is supported only in portal Web server view.

oauth: Specifies the portal server type as the cloud platform. This keyword is supported only in portal Web server view.

wifidog: Specifies the server type as WiFiDog. This keyword is supported only in portal Web server view.

Usage guidelines

Specify the portal server type on the device with the server type the device actually uses.

Examples

Specify the type of the portal authentication server as **cmcc**.

```
<Sysname> system-view
[Sysname] portal server pts
[Sysname-portal-server-pts] server-type cmcc
```

Specify the type of the portal Web server as **cmcc**.

```
<Sysname> system-view
[Sysname] portal web-server pts
[Sysname-portal-websvr-pts] server-type cmcc
```

Related commands

display portal server

shop-id

Use **shop-id** to specify the shop ID for WeChat authentication.

Use **undo shop-id** to restore the default.

Syntax

shop-id *shop-id*

undo shop-id

Default

No shop ID is specified for WeChat authentication.

Views

WeChat authentication server view

Predefined user roles

network-admin

context-admin

Parameters

shop-id: Specifies the ID of the shop where the device is deployed as a portal device for WeChat authentication.

Usage guidelines

This configuration is required for the device to provide local WeChat authentication for portal users.

To obtain the shop ID for WeChat authentication, you must perform the following tasks:

1. Go to the WeChat Official Account Admin Platform (**https://mp.weixin.qq.com**) to apply a WeChat official account.
2. Use the account to log in to the platform and enable the WeChat WiFi hotspot feature.
3. Click the device management tab, add the device: select the shop where the device is deployed, select the **portal** device type, and enter the device settings.

After the previous configurations, you will obtain the credentials (app ID, app key, and shop ID) for WeChat authentication.

When a WeChat user attempts to connect to the WiFi network provided in the specified shop, the device sends the credentials to the WeChat Official Account Platform for verification. After the credentials are verified, the device continues the portal authentication and allows the user to use the WiFi network after the authentication.

The shop ID specified in this command must be the same as the shop ID obtained from the WeChat Official Account Admin Platform.

Examples

Specify **6747662** as the shop ID for WeChat authentication.

```
<Sysname> system-view
[Sysname] portal extend-auth-server wechat
[Sysname-portal-extend-auth-server-wechat] shop-id 6747662
```

Related commands

display portal extend-auth-server

subscribe-required enable

Use **subscribe-required enable** to enable the subscribe-required feature for WeChat authentication.

Use **undo subscribe-required enable** to disable the subscribe-required feature for WeChat authentication.

Syntax

subscribe-required enable

undo subscribe-required enable

Default

The subscribe-required feature is disabled for WeChat authentication.

Views

WeChat authentication server view

Predefined user roles

network-admin

context-admin

Usage guidelines

When the subscribe-required feature is enabled, portal users must follow WeChat official accounts to pass WeChat authentication.

This feature must be used with the portal temporary pass feature. As a best practice, set the temporary pass period to 600 seconds.

Examples

Enable the subscribe-required feature for WeChat authentication.

```
<Sysname> system-view
[Sysname] portal extend-auth-server wechat
[Sysname-portal-extend-auth-server-wechat] subscribe-required enable
```

tcp-port

Use **tcp-port** to configure a listening TCP port for a local portal Web service.

Use **undo tcp-port** to restore the default.

Syntax

tcp-port *port-number*

undo tcp-port

Default

The listening TCP port number for HTTP is 80 and that for HTTPS is the TCP port number set by using the **portal local-web-server** command.

Views

Local portal Web service view

Predefined user roles

network-admin

context-admin

Parameters

port-number: Specifies the listening TCP port number in the range of 1 to 65535.

Usage guidelines

To use the local portal Web service, make sure the port number in the portal Web server URL and the port number configured in this command are the same.

For successful local portal authentication, follow these guidelines:

- Do not configure the listening TCP port number for a local portal Web service as the port number used by a known protocol. For example, do not specify port numbers 21 and 23, which are used by FTP and Telnet, respectively.
- Do not configure the HTTP listening port number as the default HTTPS listening port number 443.
- Do not configure the HTTPS listening port number as the default HTTP listening port number 80.
- Do not configure the same listening port number for HTTP and HTTPS.
- For the HTTPS-based local portal Web service and other services that use HTTPS:
  - If they use the same SSL server policy, they can use the same TCP port number to listen to HTTPS.
  - If they use different SSL server policies, they cannot use the same TCP port number to listen to HTTPS.

Examples

Set the listening port number to 2331 for the HTTP-based local portal Web service.

```
<Sysname> system-view
[Sysname] portal local-web-server http
[Sysname-portal-local-websvr-http] tcp-port 2331
```

Related commands

portal local-web-server

url

Use **url** to specify a URL for a portal Web server.

Use **undo url** to restore the default.

Syntax

url *url-string*

undo url

Default

No URL is specified for a portal Web server.

Views

Portal Web server view

Predefined user roles

network-admin

context-admin

Parameters

url-string: Specifies a URL for the portal Web server, a case-sensitive string of 1 to 256 characters. The URL string can include question marks (?). If you enter a question mark (?) in the place of this argument, the CLI does not display help information for this argument.

Usage guidelines

This command specifies a URL that can be accessed through standard HTTP or HTTPS. The URL should start with **http://** or **https://**. If the URL you specify does not start with **http://** or **https://**, the system considers the URL begins with **http://** by default.

Examples

Configure the URL for the portal Web server **wbs** as **http://www.test.com/portal**.

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] url http://www.test.com/portal
```

Related commands

display portal web-server

url-parameter

Use **url-parameter** to configure the parameters carried in the URL of a portal Web server. The access device redirects a portal user by sending the URL with the parameters to the user.

Use **undo url-parameter** to delete the parameters carried in the URL of the portal Web server.

Syntax

url-parameter *param-name* { **nas-id** | **nas-port-id** | **original-url** | **source-address** | **source-mac** [**format section** { **1** | **3** | **6** } { **lowercase** | **uppercase** }] [**encryption** { **aes** | **des** } **key** { **cipher** | **simple** } *string*] | **value** *expression* | **vlan** }

undo url-parameter *param-name*

Default

No URL parameters are configured for a portal Web server.

Views

Portal Web server view

Predefined user roles

network-admin

context-admin

Parameters

param-name: Specifies a URL parameter name, a case-sensitive string of 1 to 32 characters. Content of the parameter is determined by the following keyword you specify.

nas-id: Specifies the NAS-ID.

nas-port-id: Specifies the NAS-Port-ID.

original-url: Specifies the URL of the original webpage that a portal user visits.

source-address: Specifies the user IP address.

source-mac: Specifies the user MAC address.

format: Specifies the format of the MAC address.

section: Specifies the number of sections that a MAC address contains.

1: Specifies the one-section format XXXXXXXXXXXX.

3: Specifies the three-section format XXXX-XXXX-XXXX.

6: Specifies the six-section format XX-XX-XX-XX-XX-XX.

lowercase: Specifies the letters in a MAC address to be in lower case.

uppercase: Specifies the letters in a MAC address to be in upper case.

encryption: Specifies the encryption algorithm to encrypt the MAC address of the device oruser.

aes: Specifies the AES algorithm.

des: Specifies the DES algorithm.

key: Specifies a key for encryption.

cipher: Specifies a key in encrypted form.

simple: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the case-sensitive key string. The string length varies by the selected encryption method:

- If **des cipher** is specified, the string length is 41 characters.
- If **des simple** is specified, the string length is 8 characters.
- If **aes cipher** is specified, the string length is 1 to 73 characters.
- If **aes simple** is specified, the string length is 1 to 31 characters.

value *expression*: Specifies a custom case-sensitive string of 1 to 256 characters. The string can include question marks (?). If you enter a question mark (?) in the place of the *expression* argument, the CLI does not display help information for this argument.

vlan: Specifies the user VLAN ID.

Usage guidelines

You can configure multiple URL parameters.

To avoid redirection failure, add only necessary URL parameters to the portal Web server URL. Ensure that the total length of the portal Web server URL is no longer than 2048 bytes.

If you execute this command multiple times to configure the same URL parameter, the most recent configuration takes effect.

After you configure the URL parameters, the access device sends the portal Web server URL with these parameters to portal users. For example, assume that the URL of a portal Web server is **http://www.test.com/portal**, and you execute the **url-parameter userip source-address** and **url-parameter userurl value http://www.abc.com/welcome** commands. Then, the access device sends to the user whose IP address is 1.1.1.1 the URL **http://www.test.com/portal?userip=1.1.1.1&userurl=http://www.abc.com/welcome**.

When you configure the *param-name* argument in this command, you must use the URL parameter name supported by the actual portal server. Different portal server types support different URL parameter names.

For example, the IMC server supports parameter names **userurl**, **userip**, and **usermac** for the keywords **original-url**, **source-address**, and **source-mac**, respectively. To carry the user IP information in the portal Web server URL, you must configure the parameter name as **userip** and specify the **source-address** keyword.

If you specify the encryption algorithm for a parameter, the redirection URL carries the encrypted value for the parameter. Execute the **url-parameter usermac source-mac encryption des key simple 12345678** command. Then, the access device sends to the user with MAC address 1111-1111-1111 the URL **http://www.test.com/portal?usermac=xxxxxxxxx&userip=1.1.1.1&userurl= http://www.test.com/welcome**, where xxxxxxxxx represents the encrypted user MAC address.

Examples

Configure URL parameters **userip** and **userurl** for portal Web server **wbs**. Configure the value of the **userip** parameter as **source-address** (the IP addresses of users) and that of the **userurl** parameter as **http://www.abc.com/welcome**.

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] url-parameter userip source-address
[Sysname-portal-websvr-wbs] url-parameter userurl value http://www.abc.com/welcome
```

Configure URL parameter **usermac** for portal Web server **wbs**. Configure the value of the **usermac** parameter as **source-mac** (the MAC addresses of users) and specify DES to encrypt the MAC addresses.

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] url-parameter usermac source-mac encryption des key simple
12345678
```

Configure URL parameter **uservlan** for portal Web server **wbs**. Configure the value of the **uservlan** parameter as **vlan** (the VLAN IDs of users.)

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] url-parameter uservlan vlan
```

Related commands

display portal web-server

url

user-agent

Use **user-agent** to configure the User-Agent match string.

Use **undo user-agent** to restore the default.

Syntax

user-agent *user-agent-string*

undo user-agent

Default

The User-Agent match string is **MicroMessenger**.

Views

Local portal Web service view

Predefined user roles

network-admin

context-admin

Parameters

user-agent-string: Specifies the User-Agent match string, a case-sensitive string of 1 to 255 characters.

Examples

Configure the User-Agent match string as **text**.

```
<Sysname> system-view
[Sysname] portal local-web-server http
[Sysname-portal-local-websvr-http] user-agent text
```

user-password modify enable

Use **user-password modify enable** to enable local portal user password modification.

Use **undo user-password modify enable** to disable local portal user password modification.

Syntax

user-password modify enable

undo user-password modify enable

Default

Local portal user password modification is disabled.

Views

Local portal Web service view

Predefined user roles

network-admin

context-admin

Usage guidelines

This feature enables the local portal Web service to display the password modification button on the portal authentication page. Local portal users can change their passwords through this button.

If global password control is enabled by using the **password-control enable network-class** command, the new password of a local portal user must meet the password control requirements. For more information about password control, see password control configuraiton in *Security Configuration Guide*.

Examples

In local portal Web service view, enable local portal user password modification.

```
<Sysname> system-view
[Sysname] portal local-web-server http
[Sysname-portal-local-websvr-http] user-password modify enable
```

Related commands

password-control enable network-class

portal local-web-server

user-sync

Use **user-sync** to enable portal user synchronization for a portal authentication server.

Use **undo user-sync** to disable portal user synchronization for a portal authentication server.

Syntax

user-sync timeout *timeout*

undo user-sync

Default

Portal user synchronization is disabled for a portal authentication server.

Views

Portal authentication server view

Predefined user roles

network-admin

context-admin

Parameters

timeout *timeout*: Specifies a detection timeout for synchronization packets, in the range of 60 to 18000 seconds.

Usage guidelines

This feature enables the device to reply to and periodically detect the synchronization packets from the portal authentication server. In this way, information about online portal users on the device and on the portal authentication server remains consistent.

- For information of the users considered as nonexistent on the portal authentication server, the device deletes the information after the configured detection timeout expires.
- If the user information from the portal authentication server does not exist on the device, the device encapsulates IP addresses of the users in user heartbeat reply packets to the server. The portal authentication server then deletes the users.

Portal user synchronization requires that the portal authentication server support the portal user heartbeat feature. Now, only the IMC portal authentication server supports portal user heartbeat. To implement portal user synchronization, you need to configure the user heartbeat feature on the portal authentication server. Make sure the user heartbeat interval configured on the portal authentication server is not greater than the synchronization detection timeout configured on the access device.

Deleting a portal authentication server on the device also deletes the user synchronization configuration for the server.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Enable portal user synchronization for the portal authentication server **pts** and set the detection timeout to **600** seconds. If a use has not appeared in the synchronization packets sent by the portal authentication server for 600 seconds, the access device logs out the user.

```
<Sysname> system-view
[Sysname] portal server pts
[Sysname-portal-server-pts] user-sync timeout 600
```

Related commands

portal server

version

Use **version** to specify the version of the portal protocol.

Use **undo version** to restore the default.

Syntax

version *version-number*

undo version

Default

The version of the portal protocol is 1.

Views

MAC binding server view

Predefined user roles

network-admin

context-admin

Parameters

version-number: Specifies the portal protocol version in the range of 1 to 3.

Usage guidelines

The specified portal protocol version must be the that required by the MAC binding server.

Examples

Configure the device to use portal protocol version 2 to communicate with the MAC binding server **mts**.

```
<Sysname> system-view
[Sysname] portal mac-trigger-server mts
[Sysname-portal-mac-trigger-server-mts] version 2
```

Related commands

display portal mac-trigger-server

portal mac-trigger-server

vpn-instance

Use **vpn-instance** to specify the MPLS L3VPN where a portal Web server resides.

Use **undo vpn-instance** to restore the default.

Syntax

vpn-instance *vpn-instance-name*

undo vpn-instance

Default

A portal Web server is on the public network.

Views

Portal Web server view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance-name: Specifies the name of the MPLS L3VPN where the portal Web server resides, a case-sensitive string of 1 to 31 characters.

Usage guidelines

A portal Web server belongs to only one MPLS L3VPN.

Examples

Configure the MPLS L3VPN for the portal Web server **wbs** as **abc**.

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] vpn-instance abc
```

web-redirect url

Use **web-redirect url** to enable the Web redirect feature.

Use **undo web-redirect url** to disable the Web redirect feature.

Syntax

web-redirect [**ipv6**] **url** *url-string* [**interval** *interval*]

undo web-redirect [**ipv6**]

Default

The Web redirect feature is disabled.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ipv6: Specifies the IPv6 Web redirect feature. Do not specify this keyword for the IPv4 Web redirect feature.

url *url-string*: Specifies the URL to which the user is redirected, a string of 1 to 256 characters. The URL must exist and must be a complete URL beginning with **http://** or **https://**. The URL string can include question marks (?). If you enter a question mark (?) in the place of the *url-string* argument, the CLI does not display help information for this argument.

interval *interval*: Specifies the time interval at which the user is redirected to the specified URL. It is in the range of 60 to 86400 seconds. The default interval is 86400 seconds.

Usage guidelines

This feature redirects a user on an interface to the specified URL before the user can access an external network through a Web browser. After the specified interval, the user is redirected to the specified URL again.

The Web redirect feature takes effect only on HTTP packets that use the default port number 80.

To use the device URL as the Web redirect URL or allow users to successfully access the device URL, you must enable the HTTP service. To enable the HTTP service, use the **ip http enable** command.

To push different advertisement pages to different users, you can carry parameters in the redirect URL (by using the **url** *url-string* option) as needed. The following parameters are available:

- **userip=%c**—IP address of the user.
- **usermac=%m**—MAC address of the user.
- **nasid=%n**—NAS identifier of the device.
- **ssid=%E**—SSID with which the user associates.
- **originalurl=%o**—Original URL that the user enters in the browser.

Make sure the arrangement of the parameters conforms to the format of http://XXXX/index.html?userip=%c&usermac=%m&nasid=%n&ssid=%E&originalurl=%o.

Examples

Configure IPv4 Web redirect on GigabitEthernet 1/0/1. Set the redirect URL to **http://192.0.0.1 /index.html?userip=%c&usermac=%m&nasid=%n&ssid=%E&originalurl=%o** and the interval to 3600 seconds.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] web-redirect url http://192.0.0.1
/index.html?userip=%c&usermac=%m&nasid=%n&ssid=%E&originalurl=%o interval 3600
```

Related commands

display web-redirect rule

Contents

MAC authentication commands

display mac-authentication

Use **display mac-authentication** to display MAC authentication settings and statistics.

Syntax

display mac-authentication [**ap** *ap-name* [**radio** *radio-id*] | **interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ap *ap-name*: Specifies an AP by its name, a case-sensitive string of 1 to 64 characters. The string can contain letters, digits, underscores (_), dots (.), left brackets ([), right brackets (]), forward slashes (/), and hyphens (-).

radio *radio-id*: Specifies a radio by its ID. The value range for the *radio-id* argument varies by AP model. If you do not specify a radio, this command displays MAC authentication information for all radios on the specified AP.

interface *interface-type interface-number*: Specifies a port by its type and number. If the specified port is not enabled with MAC authentication, this command displays only global MAC authentication information.

Usage guidelines

If you do not specify any parameters, this command displays all MAC authentication information including the global settings, port-specific settings, MAC authentication statistics, and online user statistics.

Examples

Display all MAC authentication settings and statistics.

```
<Sysname> display mac-authentication
Global MAC authentication parameters:
   MAC authentication     : Enabled
   User name format       : MAC address in lowercase(xx-xx-xx-xx-xx-xx)
           Username       : mac
           Password       : Not configured
   Offline detect period  : 300 s
   Quiet period           : 60 s
   Server timeout         : 100 s
   Authentication domain  : Not configured, use default domain
 Online MAC-auth wired users    : 1
```

```
Silent MAC users:
         MAC address       VLAN ID  From port                   Port index
         0001-0000-0001    100      GigabitEthernet1/0/2        21
         0001-0000-0003    12       GigabitEthernet1/0/4        301

GigabitEthernet1/0/1  is link-up
  MAC authentication         : Enabled
  Carry User-IP              : Disabled
  Authentication domain      : Not configured
  Auth-delay timer           : Enabled
      Auth-delay period      : 60 s
  Re-auth server-unreachable : Logoff
  Guest VLAN                 : 100
  Guest VLAN auth-period     : 150 s
  Critical VLAN              : Not configured
  Critical voice VLAN        : Disabled
  Host mode                  : Multiple VLAN
  Max online users           : 256
  Authentication attempts    : successful 2, failed 3
  Current online users       : 1
         MAC address       Auth state
         0001-0000-0001    Unauthenticated

AP name: AP1  Radio ID: 1  SSID: wlan_maca_ssid
  BSSID                      : 1111-1111-1111
MAC authentication           : Enabled
  Authentication domain      : Not configured
  Max online users           : 256
  Authentication attempts    : successful 1, failed 0
  Current online users       : 2
         MAC address       Auth state
         0001-0000-0002    Authenticated
         0001-0000-0003    Unauthenticated
```

Table 1 Command output

Field	Description
MAC authentication	Whether MAC authentication is enabled globally. Support for MAC authentication depends on the device model. The MAC authentication configuration does not take effect on some device models.
User name format	User account type: MAC-based or shared. • If MAC-based accounts are used, this field displays the format settings for the username. For example, **MAC address in lowercase(xx-xx-xx-xx-xx-xx)** indicates that the MAC address is in six-section format, and letters are in lower case. • If a shared account is used, this field displays **Fixed account**.
Username	Username for MAC authentication. • If MAC-based accounts are used, this field displays **mac**. The device uses the MAC address of each user as the username

Field	Description
	and password for MAC authentication. • If a shared account is used, this field displays the username of the shared account for MAC authentication users. By default, the username is **mac**.
Password	Password for MAC authentication. • If MAC-based accounts are used or if a shared account is used but no password is configured, this field displays **Not configured**. • If a shared account is used and a password is configured, this field displays a string of asterisks (******).
Offline detect period	Offline detect timer.
Quiet period	Quiet timer.
Server timeout	Server timeout timer.
Authentication domain	MAC authentication domain specified in system view. If no authentication domain is specified in system view, this field displays **Not configured, use default domain**.
Online MAC-auth wired users	Number of wired online MAC authentication users, including users that have passed MAC authentication and users that are performing MAC authentication.
Silent MAC users	Information about silent MAC addresses.
MAC address	Silent MAC address.
VLAN ID	ID of the VLAN to which the silent MAC address belongs.
From port	Name of the port that marks the MAC address as a silent MAC address.
Port index	Index of the port that marks the MAC address as a silent MAC address.
GigabitEthernet1/0/1 is link-up	Status of the link on GigabitEthernet 1/0/1. In this example, the link is up.
MAC authentication	Whether MAC authentication is enabled on the port.
Carry User-IP	This field is not supported in the current software version. Whether user IP addresses are included in MAC authentication requests.
Authentication domain	MAC authentication domain specified for the port.
Auth-delay timer	Whether MAC authentication delay is enabled on the port.
Auth-delay period	MAC authentication delay timer.
Re-auth server-unreachable	Action taken when no server is reachable for MAC reauthentication: • **Logoff**—Logs off online MAC authentication users. • **Online**—Keeps MAC authenticated users online.
Guest VLAN	MAC authentication guest VLAN configured on the port. If no MAC authentication guest VLAN is configured, this field displays **Not configured**.
Guest VLAN auth-period	Authentication interval for users in the MAC authentication guest VLAN on the port.
Critical VLAN	MAC authentication critical VLAN configured on the port.

Field	Description
	If no MAC authentication critical VLAN is configured, this field displays **Not configured**.
Critical voice VLAN	This field is not supported in the current software version. Whether the MAC authentication critical voice VLAN feature is enabled on the port.
Host mode	• If multi-VLAN mode is enabled, this field displays **Multiple VLAN**. • If multi-VLAN mode is disabled, this field displays **Single VLAN**.
Max online users	Maximum number of concurrent online users allowed on the port.
Authentication attempts: successful 1, failed 0	MAC authentication statistics, including the number of successful and unsuccessful authentication attempts.
MAC address	MAC address of the online user.
Auth state	User status: • **Authenticated**—The user has passed MAC authentication. • **Unauthenticated**—The user failed MAC authentication.

display mac-authentication connection

Use **display mac-authentication connection** to display information about online MAC authentication users.

Syntax

display mac-authentication connection [**interface** *interface-type interface-number* | **slot** *slot-number* | **user-mac** *mac-addr* | **user-name** *user-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify a port, this command displays information about online MAC authentication users for all ports.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about online MAC authentication users for all member devices.

user-mac *mac-address*: Specifies an online MAC authentication user by its MAC address. The *mac-address* argument represents the MAC address of the user, in the form of H-H-H. If you do not specify an online MAC authentication user, this command displays online user information for all MAC authentication users.

user-name *user-name*: Specifies an online MAC authentication user by its username. The user name is a case-sensitive string of 1 to 55 characters, and it can include the domain name. If you do not specify an online MAC authentication user, this command displays online user information for all MAC authentication users.

Usage guidelines

If you do not specify any parameters, this command displays information about online MAC authentication users for all ports.

If you do not specify any parameters, this command displays information about online MAC authentication users for all member devices.

Examples

Display all online MAC authentication user information.

```
<Sysname> display mac-authentication connection
Total connections: 1

Slot ID: 0
User MAC address: 0015-e9a6-7cfe
Access interface: GigabitEthernet1/0/1
Username: ias
Authentication domain: nsfocus
Initial VLAN: 1
Authorization untagged VLAN: 100
Authorization tagged VLAN: N/A
Authorization ACL number/name: 3001
Authorization user profile: N/A
Termination action: Radius-request
Session timeout period: 2 s
Online from: 2013/03/02  13:14:15
Online duration: 0h 2m 15s

User MAC address              : 0015-e9a6-7cfe
AP name                       : ap1
Radio ID                      : 1
SSID                          : wlan_dot1x_ssid
BSSID                         : 0015-e9a6-7cf0
User name                     : ias
Authentication domain         : 1
Initial VLAN                  : 1
Authorization VLAN   : 100
Authorization ACL number      : 3001
Authorization user profile    : N/A
Authorization CAR             :
  Average input rate          : 102400 bps
  Average output rate         : 102400 bps
Authorization URL             : N/A
Termination action            : Radius-request
Session timeout period        : 2 sec
Online from                   : 2014/06/02 13:14:15
Online duration               : 0h 2m 15s
```

Table 2 Command output

Field	Description
Total connections	Total number of online MAC authentication users.
User MAC address	MAC address of the user.
Access interface	Interface through which the user accesses the device.
Authentication domain	MAC authentication domain to which the user belongs.
IPv4 address	IPv4 address of the user. If no user IPv4 address is available, this field is not displayed.
IPv6 address	IPv6 address of the user. If no user IPv6 address is available, this field is not displayed.
Initial VLAN	VLAN that holds the user before MAC authentication.
Authorization untagged VLAN	Untagged VLAN authorized to the user.
Authorization tagged VLAN	Tagged VLAN authorized to the user.
Authorization VLAN	VLAN authorized to the user.
Authorization ACL number/name	This field is not supported in the current software version. Number or name of the ACL authorized to the user. If no ACL is authorized, this field displays **N/A**. If ACL authorization fails, this field displays **(NOT effective)** after the ACL number or name.
Authorization user profile	User profile authorized to the user.
Authorization CAR	Authorization CAR attributes assigned by the server. • **Average input rate**—Average rate of inbound traffic in bps. • **Average output rate**—Average rate of outbound traffic in bps. If no authorization CAR attributes are assigned, this field displays **N/A**.
Authorization URL	URL authorized to the user.
Termination action	Action attribute assigned by the server to terminate the user session: • **Default**—Logs off the online authenticated user when the session timeout timer expires. • **Radius-request**—Reauthenticates the online user when the session timeout timer expires. If the device performs local authentication, this field displays **N/A**.
Session timeout period	Session timeout timer assigned by the server. If the device performs local authentication, this field displays **N/A**.
Online from	Time from which the MAC authentication user came online.
Online duration	Online duration of the MAC authentication user.

mac-authentication

Use **mac-authentication** to enable MAC authentication globally or on a port.

Use **undo mac-authentication** to disable MAC authentication globally or on a port.

Syntax

mac-authentication

undo mac-authentication

Default

MAC authentication is disabled globally or on any port.

Views

System view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

To use MAC authentication on a port, you must enable the feature both globally and on the port.

Support for MAC authentication depends on the device model. MAC authentication does not take effect on some device models.

Examples

Enable MAC authentication globally.

```
<Sysname> system-view
[Sysname] mac-authentication
```

Enable MAC authentication on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication
```

Related commands

display mac-authentication

mac-authentication access-user log enable

Use **mac-authentication access-user log enable** to enable MAC authentication user logging.

Use **undo mac-authentication access-user log enable** to disable MAC authentication user logging.

Syntax

mac-authentication access-user log enable [**failed-login** | **logoff** | **successful-login**] *

undo mac-authentication access-user log enable [**failed-login** | **logoff** | **successful-login**] *

Default

MAC authentication user logging is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

`failed-login`: Logs MAC authentication user login failures.

`logoff`: Logs MAC authentication user logoffs.

`successful-login`: Logs successful MAC authentication user logins.

Usage guidelines

To prevent excessive MAC authentication user log entries, use this feature only if you need to analyze abnormal MAC authentication user logins or logouts.

If you do not specify any parameters, this command enables all types of MAC authentication user logs.

Examples

Enable logging MAC authentication user login failures.

```
<Sysname> system-view
[Sysname] mac-authentication access-user log enable failed-login
```

Related commands

`info-center source maca logfile deny` (*Network Management and Monitoring Command Reference*)

mac-authentication critical vlan

Use **`mac-authentication critical vlan`** to configure a MAC authentication critical VLAN on a port.

Use **`undo mac-authentication critical vlan`** to restore the default.

Syntax

`mac-authentication critical vlan` *`critical-vlan-id`*

`undo mac-authentication critical vlan`

Default

No MAC authentication critical VLAN exists on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

context-admin

Parameters

`critical-vlan-id`: Specifies a VLAN as the MAC authentication critical VLAN. The value range for the VLAN ID is 1 to 4094. Make sure the VLAN has been created.

Usage guidelines

The MAC authentication critical VLAN accommodates users that have failed MAC authentication because all the servers in their ISP domains are unreachable. Users in the critical VLAN can access network resources in the critical VLAN.

The critical VLAN feature takes effect when MAC authentication is performed only through RADIUS servers. If a MAC authentication user fails local authentication after RADIUS authentication, the user is not assigned to the critical VLAN.

Before you delete a VLAN that has been set as a MAC authentication critical VLAN, use the **undo mac-authentication critical vlan** command to remove the critical VLAN configuration.

Examples

Configure VLAN 100 as the MAC authentication critical VLAN on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication critical vlan 100
```

Related commands

display mac-authentication

reset mac-authentication critical-vlan

mac-authentication domain

Use **mac-authentication domain** to specify a global or port-specific authentication domain.

Use **undo mac-authentication domain** to restore the default.

Syntax

mac-authentication domain *domain-name*

undo mac-authentication domain

Default

The system default authentication domain is used. For more information about the default authentication domain, see the **domain default enable** command in "AAA commands."

Views

System view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

context-admin

Parameters

domain-name: Specifies the name of an ISP domain, a case-insensitive string of 1 to 255 characters.

Usage guidelines

The global authentication domain applies to all MAC authentication-enabled ports. An authentication domain specified in Layer 2 Ethernet interface view applies only to the port. You can specify different authentication domains on different ports.

A port chooses an authentication domain for MAC authentication users in the following order:

1. Authentication domain specified on the port.
2. Global authentication domain specified in system view.
3. Default authentication domain.

Examples

Specify ISP domain **domain1** as the global MAC authentication domain.

```
<Sysname> system-view
[Sysname] mac-authentication domain domain1
```

Specify ISP domain **aabbcc** as the MAC authentication domain on GigabitEthernet 1/0/1.

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication domain aabbcc
```

Related commands

display mac-authentication

domain default enable

mac-authentication guest-vlan

Use **mac-authentication guest-vlan** to configure a MAC authentication guest VLAN on a port.

Use **undo mac-authentication guest-vlan** to restore the default.

Syntax

mac-authentication guest-vlan *guest-vlan-id*

undo mac-authentication guest-vlan

Default

No MAC authentication guest VLAN exists on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

context-admin

Parameters

guest-vlan-id: Specifies a VLAN as the MAC authentication guest VLAN. The value range for the VLAN ID is 1 to 4094. Make sure the VLAN has been created.

Usage guidelines

The MAC authentication guest VLAN accommodates users that have failed MAC authentication for any reason other than server unreachable. For example, the VLAN accommodates users with invalid passwords entered. You can deploy a limited set of network resources in the MAC authentication guest VLAN. For example, a software server for downloading software and system patches.

Before you delete a VLAN that has been set as a MAC authentication guest VLAN, use the **undo mac-authentication guest-vlan** command to remove the guest VLAN configuration.

Examples

Configure VLAN 100 as the MAC authentication guest VLAN on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication guest-vlan 100
```

Related commands

display mac-authentication

reset mac-authentication guest-vlan

mac-authentication guest-vlan auth-period

Use **mac-authentication guest-vlan auth-period** to set the interval at which the device authenticates users in the MAC authentication guest VLAN.

Use **undo mac-authentication guest-vlan auth-period** to restore the default.

Syntax

mac-authentication guest-vlan auth-period *period-value*

undo mac-authentication guest-vlan auth-period

Default

The device authenticates users in the MAC authentication guest VLAN every 30 seconds.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

context-admin

Parameters

period-value: Specifies the authentication interval for users in the MAC authentication guest VLAN. The value range is 1 to 3600, in seconds.

Examples

Set the authentication interval to 150 seconds for users in the MAC authentication guest VLAN on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication guest-vlan auth-period 150
```

Related commands

display mac-authentication

mac-authentication guest-vlan

mac-authentication host-mode multi-vlan

Use **mac-authentication host-mode multi-vlan** to enable MAC authentication multi-VLAN mode on a port.

Use **undo mac-authentication host-mode** to restore the default.

Syntax

mac-authentication host-mode multi-vlan

undo mac-authentication host-mode

Default

MAC authentication multi-VLAN mode is disabled on a port. When the port receives a packet sourced from an authenticated MAC address in a VLAN not matching the existing MAC-VLAN mapping, the device logs off and reauthenticates the user.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

The MAC authentication multi-VLAN mode prevents an authenticated online user from service interruption caused by VLAN changes on a port. When the port receives a packet sourced from the user in a VLAN not matching the existing MAC-VLAN mapping, the device neither logs off the user nor reauthenticates the user. The device creates a new MAC-VLAN mapping for the user, and traffic transmission is not interrupted. The original MAC-VLAN mapping for the user remains on the device until it dynamically ages out. As a best practice, configure this feature on hybrid or trunk ports.

Examples

Enable MAC authentication multi-VLAN mode on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication host-mode multi-vlan
```

Related commands

display mac-authentication

mac-authentication max-user

Use **mac-authentication max-user** to set the maximum number of concurrent MAC authentication users on a port.

Use **undo mac-authentication max-user** to restore the default.

Syntax

mac-authentication max-user *max-number*

undo mac-authentication max-user

Default

The default is 4294967295.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

context-admin

Parameters

max-number: Sets the maximum number of concurrent MAC authentication users on the port. The value range for this argument is 1 to 4294967295.

Usage guidelines

Set the maximum number of concurrent MAC authentication users on a port to prevent the system resources from being overused. When the maximum number is reached, the port denies subsequent MAC authentication users.

Examples

Configure GigabitEthernet 1/0/1 to support a maximum of 32 concurrent MAC authentication users.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication max-user 32
```

Related commands

display mac-authentication

mac-authentication re-authenticate server-unreachable keep-online

Use **mac-authentication re-authenticate server-unreachable keep-online** to enable the keep-online feature on a port.

Use **undo mac-authentication re-authenticate server-unreachable** to restore the default.

Syntax

mac-authentication re-authenticate server-unreachable keep-online

undo mac-authentication re-authenticate server-unreachable

Default

The keep-online feature is disabled on a port. The device logs off online MAC authentication users if no server is reachable for MAC reauthentication.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

The keep-online feature keeps authenticated MAC authentication users online when no server is reachable for MAC reauthentication.

Examples

Enable the keep-online feature for authenticated MAC authentication users on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication re-authenticate server-unreachable
keep-online
```

Related commands

display mac-authentication

mac-authentication timer

Use **mac-authentication timer** to configure a MAC authentication timer.

Use **undo mac-authentication timer** to restore the default of a MAC authentication timer.

Syntax

mac-authentication timer { **offline-detect** *offline-detect-value* | **quiet** *quiet-value* | **server-timeout** *server-timeout-value* }

undo mac-authentication timer { **offline-detect** | **quiet** | **server-timeout** }

Default

The following MAC authentication timers apply:

- The offline detect timer is 300 seconds.
- The quiet timer is 60 seconds.
- The server timeout timer is 100 seconds.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

offline-detect *offline-detect-value*: Sets the offline detect timer in seconds, in the range of 60 to 2147483647.

quiet *quiet-value*: Sets the quiet timer in seconds, in the range of 1 to 3600.

server-timeout *server-timeout-value*: Sets the server timeout timer in seconds, in the range of 100 to 300.

Usage guidelines

MAC authentication uses the following timers:

- **Offline detect timer**—Sets the interval that the device waits for traffic from a user before the device determines that the user is idle. If the device has not received traffic from a user before the timer expires, the device logs off that user and requests the accounting server to stop accounting for the user.
- **Quiet timer**—Sets the interval that the device must wait before the device can perform MAC authentication for a user that has failed MAC authentication. All packets from the MAC address are dropped during the quiet time. This quiet mechanism prevents repeated authentication from affecting system performance.
- **Server timeout timer**—Sets the interval that the device waits for a response from a RADIUS server before the device determines that the RADIUS server is unavailable. If the timer expires during MAC authentication, the user cannot access the network.

Examples

Set the server timeout timer to 150 seconds.

```
<Sysname> system-view
[Sysname] mac-authentication timer server-timeout 150
```

Related commands

display mac-authentication

mac-authentication user-name-format

Use **mac-authentication user-name-format** to configure the type of user accounts for MAC authentication users.

Use **undo mac-authentication user-name-format** to restore the default.

Syntax

mac-authentication user-name-format { **fixed** [**account** *name*] [**password** { **cipher** | **simple** } *string*] | **mac-address** [{ **with-hyphen** [**six-section** | **three-section**] | **without-hyphen** } [**lowercase** | **uppercase**]] }

undo mac-authentication user-name-format

Default

Each user's MAC address is used as the username and password for MAC authentication. The MAC addresses are in hexadecimal notation without hyphens, and letters are in lower case.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

fixed: Uses a shared account for all MAC authentication users.

account *name*: Specifies the username for the shared account. The name is a case-sensitive string of 1 to 55 characters, excluding the at sign (@). If you do not specify a username, the default name **mac** applies.

password: Specifies the password for the shared user account. If you do not specify a password for the shared account, the shared account does not have a password.

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 63 characters. Its encrypted form is a case-sensitive string of 1 to 117 characters.

mac-address: Uses MAC-based user accounts for MAC authentication users. You can also specify the format of username and password by using the following keywords:

- **with-hyphen**: Includes hyphens in the MAC address.
  - **six-section**: Hyphenates the MAC address into six groups of two hexadecimal digits, for example, xx-xx-xx-xx-xx-xx or XX-XX-XX-XX-XX-XX.
  - **three-section**: Hyphenates the MAC address into three groups of four hexadecimal digits, for example, xxxx-xxxx-xxxx or XXXX-XXXX-XXXX.

  If you do not specify the **six-section** or **three-section** keyword, the MAC address is in six-section format.
- **without-hyphen**: Excludes hyphens from the MAC address, for example, xxxxxxxxxxxx or XXXXXXXXXXXX.
- **lowercase**: Specifies letters in lower case.
- **uppercase**: Specifies letters in upper case.

Usage guidelines

If you specify the MAC-based user account, the device uses the MAC address of a user as the username and password for MAC authentication of the user. This user account type ensures high authentication security. However, you must create on the authentication server a user account for each user, using the MAC address of the user as both the username and password.

If you specify a shared user account, the device uses the specified username and password for MAC authentication of all users. Because all MAC authentication users use a single account for authentication, you only need to create one account on the authentication server. This user account type is suitable for trusted networks.

Examples

Configure a shared account for MAC authentication users, and set the username to **abc** and password to plaintext string of **xyz**.

```
<Sysname> system-view
[Sysname] mac-authentication user-name-format fixed account abc password simple xyz
```

Use MAC-based user accounts for MAC authentication users. The MAC addresses must be in hexadecimal notation without hyphens, and letters are in upper case.

```
<Sysname> system-view
[Sysname] mac-authentication user-name-format mac-address without-hyphen uppercase
```

Related commands

display mac-authentication

reset mac-authentication access-user

Use **reset mac-authentication access-user** to log off MAC authentication users.

Syntax

reset mac-authentication access-user [**interface** *interface-type interface-number* | **mac** *mac-address* | **username** *username* | **vlan** *vlan-id* | **vsi** *vsi-name*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number.

mac *mac-address*: Specifies a MAC authentication user by its MAC address. The *mac-address* argument is in the format of H-H-H.

username *username*: Specifies a MAC authentication user by its name. The *username* argument is a case-sensitive string of 1 to 253 characters.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID. The value range for the *vlan-id* argument is 1 to 4094.

vsi *vsi-name*: Specifies a VSI by its name. The *vsi-name* argument is a case-sensitive string of 1 to 31 characters.

Usage guidelines

Use this command to log off the specified MAC authentication users and clear information about these users from the device. These users must perform MAC authentication to come online again.

With a VSI specified, this command logs off a MAC authentication user if that user has passed authentication and its authorization VSI is the specified VSI.

With a VLAN specified, this command logs off the following MAC authentication users:

- Users that have passed MAC authentication and have been assigned the specified VLAN as their authorization VLAN by the server.
- Users that stay in the specified VLAN after they have passed MAC authentication, because they have not been assigned an authorization VLAN yet.
- Users that are performing MAC authentication in the specified VLAN.

To identify the VLAN in which a user is staying, use the **display mac-address** command.

If you do not specify any parameters, the **reset mac-authentication access-user** command logs off all MAC authentication users on the device.

Examples

Log off all MAC authentication users on GigabitEthernet 1/0/1.

```
<Sysname> reset mac-authentication access-user interface gigabitethernet 1/0/1
```

Related commands

display mac-authentication connection

reset mac-authentication critical-vlan

Use **reset mac-authentication critical-vlan** to remove users from the MAC authentication critical VLAN on a port.

Syntax

reset mac-authentication critical-vlan interface *interface-type interface-number* [**mac-address** *mac-address*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number.

mac-address *mac-address*: Specifies a user by its MAC address. If you do not specify this option, the command removes all users from the MAC authentication critical VLAN on the port.

Examples

Remove the user with MAC address **1-1-1** from the MAC authentication critical VLAN on GigabitEthernet 1/0/1.

```
<Sysname> reset mac-authentication critical-vlan interface gigabitethernet 1/0/1
mac-address 1-1-1
```

Related commands

display mac-authentication

mac-authentication critical vlan

reset mac-authentication guest-vlan

Use **reset mac-authentication guest-vlan** to remove users from the MAC authentication guest VLAN on a port.

Syntax

reset mac-authentication guest-vlan interface *interface-type interface-number* [**mac-address** *mac-address*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number.

mac-address *mac-address*: Specifies a user by its MAC address. If you do not specify this option, the command removes all users from the MAC authentication guest VLAN on the port.

Examples

Remove the user with MAC address **1-1-1** from the MAC authentication guest VLAN on GigabitEthernet 1/0/1.

```
<Sysname> reset mac-authentication guest-vlan interface gigabitethernet 1/0/1 mac-address 1-1-1
```

Related commands

display mac-authentication

mac-authentication guest-vlan

reset mac-authentication statistics

Use **reset mac-authentication statistics** to clear MAC authentication statistics.

Syntax

reset mac-authentication statistics [**ap** *ap-name* [**radio** *radio-id*] | **interface** *interface-type interface-number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

ap *ap-name*: Specifies an AP by its name, a case-sensitive string of 1 to 64 characters. The string can contain letters, digits, underscores (_), dots (.), left brackets ([), right brackets (]), forward slashes (/), and hyphens (-). If you do not specify an AP, this command clears MAC authentication statistics for all APs.

radio *radio-id*: Specifies a radio by its ID. The value range for the *radio-id* argument varies by AP model. If you do not specify a radio, this command clears MAC authentication statistics for all radios on the specified AP.

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify a port, this command clears both global and port-specific MAC authentication statistics.

Usage guidelines

If you do not specify any parameters, this command clears all MAC authentication statistics.

Examples

Clear MAC authentication statistics on GigabitEthernet 1/0/1.

```
<Sysname> reset mac-authentication statistics interface gigabitethernet 1/0/1
```

Related commands

display mac-authentication

Contents

IPoE commands

IPv4 IPoE commands

display ip subscriber interface-leased

Use **display ip subscriber interface-leased** to display information about IPv4 interface-leased users.

Syntax

display ip subscriber interface-leased [**interface** *interface-type interface-number*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays information about IPv4 interface-leased users for all interfaces.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about IPv4 interface-leased users for all member devices.

Examples

Display information about the IPv4 interface-leased user on GigabitEthernet 1/0/1.

```
<Sysname> display ip subscriber interface-leased interface gigabitethernet 1/0/1
Basic:
  Access interface           : GE1/0/1
  VPN instance               : N/A
  Username                   : a
  User ID                    : 0x30000000
  State                      : Online
  Service node               : Slot 1 CPU 0
  Domain                     : radius
  Login time                 : May 14 20:04:42 2014
  Online time (hh:mm:ss)     : 00:16:37

AAA:
  IP pool                    : ipoe
  Session idle time          : N/A
  Session duration           : N/A, remaining: N/A
```

```
  Remaining traffic          : N/A
  Max multicast addresses    : 4
  Multicast address list     : N/A

QoS:
  User profile               : nsfocus (active)
  Session group profile      : N/A
  Inbound CAR                : CIR 1000bps PIR 2000bps CBS 500bit (active)
  Outbound CAR               : CIR 3000bps PIR 4000bps CBS 500bit (active)

Flow statistic:
  Uplink   packets/bytes     : 0/0
  Downlink packets/bytes     : 0/0

ITA:
  Level-1 Uplink   packets/bytes: 0/0
          Downlink packets/bytes: 0/0
  Level-2 Uplink   packets/bytes: 0/0
          Downlink packets/bytes: 0/0
```

Table 1 Command output

Field	Description
Basic	Basic session information.
Access interface	Interface that connects the user.
VPN instance	MPLS L3VPN instance of the user. If the user is not in a VPN, this field displays **N/A**.
Username	Username for authentication.
User ID	User ID assigned after the user came online. If no user ID is assigned, this field displays **0xffffffff**.
State	User state: • **Init**—The user is being initiated. • **Offline**—The user is going offline. • **Auth**—The user is being authenticated. • **AuthFail**—The user failed authentication. • **AuthPass**—The user passed authentication. • **AssignedIP**—The user has an IP address. • **Online**—The user is online. • **Backup**—Backup information about the user on the primary BRAS.
Service node	Slot number and CPU number of the card that connects the user.
Domain	ISP domain.
Online time (hh:mm:ss)	Online duration for the user.
Login time	Time when the user passed authentication and logged in, in the format of MM-DD hh:mm:ss YYYY.
AAA	AAA authorization information.
IP pool	AAA-authorized DHCP address pool. If no DHCP address pool is authorized, this field displays **N/A**.

Field	Description
Session idle time	Idle time in seconds specified for online users. If the idle time expires, the user is logged out. If no idle time is specified, this field displays **N/A** and the user can remain idle without being logged out.
Session duration	AAA-authorized IPoE session duration in seconds: • **N/A**—No IPoE session duration is authorized. • **Unlimited**—The IPoE session duration is unlimited.
remaining	Remaining AAA-authorized IPoE session duration. If no session duration is authorized, this field displays **N/A**. ◦ For users on Layer 3 Ethernet interfaces and subinterfaces, this field displays the remaining time or **Unlimited**. ◦ For users on Layer 3 aggregate interfaces and subinterfaces, this field displays the remaining time or **Unlimited** only when the slot or interface is specified. If you do not specify the slot or interface, this field displays **N/A**.
Remaining traffic	Remaining AAA-authorized traffic in bytes. If no traffic is authorized, this field displays **N/A**.
Max multicast addresses	Maximum number of AAA-authorized multicast groups that a user can join.
Multicast address list	List of AAA-authorized multicast group addresses. If no multicast group is authorized, this field displays **N/A**.
QoS	QoS information.
User profile	AAA-authorized user profile: • **N/A**—No user profile is authorized. • **inactive**—User profile authorization failed or the user profile does not exist on the BRAS. • **active**—The user profile is authorized successfully. If the authorization result has not been updated, nothing is displayed.
Session group profile	AAA-authorized session group profile: • **N/A**—No session group profile is authorized. • **inactive**—Session group profile authorization failed or the session group profile does not exist on the BRAS. • **active**—The session group profile is authorized successfully. If the authorization result has not been updated, nothing is displayed.
Inbound CAR	Inbound CIR and PIR in bps and CBS in bits: • **N/A**—Inbound CAR is not authorized. • **inactive**—Inbound CAR is not authorized successfully. • **active**—Inbound CAR is authorized successfully.
Outbound CAR	Outbound CIR and PIR in bps and CBS in bits: • **N/A**—Outbound CAR is not authorized. • **inactive**—Outbound CAR is not authorized successfully. • **active**—Outbound CAR is authorized successfully.
Flow statistic	Session flow statistics.
Uplink packets/bytes	Total number and size of uplink packets.
Downlink packets/bytes	Total number and size of downlink packets.
ITA	Intelligent target accounting (ITA) information.
Level-*n* Uplink packets/bytes	Number and size of uplink packets for level *n* accounting ($1 \le n \le 8$).

Field	Description
Downlink packets/bytes	Number and size of downlink packets for level *n* accounting (1 ≤ *n* ≤ 8).

Related commands

ip subscriber enable

display ip subscriber interface-leased statistics

Use **display ip subscriber interface-leased statistics** to display IPoE session statistics for IPv4 interface-leased users.

Syntax

display ip subscriber interface-leased statistics [**interface** *interface-type interface-number*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays IPoE session statistics for IPv4 interface-leased users for all interfaces.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPoE session statistics for IPv4 interface-leased users for all member devices.

Examples

Display IPoE session statistics for IPv4 interface-leased users on the BRAS.

```
<Sysname> display ip subscriber interface-leased statistics
Total                : 100
Init                 : 0
Authenticating       : 20
Authenticate fail    : 0
Authenticate pass    : 20
Assigned IP          : 10
Online               : 50
Backup               : 0
```

Table 2 Command output

Field	Description
Total	Total number of hosts on the interface.
Init	Number of users who initiated sessions.
Authenticating	Number of users being authenticated.

Field	Description
Authenticate fail	Number of users who failed authentication.
Authenticate pass	Number of users who passed authentication.
Assigned IP	Number of users who have IP addresses.
Online	Number of online users.
Backup	Number of users whose information was backed up.

display ip subscriber offline statistics

Use **display ip subscriber offline statistics** to display offline statistics for IPv4 users.

Syntax

display ip subscriber offline statistics [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays offline statistics for IPv4 users for all interfaces.

Examples

Display offline statistics for IPv4 users on GigabitEthernet 1/0/1.

```
<Sysname> display ip subscriber offline statistics interface gigabitethernet 1/0/1
Total               : 100
User request        : 0
DHCP lease expire   : 0
AAA lease expire    : 0
Command cut         : 80
AAA terminate       : 0
Authenticate fail   : 0
Authorization fail  : 0
Idle timeout        : 10
Detect fail         : 10
Not enough resource : 0
Interface down      : 0
Interface shutdown  : 0
VSRP event          : 0
DHCP notify         : 0
```

```
Other               : 0
```

Table 3 Command output

Field	Description
Total	Total number of offline users.
User request	Number of users requesting to go offline.
DHCP lease expire	Number of users with expired DHCP leases.
AAA lease expire	Number of users with expired AAA leases.
Command cut	Number of users logged out by commands.
AAA terminate	Number of users logged out by AAA.
Authenticate fail	Number of users who failed authentication.
Authorization fail	Number of users who failed authorization.
Idle timeout	Number of users with an expired idle timeout timer.
Detect fail	Number of users who failed online detection.
Not enough resource	Number of users with insufficient hardware resources.
Interface down	Number of users on an interface that went down.
Interface shutdown	Number of users on an interface that was shut down.
VSRP event	Number of users disconnected by the VSRP event.
DHCP notify	Number of users disconnected by DHCP.
Other	Number of users disconnected from the network because of unknown causes.

Related commands

reset ip subscriber offline statistics

display ip subscriber session

Use **display ip subscriber session** to display session information for IPv4 individual users.

Syntax

display ip subscriber session [**interface** *interface-type interface-number*] [**domain** *domain-name* | **ip** *ip-address* [**vpn-instance** *vpn-instance-name*] | **mac** *mac-address* | **static** | **username** *name*] [**slot** *slot-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays session information for IPv4 individual users for all interfaces.

domain *domain-name*: Specifies an ISP domain name, a case-insensitive string of 1 to 255 characters. The name cannot contain the slash (/), back slash (\), vertical bar (|), quotation mark ("), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or at sign (@).

ip *ip-address*: Specifies the source IP address of the IPv4 individual user.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays session information for IPv4 individual users on the public network.

mac *mac-address*: Specifies the MAC address of an IPv4 individual user, in the format of H-H-H.

static: Specifies static IPoE sessions. If this parameter is not specified, this command displays information about static and dynamic sessions for IPv4 individual users.

username *name*: Specifies a username for authentication, a case-sensitive string of 1 to 255 characters.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays session information for IPv4 individual users for all member devices.

verbose: Displays detailed session information for IPv4 individual users. If this parameter is not specified, this command displays general session information.

Examples

Display general session information for the IPv4 individual user with an IP address of **1.1.1.1** in **vpn1**.

```
<Sysname> display ip subscriber session ip 1.1.1.1 vpn-instance vpn1
  Type: D-DHCP   S-Static     U-Unclassified-IP
Interface            IP address                MAC address    Type  State
--------------------------------------------------------------------------------
GE1/0/1              1.1.1.1                   000d-88f8-0eab D     Online
```

Displays detailed session information for IPv4 individual users.

```
<Sysname> display ip subscriber session verbose
 Basic:
  Description               : -
  Username                  : abc
  Domain                    : radius
  VPN instance              : N/A
  IP address                : 1.1.1.1
  MAC address               : 000d-88f8-0eab
  Service-VLAN/Customer-VLAN : -/-
  Access interface          : GE1/0/1
  User ID                   : 0x380800b5
  VPI/VCI(for ATM)          : -/-
  DHCP lease                : N/A
  DHCP remain lease         : N/A
  Login time                : May  9 08:56:29 2014
  Online time (hh:mm:ss)    : 00:16:37
  Service node              : Slot 1 CPU 0
```

```
  Type                       : Static
  State                      : Online

AAA:
  IP pool                    : N/A
  Session idle time          : N/A
  Session duration           : N/A, remaining: N/A
  Remaining traffic          : N/A
  Max multicast addresses    : 4
  Multicast address list     : N/A

QoS:
  User profile               : abc (active)
  Session group profile      : N/A
  Inbound CAR                : CIR 1000bps PIR 2000bps CBS 500bit (active)
  Outbound CAR               : CIR 3000bps PIR 4000bps CBS 500bit (active)

Flow statistic:
  Uplink   packets/bytes     : 594341/76075648
  Downlink packets/bytes     : 0/0

ITA:
  Level-1 Uplink   packets/bytes: 66038/8452864
          Downlink packets/bytes: 0/0
  Level-2 Uplink   packets/bytes: 66038/8452864
          Downlink packets/bytes: 0/0
```

Table 4 Command output

Field	Description
Basic	Basic session information.
Description	Description of the IPoE session. If the IPoE session does not have a description, this field displays a hyphen (-).
Username	Username for authentication.
Domain	ISP domain of the user.
VPN instance	MPLS L3VPN instance of the user. If the user is not in a VPN, this field displays **N/A**.
IP address	IP address of the user.
MAC address	MAC address of the user.
Service-VLAN/Customer-VLAN	Public and private VLANs of the user. If the user is not a VLAN user, this field displays **-**.
Access interface	Interface that connects the user.
User ID	User ID assigned after the user came online. If no user ID is assigned, this field displays **0xffffffff**.
VPI/VCI(for ATM)	PVC information about the ATM.
DHCP lease	DHCP-authorized IP lease in seconds: • **N/A**—No IP lease is authorized.

Field	Description
	• **Unlimited**—The IP lease is unlimited.
DHCP remain lease	Remaining DHCP-authorized IP lease. This field is valid only on the card that connects the user. On other cards, this field displays **N/A**.
Login time	Time when the user passed authentication and logged in, in the format of MM-DD hh:mm:ss YYYY.
Online time (hh:mm:ss)	Online duration for the user.
Service node	Slot number and CPU number of the card that connects the user.
Type	IPoE session types: • **DHCP**—Dynamic IPoE sessions for DHCP users. • **Unclassified-IP**—Dynamic IPoE sessions for unclassified-IP users. • **Static**—Static sessions.
State	User state: • **Init**—The user is being initiated. • **Offline**—The user is going offline. • **Auth**—The user is being authenticated. • **AuthFail**—The user failed authentication. • **AuthPass**—The user passed authentication. • **AssignedIP**—The user has an IP address. • **Online**—The user is online. • **Backup**—Backup information about the user on the primary BRAS.
AAA	AAA authorization information.
IP pool	AAA-authorized DHCP address pool. If no DHCP address pool is authorized, this field displays **N/A**.
Session idle time	Idle time in seconds specified for online users. If the idle time expires, the user is logged out. If no idle time is specified, this field displays **N/A** and the user can remain idle without being logged out.
Session duration	AAA-authorized IPoE session duration in seconds: • **N/A**—No IPoE session duration is authorized. • **Unlimited**—The IPoE session duration is unlimited.
remaining	Remaining AAA-authorized IPoE session duration. If no session duration is authorized, this field displays **N/A**. ◦ For users on Layer 3 Ethernet interfaces and subinterfaces, this field displays the remaining time or **Unlimited**. ◦ For users on Layer 3 aggregate interfaces and subinterfaces, this field displays the remaining time or **Unlimited** only when the slot or interface is specified. If you do not specify the slot or interface, this field displays **N/A**.
Remaining traffic	Remaining AAA-authorized traffic in bytes. If no traffic is authorized, this field displays **N/A**.
Max multicast addresses	Maximum number of AAA-authorized multicast groups that a user can join.
Multicast address list	List of AAA-authorized multicast group addresses. If no multicast group is authorized, this field displays **N/A**.
QoS	QoS information.
User profile	AAA-authorized user profile:

Field	Description
	• **N/A**—No user profile is authorized. • **inactive**—User profile authorization failed or the user profile does not exist on the BRAS. • **active**—The user profile is authorized successfully. If the authorization result has not been updated, nothing is displayed.
Session group profile	AAA-authorized session group profile: • **N/A**—No session group profile is authorized. • **inactive**—Session group profile authorization failed or the session group profile does not exist on the BRAS. • **active**—The session group profile is authorized successfully. If the authorization result has not been updated, nothing is displayed.
Inbound CAR	Inbound CIR and PIR in bps and CBS in bits: • **N/A**—Inbound CAR is not authorized. • **inactive**—Inbound CAR is not authorized successfully. • **active**—Inbound CAR is authorized successfully.
Outbound CAR	Outbound CIR and PIR in bps and CBS in bits: • **N/A**—Outbound CAR is not authorized. • **inactive**—Outbound CAR is not authorized successfully. • **active**—Outbound CAR is authorized successfully.
Flow statistic	Session flow statistics.
Uplink packets/bytes	Total number and size of uplink packets.
Downlink packets/bytes	Total number and size of downlink packets.
ITA	Intelligent target accounting (ITA) information.
Level-*n* Uplink packets/bytes	Number and size of uplink packets for level *n* accounting (1 ≤ *n* ≤ 8).
Downlink packets/bytes	Number and size of downlink packets for level *n* accounting (1 ≤ *n* ≤ 8).

display ip subscriber session statistics

Use **display ip subscriber session statistics** to display IPoE session statistics for IPv4 individual users.

Syntax

display ip subscriber session statistics [**session-type** { **dhcp** | **static** | **unclassified-ip** }] [**interface** *interface-type interface-number*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

session-type: Specifies a user type. If you do not specify a user type, this command displays IPoE session statistics for all types of IPv4 individual users.

dhcp: Specifies DHCP users.

static: Specifies static users.

unclassified-ip: Specifies unclassified-IP users.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays IPoE session statistics for IPv4 individual users for all interfaces.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPoE session statistics for IPv4 individual users for all member devices.

Examples

Display IPoE session statistics for IPv4 individual users on GigabitEthernet 1/0/1.

```
<Sysname> display ip subscriber session statistics session-type dhcp interface
gigabitethernet 1/0/1
Total                : 100
Init                 : 0
Authenticating       : 20
Authenticate fail    : 0
Authenticate pass    : 20
Assigned IP          : 10
Online               : 50
Backup               : 0
```

Table 5 Command output

Field	Description
Total	Total number of users on the interface.
Init	Number of users who initiated sessions.
Authenticating	Number of users being authenticated.
Authenticate fail	Number of users who failed authentication.
Authenticate pass	Number of users who passed authentication.
Assigned IP	Number of users who have IP addresses.
Online	Number of online users.
Backup	Number of users whose information was backed up.

Related commands

reset ip subscriber session

display ip subscriber subnet-leased

Use **display ip subscriber subnet-leased** to display information about IPv4 subnet-leased users.

Syntax

display ip subscriber subnet-leased [**interface** *interface-type interface-number*] [**slot** *slot-number*]

display ip subscriber subnet-leased [**interface** *interface-type interface-number*] [**chassis** *chassis-number* **slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays information about IPv4 subnet-leased users for all interfaces.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about IPv4 subnet-leased users for all member devices.

Examples

Display information about the IPv4 subnet-leased user on GigabitEthernet 1/0/1.

```
<Sysname> display ip subscriber subnet-leased interface gigabitethernet 1/0/1
Basic:
  Access interface           : GE1/0/1
  VPN instance               : N/A
  Username                   : a
  Network                    : 11.11.11.0/24
  User ID                    : 0x30000001
  State                      : Online
  Service node               : Slot 1 CPU 0
  Domain                     : radius
  Login time                 : May 14 20:08:35 2014
  Online time (hh:mm:ss)     : 00:16:37

AAA:
  IP pool                    : N/A
  Session idle time          : N/A
  Session duration           : N/A, remaining: N/A
  Remaining traffic          : N/A
  Max multicast addresses    : 4
  Multicast address list     : N/A

QoS:
  User profile               : cc (active)
  Session group profile      : N/A
```

```
  Inbound CAR               : CIR 1000bps PIR 2000bps CBS 500bit (active)
  Outbound CAR              : CIR 3000bps PIR 4000bps CBS 500bit (active)

Flow statistic:
  Uplink   packets/bytes    : 0/0
  Downlink packets/bytes    : 0/0

ITA:
  Level-1 Uplink   packets/bytes: 0/0
          Downlink packets/bytes: 0/0
  Level-2 Uplink   packets/bytes: 0/0
          Downlink packets/bytes: 0/0
```

Table 6 Command output

Field	Description
Basic	Basic session information.
Access interface	Interface that connects the user.
VPN instance	MPLS L3VPN instance of the user. If the user is not in a VPN, this field displays **N/A**.
User name	Username for authentication.
Network	Subnet of the user.
User ID	User ID assigned after the user came online. If no user ID is assigned, this field displays **0xffffffff**.
State	User state: • **Init**—The user is being initiated. • **Offline**—The user is going offline. • **Auth**—The user is being authenticated. • **AuthFail**—The user failed authentication. • **AuthPass**—The user passed authentication. • **AssignedIP**—The user has an IP address. • **Online**—The user is online. • **Backup**—Backup information about the user on the primary BRAS.
Service node	Slot number and CPU number of the card that connects the user.
Domain	ISP domain of the user.
Login time	Time when the user passed authentication and logged in, in the format of MM-DD hh:mm:ss YYYY.
Online time (hh:mm:ss)	Online duration for the user.
AAA	AAA authorization information.
IP pool	AAA-authorized DHCP address pool. If no DHCP address pool is authorized, this field displays **N/A**.
Session idle time	Idle time in seconds specified for online users. If the idle time expires, the user is logged out. If no idle time is specified, this field displays **N/A** and the user can remain idle without being logged out.
Session duration	AAA-authorized IPoE session duration in seconds: • **N/A**—No IPoE session duration is authorized. • **Unlimited**—The IPoE session duration is unlimited.

Field	Description
remaining	Remaining AAA-authorized IPoE session duration. If no session duration is authorized, this field displays **N/A**. ○ For users on Layer 3 Ethernet interfaces and subinterfaces, this field displays the remaining time or **Unlimited**. ○ For users on Layer 3 aggregate interfaces and subinterfaces, this field displays the remaining time or **Unlimited** only when the slot or interface is specified. If you do not specify the slot or interface, this field displays **N/A**.
Remaining traffic	Remaining AAA-authorized traffic in bytes. If no traffic is authorized, this field displays **N/A**.
Max multicast addresses	Maximum number of AAA-authorized multicast groups that a user can join.
Multicast address list	List of AAA-authorized multicast group addresses. If no multicast group is authorized, this field displays **N/A**.
QoS	QoS information.
User profile	AAA-authorized user profile: • **N/A**—No user profile is authorized. • **inactive**—User profile authorization failed or the user profile does not exist on the BRAS. • **active**—The user profile is authorized successfully. If the authorization result has not been updated, nothing is displayed.
Session group profile	AAA-authorized session group profile: • **N/A**—No session group profile is authorized. • **inactive**—Session group profile authorization failed or the session group profile does not exist on the BRAS. • **active**—The session group profile is authorized successfully. If the authorization result has not been updated, nothing is displayed.
Inbound CAR	Inbound CIR and PIR in bps and CBS in bits: • **N/A**—Inbound CAR is not authorized. • **inactive**—Inbound CAR is not authorized successfully. • **active**—Inbound CAR is authorized successfully.
Outbound CAR	Outbound CIR and PIR in bps and CBS in bits: • **N/A**—Outbound CAR is not authorized. • **inactive**—Outbound CAR is not authorized successfully. • **active**—Outbound CAR is authorized successfully.
Flow statistic	Session flow statistics.
Uplink packets/bytes	Total number and size of uplink packets.
Downlink packets/bytes	Total number and size of downlink packets.
ITA	Intelligent target accounting (ITA) information.
Level-*n* Uplink packets/bytes	Number and size of uplink packets for level *n* accounting ($1 \le n \le 8$).
Downlink packets/bytes	Number and size of downlink packets for level *n* accounting ($1 \le n \le 8$).

Related commands

`ip subscriber enable`

display ip subscriber subnet-leased statistics

Use **display ip subscriber subnet-leased statistics** to display IPoE session statistics for IPv4 subnet-leased users.

Syntax

display ip subscriber subnet-leased statistics [**interface** *interface-type interface-number*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays IPoE session statistics for IPv4 subnet-leased users for all interfaces.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPoE session statistics for IPv4 subnet-leased users for all member devices.

Examples

Display IPoE session statistics for IPv4 subnet-leased users on GigabitEthernet 1/0/1.

```
<Sysname> display ip subscriber subnet-leased statistics interface gigabitethernet 1/0/1
Total                : 100
Init                 : 0
Authenticating       : 20
Authenticate fail    : 0
Authenticate pass    : 20
Assigned IP          : 10
Online               : 50
Backup               : 0
```

Table 7 Command output

Field	Description
Total	Total number of users on the interface.
Init	Number of users who initiated sessions.
Authenticating	Number of users being authenticated.
Authenticate fail	Number of users who failed authentication.
Authenticate pass	Number of users who passed authentication.
Assigned IP	Number of users who have IP addresses.
Online	Number of online users.
Backup	Number of users whose information was backed up.

ip subscriber 8021p

Use **ip subscriber 8021p** to bind an ISP domain to an 802.1p list for IPv4 unclassified-IP users, static individual users, and leased users.

Use **undo ip subscriber 8021p** to remove the binding between an ISP domain and an 802.1p list.

Syntax

ip subscriber 8021p *8021p-list* **domain** *domain-name*

undo ip subscriber 8021p *8021p-list*

Default

No ISP domain is bound to an 802.1p list for IPv4 unclassified-IP users, static individual users, and leased users.

Views

Layer 3 aggregate subinterface view

Layer 3 Ethernet subinterface view

Predefined user roles

network-admin

context-admin

Parameters

8021p-list: Specifies a space-separated list of up to eight 802.1p value items. Each item specifies a 802.1p value or a range of 802.1p values in the form of start-802.1p-value to end-802.1p-value. The 802.1p value is in the range of 0 to 7.

domain *domain-name*: Specifies an ISP domain name, a case-insensitive string of 1 to 255 characters. The name cannot contain the slash (/), back slash (\), vertical bar (|), quotation mark ("), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or at sign (@).

Usage guidelines

This command configures an ISP domain for IPv4 unclassified-IP users, static individual users, and leased users who send IP packets with the specified 802.1p values.

Examples

Configure ISP domain **1pdm** for IPv4 unclassified-IP users, static individual users, and leased users who send IP packets with the specified 802.1p values on GigabitEthernet 1/0/1.100. The specified 802.1p values are in the range of 2 to 5.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1.100
[Sysname-GigabitEthernet1/0/1.100] ip subscriber service-identify 8021p second-vlan
[Sysname-GigabitEthernet1/0/1.100] ip subscriber 8021p 2 to 5 domain 1pdm
```

Related commands

ip subscriber service-identify

ip subscriber access-user log enable

Use **ip subscriber access-user log enable** to enable IPv4 IPoE user logging.

Use **undo ip subscriber access-user log enable** to disable IPv4 IPoE user logging.

Syntax

ip subscriber access-user log enable [**successful-login** | **failed-login** | **logout** [**normal**] [**abnormal**]] *

undo ip subscriber access-user log enable [**successful-login** | **failed-login** | **logout** [**normal**] [**abnormal**]] *

Default

IPv4 IPoE user logging is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

successful-login: Specifies login success logs.

failed-login: Specifies login failure logs.

logout: Specifies logout logs.

normal: Specifies normal logout logs.

abnormal: Specifies abnormal logout logs.

Usage guidelines

IMPORTANT:

Typically, disable this feature to prevent excessive IPv4 IPoE log output.

The IPv4 IPoE user logging feature enables the device to generate IPv4 IPoE logs and send them to the information center. Logs are generated after a user comes online successfully, fails to come online, normally goes offline, or abnormally goes offline. A log entry contains information such as the username, IP address, interface name, inner VLAN, outer VLAN, MAC address, and failure causes. For information about the log destination and output rule configuration in the information center, see *Network Management and Monitoring Configuration Guide*.

When you execute this command without specifying any keyword, this command enables or disables logging for login successes, login failures, normal logouts, and abnormal logouts.

Examples

Enable IPv4 IPoE user logging.

```
<Sysname> system-view
[Sysname] ip subscriber access-user log enable
```

ip subscriber dhcp domain

Use **ip subscriber dhcp domain** to configure an ISP domain for DHCPv4 users.

Use **undo ip subscriber dhcp domain** to restore the default.

Syntax

ip subscriber dhcp domain *domain-name*

undo ip subscriber dhcp domain

Default

DHCPv4 users use the default system domain.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Parameters

domain *domain-name*: Specifies an ISP domain name, a case-insensitive string of 1 to 255 characters. The name cannot contain the slash (/), back slash (\), vertical bar (|), quotation mark ("), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or at sign (@).

Usage guidelines

This command configures an ISP domain for DHCPv4 users. The specified ISP domain must exist on the BRAS.

If multiple ISP domains are available for an DHCPv4 user, the ISP domains are used in the following order:

1. Domain specified in Option 60 if the BRAS trusts Option 60 and Option 60 does not include null terminators and non-printable characters.
2. Domain specified by this command.
3. Default system domain.

Examples

Configure ISP domain **ipoe** for DHCPv4 users on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip subscriber dhcp domain ipoe
```

Related commands

ip subscriber initiator dhcp enable

ip subscriber trust

ip subscriber dhcp max-session

Use **ip subscriber dhcp max-session** to configure the maximum number of IPoE sessions for DHCPv4 users on an interface.

Use **undo ip subscriber dhcp max-session** to restore the default.

Syntax

ip subscriber dhcp max-session *max-number*

undo ip subscriber dhcp max-session

Default

The maximum number of IPoE sessions for DHCPv4 users on an interface is not configured.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Parameters

max-number: Specifies the maximum number of IPoE sessions for DHCPv4 users. The value range for this argument is 1 to 64000

Usage guidelines

If IPoE sessions for DHCPv4 users reach the maximum, no more IPoE session can be established for DHCPv4 users.

Examples

Set the maximum number of IPoE sessions to **100** for DHCPv4 users on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip subscriber dhcp max-session 100
```

Related commands

display ip subscriber session

ip subscriber initiator dhcp enable

reset ip subscriber session

ip subscriber dhcp password option60

Use **ip subscriber dhcp password option60** to specify a string from Option 60 as the password for DHCPv4 users.

Use **undo ip subscriber dhcp password option60** to restore the default.

Syntax

ip subscriber dhcp password option60 [**offset** *offset*] [**length** *length*]

undo ip subscriber dhcp password option60

Default

The BRAS does not use the password specified in Option 60 for DHCPv4 users.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Parameters

offset *offset*: Specifies an offset for the password starting byte, in the range of 1 to 63. If you do not specify this option, the first byte of the option is the starting byte.

length *length*: Specifies the length of the password string, in the range of 1 to 63. If you do not specify this option, all bytes following the starting byte are used as the password.

Usage guidelines

Passwords configured by this command are used for authentication, and must be the same as those configured on the AAA server.

A DHCPv4 user can obtain a password in various ways. If multiple passwords are available for an DHCPv4 user, the passwords are used in the following order:

1. Password configured by this command if the BRAS trusts Option 60 and Option 60 does not contain null terminators or non-printable characters.
2. Password configured by using the **ip subscriber password** command.
3. Default password: **vlan**.

Examples

Specify the string with an offset of 10 and a length of 20 bytes from Option 60 as the password for DHCPv4 users.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip subscriber dhcp password option60 offset 10 length 20
```

Related commands

ip subscriber initiator dhcp enable

ip subscriber password

ip subscriber trust

ip subscriber dhcp username

ip subscriber dhcp username

Use **ip subscriber dhcp username** to configure an authentication user naming convention for DHCPv4 users.

Use **undo ip subscriber dhcp username** to restore the default.

Syntax

ip subscriber dhcp username include { **circuit-id** [**separator** *separator*] | **client-id** [**separator** *separator*] | **nas-port-id** [**separator** *separator*] | **port** [**separator** *separator*] | **remote-id** [**separator** *separator*] | **second-vlan** [**separator** *separator*] | **slot** [**separator** *separator*] | **source-mac** [**address-separator** *address-separator*] [**separator** *separator*] | **subslot** [**separator** *separator*] | **sysname** [**separator** *separator*] | **vendor-class** [**separator** *separator*] | **vendor-specific** [**separator** *separator*] | **vlan** [**separator** *separator*] } *

undo ip subscriber dhcp username

Default

A DHCPv4 user uses its source MAC address as the authentication username.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Parameters

circuit-id: Includes the Option 82 sub-option 1 information in a username.

client-id: Includes the Option 61 information in a username.

nas-port-id: Includes the NAS-Port-ID attribute carried in the authentication request packet in a username.

port: Includes the number of the port that receives the user packets in a username.

remote-id: Includes the Option 82 sub-option 2 information in a username.

second-vlan: Includes the inner VLAN ID in a username.

slot: Includes the number of the slot that receives the user packets in a username.

source-mac: Includes the source MAC address in a username.

address-separator *address-separator*: Specifies any printable character as the separator for the MAC address. For example, if you specify a hyphen (-) as the separator, the username is the hyphen-separated MAC address (xxxx-xxxx-xxxx). If you do not specify a separator, the username is the non-separated MAC address (xxxxxxxxxxxx). Do not use the at sign (@) as the separator. The AAA server cannot parse a username containing the at sign (@).

subslot: Includes the number of the subslot that receives the user packets in a username.

sysname: Includes the name of the device that receives the user packets in a username.

vendor-class: Includes the Option 60 information in a username.

vendor-specific: Includes the Option 82 sub-option 9 information in a username.

vlan: Includes the outer VLAN ID in a username.

separator *separator*: Specifies a character for separating an option and the option that follows. Do not use the at sign (@) as the separator. The AAA server cannot parse a username containing the at sign (@).

Usage guidelines

Usernames obtained based on the naming convention are used for authentication, authorization, and accounting, and must be the same as those configured on the AAA server.

You can specify one or more keywords in a naming convention. If you use a combination of keywords, a username obtained based on the naming convention includes the specified options in the configuration order.

Options used as the username information cannot include null terminators or non-printable characters.

Examples

Configure information carried in the Client Identifier Option as the authentication usernames for DHCPv4 users on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip subscriber dhcp username include client-id
```

Configure an authentication user naming convention for DHCPv4 users on GigabitEthernet 1/0/1. Each username contains the device name, slot number, subslot number, port number, and outer VLAN, separated by the pound sign (#).

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip subscriber dhcp username include sysname separator #
slot separator # subslot separator # port separator # vlan
```

Related commands

ip subscriber initiator dhcp enable

ip subscriber password

ip subscriber dscp

Use **ip subscriber dscp** to bind an ISP domain to a DSCP list for IPv4 unclassified-IP users, static individual users, and leased users.

Use **undo ip subscriber dscp** to remove the binding between an ISP domain and a DSCP list.

Syntax

ip subscriber dscp *dscp-value-list* **domain** *domain-name*

undo ip subscriber dscp *dscp-value-list*

Default

No ISP domain is bound to a DSCP list for IPv4 unclassified-IP users, static individual users, and leased users.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Parameters

dscp-value-list: Specifies a space-separated list of up to eight DSCP value items. Each item specifies a DSCP value or a range of DSCP values in the form of start-DSCP-value to end-DSCP-value. The DSCP value is in the range of 0 to 63.

domain *domain-name*: Specifies an ISP domain name, a case-insensitive string of 1 to 255 characters. The name cannot contain the slash (/), back slash (\), vertical bar (|), quotation mark ("), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or at sign (@).

Usage guidelines

This command configures an ISP domain for IPv4 unclassified-IP users, static individual users, and leased users who send IP packets with the specified DSCP values.

Examples

Configure ISP domain **dscpdm** for IPv4 unclassified-IP users, static individual users, and leased users who send IP packets with the specified DSCP values on GigabitEthernet 1/0/1. The specified DSCP values are in the range of 1 to 4.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip subscriber service-identify dscp
[Sysname-GigabitEthernet1/0/1] ip subscriber dscp 1 to 4 domain dscpdm
```

Related commands

ip subscriber service-identify

ip subscriber enable

Use **ip subscriber enable** to enable IPoE and configure an IPoE access mode for IPv4 users.

Use **undo ip subscriber enable** to disable IPoE for IPv4 users.

Syntax

ip subscriber { **l2-connected** | **routed** } **enable**

undo ip subscriber { **l2-connected** | **routed** } **enable**

Default

IPoE is disabled for IPv4 users.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Parameters

l2-connected: Specifies the Layer 2 access mode.

routed: Specifies the Layer 3 access mode.

Usage guidelines

All IPoE configurations take effect on an interface only when IPoE is enabled on the interface.

To change the IPoE access mode on an interface, you must disable IPoE, and then enable IPoE with a new IPoE access mode.

To ensure successful traffic statistics in aggregate interface view, use the **service** command to specify a service card for traffic statistics. For more information about the **service** command, see *Layer 2—LAN Switching Command Reference*.

Examples

Enable IPoE and configure the Layer 2 access mode for IPv4 users on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip subscriber l2-connected enable
```

Related commands

service (*Layer 2—LAN Switching Command Reference*)

ip subscriber initiator dhcp enable

Use **ip subscriber initiator dhcp enable** to enable the DHCPv4 user.

Use **undo ip subscriber initiator dhcp enable** to disable the DHCPv4 user.

Syntax

ip subscriber initiator dhcp enable

undo ip subscriber initiator dhcp enable

Default

The DHCPv4 user is disabled.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Usage guidelines

If you enable the DHCP user, the first DHCP Discover or the DHCP Request packet initiates the IPoE session. If you disable the DHCP user, DHCP packets cannot initiate IPoE sessions, but existing IPoE sessions for DHCP are not affected.

You can enable the DHCP user and unclassified-IP user on the same interface.

Examples

Enable the DHCPv4 user on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip subscriber initiator dhcp enable
```

Related commands

display ip subscriber session

ip subscriber enable

ip subscriber initiator unclassified-ip enable

reset ip subscriber session

ip subscriber initiator unclassified-ip enable

Use **ip subscriber initiator unclassified-ip enable** to enable the IPv4 unclassified-IP user.

Use **undo ip subscriber initiator unclassified-ip enable** to disable the IPv4 unclassified-IP user.

Syntax

ip subscriber initiator unclassified-ip enable

undo ip subscriber initiator unclassified-ip enable

Default

The IPv4 unclassified-IP user is disabled.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Usage guidelines

If you enable the unclassified-IP user, the first IPv4 packet from a host initiates an IPoE session. If you disable the unclassified-IP user, IPv4 packets cannot initiate IPoE sessions, but existing IPoE sessions for unclassified-IP are not affected.

You can enable the DHCP user and unclassified-IP user on the same interface.

Examples

Enable the IPv4 unclassified-IP user on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip subscriber initiator unclassified-ip enable
```

Related commands

display ip subscriber session

ip subscriber enable

ip subscriber initiator dhcp enable

reset ip subscriber session

ip subscriber interface-leased

Use **ip subscriber interface-leased** to configure IPv4 interface-leased users.

Use **undo ip subscriber interface-leased** to restore the default.

Syntax

ip subscriber interface-leased username *name* **password** { **ciphertext** | **plaintext** } *string* [**domain** *domain-name*]

undo ip subscriber interface-leased

Default

No IPv4 interface-leased user exists.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Parameters

username *name*: Specifies a username for authentication, a case-sensitive string of 1 to 255 characters.

password ciphertext *string*: Specifies a ciphertext password, a case-sensitive string of 1 to 117 characters.

password plaintext *string*: Specifies a plaintext password, a case-sensitive string of 1 to 63 characters. For security purposes, the password specified in plaintext form will be stored in encrypted form.

domain *domain-name*: Specifies an ISP domain name, a case-insensitive string of 1 to 255 characters. The name cannot contain the slash (/), back slash (\), vertical bar (|), quotation mark ("), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or at sign (@). If you do not specify an ISP domain, the default system domain is used. For more information about the default system domain, see *Security Configuration Guide*.

Usage guidelines

An IPv4 interface-leased user is a group of IPv4 hosts that rent the same interface and share the same IPoE session. The BRAS authenticates, authorizes, and bills all hosts of the same interface-leased user.

You can configure only one IPv4 interface-leased user on one interface. To change the parameters of an existing IPv4 interface-leased user, use the undo form of the command to delete the user, and then reconfigure it with new parameter settings.

You cannot configure an interface-leased user on an interface configured with individual users or subnet-leased users.

Examples

Configure an IPv4 interface-leased user with a username of **intuser** and a plaintext password of **pw123** on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip subscriber interface-leased username intuser password plaintext pw123
```

Related commands

display ip subscriber interface-leased

ip subscriber nas-port-id format

Use **ip subscriber nas-port-id format** to configure NAS-Port-ID formats for IPv4 users.

Use **undo ip subscriber nas-port-id format** to restore the default.

Syntax

ip subscriber nas-port-id format cn-telecom { **version1.0** | **version2.0** }

undo ip subscriber nas-port-id format

Default

NAS-Port-ID for IPv4 users is encapsulated in the format of version 1.0.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Parameters

version 1.0: Specifies the China Telecom format.

- The version 1.0 encapsulation format varies by interface type.

  Table 8 Version 1.0 encapsulation formats

Interface type	Encapsulation format
Layer 3 Ethernet interface and Layer 3 aggregate interface	slot=*slot_num*;subslot=*subslot_num*;port=*port_num*;vlanid=0
Layer 3 Ethernet subinterface and Layer 3 aggregate subinterface (single VLAN tag)	slot=*slot_num*;subslot=*subslot_num*;port=*port_num*;vlanid=*vlan_id*
Layer 3 Ethernet subinterface and Layer 3 aggregate subinterface (Dual VLAN tags)	*slot*=*slot_num*;subslot=*subslot_num*;port=*port_num*;vlanid=*inner-vlan*;vlanid2=*outer-vlan*
ATM-based virtual Layer 3 Ethernet interface (IPoEoA)	slot=*slot_num*;subslot=*subslot_num*;port=*port_num*;vpi=*vpi*;vci=*vci*

- Version 1.0 format parameters

  Table 9 Version 1.0 format parameter description

Parameter	Description
slot_num	Specifies the slot number of the access interface on the BRAS.
subslot_num	Specifies the subslot number of the access interface on the BRAS.
port_num	Specifies the port number of the access interface on the BRAS.
vlan_id	Specifies the ID of the user's VLAN.
inner-vlan	Specifies the ID of the inner VLAN.
outer-vlan	Specifies the ID of the outer VLAN.
vpi	Specifies the VPI of the access interface on the BRAS.
vci	Specifies the VCI of the access interface on the BRAS.

`version 2.0`: Specifies the format described in *`YDT 2275-2011`* Subscriber Access Loop (Port) Identification in Broadband Access Networks.

- Version 2.0 encapsulation format:

  {eth | trunk | atm} NAS_slot/NAS_subslot/NAS_port:svlan.cvlan AccessNodeIdentifier/ANI_rack/ANI_frame/ANI_slot/ANI_subslot/ANI_port

- Version 2.0 format parameters:

  Table 10 Version 2.0 format parameter description

Parameter	Description
{eth|trunk|atm}	Specifies the type of the access interface on the BRAS as Ethernet, trunk, or ATM.
NAS_slot	Specifies the slot number of the access interface on the BRAS.
NAS_subslot	Specifies the subslot number of the access interface on the BRAS.
NAS_port	Specifies the port number of the access interface on the BRAS.
svlan	Specifies the ID of the user's SVLAN.
cvlan	Specifies the ID of the user's CVLAN.
AccessNodeIdentifier	Specifies the identifier of the access node.
ANI_rack	Specifies the rack number of the access node.

Parameter	Description
ANI_frame	Specifies the frame number of the access node.
ANI_slot	Specifies the slot number of the access node.
ANI_subslot	Specifies the subslot number of the access node.
ANI_port	Specifies the port number of the access node.

Examples

Configure version 2.0 as the format for encapsulating NAS-Port-ID on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip subscriber nas-port-id format cn-telecom version2.0
```

Related commands

ip subscriber initiator dhcp enable

ip subscriber trust

ip subscriber nas-port-id nasinfo-insert

ip subscriber nas-port-id nasinfo-insert

Use **ip subscriber nas-port-id nasinfo-insert** to include NAS information and information obtained from DHCPv4 Option 82 in NAS-Port-ID.

Use **undo ip subscriber nas-port-id nasinfo-insert** to restore the default.

Syntax

ip subscriber nas-port-id nasinfo-insert

undo ip subscriber nas-port-id nasinfo-insert

Default

The BRAS uses information obtained from DHCPv4 Option 82 as NAS-Port-ID.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Usage guidelines

Configure version 2.0 format and the trusted DHCP option before you use this command.

- If DHCP packets contain Option 82 Suboption Circuit-ID, this command includes NAS information and the obtained option information in NAS-Port-ID. Suboption Circuit-ID is not affected.
- If DHCP packets do not contain Option 82 Suboption Circuit-ID, this command includes NAS information in NAS-Port-ID and sets non-NAS parts to zeros in the following format:

  NAS_slot/NAS_subslot/NAS_port:svlan.cvlan 0/0/0/0/0/0

Examples

Include NAS information and the obtained Option 82 information in NAS-Port-ID on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip subscriber nas-port-id nasinfo-insert
```

Related commands

ip subscriber initiator dhcp enable

ip subscriber trust

ip subscriber nas-port-id format

ip subscriber nas-port-type

Use **ip subscriber nas-port-type** to configure NAS-Port-Type for an IPv4 interface.

Use **undo ip subscriber nas-port-type** to restore the default.

Syntax

ip subscriber nas-port-type { **802.11** | **adsl-cap** | **adsl-dmt** | **async** | **cable** | **ethernet** | **g.3-fax** | **hdlc** | **idsl** | **isdn-async-v110** | **isdn-async-v120** | **isdn-sync** | **piafs** | **sdsl** | **sync** | **virtual** | **wireless-other** | **x.25** | **x.75** | **xdsl** }

undo ip subscriber nas-port-type

Default

NAS-Port-Type for an IPv4 interface is Ethernet.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Parameters

802.11: Specifies the port type complying with Wireless-IEEE 802.11. The type ID is 19.

adsl-cap: Specifies the ADSL-CAP port type, including Asymmetric DSL and Carrierless Amplitude Phase Modulation. The type ID is 12.

adsl-dmt: Specifies the ADSL-DMT port type, including Asymmetric DSL and Discrete Multi-Tone. The type ID is 13.

async: Specifies the Async port type with a type ID of 0.

cable: Specifies the Cable port type with a type ID of 17.

ethernet: Specifies the Ethernet port type with a type ID of 15.

g.3-fax: Specifies the G.3 Fax port type with a type ID of 10.

hdlc: Specifies the HDLC port type with a type ID of 7.

idsl: Specifies the IDSL port type with a type ID of 14.

isdn-async-v110: Specifies the ISDN Async V.110 port type with a type ID of 4.

ISDN Async V.110: Specifies the ISDN Async V.120 port type with a type ID of 3.

isdn-sync: Specifies the ISDN Sync port type with a type ID of 2.

piafs: Specifies the port type complying with PIAFS. The type ID is 6.

sdsl: Specifies the SDSL port type with a type ID of 11.

sync: Specifies the Sync port type with a type ID of 1.

virtual: Specifies the Virtual port type with a type ID of 5.

wireless-other: Specifies the Wireless-other port type with a type ID of 18.

x.25: Specifies the X.25 port type with a type ID of 8.

x.75: Specifies the X.75 port type with a type ID of 9.

xdsl: Specifies the XDSL port type with a type ID of 16.

Usage guidelines

The NAS-Port-Type attribute carries information about the access interface. The BRAS includes the configured NAS-Port-Type in RADIUS requests sent to the RADIUS server.

Examples

Configure the port type as **sdsl** for IPv4 interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip subscriber nas-port-type sdsl
```

ip subscriber password

Use **ip subscriber password** to configure passwords for IPv4 individual users.

Use **undo ip subscriber password** to restore the default.

Syntax

ip subscriber password { **ciphertext** | **plaintext** } *string*

undo ip subscriber password

Default

The password for IPv4 individual users is **vlan**.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Parameters

ciphertext *string*: Specifies a ciphertext password, a case-sensitive string of 1 to 117 characters.

plaintext *string*: Specifies a plaintext password, a case-sensitive string of 1 to 63 characters. For security purposes, the password specified in plaintext form will be stored in encrypted form.

Usage guidelines

Passwords configured by this command are used for authentication, and must be the same as those configured on the AAA server.

A DHCPv4 user can obtain a password in various ways. For password priority, see "ip subscriber dhcp password option60."

Examples

Configure the plaintext password as **123** for IPv4 individual users on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip subscriber password plaintext 123
```

Related commands

ip subscriber dhcp username

ip subscriber unclassified-ip username

ip subscriber dhcp password option60

ip subscriber service-identify

Use **ip subscriber service-identify** to configure service identifiers for IPv4 unclassified-IP users, static individual users, and leased users.

Use **undo ip subscriber service-identify** to restore the default.

Syntax

Layer 3 Ethernet interface view, Layer 3 aggregate interface view, L3VE interface view, VEth interface view:

ip subscriber service-identify dscp

undo ip subscriber service-identify

Layer 3 Ethernet subinterface view, Layer 3 aggregate subinterface view, L3VE subinterface view, VEth subinterface view:

ip subscriber service-identify { **8021p** { **second-vlan** | **vlan** } | **dscp** | **second-vlan** | **vlan** }

undo ip subscriber service-identify

VLAN interface view:

ip subscriber service-identify { **8021p vlan** } | **dscp** | **vlan** }

undo ip subscriber service-identify

Default

No service identifier is configured for IPv4 unclassified-IP users, static individual users, and leased users.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Parameters

8021p second-vlan: Specifies the 802.1p value of the inner VLAN tag in QinQ mode as the service identifier.

8021p vlan: Specifies the 802.1p value of the VLAN tag or the 802.1p value of the outer VLAN tag in QinQ mode as the service identifier.

dscp: Specifies the DSCP value as the service identifier.

second-vlan: Specifies the inner VLAN ID in QinQ mode as the service identifier.

vlan: Specifies the VLAN ID or the outer VLAN ID in QinQ mode as the service identifier.

Usage guidelines

You must specify an identifier for a service before you bind an ISP domain to the service. Otherwise, the binding does not take effect.

IPv4 unclassified-IP users, static individual users, and leased users whose IP packets containing the specified service identifier will be assigned a service-specific ISP domain.

You can configure only one service identifier on each interface.

Examples

Configure **dscp** as the service identifier on GigabitEthernet 1/0/1 for IPv4 unclassified-IP users, static individual users, and leased users.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip subscriber service-identify dscp
```

Related commands

ip subscriber 8021p

ip subscriber dscp

ip subscriber vlan

ip subscriber session static

Use **ip subscriber session static** to configure IPv4 static IPoE sessions.

Use **undo ip subscriber session static** to delete IPv4 static IPoE sessions.

Syntax

ip subscriber session static ip *ip-address* [**vlan** *vlan-id* [**second-vlan** *vlan-id*]] [**mac** *mac-address*] [**domain** *domain-name*] [**description** *string*]

undo ip subscriber session static ip *ip-address* [**vlan** *vlan-id* [**second-vlan** *vlan-id*]]

Default

No IPv4 static IPoE session exists.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Parameters

ip *ip-address*: Specifies a user IPv4 address.

vlan *vlan-id*: Specifies an outer VLAN ID of the user packet, in the range of 1 to 4094. This option is available only for subinterfaces.

second-vlan *vlan-id*: Specifies an inner VLAN ID of the user packet, in the range of 1 to 4094. This option is available only for subinterfaces.

mac *mac-address*: Specifies a user MAC address in the form of H-H-H.

domain *domain-name*: Specifies an ISP domain name, a case-insensitive string of 1 to 255 characters. The name cannot contain the slash (/), back slash (\), vertical bar (|), quotation mark ("), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or at sign (@). If you do not specify an ISP domain, the default system domain is used. For more information about the default system domain, see *Security Configuration Guide*.

description *string*: Specifies the static session description, a case-insensitive string of 1 to 31 characters. If this option is not specified, the static session does not have a description. The description cannot contain the following characters: forward slashes (/), backslashes (\), vertical bars (|), quotation marks ("), colons (:), asterisks (*), question marks (?), left angle brackets (<), right angle brackets (>), and at signs (@).

Usage guidelines

Static IPoE sessions have higher priority than dynamic IPoE sessions. If a user IP or DHCP packet matches a static IPoE session, the static IPoE session overwrites the existing dynamic IPoE session.

When the IP address specified in a static session overlaps with the assignable IP addresses in the DHCP address pool, you must use the **dhcp server forbidden-ip** or **forbidden-ip** command to exclude the overlapping IP address in the DHCPv4 address pool from dynamic address allocation. For more information about excluding IP addresses from dynamic allocation, see DHCP configuration in *Layer 3—IP Services Configuration Guide*.

You can configure multiple static IPoE sessions on an interface. Static IPv4 IPoE sessions include the following types:

- A session with a specified IPv4 address.
- A session with a specified IPv4 address and outer VLAN ID.
- A session with a specified IPv4 address, outer VLAN ID, and inner VLAN ID.

For each session type, configuration fails if the settings are identical to the settings of an existing session.

To change the parameters of an existing IPoE session, use the undo form of the command to delete the session, and then reconfigure it with new parameter settings.

You cannot configure a static IPoE session on an interface configured with dedicated-interface or subnet-leased users.

Examples

Configure an IPv4 static IPoE session with an IP address of 1.1.1.1 and an ISP domain of **dm1** on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip subscriber session static ip 1.1.1.1 domain dm1
```

Related commands

display ip subscriber session

ip subscriber subnet-leased

Use **ip subscriber subnet-leased** to configure IPv4 subnet-leased users.

Use **undo ip subscriber subnet-leased** to delete IPv4 subnet-leased users.

Syntax

ip subscriber subnet-leased ip *ip-address* { *mask* | *mask-length* } **username** *name* **password** { **ciphertext** | **plaintext** } *string* [**domain** *domain-name*]

undo ip subscriber subnet-leased ip *ip-address* { *mask* | *mask-length* }

Default

No IPv4 subnet-leased user exists.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Parameters

ip *ip-address*: Specifies a user IPv4 address.

mask: Specifies an IP address mask in dotted decimal notation.

mask-length: Specifies a mask length, an integer in the range of 0 to 32.

username *name*: Specifies a username for authentication, a case-sensitive string of 1 to 255 characters.

password: Specifies a password for authentication.

ciphertext *string*: Specifies a ciphertext password, a case-sensitive string of 1 to 117 characters.

plaintext *string*: Specifies a plaintext password, a case-sensitive string of 1 to 63 characters. For security purposes, the password specified in plaintext form will be stored in encrypted form.

domain *domain-name*: Specifies an ISP domain name, a case-insensitive string of 1 to 255 characters. The name cannot contain the slash (/), back slash (\), vertical bar (|), quotation mark ("), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or at sign (@). If you do not specify an ISP domain, the default system domain is used. For more information about the default system domain, see *Security Configuration Guide*.

Usage guidelines

An IPv4 subnet-leased user is a group of IPv4 hosts that rent the same subnet of an interface and share the same IPoE session. The BRAS authenticates, authorizes, and bills all hosts of the same subnet-leased user.

You can configure only one IPv4 subnet-leased user on each subnet.

You cannot configure a subnet-leased user on an interface configured with individual users or interface-leased users.

Examples

Configure an IPv4 subnet-leased user for subnet **1.1.1.1/24** with a username of **netuser** and a plaintext password of **pw123** on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip subscriber subnet-leased ip 1.1.1.1 24 username netuser
password plaintext pw123
```

Related commands

display ip subscriber subnet-leased

ip subscriber timer quiet

Use **ip subscriber timer quiet** to configure a quiet timer for IPv4 users.

Use **undo ip subscriber timer quiet** to restore the default.

Syntax

ip subscriber timer quiet *time*

undo ip subscriber timer quiet

Default

No quite timer is configured for IPv4 users.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Parameters

time: Specifies the quiet timer in the range of 10 to 3600 seconds.

Usage guidelines

IPoE starts the quiet timer after a user fails authentication. It discards packets from the user during the quiet time. After the quiet timer expires, IPoE performs authentication upon receiving a packet from the user.

Examples

Set the quiet time to **100** seconds for IPv4 users on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip subscriber timer quiet 100
```

ip subscriber trust

Use **ip subscriber trust** to configure a trusted option for DHCPv4 users.

Use **undo ip subscriber trust** to cancel a trusted option.

Syntax

ip subscriber trust { **option60** | **option82** }

undo ip subscriber trust { **option60** | **option82** }

Default

No trusted options are configured for DHCPv4 users.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Parameters

option60: Specifies Option 60 as the trusted option.

option82: Specifies Option 82 as the trusted option.

Usage guidelines

If the BRAS trusts DHCPv4 Option 60, the following option information is used as the ISP domain:

- All information in Option 60 if the option does not contain invalid characters or the at sign (@).

  Invalid characters include the slash (/), back slash (\), vertical bar (|), quotation mark ("), colon (:), asterisk (*), question mark (?), left angle bracket (<), and right angle bracket (>).
- Information that follows the last at sign (@) if the option contains at signs (@) and does not contain invalid characters.

If the BRAS does not trust DHCPv4 Option 60, the ISP domains are used in the following order:

1. Domain specified in the **ip subscriber dhcp domain** command.
2. Default system domain.

If the BRAS trusts DHCPv4 Option 82, it obtains the following information from the option and uses the information to encapsulate RADIUS attributes:

- Obtains the Circuit-ID information and uses it to encapsulate NAS-Port-ID that adopts version 2.0 as the encapsulation format.
- Obtains the Circuit-ID information and uses it to encapsulate DSL_AGENT_CIRCUIT_ID.
- Obtains the Remote-ID information and uses it to encapsulate DSL_AGENT_REMOTE_ID.

If the BRAS does not trust DHCPv4 Option 82, it does not use the Option 82 to encapsulate RADIUS attributes.

Examples

Configure DHCPv4 Option 82 as a trusted option on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip subscriber trust option82
```

Related commands

ip subscriber dhcp domain

ip subscriber initiator dhcp enable

ip subscriber nas-port-id format

ip subscriber nas-port-id nasinfo-insert

ip subscriber unclassified-ip domain

Use **ip subscriber unclassified-ip domain** to configure an ISP domain for IPv4 unclassified-IP users, static individual users, and leased users.

Use **undo ip subscriber unclassified-ip domain** to restore the default.

Syntax

ip subscriber unclassified-ip domain *domain-name*

undo ip subscriber unclassified-ip domain

Default

IPv4 unclassified-IP users, static individual users, and leased users use the default system ISP domain.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Parameters

domain *domain-name*: Specifies an ISP domain name, a case-insensitive string of 1 to 255 characters. The name cannot contain the slash (/), back slash (\), vertical bar (|), quotation mark ("), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or at sign (@).

Usage guidelines

This command configures an ISP domain for IPv4 unclassified-IP users, static individual users, and leased users. The configured ISP domain must exist on the BRAS.

The BRAS selects an ISP domain for an IPv4 unclassified-IP user, static individual user, or leased user in the following order:

1. Service-specific domain.
2. Domain specified by this command.
3. Default system domain.

Examples

Configure ISP domain **ipoe** for IPv4 unclassified-IP users, static individual users, and leased users on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip subscriber unclassified-ip domain ipoe
```

Related commands

ip subscriber initiator unclassified-ip enable

ip subscriber service-identify

ip subscriber unclassified-ip max-session

Use **ip subscriber unclassified-ip max-session** to configure the maximum number of IPoE sessions for IPv4 unclassified-IP users on an interface.

Use **undo ip subscriber unclassified-ip max-session** to restore the default.

Syntax

ip subscriber unclassified-ip max-session *max-number*

undo ip subscriber unclassified-ip max-session

Default

The maximum number of IPoE sessions for IPv4 unclassified-IP users on an interface is not configured.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Parameters

max-number: Specifies the maximum number of IPoE sessions for IPv4 unclassified-IP users. The value range for this argument is 1 to 64000.

Usage guidelines

If IPoE sessions for IPv4 unclassified-IP users reach the maximum, no more IPoE session can be initiated for IPv4 unclassified-IP users.

Examples

Set the maximum number of IPoE sessions to **100** for IPv4 unclassified-IP users on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip subscriber unclassified-ip max-session 100
```

Related commands

display ip subscriber session

ip subscriber initiator unclassified-ip enable

reset ip subscriber session

ip subscriber unclassified-ip username

Use **ip subscriber unclassified-ip username** to configure an authentication user naming convention for IPv4 unclassified-IP users and static individual users.

Use **undo ip subscriber unclassified-ip username** to restore the default.

Syntax

ip subscriber unclassified-ip username include { **nas-port-id** [**separator** *separator*] | **port** [**separator** *separator*] | **second-vlan** [**separator** *separator*] | **slot** [**separator** *separator*] | **source-ip** [**address-separator** *address-separator*] [**separator** *separator*] | **source-mac** [**address-separator** *address-separator*] [**separator** *separator*] | **subslot** [**separator** *separator*] | **sysname** [**separator** *separator*] | **vlan** [**separator** *separator*] } *

undo ip subscriber unclassified-ip username

Default

An IPv4 unclassified-IP user or static individual user uses its source IPv4 address as the authentication username.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Parameters

nas-port-id: Includes the NAS-Port-ID attribute in a username.

port: Includes the number of the port that receives the user packets in a username.

second-vlan: Includes the inner VLAN ID in a username.

slot: Includes the number of the slot that receives the user packets in a username.

source-ip: Includes the source IP address in a username.

address-separator *address-separator*: Specifies any printable character as the separator for the IPv4 address. For example, if you specify a hyphen (-) as the separator, the username is the hyphen-separated IP address (xxxx-xxxx-xxxx). If you do not specify a separator, the username is the dot-separated IP address (x.x.x.x). Do not use the at sign (@) as the separator. The AAA server cannot parse a username containing the at sign (@).

source-mac: Includes the source MAC address in a username.

address-separator *address-separator*: Specifies any printable character as the separator for the MAC address. For example, if you specify a hyphen (-) as the separator, the username is the hyphen-separated MAC address (xxxx-xxxx-xxxx). If you do not specify a separator, the username is the non-separated MAC address (xxxxxxxxxxxx). Do not use the at sign (@) as the separator. The AAA server cannot parse a username containing the at sign (@).

subslot: Includes the number of the subslot that receives the user packets in a username.

sysname: Includes the name of the device that receives the user packets in a username.

vlan: Includes the outer VLAN ID in a username.

separator *separator*: Specifies a character for separating an option and the option that follows. Do not use the at sign (@) as the separator. The AAA server cannot parse a username containing the at sign (@).

Usage guidelines

Usernames obtained based on the naming convention are used for authentication and must be the same as those configured on the AAA server.

You can specify one or more keywords in a naming convention. If you use a combination of keywords, a username obtained based on the naming convention includes the specified options in the configuration order.

Examples

Configure the source IPv4 address as the authentication usernames for IPv4 unclassified-IP users and static individual users on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ip subscriber unclassified-ip username include source-ip
```

Configure an authentication user naming convention for IPv4 unclassified-IP users and static individual users on GigabitEthernet 1/0/1. Each username contains the device name, slot number, subslot number, port number, and outer VLAN, separated by the pound sign (#).

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip subscriber unclassified-ip username include sysname
separator # slot separator # subslot separator # port separator # vlan
```

Related commands

ip subscriber initiator unclassified-ip enable

ip subscriber password

ip subscriber user-detect

Use **ip subscriber user-detect** to configure online detection for IPv4 individual users.

Use **undo ip subscriber user-detect** to restore the default.

Syntax

ip subscriber user-detect { **arp** | **icmp** } **retry** *retries* **interval** *interval*

undo ip subscriber user-detect

Default

Online detection for IPv4 individual users is disabled.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Parameters

arp: Specifies the ARP request packet as detection packets.

icmp: Specifies the ICMP request packet as detection packets.

retry *retries*: Specifies the maximum number of detection attempts following the first detection attempt, in the range of 2 to 5.

interval *interval*: Configures the detection timer for each attempt, in the range of 30 to 1200 seconds.

Usage guidelines

Online detection enables the BRAS to periodically detect the status of an IPv4 individual user. It uses ARP and ICMP requests to detect IPv4 individual users. If IPv4 individual users and the interface are in different subnets, only ICMP request packets can be used for detection.

After you configure online detection, the BRAS starts a detection timer to detect online users. If the BRAS does not receive user packets before the detection timer expires, it sends a detection packet to the user.

- If the BRAS receives user packets within the maximum detection attempts, the BRAS assumes that the user is online. It resets the detection timer, and starts the next detection attempt.

- If the BRAS does not receive user packets after detection attempts reach the maximum, the BRAS assumes that the user is offline and deletes the user session.

Examples

Configure online detection on GigabitEthernet 1/0/1. The maximum number of detection attempts is **5**, the detection timer is **100** seconds, and the detection packet type is **ARP.**

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip subscriber user-detect arp retry 5 interval 100
```

Related commands

ip subscriber enable

ip subscriber vlan

Use **ip subscriber vlan** to bind an ISP domain to a VLAN list for IPv4 unclassified-IP users, static individual users, and leased users.

Use **undo ip subscriber vlan** to remove the binding between an ISP domain and a VLAN list.

Syntax

ip subscriber vlan *vlan-list* **domain** *domain-name*

undo ip subscriber vlan *vlan-list*

Default

No ISP domain is bound to a VLAN list for IPv4 unclassified-IP users, static individual users, and leased users.

Views

Layer 3 aggregate subinterface view

Layer 3 Ethernet subinterface view

Predefined user roles

network-admin

context-admin

Parameters

vlan-list: Specifies a space-separated list of up to 10 VLAN ID items. Each item specifies a VLAN by its ID or a range of VLANs in the form of start-VLAN-ID to end-VLAN-ID. The VLAN ID is in the range of 1 to 4094.

domain *domain-name*: Specifies an ISP domain name, a case-insensitive string of 1 to 255 characters. The name cannot contain the slash (/), back slash (\), vertical bar (|), quotation mark ("), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or at sign (@).

Usage guidelines

This command configures an ISP domain for IPv4 unclassified-IP users, static individual users, and leased users who send IP packets with the specified VLAN IDs.

Examples

Configure an ISP domain for IPv4 unclassified-IP users, static individual users, and leased users who send IP packets with the specified VLAN IDs on GigabitEthernet 1/0/1.100. The specified VLAN IDs are in the range of 2 to 100.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1.100
```

```
[Sysname-GigabitEthernet1/0/1.100] ip subscriber service-identify second-vlan
[Sysname-GigabitEthernet1/0/1.100] ip subscriber vlan 2 to 100 domain vlandm
```

Related commands

ip subscriber service-identify

ip subscriber whitelist enable

Use **ip subscriber whitelist enable** to enable the IPv4 IPoE whitelist feature.

Use **undo ip subscriber whitelist enable** to disable the IPv4 IPoE whitelist feature.

Syntax

ip subscriber whitelist enable

undo ip subscriber whitelist enable

Default

The IPv4 IPoE whitelist feature is disabled.

Views

Layer 3 Ethernet interface/subinterface view

Layer 3 aggregate interface/subinterface view

Predefined user roles

network-admin

context-admin

Usage guidelines

With this feature enabled, only IPv4 traffic matching static IPv4 IPoE sessions can initiate IPoE authentication, and IPoE directly permits the other traffic without any processing.

In some scenarios, an interface might need to have both IPoE and portal authentication enabled. For example, both dumb terminals and broadband dial-up users exist on an interface. Dumb terminals (for example, monitoring cameras) need to come online through IPoE without portal authentication, and broadband dial-up users need to come online through portal Web authentication. In this case, you can enable the IPv4 IPoE whitelist feature on the interface. When both the IPv4 IPoE whitelist feature and portal authentication are enabled on an interface, the following rules apply:

- If the IPv4 traffic of a user matches a static IPv4 IPoE session, the user is processed by the static IPv4 IPoE authentication flow. For an IPoE user to bypass authentication, specify the authentication and authorization modes as **none** in the ISP domain of the IPoE user.
- If the IPv4 traffic of a user does not match any IPv4 IPoE session, the user is processed by portal authentication.

Examples

Enable the IPv4 IPoE whitelist feature on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip subscriber whitelist enable
```

reset ip subscriber offline statistics

Use **reset ip subscriber offline statistics** to remove offline statistics for IPv4 users.

Syntax

reset ip subscriber offline statistics [**interface** *interface-type interface-number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command removes offline statistics for IPv4 users for all interfaces.

Examples

Remove offline statistics for all IPv4 users on GigabitEthernet 1/0/1.

```
<Sysname> reset ip subscriber offline statistics interface gigabitethernet 1/0/1
```

Related commands

display ip subscriber offline statistics

reset ip subscriber session

Use **reset ip subscriber session** to delete dynamic IPv4 IPoE sessions and log out the users.

Syntax

reset ip subscriber session [**interface** *interface-type interface-number*] [**domain** *domain-name* | **ip** *ip-address* [**vpn-instance** *vpn-instance-name*] | **mac** *mac-address* | **username** *name*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command deletes dynamic IPv4 IPoE sessions for all interfaces.

domain *domain-name*: Specifies an ISP domain name, a case-insensitive string of 1 to 255 characters.

ip *ip-address*: Specifies the IP address of the IPoE session to be deleted.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command deletes IPv4 IPoE sessions on the public network.

mac *mac-address*: Specifies the MAC address of an IPv4 IPoE session to be deleted, in the format of H-H-H.

username *name*: Specifies the username of the IPv4 IPoE session to be deleted, a case-sensitive string of 1 to 255 characters.

Usage guidelines

If you do not specify any parameters, this command deletes all dynamic IPv4 IPoE sessions.

To delete static IPoE sessions for static users and leased users, use the **undo** commands.

Examples

Delete dynamic IPv4 IPoE sessions and log out the users on GigabitEthernet 1/0/1.

```
<Sysname> reset ip subscriber session interface gigabitethernet 1/0/1
```

Related commands

display ip subscriber session

IPv6 IPoE commands

display ipv6 subscriber interface-leased

Use **display ipv6 subscriber interface-leased** to display information about IPv6 interface-leased users.

Syntax

display ipv6 subscriber interface-leased [**interface** *interface-type interface-number*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays information about IPv6 interface-leased users for all interfaces.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about IPv6 interface-leased users for all member devices.

Examples

Display information about the IPv6 interface-leased user on GigabitEthernet 1/0/1.

```
<Sysname> display ipv6 subscriber interface-leased interface gigabitethernet 1/0/1
Basic:
  Access interface           : GE1/0/1
  VPN instance               : N/A
  Username                   : a
  User ID                    : 0x40000000
  State                      : Online
```

```
  Service node               : Slot 1 CPU 0
  Domain                     : radius6
  Login time                 : May 14 20:20:11 2014
  Online time (hh:mm:ss)     : 00:16:37

AAA:
  IP pool                    : ipoe
  Session idle time          : N/A
  Session duration           : N/A, remaining: N/A
  Remaining traffic          : N/A
  Max multicast addresses    : 4
  Multicast address list     : N/A

QoS:
  User profile               : nsfocus (active)
  Session group profile      : N/A
  Inbound CAR                : CIR 1000bps PIR 2000bps CBS 500bit (active)
  Outbound CAR               : CIR 3000bps PIR 4000bps CBS 500bit (active)

Flow statistic:
  Uplink   packets/bytes     : 0/0
  Downlink packets/bytes     : 0/0

ITA:
  Level-1 Uplink   packets/bytes: 0/0
          Downlink packets/bytes: 0/0
  Level-2 Uplink   packets/bytes: 0/0
          Downlink packets/bytes: 0/0
```

Table 11 Command output

Field	Description
Basic	Basic session information.
Access interface	Interface that connects the user.
VPN instance	MPLS L3VPN instance of the user. If the user is not in a VPN, this field displays **N/A**.
Username	Username for authentication.
User ID	User ID assigned after the user came online. If no user ID is assigned, this field displays **0xffffffff**.
State	User state: • **Init**—The user is being initiated. • **Offline**—The user is going offline. • **Auth**—The user is being authenticated. • **AuthFail**—The user failed authentication. • **AuthPass**—The user passed authentication. • **AssignedIP**—The user has an IP address. • **Online**—The user is online. • **Backup**—Backup information about the user on the primary BRAS.

Field	Description
Service node	Slot number and CPU number of the card that connects the user.
Domain	ISP domain.
Login time	Time when the user passed authentication and logged in, in the format of MM-DD hh:mm:ss YYYY.
Online time (hh:mm:ss)	Online duration for the user.
AAA	AAA authorization information.
IP pool	AAA-authorized DHCP address pool. If no DHCP address pool is authorized, this field displays **N/A**.
Session idle time	Idle time in seconds specified for online users. If the idle time expires, the user is logged out. If no idle time is specified, this field displays **N/A** and the user can remain idle without being logged out.
Session duration	AAA-authorized IPoE session duration in seconds: • **N/A**—No IPoE session duration is authorized. • **Unlimited**—The IPoE session duration is unlimited.
remaining	Remaining AAA-authorized IPoE session duration. If no session duration is authorized, this field displays **N/A**. ○ For users on Layer 3 Ethernet interfaces and subinterfaces, this field displays the remaining time or **Unlimited**. ○ For users on Layer 3 aggregate interfaces and subinterfaces, this field displays the remaining time or **Unlimited** only when the slot or interface is specified. If you do not specify the slot or interface, this field displays **N/A**.
Remaining traffic	Remaining AAA-authorized traffic in bytes. If no traffic is authorized, this field displays **N/A**.
Max multicast addresses	Maximum number of AAA-authorized multicast groups that a user can join.
Multicast address list	List of AAA-authorized multicast group addresses. If no multicast group is authorized, this field displays **N/A**.
QoS	QoS information.
User profile	AAA-authorized user profile: • **N/A**—No user profile is authorized. • **inactive**—User profile authorization failed or the user profile does not exist on the BRAS. • **active**—The user profile is authorized successfully. If the authorization result has not been updated, nothing is displayed.
Session group profile	AAA-authorized session group profile: • **N/A**—No session group profile is authorized. • **inactive**—Session group profile authorization failed or the session group profile does not exist on the BRAS. • **active**—The session group profile is authorized successfully. If the authorization result has not been updated, nothing is displayed.
Inbound CAR	Inbound CIR and PIR in bps and CBS in bits: • **N/A**—Inbound CAR is not authorized. • **inactive**—Inbound CAR is not authorized successfully. • **active**—Inbound CAR is authorized successfully.
Outbound CAR	Outbound CIR and PIR in bps and CBS in bits: • **N/A**—Outbound CAR is not authorized.

Field	Description
	• **inactive**—Outbound CAR is not authorized successfully. • **active**—Outbound CAR is authorized successfully.
Flow statistic	Session flow statistics.
Uplink packets/bytes	Total number and size of uplink packets.
Downlink packets/bytes	Total number and size of downlink packets.
ITA	Intelligent target accounting (ITA) information.
Level-*n* Uplink packets/bytes	Number and size of uplink packets for level *n* accounting (1 ≤ *n* ≤ 8).
Downlink packets/bytes	Number and size of downlink packets for level *n* accounting (1 ≤ *n* ≤ 8).

Related commands

ipv6 subscriber enable

display ipv6 subscriber interface-leased statistics

Use **display ipv6 subscriber interface-leased statistics** to display IPoE session statistics for IPv6 interface-leased users.

Syntax

display ipv6 subscriber interface-leased statistics [**interface** *interface-type interface-number*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays IPoE session statistics for IPv6 interface-leased users for all interfaces.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPoE session statistics for IPv6 interface-leased users for all member devices.

Examples

Display IPoE session statistics for IPv6 interface-leased users on the BRAS.

```
<Sysname> display ipv6 subscriber interface-leased statistics
Total                : 100
Init                 : 0
Authenticating       : 20
Authenticate fail    : 0
Authenticate pass    : 20
Assigned IP          : 10
```

```
Online               : 50
Backup               : 0
```

Table 12 Command output

Field	Description
Total	Total number of users on the interface.
Init	Number of users who initiated sessions.
Authenticating	Number of users being authenticated.
Authenticate fail	Number of users who failed authentication.
Authenticate pass	Number of users who passed authentication.
Assigned IP	Number of users who have IP addresses.
Online	Number of online users.
Backup	Number of users whose information was backed up.

display ipv6 subscriber offline statistics

Use **display ipv6 subscriber offline statistics** to display offline statistics for IPv6 users.

Syntax

display ipv6 subscriber offline statistics [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays offline statistics for IPv6 users for all interfaces.

Examples

Display offline statistics for IPv6 users on GigabitEthernet 1/0/1.

```
<Sysname> display ipv6 subscriber offline statistics interface gigabitethernet 1/0/1
Total               : 100
User request        : 0
DHCP lease expire   : 0
AAA lease expire    : 0
Command cut         : 80
AAA terminate       : 0
Authenticate fail   : 0
Authorization fail  : 0
```

```
Idle timeout        : 10
Detect fail         : 10
Not enough resource : 0
Interface down      : 0
Interface shutdown  : 0
VSRP event          : 0
DHCP notify         : 0
Other               : 0
```

Table 13 Command output

Field	Description
Total	Total number of offline users.
User request	Number of users requesting to go offline.
DHCP lease expired	Number of users with expired DHCP leases.
AAA lease expired	Number of users with expired AAA leases.
Command cut	Number of users logged out by commands.
AAA terminate	Number of users logged out by AAA.
Authenticate fail	Number of users who failed authentication.
Authorization fail	Number of users who failed authorization.
Idle timeout	Number of users with an expired idle timeout timer.
Detect fail	Number of users who failed online detection.
Not enough resource	Number of users with insufficient hardware resources.
Interface down	Number of users on an interface that went down.
Interface shutdown	Number of users on an interface that was shut down.
VSRP event	Number of users disconnected as requested by the VSRP event.
DHCP notify	Number of users disconnected by DHCP.
Other	Number of users disconnected from the network because of unknown causes.

Related commands

reset ipv6 subscriber offline statistics

display ipv6 subscriber session

Use **display ipv6 subscriber session** to display session information for IPv6 individual users.

Syntax

display ipv6 subscriber session [**interface** *interface-type interface-number*] [**domain** *domain-name* | **ipv6** *ipv6-address* [**vpn-instance** *vpn-instance-name*] | **mac** *mac-address* | **static** | **username** *name*] [**slot** *slot-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays session information for IPv6 individual users for all interfaces.

domain *domain-name*: Specifies an ISP domain name, a case-insensitive string of 1 to 255 characters. The name cannot contain the slash (/), back slash (\), vertical bar (|), quotation mark ("), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or at sign (@).

ip *ip-address*: Specifies the source IP address of the IPv6 individual user.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays session information for IPv6 individual users on the public network.

mac *mac-address*: Specifies the MAC address of an IPv6 individual user, in the format of H-H-H.

static: Specifies static IPoE sessions. If this parameter is not specified, this command displays information about static and dynamic sessions for IPv6 individual users.

username *name*: Specifies the username of the IPv6 individual user, a case-sensitive string of 1 to 255 characters.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays session information for IPv6 individual users for all member devices.

verbose: Displays detailed session information for IPv6 individual users. If this parameter is not specified, this command displays general session information.

Examples

Display general session information for the IPv6 individual user with an IP address of **2000::1** in **vpn1**.

```
<Sysname> display ipv6 subscriber session ipv6 2000::1 vpn-instance vpn1
Type: D-DHCP   S-Static     U-Unclassified-IP   N-NDRS
Interface            IP address                MAC address    Type  State
--------------------------------------------------------------------------------
RAGG1024             2000::1                   000d-88f8-0eab D     Online
```

Displays detailed session information for IPv6 individual users.

```
<Sysname> display ipv6 subscriber session verbose
Basic:
  Description               : -
  Username                  : abc
  Domain                    : radius6
  VPN instance              : N/A
  IP address                : 2000::1
  MAC address               : 000d-88f8-0eab
  Service-VLAN/Customer-VLAN : -/-
  Access interface          : GE1/0/1
```

```
  User ID                    : 0x48080008
  VPI/VCI(for ATM)           : -/-
  DHCP lease                 : N/A
  DHCP remain lease          : N/A
  Login time                 : May  9 09:10:01 2014
  Online time (hh:mm:ss)     : 00:16:37
  Service node               : Slot 1 CPU 0
  Type                       : Unclassified-IP
  State                      : Online

AAA:
  IP pool                    : N/A
  Session idle time          : N/A
  Session duration           : N/A, remaining: N/A
  Remaining traffic          : N/A
  Max multicast addresses    : 4
  Multicast address list     : N/A

QoS:
  User profile               : nsfocus (active)
  Session group profile      : N/A
  Inbound CAR                : CIR 1000bps PIR 2000bps CBS 500bit (active)
  Outbound CAR               : CIR 3000bps PIR 4000bps CBS 500bit (active)

Flow statistic:
  Uplink   packets/bytes     : 0/0
  Downlink packets/bytes     : 0/0

ITA:
  Level-1 Uplink   packets/bytes: 0/0
          Downlink packets/bytes: 0/0
  Level-2 Uplink   packets/bytes: 0/0
          Downlink packets/bytes: 0/0
```

Figure 1 Command output

Field	Description
Basic	Basic session information.
Description	Description of the IPoE session. If the IPoE session does not have a description, this field displays a hyphen (-).
Username	Username for authentication.
Domain	ISP domain of the user.
VPN instance	MPLS L3VPN instance of the user. If the user is not in a VPN, this field displays **N/A**.
IP address	IP address of the user.
MAC address	MAC address of the user.
Service-VLAN/Customer-VLAN	Public and private VLANs of the user. If the user is not a VLAN user, this field displays **-**.

Field	Description
Access interface	Interface that connects the user.
User ID	User ID assigned after the user came online. If no user ID is assigned, this field displays **0xffffffff**.
VPI/VCI(for ATM)	PVC information about the ATM.
DHCP lease	DHCP-authorized IP lease in seconds: • **N/A**—No IP lease is authorized. • **Unlimited**—The IP lease is unlimited.
DHCP remain lease	Remaining DHCP-authorized IP lease. This field is valid only on the card that connects the user. On other cards, this field displays **N/A**.
Login time	Time when the user passed authentication and logged in, in the format of MM-DD hh:mm:ss YYYY.
Online time (hh:mm:ss)	Online duration for the user.
Service node	Slot number and CPU number of the card that connects the user.
Type	IPoE session types: • **DHCP**—Dynamic IPoE sessions for DHCP users. • **Unclassified-IP**—Dynamic IPoE sessions for unclassified-IP users. • **Static**—Static sessions. • **NDRS**—Dynamic sessions for IPv6-ND-RS users.
State	User state: • **Init**—The user is being initiated. • **Offline**—The user is going offline. • **Auth**—The user is being authenticated. • **AuthFail**—The user failed authentication. • **AuthPass**—The user passed authentication. • **AssignedIP**—The user has an IP address. • **Online**—The user is online. • **Backup**—Backup information about the user on the primary BRAS.
AAA	AAA authorization information.
IP pool	AAA-authorized DHCP address pool. If no DHCP address pool is authorized, this field displays **N/A**.
Session idle time	Idle time in seconds specified for online users. If the idle time expires, the user is logged out. If no idle time is specified, this field displays **N/A** and the user can remain idle without being logged out.
Session duration	AAA-authorized IPoE session duration in seconds: • **N/A**—No IPoE session duration is authorized. • **Unlimited**—The IPoE session duration is unlimited.
remaining	Remaining AAA-authorized IPoE session duration. If no session duration is authorized, this field displays **N/A**. ◦ For users on Layer 3 Ethernet interfaces and subinterfaces, this field displays the remaining time or **Unlimited**. ◦ For users on Layer 3 aggregate interfaces and subinterfaces, this field displays the remaining time or **Unlimited** only when the slot or interface is specified. If you do not specify the slot or interface, this field displays **N/A**.

Field	Description
Remaining traffic	Remaining AAA-authorized traffic in bytes. If no traffic is authorized, this field displays **N/A**.
Max multicast addresses	Maximum number of AAA-authorized multicast groups that a user can join.
Multicast address list	List of AAA-authorized multicast group addresses. If no multicast group is authorized, this field displays **N/A**.
QoS	QoS information.
User profile	AAA-authorized user profile: • **N/A**—No user profile is authorized. • **inactive**—User profile authorization failed or the user profile does not exist on the BRAS. • **active**—The user profile is authorized successfully. If the authorization result has not been updated, nothing is displayed.
Session group profile	AAA-authorized session group profile: • **N/A**—No session group profile is authorized. • **inactive**—Session group profile authorization failed or the session group profile does not exist on the BRAS. • **active**—The session group profile is authorized successfully. If the authorization result has not been updated, nothing is displayed.
Inbound CAR	Inbound CIR and PIR in bps and CBS in bits: • **N/A**—Inbound CAR is not authorized. • **inactive**—Inbound CAR is not authorized successfully. • **active**—Inbound CAR is authorized successfully.
Outbound CAR	Outbound CIR and PIR in bps and CBS in bits: • **N/A**—Outbound CAR is not authorized. • **inactive**—Outbound CAR is not authorized successfully. • **active**—Outbound CAR is authorized successfully.
Flow statistic	Session flow statistics.
Uplink packets/bytes	Total number and size of uplink packets.
Downlink packets/bytes	Total number and size of downlink packets.
ITA	Intelligent target accounting (ITA) information.
Level-*n* Uplink packets/bytes	Number and size of uplink packets for level *n* accounting (1 ≤ *n* ≤ 8).
Downlink packets/bytes	Number and size of downlink packets for level *n* accounting (1 ≤ *n* ≤ 8).

Related commands

`ipv6 subscriber enable`

display ipv6 subscriber session statistics

Use **`display ipv6 subscriber session statistics`** to display IPoE session statistics for IPv6 individual users.

Syntax

display ipv6 subscriber session statistics [**session-type** { **dhcp** | **ndrs** | **static** | **unclassified-ip** }] [**interface** *interface-type interface-number*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

session-type: Specifies a user type. If you do not specify a user type, this command displays IPoE session statistics for all types of IPv6 individual users.

dhcp: Specifies DHCP users.

ndrs: Specifies IPv6-ND-RS users.

static: Specifies static users.

unclassified-ip: Specifies unclassified-IP users.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays IPoE session statistics for IPv6 individual users for all interfaces.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPoE session statistics for IPv6 individual users for all member devices.

Examples

Display IPoE session statistics for IPv6 individual users on GigabitEthernet 1/0/1.

```
<Sysname> display ipv6 subscriber session statistics session-type dhcp interface
gigabitethernet 1/0/1
Total                : 100
Init                 : 0
Authenticating       : 20
Authenticate fail    : 0
Authenticate pass    : 20
Assigned IP          : 10
Online               : 50
Backup               : 0
```

Table 14 Command output

Field	Description
Total	Total number of users on the interface.
Init	Number of users who initiated sessions.
Authenticating	Number of users being authenticated.
Authenticate fail	Number of users who failed authentication.

Field	Description
Authenticate pass	Number of users who passed authentication.
Assigned IP	Number of users who have IP addresses.
Online	Number of online users.
Backup	Number of users whose information was backed up.

Related commands

reset ipv6 subscriber session

display ipv6 subscriber subnet-leased

Use **display ipv6 subscriber subnet-leased** to display information about IPv6 subnet-leased users.

Syntax

display ipv6 subscriber subnet-leased [**interface** *interface-type interface-number*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays information about IPv6 subnet-leased users for all interfaces.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about IPv6 subnet-leased users for all member devices.

Examples

Display information about the IPv6 subnet-leased user on GigabitEthernet 1/0/1.

```
<Sysname> display ipv6 subscriber subnet-leased interface gigabitethernet 1/0/1
Basic:
  Access interface           : GE1/0/1
  VPN instance               : N/A
  Username                   : a
  Network                    : 99::/64
  User ID                    : 0x40000001
  State                      : Online
  Service node               : Slot 1 CPU 0
  Domain                     : radius6
  Login time                 : May 14 20:22:14 2014
  Online time (hh:mm:ss)     : 00:16:37
```

```
AAA:
  IP pool                    : N/A
  Session idle time          : N/A
  Session duration           : N/A, remaining: N/A
  Remaining traffic          : N/A
  Max multicast addresses    : 4
  Multicast address list     : N/A

QoS:
  User profile               : nsfocus (active)
  Session group profile      : N/A
  Inbound CAR                : CIR 1000bps PIR 2000bps CBS 500bit (active)
  Outbound CAR               : CIR 3000bps PIR 4000bps CBS 500bit (active)

Flow statistic:
  Uplink   packets/bytes     : 0/0
  Downlink packets/bytes     : 0/0

ITA:
  Level-1 Uplink   packets/bytes: 0/0
          Downlink packets/bytes: 0/0
  Level-2 Uplink   packets/bytes: 0/0
          Downlink packets/bytes: 0/0
```

Table 15 Command output

Field	Description
Basic	Basic session information.
Access interface	Interface that connects the user.
VPN instance	MPLS L3VPN instance of the user. If the user is not in a VPN, this field displays **N/A**.
User name	Username for authentication.
Network	Subnet of the user.
User ID	User ID assigned after the user came online. If no user ID is assigned, this field displays **N/A**.
State	User state: • **Init**—The user is being initiated. • **Offline**—The user is going offline. • **Auth**—The user is being authenticated. • **AuthFail**—The user failed authentication. • **AuthPass**—The user passed authentication. • **AssignedIP**—The user has an IP address. • **Online**—The user is online. • **Backup**—Backup information about the user on the primary BRAS.
Service node	Slot number and CPU number of the card that connects the user.
Domain	ISP domain of the user.
Login time	Time when the user passed authentication and logged in, in the format of MM-DD

Field	Description
	hh:mm:ss YYYY.
Online time (hh:mm:ss)	Online duration for the user.
AAA	AAA authorization information.
IP pool	AAA-authorized DHCP address pool. If no DHCP address pool is authorized, this field displays **N/A**.
Session idle time	Idle time in seconds specified for online users. If the idle time expires, the user is logged out. If no idle time is specified, this field displays **N/A** and the user can remain idle without being logged out.
Session duration	AAA-authorized IPoE session duration in seconds: • **N/A**—No IPoE session duration is authorized. • **Unlimited**—The IPoE session duration is unlimited.
remaining	Remaining AAA-authorized IPoE session duration. If no session duration is authorized, this field displays **N/A**. ○ For users on Layer 3 Ethernet interfaces and subinterfaces, this field displays the remaining time or **Unlimited**. ○ For users on Layer 3 aggregate interfaces and subinterfaces, this field displays the remaining time or **Unlimited** only when the slot or interface is specified. If you do not specify the slot or interface, this field displays **N/A**.
Remaining traffic	Remaining AAA-authorized traffic in bytes. If no traffic is authorized, this field displays **N/A**.
Max multicast addresses	Maximum number of AAA-authorized multicast groups that a user can join.
Multicast address list	List of AAA-authorized multicast group addresses. If no multicast group is authorized, this field displays **N/A**.
QoS	QoS information.
User profile	AAA-authorized user profile: • **N/A**—No user profile is authorized. • **inactive**—User profile authorization failed or the user profile does not exist on the BRAS. • **active**—The user profile is authorized successfully. If the authorization result has not been updated, nothing is displayed.
Session group profile	AAA-authorized session group profile: • **N/A**—No session group profile is authorized. • **inactive**—Session group profile authorization failed or the session group profile does not exist on the BRAS. • **active**—The session group profile is authorized successfully. If the authorization result has not been updated, nothing is displayed.
Inbound CAR	Inbound CIR and PIR in bps and CBS in bits: • **N/A**—Inbound CAR is not authorized. • **inactive**—Inbound CAR is not authorized successfully. • **active**—Inbound CAR is authorized successfully.
Outbound CAR	Outbound CIR and PIR in bps and CBS in bits: • **N/A**—Outbound CAR is not authorized. • **inactive**—Outbound CAR is not authorized successfully. • **active**—Outbound CAR is authorized successfully.
Flow statistic	Session flow statistics.

Field	Description
Uplink packets/bytes	Total number and size of uplink packets.
Downlink packets/bytes	Total number and size of downlink packets.
ITA	Intelligent target accounting (ITA) information.
Level-*n* Uplink packets/bytes	Number and size of uplink packets for level *n* accounting (1 ≤ *n* ≤ 8).
Downlink packets/bytes	Number and size of downlink packets for level *n* accounting (1 ≤ *n* ≤ 8).

Related commands

ipv6 subscriber enable

display ipv6 subscriber subnet-leased statistics

Use **display ipv6 subscriber subnet-leased statistics** to display IPoE session statistics for IPv6 subnet-leased users.

Syntax

display ipv6 subscriber subnet-leased statistics [**interface** *interface-type interface-number*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays IPoE session statistics for IPv6 subnet-leased users for all interfaces.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPoE session statistics for IPv6 subnet-leased users for all member devices.

Examples

Display IPoE session statistics for IPv6 subnet-leased users on GigabitEthernet 1/0/1.

```
<Sysname> display ipv6 subscriber subnet-leased statistics interface gigabitethernet
1/0/1
Total               : 100
Init                : 0
Authenticating      : 20
Authenticate fail   : 0
Authenticate pass   : 20
Assigned IP         : 10
Online              : 50
```

```
Backup                : 0
```

Table 16 Command output

Field	Description
Total	Total number of users on the interface.
Init	Number of users who initiated sessions.
Authenticating	Number of users being authenticated.
Authenticate fail	Number of users who failed authentication.
Authenticate pass	Number of users who passed authentication.
Assigned IP	Number of users who have IP addresses.
Online	Number of online users.
Backup	Number of users whose information was backed up.

ipv6 subscriber 8021p

Use **ipv6 subscriber 8021p** to bind an ISP domain to an 802.1p list for IPv6 unclassified-IP users, static individual users, and leased users.

Use **undo ipv6 subscriber 8021p** to remove the binding between an ISP domain and an 802.1p list.

Syntax

ipv6 subscriber 8021p *8021p-list* **domain** *domain-name*

undo ipv6 subscriber 8021p *8021p-list*

Default

No ISP domain is bound to an 802.1p list for IPv6 unclassified-IP users, static individual users, and leased users.

Views

Layer 3 aggregate subinterface view

Layer 3 Ethernet subinterface view

Predefined user roles

network-admin

context-admin

Parameters

8021p-list: Specifies a space-separated list of up to eight 802.1p value items. Each item specifies a 802.1p value or a range of 802.1p values in the form of start-802.1p-value to end-802.1p-value. The 802.1p value is in the range of 0 to 7.

domain *domain-name*: Specifies an ISP domain name, a case-insensitive string of 1 to 255 characters. The name cannot contain the slash (/), back slash (\), vertical bar (|), quotation mark ("), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or at sign (@).

Usage guidelines

This command configures an ISP domain for IPv6 unclassified-IP users, static individual users, and leased users who send IP packets with the specified 802.1p values.

Examples

Configure ISP domain **1pdm** for IPv6 unclassified-IP users, static individual users, and leased users who send IP packets with the specified 802.1p values on GigabitEthernet 1/0/1.100. The specified 802.1p values are in the range of 2 to 5.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1.100
[Sysname-GigabitEthernet1/0/1.100] ipv6 subscriber service-identify 8021p second-vlan
[Sysname-GigabitEthernet1/0/1.100] ipv6 subscriber 8021p 2 to 5 domain 1pdm
```

Related commands

ipv6 subscriber service-identify

ipv6 subscriber access-user log enable

Use **ipv6 subscriber access-user log enable** to enable IPv6 IPoE user logging.

Use **undo ipv6 subscriber access-user log enable** to disable IPv6 IPoE user logging.

Syntax

ipv6 subscriber access-user log enable [**successful-login** | **failed-login** | **logout** [**normal**] [**abnormal**]] *

undo ipv6 subscriber access-user log enable [**successful-login** | **failed-login** | **logout** [**normal**] [**abnormal**]] *

Default

IPv6 IPoE user logging is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

successful-login: Specifies login success logs.

failed-login: Specifies login failure logs.

logout: Specifies logout logs.

normal: Specifies normal logout logs.

abnormal: Specifies abnormal logout logs.

Usage guidelines

IMPORTANT:

Typically, disable this feature to prevent excessive IPoE log output.

The IPv6 IPoE user logging feature enables the device to generate IPv6 IPoE logs and send them to the information center. Logs are generated after a user comes online successfully, fails to come online, normally goes offline, or abnormally goes offline. A log entry contains information such as the username, IP address, interface name, inner VLAN, outer VLAN, MAC address, and failure causes. For information about the log destination and output rule configuration in the information center, see *Network Management and Monitoring Configuration Guide*.

When you execute this command without specifying any keyword, this command enables or disables logging for login successes, login failures, normal logouts, and abnormal logouts.

Examples

Enable IPv6 IPoE user logging.

```
<Sysname> system-view
[Sysname] ip subscriber access-user log enable
```

ipv6 subscriber dhcp domain

Use **ipv6 subscriber dhcp domain** to configure an ISP domain for DHCPv6 users.

Use **undo ipv6 subscriber dhcp domain** to restore the default.

Syntax

ipv6 subscriber dhcp domain *domain-name*

undo ipv6 subscriber dhcp domain

Default

DHCPv6 users use the default system domain.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Parameters

domain *domain-name*: Specifies an ISP domain name, a case-insensitive string of 1 to 255 characters. The name cannot contain the slash (/), back slash (\), vertical bar (|), quotation mark ("), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or at sign (@).

Usage guidelines

This command specifies an ISP domain for DHCPv6 users. The specified ISP domain must exist on the BRAS.

If multiple ISP domains are available for an DHCPv6 user, the ISP domains are used in the following order:

1. Domain specified in Option 16 if the BRAS trusts Option 16 and Option 16 does not include null terminators and non-printable characters.
2. Domain specified by this command.
3. Default system domain.

Examples

Configure ISP domain **ipoe** for DHCPv6 users on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber dhcp domain ipoe
```

Related commands

ipv6 subscriber dhcp username

ipv6 subscriber initiator dhcp enable

ipv6 subscriber trust

ipv6 subscriber dhcp max-session

Use **ipv6 subscriber dhcp max-session** to configure the maximum number of IPoE sessions for DHCPv6 users on an interface.

Use **undo ip subscriber dhcp max-session** to restore the default.

Syntax

ipv6 subscriber dhcp max-session *max-number*

undo ipv6 subscriber dhcp max-session

Default

The maximum number of IPoE sessions for DHCPv6 users on an interface is not configured.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Parameters

max-number: Specifies the maximum number of IPoE sessions for DHCPv6 users. The value range for this argument is 1 to 64000.

Usage guidelines

If IPoE sessions for DHCPv6 users reach the maximum, no more IPoE session can be established for DHCPv6 users.

Examples

Set the maximum number of IPoE sessions to **100** for DHCPv6 users on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber dhcp max-session 100
```

Related commands

display ipv6 subscriber session

ipv6 subscriber initiator dhcp enable

reset ipv6 subscriber session

ipv6 subscriber dhcp password option16

Use **ipv6 subscriber dhcp password option16** to specify a string from Option 16 as the password for DHCPv6 users.

Use **undo ipv6 subscriber dhcp password option16** to restore the default.

Syntax

ipv6 subscriber dhcp password option16 [**offset** *offset*] [**length** *length*]

undo ipv6 subscriber dhcp password option16

Default

The BRAS does not use the password specified in Option 16 for DHCPv6 users.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Parameters

offset *offset*: Specifies an offset for the password starting byte, in the range of 1 to 63. If you do not specify this option, the first byte of the option is the starting byte.

length *length*: Specifies the length of the password string, in the range of 1 to 63. If you do not specify this option, all bytes following the starting byte are used as the password.

Usage guidelines

Passwords configured by using this command are used for authentication, and must be the same as those configured on the AAA server.

A DHCPv6 user can obtain a password in various ways. If multiple passwords are available for an DHCPv6 user, the passwords are used in the following order:

1. Password configured by using this command if the BRAS trusts Option 16 and Option 16 does not contain null terminators or non-printable characters.
2. Password configured by using the **ipv6 subscriber password** command.
3. Default password: **vlan**.

Examples

Specify the string with an offset of 10 and a length of 20 bytes from Option 16 as the password for DHCPv6 users.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber dhcp password option16 offset 10 length
20
```

Related commands

ipv6 subscriber initiator dhcp enable

ipv6 subscriber password

ipv6 subscriber trust

ipv6 subscriber dhcp username

ipv6 subscriber dhcp username

Use **ipv6 subscriber dhcp username** to configure an authentication user naming convention for DHCPv6 users.

Use **undo ipv6 subscriber dhcp username** to restore the default.

Syntax

ipv6 subscriber dhcp username include { **circuit-id** [**separator** *separator*] | **client-id** [**separator** *separator*] | **nas-port-id** [**separator** *separator*] | **port** [**separator** *separator*] | **remote-id** [**separator** *separator*] | **second-vlan** [**separator** *separator*] | **slot** [**separator** *separator*] | **source-mac** [**address-separator** *address-separator*] [**separator** *separator*] | **subslot** [**separator** *separator*] | **sysname** [**separator** *separator*] | **vendor-class** [**separator** *separator*] | **vendor-specific** [**separator** *separator*] | **vlan** [**separator** *separator*] } *

undo ipv6 subscriber dhcp username

Default

A DHCPv6 user uses its source MAC address as the authentication username.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Parameters

circuit-id: Includes the Option 18 information in a username.

client-id: Includes the Option 1 information in a username.

nas-port-id: Includes the NAS-Port-ID attribute carried in the authentication request packet in a username.

port: Includes the number of the port that receives the user packets in a username.

remote-id: Includes the Option 37 information in a username.

second-vlan: Includes the inner VLAN ID in a username.

slot: Includes the number of the slot that receives the user packets in a username.

source-mac: Includes the source MAC address in a username.

address-separator *address-separator*: Specifies any printable character as the separator for the MAC address. For example, if you specify a hyphen (-) as the separator, the username is the hyphen-separated MAC address (xxxx-xxxx-xxxx). If you do not specify a separator, the username is the non-separated MAC address (xxxxxxxxxxxx). Do not use the at sign (@) as the separator. The AAA server cannot parse a username containing the at sign (@).

subslot: Includes the number of the subslot that receives the user packets in a username.

sysname: Includes the name of the device that receives the user packets in a username.

vendor-class: Includes the Option 16 information in a username.

vendor-specific: Includes the Option 17 information in a username.

vlan: Includes the outer VLAN ID in a username.

separator *separator*: Specifies a character for separating an option and the option that follows. Do not use the at sign (@) as the separator. The AAA server cannot parse a username containing the at sign (@).

Usage guidelines

Usernames obtained based on the naming convention are used for authentication, authorization, and accounting, and must be the same as those configured on the AAA server.

You can specify one or more keywords in a naming convention. If you use a combination of keywords, a username obtained based on the naming convention includes the specified options in the configuration order.

Options used as the username information cannot include null terminators or non-printable characters.

Examples

Configure information carried in the **client-id** option as the authentication usernames for DHCPv6 users on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber dhcp username include client-id
```

Configure an authentication user naming convention for DHCPv6 users on GigabitEthernet 1/0/1. Each username contains the device name, slot number, subslot number, port number, and outer VLAN, separated by the pound sign (#).

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber dhcp username include sysname separator
# slot separator # subslot separator # port separator # vlan
```

Related commands

ipv6 subscriber initiator dhcp enable

ipv6 subscriber password

ipv6 subscriber dscp

Use **ipv6 subscriber dscp** to bind an ISP domain to a DSCP list for IPv6 unclassified-IP users, static individual users, and leased users.

Use **undo ipv6 subscriber dscp** to remove the binding between an ISP domain and a DSCP list.

Syntax

ipv6 subscriber dscp *dscp-value-list* **domain** *domain-name*

undo ipv6 subscriber dscp *dscp-value-list*

Default

No ISP domain is bound to a DSCP list for IPv6 unclassified-IP users, static individual users, and leased users.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Parameters

dscp-value-list: Specifies a space-separated list of up to eight DSCP value items. Each item specifies a DSCP value or a range of DSCP values in the form of start-DSCP-value to end-DSCP-value. The DSCP value is in the range of 0 to 63.

domain *domain-name*: Specifies an ISP domain name, a case-insensitive string of 1 to 255 characters. The name cannot contain the slash (/), back slash (\), vertical bar (|), quotation mark ("), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or at sign (@).

Usage guidelines

This command configures an ISP domain for IPv6 unclassified-IP users, static individual users, and leased users who send IP packets with the specified DSCP values.

Examples

Configure ISP domain **dscpdm** for IPv6 unclassified-IP users, static individual users, and leased users who send IP packets with the specified DSCP values on GigabitEthernet 1/0/1. The specified DSCP values are in the range of 1 to 4.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber service-identify dscp
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber dscp 1 to 4 domain dscpdm
```

Related commands

ipv6 subscriber service-identify

ipv6 subscriber enable

Use **ipv6 subscriber enable** to enable IPoE and configure an IPoE access mode for IPv6 users.

Use **undo ipv6 subscriber enable** to disable IPoE.

Syntax

ipv6 subscriber { **l2-connected** | **routed** } **enable**

undo ipv6 subscriber { **l2-connected** | **routed** } **enable**

Default

IPoE is disabled for IPv6 users.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Parameters

l2-connected: Specifies the Layer 2 access mode.

routed: Specifies the Layer 3 access mode.

Usage guidelines

All IPoE configurations take effect on an interface only when IPoE is enabled on the interface.

To change the IPoE access mode on an interface, you must disable IPoE, and then enable IPoE with a new IPoE access mode.

To ensure successful traffic statistics in aggregate interface view, use the **service** command to specify a service card for traffic statistics. For more information about the **service** command, see *Layer 2—LAN Switching Command Reference*.

Examples

Enable IPoE and configure the Layer 2 access mode for IPv6 users on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber l2-connected enable
```

Related commands

service (*Layer 2—LAN Switching Command Reference*)

ipv6 subscriber initiator dhcp enable

Use **ipv6 subscriber initiator dhcp enable** to enable the DHCPv6 user.

Use **undo ipv6 subscriber initiator dhcp enable** to disable the DHCPv6 user.

Syntax

ipv6 subscriber initiator dhcp enable

undo ipv6 subscriber initiator dhcp enable

Default

The DHCPv6 user is disabled.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Usage guidelines

If you enable the DHCP user, the first DHCP Solicitor or the DHCP Request packet initiates the IPoE session. If you disable the DHCP user, DHCP packets cannot initiate IPoE sessions, but existing IPoE sessions for DHCPv6 are not affected.

You can enable the DHCP user, IPv6-ND-RS user, and unclassified-IP user on the same interface.

Examples

Enable the DHCPv6 user on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber initiator dhcp enable
```

Related commands

display ipv6 subscriber session

ipv6 subscriber enable

ipv6 subscriber initiator ndrs enable

ipv6 subscriber initiator unclassified-ip enable

reset ipv6 subscriber session

ipv6 subscriber initiator ndrs enable

Use **ipv6 subscriber initiator ndrs enable** to enable the IPv6-ND-RS user.

Use **undo ipv6 subscriber initiator ndrs enable** to disable the IPv6-ND-RS user.

Syntax

ipv6 subscriber initiator ndrs enable

undo ipv6 subscriber initiator ndrs enable

Default

The IPv6-ND-RS user is disabled.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Usage guidelines

If you enable the IPV6-ND-RS user, the first IPv6 ND RS packet initiates the IPoE session. If you disable the IPV6-ND-RS user, IPv6 ND RS packets cannot initiate IPoE sessions, but existing IPoE sessions for IPv6-ND-RS are not affected.

You can enable the DHCP user, IPv6-ND-RS user, and unclassified-IP user on the same interface.

Examples

Enable the IPv6-ND-RS user on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber initiator ndrs enable
```

Related commands

display ipv6 subscriber session

ipv6 subscriber enable

ipv6 subscriber initiator dhcp enable

ipv6 subscriber initiator unclassified-ip enable

reset ipv6 subscriber session

ipv6 subscriber initiator unclassified-ip enable

Use **ipv6 subscriber initiator unclassified-ip enable** to enable the IPv6 unclassified-IP user.

Use **undo ipv6 subscriber initiator unclassified-ip enable** to disable the IPv6 unclassified-IP user.

Syntax

ipv6 subscriber initiator unclassified-ip enable

undo ipv6 subscriber initiator unclassified-ip enable

Default

The IPv6 unclassified-IP user is disabled.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Usage guidelines

If you enable the unclassified-IP user, the first IPv6 packet from a host initiates an IPoE session. If you disable the unclassified-IP user, IPv6 packets cannot initiate IPoE sessions, but existing IPoE sessions for IPv6 unclassified-IP are not affected.

You can enable the DHCP user, IPv6-ND-RS user, and unclassified-IP user on the same interface.

Examples

Enable the IPv6 unclassified-IP user on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber initiator unclassified-ip enable
```

Related commands

display ipv6 subscriber session

ipv6 subscriber enable

ipv6 subscriber initiator dhcp enable

ipv6 subscriber initiator ndrs enable

reset ipv6 subscriber session

ipv6 subscriber interface-leased

Use **ipv6 subscriber interface-leased** to configure IPv6 interface-leased users.

Use **undo ipv6 subscriber interface-leased** to restore the default.

Syntax

ipv6 subscriber interface-leased username *name* **password** { **ciphertext** | **plaintext** } *string* [**domain** *domain-name*]

undo ipv6 subscriber interface-leased

Default

No IPv6 interface-leased user exists.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Parameters

username *name*: Specifies a username for authentication, a case-sensitive string of 1 to 255 characters.

password ciphertext *string*: Specifies a ciphertext password, a case-sensitive string of 1 to 117 characters.

password plaintext *string*: Specifies a plaintext password, a case-sensitive string of 1 to 63 characters. For security purposes, the password specified in plaintext form will be stored in encrypted form.

domain *domain-name*: Specifies an ISP domain name, a case-insensitive string of 1 to 255 characters. The name cannot contain the slash (/), back slash (\), vertical bar (|), quotation mark ("), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or at sign (@). If you do not specify an ISP domain, the default system domain is used. For more information about the default system domain, see *Security Configuration Guide*.

Usage guidelines

An IPv6 interface-leased user is a group of IPv6 hosts that rent the same interface and share the same IPoE session. The BRAS authenticates, authorizes, and bills all hosts of the same interface-leased user.

You can configure only one IPv6 interface-leased user on each interface. To change the parameters of an existing IPv6 interface-leased user, use the undo form of the command to delete the user, and then reconfigure it with new parameter settings.

You cannot configure an interface-leased user on an interface configured with individual users or subnet-leased users.

Examples

Configure an IPv6 interface-leased user with a username of **intuser** and a plaintext password of **pw123** on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber interface-leased username intuser
password plaintext pw123
```

Related commands

display ipv6 subscriber interface-leased

ipv6 subscriber nas-port-id format

Use **ipv6 subscriber nas-port-id format** to configure NAS-Port-ID formats for IPv6 users.

Use **undo ipv6 subscriber nas-port-id format** to restore the default.

Syntax

ipv6 subscriber nas-port-id format cn-telecom { **version1.0** | **version2.0** }

undo ipv6 subscriber nas-port-id format

Default

NAS-Port-ID for IPv6 users is encapsulated in the format of version 1.0.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Parameters

`version 1.0`: Specifies the China Telecom format.

- The version 1.0 encapsulation format varies by interface type.

  Table 17 Version 1.0 encapsulation formats

Interface type	Encapsulation format
Layer 3 Ethernet interface and Layer 3 aggregate interface	slot=*slot_num*;subslot=*subslot_num*;port=*port_num*;vlanid=0
Layer 3 Ethernet subinterface and Layer 3 aggregate subinterface (single VLAN tag)	slot=*slot_num*;subslot=*subslot_num*;port=*port_num*;vlanid=*vlan_id*
Layer 3 Ethernet subinterface and Layer 3 aggregate subinterface (Dual VLAN tags)	*slot*=*slot_num*;subslot=*subslot_num*;port=*port_num*;vlanid=*inner-vlan*;vlanid2=*outer-vlan*
ATM-based virtual Layer 3 Ethernet interface (IPoEoA)	slot=*slot_num*;subslot=*subslot_num*;port=*port_num*;vpi=*vpi*;vci=*vci*

- Version 1.0 format parameters

  Table 18 Version 1.0 format parameter description

Parameter	Description
slot_num	Specifies the slot number of the access interface on the BRAS.
subslot_num	Specifies the subslot number of the access interface on the BRAS.
port_num	Specifies the port number of the access interface on the BRAS.
vlan_id	Specifies the ID of the user's VLAN.
inner-vlan	Specifies the ID of the inner VLAN.
outer-vlan	Specifies the ID of the outer VLAN.
vpi	Specifies the VPI of the access interface on the BRAS.
vci	Specifies the VCI of the access interface on the BRAS.

`version 2.0`: Specifies the format described in *`YDT 2275-2011 Subscriber Access Loop (Port) Identification in Broadband Access Networks`*.

- Version 2.0 encapsulation format:

  {eth | trunk | atm} NAS_slot/NAS_subslot/NAS_port:svlan.cvlan AccessNodeIdentifier/ANI_rack/ANI_frame/ANI_slot/ANI_subslot/ANI_port

- Version 2.0 format parameters:

Table 19 Version 2.0 format parameter description

Parameter	Description
{eth|trunk|atm}	Specifies the type of the access interface on the BRAS as Ethernet, trunk, or ATM.
NAS_slot	Specifies the slot number of the access interface on the BRAS.
NAS_subslot	Specifies the subslot number of the access interface on the BRAS.
NAS_port	Specifies the port number of the access interface on the BRAS.
svlan	Specifies the ID of the user's SVLAN.
cvlan	Specifies the ID of the user's CVLAN.
AccessNodeIdentifier	Specifies the identifier of the access node.
ANI_rack	Specifies the rack number of the access node.
ANI_frame	Specifies the frame number of the access node.
ANI_slot	Specifies the slot number of the access node.
ANI_subslot	Specifies the subslot number of the access node.
ANI_port	Specifies the port number of the access node.

Examples

Configure version 2.0 as the format for encapsulating NAS-Port-ID on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber nas-port-id format cn-telecom version2.0
```

Related commands

ipv6 subscriber initiator dhcp enable

ipv6 subscriber trust

ipv6 subscriber nas-port-id nasinfo-insert

ipv6 subscriber nas-port-id nasinfo-insert

Use **ipv6 subscriber nas-port-id nasinfo-insert** to include NAS information and information obtained from DHCPv6 Option 18 in NAS-Port-ID.

Use **undo ipv6 subscriber nas-port-id nasinfo-insert** to restore the default.

Syntax

ipv6 subscriber nas-port-id nasinfo-insert

undo ipv6 subscriber nas-port-id nasinfo-insert

Default

The BRAS uses information obtained from DHCPv6 Option 18 as NAS-Port-ID.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Usage guidelines

Configure version 2.0 format and the trusted DHCP option before you use this command.

- If DHCP packets contain Option 18, this command includes NAS information and the obtained option information in NAS-Port-ID. Option 18 is not affected.
- If DHCP packets do not contain Option 18, this command includes NAS information in NAS-Port-ID and sets non-NAS parts to zeros in the following format:

  NAS_slot/NAS_subslot/NAS_port:svlan.cvlan 0/0/0/0/0/0

Examples

Include NAS information and the obtained Option 18 information in NAS-Port-ID on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber nas-port-id format cn-telecom version2.0
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber trust option18
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber nas-port-id nasinfo-insert
```

Related commands

ipv6 subscriber initiator dhcp enable

ipv6 subscriber trust

ipv6 subscriber nas-port-id format

ipv6 subscriber nas-port-type

Use **ipv6 subscriber nas-port-type** to configure NAS-Port-Type for an IPv6 interface.

Use **undo ipv6 subscriber nas-port-type** to restore the default.

Syntax

ipv6 subscriber nas-port-type { **802.11** | **adsl-cap** | **adsl-dmt** | **async** | **cable** | **ethernet** | **g.3-fax** | **hdlc** | **idsl** | **isdn-async-v110** | **isdn-async-v120** | **isdn-sync** | **piafs** | **sdsl** | **sync** | **virtual** | **wireless-other** | **x.25** | **x.75** | **xdsl** }

undo ipv6 subscriber nas-port-type

Default

NAS-Port-Type for an IPv6 interface is Ethernet.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Parameters

802.11: Specifies the port type complying with Wireless-IEEE 802.11. The type ID is 19.

adsl-cap: Specifies the ADSL-CAP port type, including Asymmetric DSL and Carrierless Amplitude Phase Modulation. The type ID is 12.

adsl-dmt: Specifies the ADSL-DMT port type, including Asymmetric DSL and Discrete Multi-Tone. The type ID is 13.

async: Specifies the Async port type with a type ID of 0.

cable: Specifies the Cable port type with a type ID of 17.

ethernet: Specifies the Ethernet port type with a type ID of 15.

g.3-fax: Specifies the G.3 Fax port type with a type ID of 10.

hdlc: Specifies the HDLC port type with a type ID of 7.

idsl: Specifies the IDSL port type with a type ID of 14.

isdn-async-v110: Specifies the ISDN Async V.110 port type with a type ID of 4.

ISDN Async V.110: Specifies the ISDN Async V.120 port type with a type ID of 3.

isdn-sync: Specifies the ISDN Sync port type with a type ID of 2.

piafs: Specifies the port type complying with PIAFS. The type ID is 6.

sdsl: Specifies the SDSL port type with a type ID of 11.

sync: Specifies the Sync port type with a type ID of 1.

virtual: Specifies the Virtual port type with a type ID of 5.

wireless-other: Specifies the Wireless-other port type with a type ID of 18.

x.25: Specifies the X.25 port type with a type ID of 8.

x.75: Specifies the X.75 port type with a type ID of 9.

xdsl: Specifies the XDSL port type with a type ID of 16.

Usage guidelines

The NAS-Port-Type attribute carries information about the access interface. The BRAS includes the configured NAS-Port-Type in RADIUS requests sent to the RADIUS server.

Examples

Configure the port type as **sdsl** for IPv6 interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber nas-port-type sdsl
```

ipv6 subscriber ndrs domain

Use **ipv6 subscriber ndrs domain** to configure an ISP domain for IPv6-ND-RS users.

Use **undo ipv6 subscriber ndrs domain** to restore the default.

Syntax

ipv6 subscriber ndrs domain *domain-name*

undo ipv6 subscriber ndrs domain

Default

IPv6-ND-RS users use the default system ISP domain.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Parameters

domain *domain-name*: Specifies an ISP domain name, a case-insensitive string of 1 to 255 characters. The name cannot contain the slash (/), back slash (\), vertical bar (|), quotation mark ("), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or at sign (@).

Usage guidelines

This command specifies an ISP domain for IPv6-ND-RS users. The specified ISP domain must exist on the BRAS.

If you do not use this command to configure the ISP domain, the default system domain is used.

Examples

Configure ISP domain **ipoe** for IPv6-ND-RS users on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber ndrs domain ipoe
```

Related commands

ipv6 subscriber initiator ndrs enable

ipv6 subscriber ndrs max-session

Use **ipv6 subscriber ndrs max-session** to configure the maximum number of IPoE sessions for IPv6-ND-RS users on an interface.

Use **undo ipv6 subscriber ndrs max-session** to restore the default.

Syntax

ipv6 subscriber ndrs max-session *max-number*

undo ipv6 subscriber ndrs max-session

Default

The maximum number of IPoE sessions for IPv6-ND-RS users on an interface is not configured.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Parameters

max-number: Specifies the maximum number of IPoE sessions for IPv6-ND-RS users. The value range for this argument is 1 to 64000.

Usage guidelines

If IPoE sessions for IPv6-ND-RS user reach the maximum, no more IPoE session can be initiated IPv6 ND RS packets.

Examples

Set the maximum number of IPoE sessions to **100** for IPv6-ND-RS users on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber ndrs max-session 100
```

Related commands

display ipv6 subscriber session

ipv6 subscriber initiator ndrs enable

reset ipv6 subscriber session

ipv6 subscriber ndrs username

Use **ipv6 subscriber ndrs username** to configure an authentication user naming convention for IPv6-ND-RS users.

Use **undo ipv6 subscriber ndrs username** to restore the default.

Syntax

ipv6 subscriber ndrs username include { **nas-port-id** [**separator** *separator*] | **port** [**separator** *separator*] | **second-vlan** [**separator** *separator*] | **slot** [**separator** *separator*] | **source-mac** [**address-separator** *address-separator*] [**separator** *separator*] | **subslot** [**separator** *separator*] | **sysname** [**separator** *separator*] | **vlan** [**separator** *separator*] } *

undo ipv6 subscriber ndrs username

Default

An IPv6-ND-RS user uses its source MAC address as the authentication username.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Parameters

nas-port-id: Includes the NAS-Port-ID attribute in a username.

port: Includes the number of the port that receives the user packets in a username.

second-vlan: Includes the inner VLAN ID in a username.

slot: Includes the number of the slot that receives the user packets in a username.

source-mac: Includes the source MAC address in a username.

separator *separator*: Specifies any printable character as the separator for the MAC address. For example, if you specify a hyphen (-) as the separator, the username is the hyphen-separated MAC address (xxxx-xxxx-xxxx). If you do not specify a separator, the username is the non-separated MAC address (xxxxxxxxxxxx). Do not use the at sign (@) as the separator. The AAA server cannot parse a username containing the at sign (@).

subslot: Includes the number of the subslot that receives the user packets in a username.

sysname: Includes the name of the device that receives the user packets in a username.

vlan: Includes the outer VLAN ID in a username.

separator *separator*: Specifies a character for separating an option and the option that follows. Do not use the at sign (@) as the separator. The AAA server cannot parse a username containing the at sign (@).

Usage guidelines

Usernames obtained based on the naming convention are used for authentication and must be the same as those configured on the AAA server.

You can specify one or more keywords in a naming convention. If you use a combination of keywords, a username obtained based on the naming convention includes the specified options in the configuration order.

Examples

Configure the source MAC addresses as the authentication usernames for IPv6-ND-RS users on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber ndrs username include source-mac
```

Configure an authentication user naming convention for IPv6-ND-RS users on GigabitEthernet 1/0/1. Each username contains the device name, slot number, subslot number, port number, and outer VLAN, separated by the pound sign (#).

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber ndrs username include sysname separator
# slot separator # subslot separator # port separator # vlan
```

Related commands

ipv6 subscriber initiator ndrs enable

ipv6 subscriber password

ipv6 subscriber password

Use **ipv6 subscriber password** to configure passwords for IPv6 individual users.

Use **undo ipv6 subscriber password** to restore the default.

Syntax

ipv6 subscriber password { **ciphertext** | **plaintext** } *string*

undo ipv6 subscriber password

Default

The password for IPv6 individual users is **vlan**.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Usage guidelines

Passwords configured by this command are used for authentication, and must be the same as those configured on the AAA server.

A DHCPv6 user can obtain a password in various ways. For password priority, see "ipv6 subscriber dhcp password option16."

Parameters

ciphertext *string*: Specifies a ciphertext password, a case-sensitive string of 1 to 117 characters.

plaintext *string*: Specifies a plaintext password, a case-sensitive string of 1 to 63 characters. For security purposes, the password specified in plaintext form will be stored in encrypted form.

Examples

Configure the plaintext password as **123** for IPv6 individual users on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber password plaintext 123
```

Related commands

ipv6 subscriber dhcp username

ipv6 subscriber enable

ipv6 subscriber unclassified-ip username

ipv6 subscriber dhcp password option16

ipv6 subscriber service-identify

Use **ip subscriber service-identify** to configure service identifier for IPv6 unclassified-IP users, static individual users, and leased users.

Use **undo ipv6 subscriber service-identify** to restore the default.

Syntax

Layer 3 Ethernet interface view, Layer 3 aggregate interface view, L3VE interface view, VEth interface view:

ipv6 subscriber service-identify dscp

undo ipv6 subscriber service-identify

Layer 3 Ethernet subinterface view, Layer 3 aggregate subinterface view, L3VE subinterface view, VEth subinterface view:

ipv6 subscriber service-identify { **8021p** { **second-vlan** | **vlan** } | **dscp** | **second-vlan** | **vlan** }

undo ipv6 subscriber service-identify

VLAN interface view:

ipv6 subscriber service-identify { **8021p vlan** } | **dscp** | **vlan** }

undo ipv6 subscriber service-identify

Default

No service identifier is configured for IPv6 unclassified-IP users, static individual users, and leased users.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Parameters

8021p second-vlan: Specifies the 802.1p value of the inner VLAN tag in QinQ mode as the service identifier.

8021p vlan: Specifies the 802.1p value of the VLAN tag or the 802.1p value of the outer VLAN tag in QinQ mode as the service identifier.

dscp: Specifies the DSCP value as the service identifier.

second-vlan: Specifies the inner VLAN ID in QinQ mode as the service identifier.

vlan: Specifies the VLAN ID or the outer VLAN ID in QinQ mode as the service identifier.

Usage guidelines

You must specify an identifier for a service before you bind an ISP domain to the service. Otherwise, the binding does not take effect.

IPv6 unclassified-IP users, static individual users, and leased users whose IP packets containing the specified service identifier will be assigned a service-specific ISP domain.

You can configure only one service identifier on each interface.

Examples

Configure **dscp** as the service identifier on GigabitEthernet 1/0/1 for IPv6 unclassified-IP users, static individual users, and leased users.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber service-identify dscp
```

Related commands

ipv6 subscriber 8021p

ipv6 subscriber dscp

ipv6 subscriber vlan

ipv6 subscriber session static

Use **ipv6 subscriber session static** to configure IPv6 static IPoE sessions.

Use **undo ipv6 subscriber session static** to delete IPv6 static IPoE sessions.

Syntax

ipv6 subscriber session static ipv6 *ipv6-address* [**vlan** *vlan-id* [**second-vlan** *vlan-id*]] [**mac** *mac-address*] [**domain** *domain-name*] [**description** *string*]

undo ipv6 subscriber session static ipv6 *ipv6-address* [**vlan** *vlan-id* [**second-vlan** *vlan-id*]]

Default

No IPv6 static IPoE session exists.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Parameters

ip *ip-address*: Specifies a user IPv6 address.

vlan *vlan-id*: Specifies an outer VLAN ID of the user packet, in the range of 1 to 4094. This option is available only for subinterfaces.

second-vlan *vlan-id*: Specifies an inner VLAN ID of the user packet, in the range of 1 to 4094. This option is available only for subinterfaces.

mac *mac-address*: Specifies a user MAC address in the form of H-H-H.

domain *domain-name*: Specifies an ISP domain name, a case-insensitive string of 1 to 255 characters. The name cannot contain the slash (/), back slash (\), vertical bar (|), quotation mark ("), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or at sign (@). If you do not specify an ISP domain, the default system domain is used. For more information about the default system domain, see *Security Configuration Guide*.

description *string*: Specifies the static session description, a case-insensitive string of 1 to 31 characters. If this option is not specified, the static session does not have a description. The description cannot contain the following characters: forward slashes (/), backslashes (\), vertical bars (|), quotation marks ("), colons (:), asterisks (*), question marks (?), left angle brackets (<), right angle brackets (>), and at signs (@).

Usage guidelines

Static IPoE sessions have higher priority than dynamic IPoE sessions. If a user IP, DHCP, or ND RS packet matches a static IPoE session, the static IPoE session overwrites the existing dynamic IPoE session.

When the IPv6 address specified in a static session overlaps with the assignable IPv6 addresses in the DHCP address pool, you must use the **ipv6 dhcp server forbidden-address** command to exclude the overlapping IPv6 address in the DHCPv6 address pool from dynamic address allocation. For more information about excluding IPv6 addresses from dynamic allocation, see DHCPv6 configuration in *Layer 3—IP Services Configuration Guide*.

You can configure multiple static IPoE sessions on an interface. Static IPv6 IPoE sessions include the following types:

- A session with a specified IPv6 address.
- A session with a specified IPv6 address and outer VLAN ID.
- A session with a specified IPv6 address, outer VLAN ID, and inner VLAN ID.

For each session type, configuration fails if the settings are identical to the settings of an existing session.

To change the parameters of an existing IPoE session, use the undo form of the command to delete the session, and then reconfigure it with new parameter settings.

You cannot configure a static IPoE session on an interface configured with dedicated-interface or subnet-leased users.

Examples

Configure an IPv6 static IPoE session with an IP address of 2000::1 and an ISP domain of **dm1** on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber session static ipv6 2000::1 domain dm1
```

Related commands

display ipv6 subscriber session

ipv6 subscriber subnet-leased

Use **ipv6 subscriber subnet-leased** to configure IPv6 subnet-leased users.

Use **undo ipv6 subscriber subnet-leased** to delete IPv6 subnet-leased users.

Syntax

ipv6 subscriber subnet-leased ipv6 *ipv6-address prefix-length* **username** *name* **password** { **ciphertext** | **plaintext** } *string* [**domain** *domain-name*]

undo ipv6 subscriber subnet-leased ipv6 *ipv6-address prefix-length*

Default

No IPv6 subnet-leased user exists.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Parameters

ip *ip-address*: Specifies a user IPv6 address.

prefix-length: Specified the IPv6 prefix length in the range of 1 to 127.

username *name*: Specifies a username for authentication, a case-sensitive string of 1 to 255 characters.

password: Specifies a password for authentication.

ciphertext *string*: Specifies a ciphertext password, a case-sensitive string of 1 to 117 characters.

plaintext *string*: Specifies a plaintext password, a case-sensitive string of 1 to 63 characters. For security purposes, the password specified in plaintext form will be stored in encrypted form.

domain *domain-name*: Specifies an ISP domain name, a case-insensitive string of 1 to 255 characters. The name cannot contain the slash (/), back slash (\), vertical bar (|), quotation mark ("), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or at sign (@). If you do not specify an ISP domain, the default system domain is used. For more information about the default system domain, see *Security Configuration Guide*.

Usage guidelines

An IPv6 subnet-leased user is a group of IPv6 hosts that rent the same subnet of an interface and share the same IPoE session. The BRAS authenticates, authorizes, and bills all hosts of the same subnet-leased user.

You can configure only one IPv6 subnet-leased user on each subnet.

You cannot configure a subnet-leased user on an interface configured with individual users or interface-leased users.

Examples

Configure an IPv6 subnet-leased user with an IPv6 prefix of **2001:10::100**, prefix length of **64**, a username of **netuser,** and a plaintext password of **pw123** on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber subnet-leased ipv6 2001:10::100 64
username netuser password plaintext pw123
```

Related commands

display ipv6 subscriber subnet-leased

ipv6 subscriber timer quiet

Use **ipv6 subscriber timer quiet** to configure a quiet timer for IPv6 users.

Use **undo ipv6 subscriber timer quiet** to restore the default.

Syntax

ipv6 subscriber timer quiet *time*

undo ipv6 subscriber timer quiet

Default

No quite timer is configured for IPv6 users.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Parameters

time: Specifies the quiet timer in the range of 10 to 3600 seconds.

Usage guidelines

IPoE starts the quiet timer after a user fails authentication. It discards packets from the user during the quiet time. After the quiet timer expires, IPoE performs authentication upon receiving a packet from the user.

Examples

Set the quiet time to **100** seconds for IPv6 users on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber timer quiet 100
```

Related commands

ipv6 subscriber initiator dhcp enable

ipv6 subscriber initiator unclassified-ip enable

ipv6 subscriber trust

Use **ipv6 subscriber trust** to configure a trusted option for DHCPv6 users.

Use **undo ipv6 subscriber trust** to cancel a trusted option.

Syntax

ipv6 subscriber trust { **option16** | **option18** | **option37** }

undo ipv6 subscriber trust { **option16** | **option18** | **option37** }

Default

No trusted options are configured for DHCPv6 users.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Parameters

option16: Specifies Option 16 as the trusted option.

option18: Specifies Option 18 as the trusted option.

option37: Specifies Option 37 as the trusted option.

Usage guidelines

If the BRAS trusts DHCPv6 Option 16, the following option information is used as the ISP domain:

- All information in Option 16 if the option does not contain invalid characters or the at sign (@).

  Invalid characters include the slash (/), back slash (\), vertical bar (|), quotation mark ("), colon (:), asterisk (*), question mark (?), left angle bracket (<), and right angle bracket (>).
- Information that follows the last at sign (@) if the option contains at signs (@) and does not contain invalid characters.

If the BRAS does not trust DHCPv6 Option 16, the ISP domains are used in the following order:

1. Domain specified in the **ipv6 subscriber dhcp domain** command.
2. Default system domain.

If the BRAS trusts DHCPv6 Option 18 or Option 37, it obtains the following information from the option and uses the information to encapsulate RADIUS attributes:

- Obtains information from Option 18 and uses it to encapsulate NAS-Port-ID that adopts version 2.0 as the encapsulation format.
- Obtains information from Option 18 and uses it to encapsulate DSL_AGENT_CIRCUIT_ID.
- Obtains information from Option 37 and uses it to encapsulate DSL_AGENT_REMOTE_ID.

Examples

Configure DHCPv6 Option 18 as a trusted option on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber trust option18
```

Related commands

ipv6 subscriber dhcp domain

ipv6 subscriber initiator dhcp enable

ipv6 subscriber nas-port-id format

ipv6 subscriber nas-port-id nasinfo-insert

ipv6 subscriber unclassified-ip domain

Use **ipv6 subscriber unclassified-ip domain** to configure an ISP domain for IPv6 unclassified-IP users, static individual users, and leased users.

Use **undo ipv6 subscriber unclassified-ip domain** to restore the default.

Syntax

ipv6 subscriber unclassified-ip domain *domain-name*

undo ipv6 subscriber unclassified-ip domain

Default

IPv6 unclassified-IP users, static individual users, and leased users use the default system ISP domain.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Parameters

domain *domain-name*: Specifies an ISP domain name, a case-insensitive string of 1 to 255 characters. The name cannot contain the slash (/), back slash (\), vertical bar (|), quotation mark ("), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or at sign (@).

Usage guidelines

This command configures an ISP domain for IPv6 unclassified-IP users, static individual users, and leased users. The configured ISP domain must exist on the BRAS.

The BRAS selects an ISP domain for an IPv6 unclassified-IP user, static individual user, or leased user in the following order:

1. Service-specific domain.
2. Domain specified by this command.
3. Default system domain.

Examples

Configure ISP domain **ipoe** for IPv6 unclassified-IP users, static individual users, and leased users on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber unclassified-ip domain ipoe
```

Related commands

ipv6 subscriber initiator unclassified-ip enable

ipv6 subscriber service-identify

ipv6 subscriber unclassified-ip max-session

Use **ipv6 subscriber unclassified-ip max-session** to configure the maximum number of IPoE sessions for IPv6 unclassified-IP users on an interface.

Use **undo ipv6 subscriber unclassified-ip max-session** to restore the default.

Syntax

ipv6 subscriber unclassified-ip max-session *max-number*

undo ipv6 subscriber unclassified-ip max-session

Default

The maximum number of IPoE sessions for IPv6 unclassified-IP users on an interface is not configured.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Parameters

max-number: Specifies the maximum number of IPoE sessions for IPv6 unclassified-IP users. The value range for this argument is 1 to 64000.

Usage guidelines

If IPoE sessions for IPv6 unclassified-IP users reach the maximum, no more IPoE session can be initiated for IPv6 unclassified-IP users.

Examples

Set the maximum number of IPoE sessions to **100** for IPv6 unclassified-IP users on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber unclassified-ip max-session 100
```

Related commands

display ipv6 subscriber session

ipv6 subscriber initiator unclassified-ip enable

reset ipv6 subscriber session

ipv6 subscriber unclassified-ip username

Use **ipv6 subscriber unclassified-ip username** to configure an authentication user naming convention for IPv6 unclassified-IP users and static individual users.

Use **undo ipv6 subscriber unclassified-ip username** to restore the default.

Syntax

ipv6 subscriber unclassified-ip username include { **nas-port-id** [**separator** *separator*] | **port** [**separator** *separator*] | **second-vlan** [**separator** *separator*] | **slot** [**separator** *separator*] | **source-ip** [**address-separator** *address-separator*] [**separator** *separator*] | **source-mac** [**address-separator** *address-separator*] [**separator** *separator*] | **subslot** [**separator** *separator*] | **sysname** [**separator** *separator*] | **vlan** [**separator** *separator*] } *

undo ipv6 subscriber unclassified-ip username

Default

An IPv6 unclassified-IP user or static individual user uses its source IPv6 address as the authentication username.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Parameters

nas-port-id: Includes the NAS-Port-ID attribute in a username.

port: Includes the number of the port that receives the user packets in a username.

second-vlan: Includes the inner VLAN ID in a username.

slot: Includes the number of the slot that receives the user packets in a username.

source-ip: Includes the source IP address in a username.

address-separator *address-separator*: Specifies any printable character as the separator for the IPv6 address. For example, if you specify a hyphen (-) as the separator, the username is the hyphen-separated IPv6 address (x-x-x). If you do not specify a separator, the username is the colon-separated IPv6 address (x::x:x). Do not use the at sign (@) as the separator. The AAA server cannot parse a username containing the at sign (@).

source-mac: Includes the source MAC address in a username.

address-separator *address-separator*: Specifies any printable character as the separator for the MAC address. For example, if you specify a hyphen (-) as the separator, the username is the hyphen-separated MAC address (xxxx-xxxx-xxxx). If you do not specify a separator, the username is the non-separated MAC address (xxxxxxxxxxxx). Do not use the at sign (@) as the separator. The AAA server cannot parse a username containing the at sign (@).

subslot: Includes the number of the subslot that receives the user packets in a username.

sysname: Includes the name of the device that receives the user packets in a username.

vlan: Includes the outer VLAN ID in a username.

separator *separator*: Specifies a character for separating an option and the option that follows. Do not use the at sign (@) as the separator. The AAA server cannot parse a username containing the at sign (@).

Usage guidelines

Usernames obtained based on the naming convention are used for authentication and must be the same as those configured on the AAA server.

You can specify one or more keywords in a naming convention. If you use a combination of keywords, a username obtained based on the naming convention includes the specified options in the configuration order.

Examples

Configure the source IPv6 addresses as the authentication usernames for IPv6 unclassified-IP users and static individual users on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber unclassified-ip username include
source-ip
```

Configure an authentication user naming convention for IPv6 unclassified-IP users and static individual users on GigabitEthernet 1/0/1. Each username contains the device name, slot number, subslot number, port number, and outer VLAN, separated by the pound sign (#).

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber unclassified-ip username include sysname
separator # slot separator # subslot separator # port separator # vlan
```

Related commands

ipv6 subscriber initiator unclassified-ip enable

ipv6 subscriber password

ipv6 subscriber user-detect

Use **ipv6 subscriber user-detect** to configure online detection for IPv6 individual users.

Use **undo ipv6 subscriber user-detect** to restore the default.

Syntax

ipv6 subscriber user-detect { **icmpv6** | **nd** } **retry** *retries* **interval** *interval*

undo ipv6 subscriber user-detect

Default

Online detection for IPv6 individual users is disabled.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Parameters

icmpv6: Specifies the ICMPv6 request packet as detection packets.

nd: Specifies the NS packet of the ND protocol as detection packets.

retry *retries*: Specifies the maximum number of detection attempts following the first detection attempt, in the range of 2 to 5.

interval *interval*: Configures the detection timer in the range of 30 to 1200 seconds.

Usage guidelines

Online detection enables the BRAS to periodically detect the status of an IPv6 individual user. It uses NS requests of the ND protocol and ICMPv6 requests to detect IPv6 individual users. If IPv6 individual users and the interface are in different subnets, only ICMPv6 request packets can be used for detection.

After you configure online detection, the BRAS starts a detection timer to detect online users. If the BRAS does not receive user packets before the detection timer expires, it sends a detection packet to the user.

- If the BRAS receives user packets within the maximum detection attempts, the BRAS assumes that the user is online. It resets the detection timer, and starts the next detection attempt.
- If the BRAS does not receive user packets after detection attempts reach the maximum, the BRAS assumes that the user is offline and deletes the user session.

Examples

Configure online detection on GigabitEthernet 1/0/1. The maximum number of detection attempts is **3**, the detection timer is **50** seconds, and the detection packet type is **ND.**

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber user-detect nd retry 3 interval 50
```

Related commands

ipv6 subscriber enable

ipv6 subscriber vlan

Use **ipv6 subscriber vlan** to bind an ISP domain to a VLAN list for IPv6 unclassified-IP users, static individual users, and leased users.

Use **undo ipv6 subscriber vlan** to remove the binding between an ISP domain and a VLAN list.

Syntax

ipv6 subscriber vlan *vlan-list* **domain** *domain-name*

undo ipv6 subscriber vlan *vlan-list*

Default

No ISP domain is bound to a VLAN list for IPv6 unclassified-IP users, static individual users, and leased users.

Views

Layer 3 aggregate subinterface view

Layer 3 Ethernet subinterface view

L3VE subinterface view

VEth subinterface view

VLAN interface view

Predefined user roles

network-admin

context-admin

Parameters

vlan-list: Specifies a space-separated list of up to 10 VLAN ID items. Each item specifies a VLAN by its ID or a range of VLANs in the form of start-VLAN-ID to end-VLAN-ID. The VLAN ID is in the range of 1 to 4094.

domain *domain-name*: Specifies an ISP domain name, a case-insensitive string of 1 to 255 characters. The name cannot contain the slash (/), back slash (\), vertical bar (|), quotation mark ("), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or at sign (@).

Usage guidelines

This command configures an ISP domain for IPv6 unclassified-IP users, static individual users, and leased users who send IP packets with the specified VLAN IDs.

Examples

Configure ISP domain **vlandm** for IPv6 users who send IP packets with the specified VLAN IDs on GigabitEthernet 1/0/1.100. The specified VLAN IDs are in the range of 2 to 100.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1.100
[Sysname-GigabitEthernet1/0/1.100] ipv6 subscriber service-identify second-vlan
[Sysname-GigabitEthernet1/0/1.100] ipv6 subscriber vlan 2 to 100 domain vlandm
```

Related commands

ipv6 subscriber service-identify

ipv6 subscriber whitelist enable

Use **ipv6 subscriber whitelist enable** to enable the IPv6 IPoE whitelist feature.

Use **undo ipv6 subscriber whitelist enable** to disable the IPv6 IPoE whitelist feature.

Syntax

ipv6 subscriber whitelist enable

undo ipv6 subscriber whitelist enable

Default

The IPv6 IPoE whitelist feature is disabled.

Views

Layer 3 aggregate interface/subinterface view

Layer 3 Ethernet interface/subinterface view

Predefined user roles

network-admin

context-admin

Usage guidelines

With this feature enabled, only IPv6 traffic matching static IPv6 IPoE sessions can initiate IPoE authentication, and IPoE directly permits the other traffic without any processing.

In some scenarios, an interface might need to have both IPoE and portal authentication enabled. For example, both dumb terminals and broadband dial-up users exist on an interface. Dumb terminals

(for example, monitoring cameras) need to come online through IPoE without portal authentication, and broadband dial-up users need to come online through portal Web authentication. In this case, you can enable the IPv6 IPoE whitelist feature on the interface. When both the IPv6 IPoE whitelist feature and portal authentication are enabled on an interface, the following rules apply:

- If the IPv6 traffic of a user matches a static IPv6 IPoE session, the user is processed by the static IPv6 IPoE authentication flow. For an IPoE user to bypass authentication, specify the authentication and authorization modes as **none** in the ISP domain of the IPoE user.
- If the IPv6 traffic of a user does not match any IPv6 IPoE session, the user is processed by portal authentication.

Examples

Enable the IPv6 IPoE whitelist feature on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber whitelist enable
```

reset ipv6 subscriber offline statistics

Use **reset ipv6 subscriber offline statistics** to remove offline statistics for IPv6 users.

Syntax

reset ipv6 subscriber offline statistics [**interface** *interface-type interface-number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command removes offline statistics for IPv6 users for all interfaces.

Examples

Remove offline statistics for all IPv6 users on GigabitEthernet1/0/1.

```
<Sysname> reset ipv6 subscriber offline statistics
```

Related commands

display ipv6 subscriber offline statistics

reset ipv6 subscriber session

Use **reset ipv6 subscriber session** to delete dynamic IPv6 IPoE sessions and log out users.

Syntax

reset ipv6 subscriber session [**interface** *interface-type interface-number*] [**domain** *domain-name* | **ipv6** *ipv6-address* [**vpn-instance** *vpn-instance-name*] | **mac** *mac-address* | **username** *name*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command deletes dynamic IPv6 IPoE sessions for all interfaces.

domain *domain-name*: Specifies an ISP domain name, a case-insensitive string of 1 to 255 characters. The name cannot contain the slash (/), back slash (\), vertical bar (|), quotation mark ("), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or at sign (@).

ipv6 *ipv6-address*: Specifies the IPv6 address of the IPoE session to be deleted.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command deletes IPv6 IPoE sessions on the public network.

mac *mac-address*: Specifies the MAC address of an IPv6 IPoE session to be deleted, in the format of H-H-H.

username *name*: Specifies the username of the IPv6 IPoE session to be deleted, a case-sensitive string of 1 to 255 characters.

Usage guidelines

If you do not specify any parameters, this command deletes all dynamic IPv6 IPoE sessions.

To delete static IPoE sessions for static users and leased users, use the **undo** commands.

Examples

Delete dynamic IPv6 IPoE sessions and log out users on GigabitEthernet 1/0/1.

```
<Sysname> reset ipv6 subscriber session interface gigabitethernet 1/0/1
```

Related commands

display ipv6 subscriber session

Contents

Public key management commands

display public-key local public

Use **display public-key local public** to display local public keys.

Syntax

display public-key local { **dsa** | **ecdsa** | **rsa** | **sm2** } **public** [**name** *key-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

dsa: Specifies the DSA key pair type.

ecdsa: Specifies the ECDSA key pair type.

rsa: Specifies the RSA key pair type.

sm2: Specifies the SM2 key pair type.

name *key-name*: Specifies a local key pair by its name, a case-insensitive string of 1 to 64 characters. Valid characters are letters, digits, and hyphens (-). If you do not specify a key pair, this command displays the public keys of all local key pairs of the specified type.

Usage guidelines

You can copy and distribute the public key of a local key pair to peer devices.

You cannot display a host public key that has the default key pair name by specifying the **name** *key-name* option. To view a host public key that has the default key pair name, display all local public keys by using this command without specifying a key pair name.

Examples

Display all local RSA public keys.

```
<Sysname> display public-key local rsa public

=============================================
Key name: hostkey (default)
Key type: RSA
Key length: 1024
Time when key pair created: 15:40:48 2011/05/12
Key code:
   30819F300D06092A864886F70D010101050003818D0030818902818100DAA4AAFEFE04C2C9
   667269BB8226E26331E30F41A8FF922C7338208097E84332610632B49F75DABF6D871B80CE
   C1BA2B75020077C74745C933E2F390DC0B39D35B88283D700A163BB309B19F8F87216A44AB
   FBF6A3D64DEB33E5CEBF2BCF26296778A26A84F4F4C5DBF8B656ACFA62CD96863474899BC1
```

```
   2DA4C04EF5AE0835090203010001
=========================================
Key name: serverkey (default)
Key type: RSA
Key length: 768
Time when key pair created: 15:40:48 2011/05/12
Key code:
   307C300D06092A864886F70D0101010500036B003068026100CAB4CACCA16442AD5F453442
   762F03897E0D494FEDE69224F5C051A441D290976733A278C9F0C0F5A198E66143EAB54A64
   DB608269CAE844B1E7CC64AD7E808972E7CF887F3B657F056E7930FC84FBF1AD83A01CC47E
   9D85C13413996ECD093B0203010001
=========================================
Key name: rsa1
Key type: RSA
Key length: 1024
Time when key pair created: 15:42:26 2011/05/12
Key code:
   30819F300D06092A864886F70D010101050003818D003081890281810 0DEBC46F217DDF11D
   426E7095AA45CD6BF1F87343D952569AC223A01365E0D8C91D49D347C143C5D8FAADA896AA
   1A827E580F2502F1926F52197230E1DE391A64015C43DD79DC4E9E171BAEA1DEB4C71DAED7
   9A6EDFD460D8945D27D39B7C9822D56AEA5B7C2CCFF1B6BC524AD498C3B87D4BD6EB36AF03
   92D8C6D940890BF4290203010001
```

Display all local DSA public keys.

```
<Sysname> display public-key local dsa public

=========================================
Key name: dsakey (default)
Key type: DSA
Key length: 1024
Time when key pair created: 15:41:37 2011/05/12
Key code:
   308201B73082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD
   96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
   DBD13EC8B274DA9F75BA26CCB9877236027 87E922BA84421F22C3C89CB9B06FD60FE01941D
   DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
   7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
   4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
   35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
   91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
   585DA7F42519718CC9B09EEF0381840002818041912CE34D12BCD2157E7AB1C2F03B3EF395
   100F3DB4A9E2FDFE860C1BD663D676438F7DA40A9406D61CA9079AF13E330489F1C76785DE
   52DA649AC8BC04B6D39CD7C52CD0A14F75F7491A91D31D6AC22340B5981B27A915CDEC4F09
   887E541EC1E5302D500F68E7AC29A084463C60F9EE266985A502FC92193E1CF4D265C4BA
=========================================
Key name: dsa1
Key type: DSA
Key length: 1024
Time when key pair created: 15:35:42 2011/05/12
```

```
Key code:
   308201B83082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD
   96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
   DBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941D
   DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
   7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
   4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
   35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
   91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
   585DA7F42519718CC9B09EEF0381850002818100A1E456C8DA2AD1BB83B1BDF2A1A6B5A6E8
   3642B460402445DA7E4036715F468F76655E114D460B7112F57143EE020AEF4A5BFAD07B74
   0FBCB1C64DA8A2BCE619283421445EEC77D3CF0D11866E9656AD6511F4926F8376967B0AB7
   15F9FB7B514BC1174155DD6E073B1FCB3A2749E6C5FEA81003E16729497D0EAD9105E3E76A
```

Display all local ECDSA public keys.

```
<Sysname> display public-key local ecdsa public

==============================================
Key name: ecdsakey (default)
Key type: ECDSA
Key length: 192
Time when key pair created: 15:42:04 2011/05/12
Key code:
   3049301306072A8648CE3D020106082A8648CE3D03010103320004C10CF7CE42193F7FC2AF
   68F5DC877835A43009DB6135558A7FB8316C361B0690B4FD84A14C0779C76DD6145BF9362B
   1D
==============================================
Key name: ecdsa1
Key type: ECDSA
Key length: 192
Time when key pair created: 15:43:33 2011/05/12
Key code:
   3049301306072A8648CE3D020106082A8648CE3D03010103320004A1FB84D92315B8DB72D1
   AE672C7CFA5135D5F5B02377F2F092F182EC83B5819795BC94CCBD3EBA7D4F0F2B2EB20C58
   4D
```

Display the public keys of all local SM2 key pairs.

```
<Sysname> display public-key local sm2 public

==============================================
Key name: sm2key (default)
Key type: SM2
Key length: 256
Time when key pair created: 15:42:04 2016/08/15
Key code:
   3059301306072A8648CE3D020106082A811CCF5501822D03420004DC5D3CCDD4F5E7AC9803
   D7F55ADC0668C067859482999C390B1648BE91FB567150A6C909706BB04AFE8709D5EC884C
   BD4EE36F38E8AD7DBCFB52286BF22CB146
==============================================
Key name: sm21
```

```
Key type: SM2
Key length: 256
Time when key pair created: 15:43:33 2016/08/15
Key code:
   3059301306072A8648CE3D020106082A811CCF5501822D034200047A8EF255A75A90FA9239
   1B2BDD58B6F19E7D0158200E80297E434109A68A66160A20B5267ECB1706CA50A7ED04A89A
   007AFEFF8335441347EB2EB69CFB4CD459
```

Display the public key of local RSA key pair **rsa1**.

```
<Sysname> display public-key local rsa public name rsa1

=============================================
Key name: rsa1
Key type: RSA
Key length: 1024
Time when key pair created: 15:42:26 2011/05/12
Key code:
   30819F300D06092A864886F70D010101050003818D0030818902818100DEBC46F217DDF11D
   426E7095AA45CD6BF1F87343D952569AC223A01365E0D8C91D49D347C143C5D8FAADA896AA
   1A827E580F2502F1926F52197230E1DE391A64015C43DD79DC4E9E171BAEA1DEB4C71DAED7
   9A6EDFD460D8945D27D39B7C9822D56AEA5B7C2CCFF1B6BC524AD498C3B87D4BD6EB36AF03
   92D8C6D940890BF4290203010001
```

Display the public key of local DSA key pair **dsa1**.

```
<Sysname> display public-key local dsa public name dsa1

=============================================
Key name: dsa1
Key type: DSA
Key length: 1024
Time when key pair created: 15:35:42 2011/05/12
Key code:
   308201B83082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD
   96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
   DBD13EC8B274DA9F75BA26CCB9877236027787E922BA84421F22C3C89CB9B06FD60FE01941D
   DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
   7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
   4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
   35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
   91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
   585DA7F42519718CC9B09EEF0381850002818100A1E456C8DA2AD1BB83B1BDF2A1A6B5A6E8
   3642B460402445DA7E4036715F468F76655E114D460B7112F57143EE020AEF4A5BFAD07B74
   0FBCB1C64DA8A2BCE619283421445EEC77D3CF0D11866E9656AD6511F4926F8376967B0AB7
   15F9FB7B514BC1174155DD6E073B1FCB3A2749E6C5FEA81003E16729497D0EAD9105E3E76A
```

Display the public key of the local ECDSA key pair **ecdsa1**.

```
<Sysname> display public-key local ecdsa public name ecdsa1

=============================================
Key name: ecdsa1
Key type: ECDSA
```

```
Key length: 192
Time when key pair created: 15:43:33 2011/05/12
Key code:
   3049301306072A8648CE3D020106082A8648CE3D03010103320004A1FB84D92315B8DB72D1
   AE672C7CFA5135D5F5B02377F2F092F182EC83B5819795BC94CCBD3EBA7D4F0F2B2EB20C58
   4D
```

Display the public key of local SM2 key pair **sm21**.

```
<Sysname> display public-key local sm2 public name sm21
=========================================
Key name: sm21
Key type: SM2
Key length: 256
Time when key pair created: 15:43:33 2016/08/15
Key code:
   3059301306072A8648CE3D020106082A811CCF5501822D034200047A8EF255A75A90FA9239
   1B2BDD58B6F19E7D0158200E80297E434109A68A66160A20B5267ECB1706CA50A7ED04A89A
   007AFEFF8335441347EB2EB69CFB4CD459
```

Display the public key of SM2 key pair **sm-hardware** (created by a hardware crypto device).

```
<Sysname> display public-key local sm2 public name sm2-hardware

=========================================
Key name: sm2-hardware
Key type: SM2
Key length: 256
Storage device serial number: 2016091400125014
Time when key pair created: 08:52:02 2017/09/06
Key code:
   043685DF5943674D61D096D3218C235728467ED4699893777EB2D4D77D302B44DC87C587A0
   7A9EC72802BCB13EFAF77E0E744FB49FA8C2A23BCDE7BB1E91462697
```

Table 1 Command output

Field	Description
Key name	Name of the local key pair. If you did not specify a name when creating the key pair, the default name is used followed by the word **default** in brackets. The following is the default key pair name for each key algorithm: • **hostkey**—Default RSA host key pair name. • **serverkey**—Default RSA server key pair name. • **dsakey**—Default DSA host key pair name. • **ecdsakey**—Default ECDSA host key pair name. • **sm2key**—Default SM2 host key pair name.
Key type	Options include: • RSA. • DSA. • ECDSA. • SM2.
Key length	Key length in bits.

Field	Description
Storage device serial number	Serial number of the crypto device that generated the key pair. This field is not displayed if the key pair is created by a software algorithm.
Time when key pair created	Date and time when the local key pair was created.
Key code	Public key string.

Related commands

public-key local create

display public-key peer

Use **display public-key peer** to display information about peer host public keys.

Syntax

display public-key peer [**brief** | **name** *publickey-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

brief: Displays brief information about all peer host public keys. The brief information includes only the key type, key modulus, and key name.

name *publickey-name*: Displays detailed information about a peer host public key, including its key code. The *publickey-name* argument specifies a peer host public by its name, a case-sensitive string of 1 to 64 characters.

Usage guidelines

If you do not specify any keywords, this command displays detailed information about all peer host public keys configured on the local device.

You can use the **public-key peer** command or the **public-key peer import sshkey** command to configure a peer host public key on the local device.

Examples

Display detailed information about peer host public key **idrsa**.

```
<Sysname> display public-key peer name idrsa

=========================================
Key name: idrsa
Key type: RSA
Key length: 1024
Key code:
   30819F300D06092A864886F70D010101050003818D0030818902818100C5971581A78B5388
   B3C9063EC6B53D395A6704D9752B6F9B7B1F734EEB5DD509F0B050662C46FFB8D27F797E37
```

```
918F6270C5793F1FC63638970A0E4D51A3CEF7CFF6E92BFAFD73F530E0BDE27056E81F2525
6D0883836FD8E68031B2C272FE2EA75C87734A7B8F85B8EBEB3BD51CC26916AF3B3FDC32C3
42C142D41BB4884FEB0203010001
```

Table 2 Command output

Field	Description
Key name	Name of the peer host public key.
Key type	Key type: RSA, DSA or ECDSA.
Key length	Key length in bits.
Key code	Public key string.

Display brief information about all peer host public keys.

```
<Sysname> display public-key peer brief
Type  Modulus  Name
--------------------------
RSA   1024    idrsa
DSA   1024    10.1.1.1
```

Table 3 Command output

Field	Description
Type	Key type: RSA, DSA or ECDSA.
Modulus	Key modulus length in bits.
Name	Name of the peer host public key.

Related commands

public-key peer

public-key peer import sshkey

peer-public-key end

Use **peer-public-key end** to return from public key view to system view and save the configured peer host public key.

Syntax

peer-public-key end

Views

Public key view

Predefined user roles

network-admin

context-admin

Usage guidelines

After you type the peer host public key on the local device, use this command to exit public key view and to save the peer host public key.

The system verifies the public key before saving it. If the key is not in the correct format, the system discards the key and displays an error message. If the key is valid, for example, the key was displayed by the **display public-key local public** command, the system saves the key.

Examples

Exit public key view and save the configured peer host public key.

```
<Sysname> system-view
[Sysname] public-key peer key1
Enter public key view. Return to system view with "peer-public-key end" command.
[Sysname-pkey-public-key-key1]30819F300D06092A864886F70D010101050003818D0030818902818
100C0EC8014F82515F6335A0A
[Sysname-pkey-public-key-key1]EF8F999C01EC94E5760A079BD73E4F4D97F3500EDB308C29481B77E
719D1643135877E13B1C531B4
[Sysname-pkey-public-key-key1]FF1877A5E2E7B1FA4710DB0744F66F6600EEFE166F1B854E2371D5B
952ADF6B80EB5F52698FCF3D6
[Sysname-pkey-public-key-key1]1F0C2EAAD9813ECB16C5C7DC09812D4EE3E9A0B074276FFD4AF2050
BD4A9B1DDE675AC30CB020301
[Sysname-pkey-public-key-key1]0001
[Sysname-pkey-public-key-key1] peer-public-key end
[Sysname]
```

Related commands

display public-key local public

display public-key peer

public-key peer

public-key local create

Use **public-key local create** to create local key pairs.

Syntax

public-key local create { **dsa** | **ecdsa** [**secp192r1** | **secp256r1** | **secp384r1** | **secp521r1**] | **rsa** } [**name** *key-name*]

public-key local create sm2 [**name** *key-name*] [**on** *device-name*]

Default

No local key pairs exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

dsa: Specifies the DSA key pair type.

ecdsa: Specifies the ECDSA key pair type.

- **secp192r1**: Uses the secp192r1 curve to create a 192-bit ECDSA key pair.
- **secp256r1**: Uses the secp256r1 curve to create a 256-bit ECDSA key pair.

- **secp384r1**: Uses the secp384r1 curve to create a 384-bit ECDSA key pair.
- **secp521r1**: Uses the secp521r1 curve to create a 521-bit ECDSA key pair.

By default, the secp192r1 curve is used.

rsa: Specifies the RSA key pair type.

sm2: Specifies the SM2 key pair type.

name *key-name*: Assigns a name to the key pair. The *key-name* argument is a case-insensitive string of 1 to 64 characters. Valid characters are letters, digits, and hyphens (-). If you do not assign a name to the key pair, the key pair takes the default name (see Table 4).

on *device-name*: Specifies the crypto device to be used to generate the SM2 key pair. The *device-name* argument specifies the device name, a case-sensitive string of 1 to 31 characters. If you do not specify a crypto device, the SM2 key pair will be created by a software algorithm. You can view the names of available crypto devices by entering a question mark (?) after the **on** keyword.

Table 4 Default local key pair names

Type	Default name
RSA	• Host key pair: **hostkey** • Server key pair: **serverkey**
DSA	**dsakey**
ECDSA	**ecdsakey**
SM2	**sm2key**

Usage guidelines

The key algorithm must be the same as required by the security application.

When you create an RSA or DSA key pair, enter an appropriate key modulus length at the prompt. The longer the key modulus length, the higher the security, and the longer the key generation time.

When you create an ECDSA key pair, choose the appropriate elliptic curve. The elliptic curve determines the ECDSA key length. The longer the key length, the higher the security, and the longer the key generation time.

When you create an SM key pair, you do not need to specify the key length. Only a 256-bit SM2 key pair can be created.

See Table 5 for more information about key modulus lengths and key lengths.

If you do not assign the key pair a name, the system assigns the default name to the key pair and marks the key pair as **default**. You can also assign the default name to another key pair, but the system does not mark the key pair as **default**. The name of a key pair must be unique among all manually named key pairs that use the same key algorithm. If a name conflict occurs, the system asks whether you want to overwrite the existing key pair.

The key pairs are automatically saved and can survive system reboots.

Table 5 A comparison of different types of asymmetric key algorithms

Type	Generated key pairs	Modulus/key length
RSA	• One host key pair, if you specify a key pair name. • One server key pair and one host key pair, if you do not specify a key pair name. Both key pairs use their default names. **NOTE:** Only SSH 1.5 uses the RSA server key pair.	Key modulus length: 512 to 2048 bits. Default: 1024 bits. To ensure security, use a minimum of 768 bits.
DSA	One host key pair.	Key modulus length: 512 to 2048 bits. Default: 1024 bits. To ensure security, use a minimum of 768 bits.
ECDSA	One host key pair.	Key length: 192, 256, 384, or 521 bits.
SM2	One host key pair.	Key length: 256 bits.

Examples

Create local RSA key pairs with default names.

```
<Sysname> system-view
[Sysname] public-key local create rsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
...++++++
.++++++
..++++++++
....++++++++
Create the key pair successfully.
```

Create a local DSA key pair with the default name.

```
<Sysname> system-view
[Sysname] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.....................................+..+.............
.......+..........+............+............+...+.....+.............+..+...
...+................+.........+...+....+.......+.....+...........+.........+.
.......................+........+.........+............+.....+...+..........
..............+.........+.........+...........+........+....+.................
.....++++++++++++++++++++++++++++++++++++++++++++++++++*
Create the key pair successfully.
```

Create a local ECDSA key pair with the default name.

```
<Sysname> system-view
[Sysname] public-key local create ecdsa
Generating Keys...
Create the key pair successfully.
```

Create a local SM2 key pair with the default name.

```
<Sysname> system-view
[Sysname] public-key local create sm2
Generating Keys...
Create the key pair successfully.
```

Create a local RSA key pair named **rsa1**.

```
<Sysname> system-view
[Sysname] public-key local create rsa name rsa1
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
...++++++
..............................++++++
Create the key pair successfully.
```

Create a local DSA key pair named **dsa1**.

```
<Sysname> system-view
[Sysname] public-key local create dsa name dsa1
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.....................................+..+.............
.......+..........+............+............+...+.....+............+..+...
...+.................+..........+...+....+.......+.....+............+.........+.
.........................+........+..........+.............+.....+...+..........
..............+.........+..........+...........+........+....+.................
.....++++++++++++++++++++++++++++++++++++++++++++++++++*
Create the key pair successfully.
```

Create a local ECDSA key pair named **ecdsa1**.

```
<Sysname> system-view
[Sysname] public-key local create ecdsa name ecdsa1
Generating Keys...
Create the key pair successfully.
```

Create a local SM2 key pair named **sm2**.

```
<Sysname> system-view
[Sysname] public-key local create sm2 name sm2
Generating Keys...
Create the key pair successfully.
```

Related commands

display public-key local public

public-key local destroy

public-key local destroy

Use **public-key local destroy** to destroy local key pairs.

Syntax

public-key local destroy { **dsa** | **ecdsa** | **rsa** | **sm2** } [**name** *key-name*]

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

dsa: Specifies the DSA key pair type.

ecdsa: Specifies the ECDSA key pair type.

rsa: Specifies the RSA key pair type.

sm2: Specifies the SM2 key pair type.

name *key-name*: Specifies a local key pair by its name, a case-insensitive string of 1 to 64 characters. Valid characters are letters, digits, and hyphens (-). If you do not specify a key pair, this command destroys all key pairs of the specified type.

Usage guidelines

To avoid key compromise, destroy the local key pair and generate a new pair after in any of the following situations:

- An intrusion event has occurred.
- The storage media of the device is replaced.
- The key pair has been used for a long time and there is a risk of key compromise or decryption.
- The local certificate has expired. For more information about local certificates, see PKI configuration in *Security Configuration Guide*.

Examples

Destroy the local RSA key pairs with the default names.

```
<Sysname> system-view
[Sysname] public-key local destroy rsa
Confirm to destroy the key pair? [Y/N]:y
```

Destroy the local DSA key pair with the default name.

```
<Sysname> system-view
[Sysname] public-key local destroy dsa
Confirm to destroy the key pair? [Y/N] :y
```

Destroy the local ECDSA key pair with the default name.

```
<Sysname> system-view
[Sysname] public-key local destroy ecdsa
Confirm to destroy the key pair? [Y/N]:y
```

Destroy the local SM2 key pair with the default name.

```
<Sysname> system-view
[Sysname] public-key local destroy sm2
Confirm to destroy the key pair? [Y/N]:y
```

Destroy local RSA key pair **rsa1**.

```
<Sysname> system-view
[Sysname] public-key local destroy rsa name rsa1
Confirm to destroy the key pair? [Y/N]:y
```

Destroy local DSA key pair **dsa1**.

```
<Sysname> system-view
[Sysname] public-key local destroy dsa name dsa1
Confirm to destroy the key pair? [Y/N] :y
```

Destroy local ECDSA key pair **ecdsa1**.

```
<Sysname> system-view
[Sysname] public-key local destroy ecdsa name ecdsa1
Confirm to destroy the key pair? [Y/N]:y
```

Destroy local SM2 key pair **sm2**.

```
<Sysname> system-view
[Sysname] public-key local destroy sm2 name sm2
Confirm to destroy the key pair? [Y/N]:y
```

Related commands

public-key local create

public-key local export dsa

Use **public-key local export dsa** to export a local DSA host public key.

Syntax

public-key local export dsa [**name** *key-name*] { **openssh** | **ssh2** } [*filename*]

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

name *key-name*: Specifies a local DSA key pair by its name, a case-insensitive string of 1 to 64 characters. Valid characters are letters, digits, and hyphens (-). If you do not specify a key pair, this command exports the host public key of the local DSA key pair with the default name.

openssh: Exports the host public key in OpenSSH format.

ssh2: Exports the host public key in SSH 2.0 format.

filename: Specifies the name of the file for saving the DSA host public key. The name cannot be all dots (.), hostkey, serverkey, dsakey, ecdsakey, or sm2key, and cannot start with a slash (/) or contain **./** or **../**. The file name is a case-insensitive string of 1 to 128 characters. For more information about file names, see file system management in *Fundamentals Configuration Guide*. If you do not specify a file name, this command displays the key on the monitor screen.

Usage guidelines

You can use this command to export a local DSA host public key before distributing it to a peer device.

To distribute a local DSA host public key to a peer device:

1. Save the exported local host public key to a file by using one of the following methods:
   - Use the **public-key local export dsa** [**name** *key-name*] { **openssh** | **ssh2** } command to export the local host public key, and then copy and paste the key to a file.
   - Use the **public-key local export dsa** [**name** *key-name*] { **openssh** | **ssh2** } *filename* command to export the key to a file. You cannot export the key to the **pkey** folder or its subfolders.
2. Transfer a copy of the file to the peer device, for example, by using FTP in binary mode or TFTP. For more information about FTP and TFTP, see *Fundamentals Configuration Guide*.
3. On the peer device, use the **public-key peer import sshkey** command to import the host public key from the file.

SSH 2.0 and OpenSSH are different public key formats. Choose the correct format that is supported on the device where you import the host public key.

Examples

Export the host public key of the local DSA key pair with the default name in OpenSSH format to a file named **key.pub**.

```
<Sysname> system-view
[Sysname] public-key local export dsa openssh key.pub
```

Display the host public key of the local DSA key pair with the default name in SSH 2.0 format.

```
<Sysname> system-view
[Sysname] public-key local export dsa ssh2
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "dsa-key-2011/05/12"
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5sJlhUiJ3
B7b0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKNl/BnjXcitTQchQbz
WCFLFqL6xLNolQOHgRx9ozAAAAFQDHcyGMc37I7pk7Ty3tMPSO2s6RXwAAAIEAgiaQCeFOxHS68pMuadOx8YU
XrZWUGEzN/OrpbsTV75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UILiLFs3ThbdABMs5xsCAhcJGscXthI5HH
bB+y6IMXwb2BcdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9LFYXaf0JRlxjMmwnu8AAACAQZEs400SvNIVfnqxw
vA7PvOVEA89tKni/f6GDBvWY9Z2Q499pAqUBtYcqQea8T4zBInxx2eF3lLaZJrIvAS205zXxSzQoU9190kakd
MdasIjQLWYGyepFc3sTwmIflQeweUwLVAPaOesKaCERjxg+e4maYWlAvySGT4c9NJlxLo=
---- END SSH2 PUBLIC KEY ----
```

Display the host public key of the local DSA key pair with the default name in OpenSSH format.

```
<Sysname> system-view
[Sysname] public-key local export dsa openssh
ssh-dss
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5sJlhUiJ3
B7b0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKNl/BnjXcitTQchQbz
WCFLFqL6xLNolQOHgRx9ozAAAAFQDHcyGMc37I7pk7Ty3tMPSO2s6RXwAAAIEAgiaQCeFOxHS68pMuadOx8YU
XrZWUGEzN/OrpbsTV75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UILiLFs3ThbdABMs5xsCAhcJGscXthI5HH
bB+y6IMXwb2BcdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9LFYXaf0JRlxjMmwnu8AAACAQZEs400SvNIVfnqxw
vA7PvOVEA89tKni/f6GDBvWY9Z2Q499pAqUBtYcqQea8T4zBInxx2eF3lLaZJrIvAS205zXxSzQoU9190kakd
MdasIjQLWYGyepFc3sTwmIflQeweUwLVAPaOesKaCERjxg+e4maYWlAvySGT4c9NJlxLo= dsa-key
```

Export the host public key of local DSA key pair **dsa1** in OpenSSH format to file **dsa1.pub**.

```
<Sysname> system-view
[Sysname] public-key local export dsa name dsa1 openssh dsa1.pub
```

Display the host public key of local DSA key pair **dsa1** in SSH 2.0 format.

```
<Sysname> system-view
[Sysname] public-key local export dsa name dsa1 ssh2
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "dsa-key-2011/05/12"
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5sJlhUiJ3
B7b0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKNl/BnjXcitTQchQbz
WCFLFqL6xLNolQOHgRx9ozAAAAFQDHcyGMc37I7pk7Ty3tMPSO2s6RXwAAAIEAgiaQCeFOxHS68pMuadOx8YU
XrZWUGEzN/OrpbsTV75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UILiLFs3ThbdABMs5xsCAhcJGscXthI5HH
bB+y6IMXwb2BcdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9LFYXaf0JRlxjMmwnu8AAACBAKHkVsjaKtG7g7G98
qGmtaboNkK0YEAkRdp+QDZxX0aPdmVeEU1GC3ES9XFD7gIK70pb+tB7dA+8scZNqKK85hkoNCFEXux3088NEY
ZullatZRH0km+DdpZ7CrcV+ft7UUvBF0FV3W4HOx/LOidJ5sX+qBAD4WcpSX0OrZEF4+dq
---- END SSH2 PUBLIC KEY ----
```

Display the host public key of local DSA key pair **dsa1** in OpenSSH format.

```
<Sysname> system-view
[Sysname] public-key local export dsa name dsa1 openssh
ssh-dss
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5sJlhUiJ3
B7b0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKNl/BnjXcitTQchQbz
WCFLFqL6xLNolQOHgRx9ozAAAAFQDHcyGMc37I7pk7Ty3tMPSO2s6RXwAAAIEAgiaQCeFOxHS68pMuadOx8YU
XrZWUGEzN/OrpbsTV75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UILiLFs3ThbdABMs5xsCAhcJGscXthI5HH
bB+y6IMXwb2BcdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9LFYXaf0JRlxjMmwnu8AAACBAKHkVsjaKtG7g7G98
qGmtaboNkK0YEAkRdp+QDZxX0aPdmVeEU1GC3ES9XFD7gIK70pb+tB7dA+8scZNqKK85hkoNCFEXux3088NEY
ZullatZRH0km+DdpZ7CrcV+ft7UUvBF0FV3W4HOx/LOidJ5sX+qBAD4WcpSX0OrZEF4+dq dsa-key
```

Related commands

public-key local create

public-key peer import sshkey

public-key local export ecdsa

Use **public-key local export ecdsa** to export a local ECDSA host public key.

Syntax

public-key local export ecdsa [**name** *key-name*] { **openssh** | **ssh2** } [*filename*]

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

name *key-name*: Specifies a local ECDSA key pair by its name, a case-insensitive string of 1 to 64 characters. Valid characters are letters, digits, and hyphens (-). If you do not specify a key pair, this command exports the host public key of the local ECDSA key pair with the default name.

openssh: Exports the host public key in OpenSSH format.

ssh2: Exports the host public key in SSH 2.0 format.

filename: Specifies the name of the file for saving the local host public key. The name cannot be all dots (.), hostkey, serverkey, dsakey, ecdsakey, or sm2key, and cannot start with a slash (/) or contain **./** or **../**.The file name is a case-insensitive string of 1 to 128 characters. For more information

about file names, see file system management in *Fundamentals Configuration Guide*. If you do not specify a file name, this command displays the key on the monitor screen.

Usage guidelines

You can use this command to export a local ECDSA host public key before distributing it to a peer device.

To distribute a local ECDSA host public key to a peer device:

1. Save the exported ECDSA host public key to a file by using one of the following methods:
   - Use the **public-key local export ecdsa** [**name** *key-name*] { **openssh** | **ssh2** } command to export the local host public key, and then copy and paste it to a file.
   - Use the **public-key local export ecdsa** [**name** *key-name*] { **openssh** | **ssh2** } *filename* command to export the host public key to a file. You cannot export the key to the **pkey** folder or its subfolders.
2. Transfer a copy of the file to the peer device, for example, by using FTP in binary mode or TFTP. For more information about FTP and TFTP, see *Fundamentals Configuration Guide*.
3. On the peer device, use the **public-key peer import sshkey** command to import the host public key from the file.

SSH 2.0 and OpenSSH are different public key formats. Choose the correct format that is supported by the device where you import the host public key.

Only the ECDSA host public key generated by using the secp256r1 curve can be exported.

Examples

Export the host public key of the local ECDSA key pair with the default name in OpenSSH format to file **key.pub**.

```
<Sysname> system-view
[Sysname] public-key local export ecdsa openssh key.pub
```

Display the host public key of the local ECDSA key pair with the default name in SSH 2.0 format.

```
<Sysname> system-view
[Sysname] public-key local export ecdsa ssh2
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "ecdsa-sha2-nistp256-2014/07/06"
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBREw5tkARpbV+sYArt/xcW+UJEAevx7O
ckTtTLPBiLP5bWkSdKbvo+3oHRuIyZqmNTIcxuBjuBap+pHc919C58=
---- END SSH2 PUBLIC KEY ----
```

Display the host public key of the local ECDSA key pair with the default name in OpenSSH format.

```
<Sysname> system-view
[Sysname] public-key local export ecdsa openssh
ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBREw5tkARpbV+sYArt/xcW+UJEAevx7O
ckTtTLPBiLP5bWkSdKbvo+3oHRuIyZqmNTIcxuBjuBap+pHc919C58=
 ecdsa-key
```

Related commands

public-key local create

public-key peer import sshkey

public-key local export rsa

Use **public-key local export rsa** to export a local RSA host public key.

Syntax

public-key local export rsa [**name** *key-name*] { **openssh** | **ssh1** | **ssh2** } [*filename*]

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

name *key-name*: Specifies a local RSA key pair by its name, a case-insensitive string of 1 to 64 characters. Valid characters are letters, digits, and hyphens (-). If you do not specify a key pair, this command exports the host public key of the local RSA key pair with the default name.

openssh: Exports the host public key in OpenSSH format.

ssh1: Exports the host public key in SSH 1.5 format.

ssh2: Exports the host public key in SSH 2.0 format.

filename: Specifies the name of the file for saving the local host public key. The name cannot be all dots (.), hostkey, serverkey, dsakey, ecdsakey, or sm2key, and cannot start with a slash (/) or contain **./** or **../**. The file name is a case-insensitive string of 1 to 128 characters. For more information about file names, see file system management in *Fundamentals Configuration Guide*. If you do not specify a file name, this command displays the key on the monitor screen.

Usage guidelines

You can use this command to export a local RSA host public key before distributing it to a peer device.

To distribute a local RSA host public key to a peer device:

1. Save the exported local host public key to a file by using one of the following methods:
   - Use the **public-key local export rsa** [**name** *key-name*] { **openssh** | **ssh2** } command to export the key, and then copy and paste it to a file.
   - Use the **public-key local export rsa** [**name** *key-name*] { **openssh** | **ssh2** } *filename* command to export key to a file. You cannot export the key to the **pkey** folder or its subfolders.
2. Transfer a copy of the file to the peer device, for example, by using FTP in binary mode or TFTP. For more information about FTP and TFTP, see *Fundamentals Configuration Guide*.
3. On the peer device, use the **public-key peer import sshkey** command to import the host public key from the file.

Choose the correct public key format that is supported on the device where you import the host public key.

Examples

Export the host public key of the local RSA key pair with the default name in OpenSSH format to file **key.pub**.

```
<Sysname> system-view
[Sysname] public-key local export rsa openssh key.pub
```

Display the host public key of the local RSA key pair with the default name in SSH 2.0 format.

```
<Sysname> system-view
[Sysname] public-key local export rsa ssh2
---- BEGIN SSH2 PUBLIC KEY ----
```

```
Comment: "rsa-key-2011/05/12"
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDapKr+/gTCyWZyabuCJuJjMeMPQaj/kixzOCCAl+hDMmEGMrSfddq/b
YcbgM7Buit1AgB3x0dFyTPi85DcCznTW4goPXAKFjuzCbGfj4chakSr+/aj1k3rM+XOvyvPJilneKJqhPT0xd
v4tlas+mLNloY0dImbwS2kwE71rgg1CQ==
---- END SSH2 PUBLIC KEY ----
```

Display the host public key of the local RSA key pair with the default name in OpenSSH format.

```
<Sysname> system-view
[Sysname] public-key local export rsa openssh
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDapKr+/gTCyWZyabuCJuJjMeMPQaj/kixzOCCAl+hDMmEGMrSfddq/b
YcbgM7Buit1AgB3x0dFyTPi85DcCznTW4goPXAKFjuzCbGfj4chakSr+/aj1k3rM+XOvyvPJilneKJqhPT0xd
v4tlas+mLNloY0dImbwS2kwE71rgg1CQ== rsa-key
```

Export the host public key of local RSA key pair **rsa1** in OpenSSH format to file **rsa1.pub**.

```
<Sysname> system-view
[Sysname] public-key local export rsa name rsa1 openssh rsa1.pub
```

Display the host public key of local RSA key pair **rsa1** in SSH 2.0 format.

```
<Sysname> system-view
[Sysname] public-key local export rsa name rsa1 ssh2
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-2011/05/12"
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDevEbyF93xHUJucJWqRc1r8fhzQ9lSVprCI6ATZeDYyR1J00fBQ8XY+
q2olqoagn5YDyUC8ZJvUhlyMOHeORpkAVxD3XncTp4XG66h3rTHHa7Xmm7f1GDYlF0n05t8mCLVaupbfCzP8b
a8UkrUmMO4fUvW6zavA5LYxtlAiQv0KQ==
---- END SSH2 PUBLIC KEY ----
```

Display the host public key of local RSA key pair **rsa1** in OpenSSH format.

```
<Sysname> system-view
[Sysname] public-key local export rsa name rsa1 openssh
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDevEbyF93xHUJucJWqRc1r8fhzQ9lSVprCI6ATZeDYyR1J00fBQ8XY+
q2olqoagn5YDyUC8ZJvUhlyMOHeORpkAVxD3XncTp4XG66h3rTHHa7Xmm7f1GDYlF0n05t8mCLVaupbfCzP8b
a8UkrUmMO4fUvW6zavA5LYxtlAiQv0KQ== rsa-key
```

Related commands

public-key local create

public-key peer import sshkey

public-key local export sm2

Use **public-key local export sm2** to export a local SM2 host public key.

Syntax

public-key local export sm2 [**name** *key-name*] { **openssh** | **ssh2** } [*filename*]

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

name *key-name*: Specifies a local SM2 key pair by its name, a case-insensitive string of 1 to 64 characters. Valid characters are letters, digits, and hyphens (-). If you do not specify a key pair, this command exports the host public key of the local SM2 key pair with the default name.

openssh: Exports the host public key in OpenSSH format.

ssh2: Exports the host public key in SSH2.0 format.

filename: Specifies the name of the file for saving the local host public key. The name cannot be all dots (.), hostkey, serverkey, dsakey, sm2key, or ecdsakey, and cannot start with a slash (/) or contain **./** or **../**. The file name is a case-insensitive string of 1 to 128 characters. For more information about file names, see file system management in *Fundamentals Configuration Guide*. If you do not specify a file name, this command displays the key on the monitor screen.

Usage guidelines

You can use this command to export a local SM2 host public key before distributing it to a peer device.

To distribute a local SM2 host public key to a peer device:

1. Save the exported local host public key to a file by using one of the following methods:
   - Use the **public-key local export sm2** [**name** *key-name*] { **openssh** | **ssh2** } command to export the key, and then copy and paste it to a file.
   - Use the **public-key local export sm2** [**name** *key-name*] { **openssh** | **ssh2** } *filename* command to export key to a file. You cannot export the key to the **pkey** folder or its subfolders.
2. Transfer a copy of the file to the peer device, for example, by using FTP in binary mode or TFTP. For more information about FTP and TFTP, see *Fundamentals Configuration Guide*.
3. On the peer device, use the **public-key peer import sshkey** command to import the host public key from the file.

SSH2.0 and OpenSSH are different public key formats. Choose the correct public key format that is supported on the device where you import the host public key.

Examples

Export the host public key of the local SM2 key pair with the default name in OpenSSH format to file **key.pub**.

```
<Sysname> system-view
[Sysname] public-key local export sm2 openssh key.pub
```

Display the host public key of the local SM2 key pair with the default name in SSH2.0 format.

```
<Sysname> system-view
[Sysname] public-key local export sm2 ssh2
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "sm2-key-2016/09/12"
AAAAB3NtMi1rZXkAAABBBJo0XIySNcZiJq/N81QQozLcdBneur2w/E1gIRAfHM5SwDspD22aMdg5dRQr
IFrN6XMXdftV5vwI9qWX/tGMH0g=
---- END SSH2 PUBLIC KEY ----
```

Display the host public key of the local SM2 key pair with the default name in OpenSSH format.

```
<Sysname> system-view
[Sysname] public-key local export sm2 openssh
ssh-sm2 AAAAB3NtMi1rZXkAAABBBJo0XIySNcZiJq/N81QQozLcdBneur2w/E1gIRAfHM5SwDspD22a
Mdg5dRQrIFrN6XMXdftV5vwI9qWX/tGMH0g= sm2-key
```

Related commands

public-key local create

public-key peer import sshkey

public-key local import

Use **public-key local import** to import local key pairs.

Syntax

public-key local import { **ecdsa** | **rsa** } [*key-name*] **filename** *filename*

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ecdsa: Specifies the ECDSA key pair type.

rsa: Specifies the RSA key pair type.

key-name: Assigns a name to the key pair. The *key-name* argument is a case-insensitive string of 1 to 64 characters. Valid characters are letters, digits, and hyphens (-). If you do not assign a name to the key pair, the RSA and ECDSA key pairs take the default name **hostkey** and **ecdsakey**, respectively.

filename *filename*: Specifies the name of the file that stores the key pair to be imported. The file name is a case-sensitive string of 1 to 128 characters. The key pair file must already exist on the device and must be in PEM format.

Usage guidelines

If the certificate and the key pair are saved in separate files, the device cannot import the key pair by importing the certificate. In this case, you can execute this command to import the key pair from the key pair file to the device. Before executing this command, upload the key pair file to the device through FTP or other methods.

The key pairs imported by using this command are automatically saved and can survive system reboots.

The device supports importing the RSA host key pair but not the RSA server key pair.

If you do not assign the key pair a name, the system assigns the default name to the key pair and marks the key pair as **default**. You can also assign the default name to another key pair, but the system does not mark the key pair as **default**. The name of a key pair must be unique among all manually named key pairs that use the same key algorithm. If a name conflict occurs, the system asks whether you want to overwrite the existing key pair.

To import the encrypted key pair into the device successfully, provide the decryption password.

See Table 6 for information about the supported key modulus lengths and key lengths.

Table 6 Length of key pair

Type	Modulus/key length
RSA	Key modulus length: 512 to 2048 bits.
ECDSA	Key length: 192, 256, 384, or 521 bits.

Examples

Import the encrypted local RSA key pair **rsa1** from the **private_key.pem** file.

```
<Sysname> system-view
[Sysname] public-key local import rsa rsa1 filename private_key.pem
Please input the password:
Importing Keys...
Key pair imported successfully.
```

Related commands

display public-key local public

public-key peer

Use **public-key peer** to assign a name to a peer host public key and enter public key view, or enter the view of an existing peer host public key.

Use **undo public-key peer** to delete a peer host public key.

Syntax

public-key peer *keyname*

undo public-key peer *keyname*

Default

No peer host public keys exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

keyname: Specifies a key name, a case-sensitive string of 1 to 64 characters.

Usage guidelines

After you execute this command to enter the public key view, type the public key. Spaces and carriage returns are allowed, but are not saved.

To configure a peer host public key on the local device, first obtain the peer public key in hexadecimal notation, and then perform the following tasks on the local device:

1. Execute the **public-key peer** command to enter public key view.
2. Type the public key.
3. Execute the **peer-public-key end** command to save the public key and return to system view.

The public key you type in the public key view must be in a correct format. If the peer device is an NSFOCUS device, use the **display public-key local public** command to display and record its public key.

Examples

Assign name **key1** to the peer host public key and enter public key view.

```
<Sysname> system-view
```

```
[Sysname] public-key peer key1
Enter public key view. Return to system view with "peer-public-key end" command.
[Sysname-pkey-public-key-key1]
```

Related commands

display public-key local public

display public-key peer

peer-public-key end

public-key peer import sshkey

Use **public-key peer import sshkey** to import a peer host public key from a public key file.

Use **undo public-key peer** to remove a peer host public key.

Syntax

public-key peer *keyname* **import sshkey** *filename*

undo public-key peer *keyname*

Default

No peer host public keys exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

keyname: Specifies a name for a peer host public key, a case-sensitive string of 1 to 64 characters.

filename: Specifies a public key file by its name. The name cannot be all dots (.), hostkey, serverkey, dsakey, ecdsakey, or sm2key, and cannot start with a slash (/) or contain **./** or **../**. The file name is a case-insensitive string of 1 to 128 characters. For more information about file names, see file system management in *Fundamentals Configuration Guide*.

Usage guidelines

After you configure this command, the system automatically transforms the host public key to the PKCS format, and saves the key.

Before you use this command, make sure you have got a copy of the public key file from the peer device through FTP in binary mode or through TFTP.

The device supports importing public keys in the format of SSH 1.5, SSH 2.0 and OpenSSH.

Examples

Import peer host public key **key2** from public key file **key.pub**.

```
<Sysname> system-view
[Sysname] public-key peer key2 import sshkey key.pub
```

Related commands

display public-key peer

public-key local export dsa

```
public-key local export ecdsa
public-key local export rsa
```

Contents

PKI commands

attribute

Use **attribute** to configure a rule to filter certificates based on an attribute in the certificate issuer name, subject name, or alternative subject name field.

Use **undo attribute** to remove an attribute rule.

Syntax

attribute *id* { **alt-subject-name** { **fqdn** | **ip** } | { **issuer-name** | **subject-name** } { **dn** | **fqdn** | **ip** } } { **ctn** | **equ** | **nctn** | **nequ** } *attribute-value*

undo attribute *id*

Default

No attribute rules exist.

Views

Certificate attribute group view

Predefined user roles

network-admin

context-admin

Parameters

id: Specifies a rule ID in the range of 1 to 16.

alt-subject-name: Specifies the alternative subject name field.

fqdn: Specifies the FQDN attribute.

ip: Specifies the IP address attribute.

dn: Specifies the DN attribute.

issuer-name: Specifies the issuer name field.

subject-name: Specifies the subject name field.

ctn: Specifies the contain operation.

equ: Specifies the equal operation.

nctn: Specifies the not-contain operation.

nequ: Specifies the not-equal operation.

attribute-value: Sets an attribute value, a case-insensitive string of 1 to 128 characters.

Usage guidelines

Different certificate fields support different attributes.

- The subject name field and the issuer name field can contain a single DN, multiple FQDNs, and multiple IP addresses.
- The alternative subject name field can contain multiple FQDNs and IP addresses but zero DNs.

An attribute rule is a combination of an attribute-value pair with an operation keyword, as listed in Table 1.

Table 1 Combinations of attribute-value pairs and operation keywords

Operation	DN	FQDN/IP
ctn	The DN contains the specified attribute value.	Any FQDN or IP address contains the specified attribute value.
nctn	The DN does not contain the specified attribute value.	None of the FQDNs or IP addresses contain the specified attribute value.
equ	The DN is the same as the specified attribute value.	Any FQDN or IP address is the same as the specified attribute value.
nequ	The DN is not the same as the specified attribute value.	None of the FQDNs or IP addresses are the same as the specified attribute value.

A certificate matches an attribute rule if it contains an attribute that matches the criterion defined in the rule. For example, a certificate matches the **attribute 1 subject-name dn ctn abc** rule if it meets the following conditions:

- The subject name field of the certificate contains the DN attribute.
- The DN attribute value contains the **abc** string.

A certificate matches an attribute group if it matches all attribute rules in the group.

Examples

Create a certificate attribute group and enter its view.

```
<Sysname> system-view
[Sysname] pki certificate attribute-group mygroup
```

Configure an attribute rule to match certificates that contain the **abc** string in the subject DN.

```
[Sysname-pki-cert-attribute-group-mygroup] attribute 1 subject-name dn ctn abc
```

Configure an attribute rule to match certificates that do not contain FQDN **abc** in the issuer name field.

```
[Sysname-pki-cert-attribute-group-mygroup] attribute 2 issuer-name fqdn nequ abc
```

Configure an attribute rule to match certificates that do not contain IP address **10.0.0.1** in the alternative subject name field.

```
[Sysname-pki-cert-attribute-group-mygroup] attribute 3 alt-subject-name ip nequ 10.0.0.1
```

Related commands

display pki certificate attribute-group

rule

ca identifier

Use **ca identifier** to specify the trusted CA.

Use **undo ca identifier** to restore the default.

Syntax

ca identifier *name*

undo ca identifier

Default

No trusted CA is specified.

Views

PKI domain view

Predefined user roles

network-admin

context-admin

Parameters

name: Specifies the trusted CA by its name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

To obtain a CA certificate in a PKI domain, you must specify the trusted CA name. The trusted CA name uniquely identifies the CA to be used if multiple CAs exist on the CA server specified for the PKI domain.

Make sure the specified CA name is consistent with the name of the CA that owns the CA certificate to be obtained.

Examples

Set the name of the trusted CA to **new-ca**.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] ca identifier new-ca
```

certificate request entity

Use **certificate request entity** to specify the PKI entity for certificate request.

Use **undo certificate request entity** to restore the default.

Syntax

certificate request entity *entity-name*

undo certificate request entity

Default

No PKI entity is specified for certificate request.

Views

PKI domain view

Predefined user roles

network-admin

context-admin

Parameters

entity-name: Specifies a PKI entity by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

A PKI entity describes the identity attributes of an entity for certificate request, including the following information:

- Common name.
- Organization.
- Unit in the organization.
- Locality.
- State and country where the entity resides.
- FQDN.

- IP address.

You can specify only one PKI entity for a PKI domain. If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify PKI entity **en1** for certificate request in PKI domain **aaa**.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] certificate request entity en1
```

Related commands

pki entity

certificate request from

Use **certificate request from** to specify the type of certificate request reception authority.

Use **undo certificate request from** to restore the default.

Syntax

certificate request from { **ca** | **ra** }

undo certificate request from

Default

The type of certificate request reception authority is not specified.

Views

PKI domain view

Predefined user roles

network-admin

context-admin

Parameters

ca: Sends certificate requests to the CA.

ra: Sends certificate requests to the RA.

Usage guidelines

The CA server determines whether the CA or RA accepts certificate requests. This authority setting must be consistent with the setting on the CA server.

Examples

Sends certificate requests to the RA.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] certificate request from ra
```

certificate request mode

Use **certificate request mode** to set the certificate request mode.

Use **undo certificate request mode** to restore the default.

Syntax

certificate request mode { **auto** [**password** { **cipher** | **simple** } *string* | **renew-before-expire** *days* [**reuse-public-key**] [**automatic-append common-name**]] * | **manual** }

undo certificate request mode

Default

The certificate request mode is manual.

Views

PKI domain view

Predefined user roles

network-admin

context-admin

Parameters

auto: Specifies the auto certificate request mode.

password: Specifies a password for certificate revocation.

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 31 characters. Its encrypted form is a case-sensitive string of 1 to 73 characters.

renew-before-expire *days*: Configures the system to automatically request a new certificate the specified number of days before the current certificate expires. The value range for the *days* argument is 0 to 365. Value 0 indicates that the request for a new certificate is made when the old certificate expires, which might cause service interruptions.

reuse-public-key: Reuses the key pair in the old certificate for the new certificate. If you do not specify this keyword, the system generates a new key pair for the new certificate. The old key pair is replaced with the new one when the new certificate is received from the CA.

automatic-append common-name: Automatically appends random data to the common name of the PKI entity for the new certificate. If you do not specify this keyword, the common name of the PKI entity will be unchanged in the new certificate.

manual: Specifies the manual certificate request mode.

Usage guidelines

A certificate request can be submitted to a CA in offline or online mode. In online mode, a certificate request can be automatically or manually submitted:

- **Auto request mode**—A PKI entity automatically obtains the CA certificate and submits a certificate request to the CA when both of the following conditions exist:
  - An associated application (IKE, for example) performs identity authentication.
  - No certificate is available for the application on the device.

  In auto request mode, specify the password for certificate revocation as required by the CA policy.
- **Manual request mode**—You must manually obtain the CA certificate and submit certificate requests.

To avoid service interruptions caused by certificate expiration, specify the **renew-before-expire** *days* option to enable certificate auto-renewal in auto certificate request

mode. Certificate auto-renewal allows the system to automatically request a new certificate the specified number of days before the old certificate expires. The old certificate is replaced immediately when the new certificate is received.

Examples

Set the certificate request mode to **auto**.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] certificate request mode auto
```

Set the certificate request mode to **auto**, and set the certificate revocation password in plain text to **123456**.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] certificate request mode auto password simple 123456
```

Set the certificate request mode to **auto**, and set the certificate revocation password in plain text to **123456**. Configure the system to automatically request a new certificate by using a new key pair 60 days before the certificate expires.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] certificate request mode auto password simple 123456
renew-before-expire 60
```

Related commands

pki request-certificate

certificate request polling

Use **certificate request polling** to set the polling interval and the maximum number of attempts to query certificate request status.

Use **undo certificate request polling** to restore the defaults.

Syntax

certificate request polling { **count** *count* | **interval** *interval* }

undo certificate request polling { **count** | **interval** }

Default

The polling interval is 20 minutes, and the maximum number of attempts is 50.

Views

PKI domain view

Predefined user roles

network-admin

context-admin

Parameters

count *count*: Specifies the maximum number of query attempts. The value range is 1 to 100.

interval *interval*: Specifies a polling interval in minutes. The value range is 5 to 168.

Usage guidelines

After a PKI entity submits a certificate request, it might take the CA server a while to issue the certificate if the CA administrator must manually approve the certificate request. During this period,

the PKI entity periodically queries the CA server for the certificate request status. The periodic query operation stops until the PKI entity obtains the certificate or the maximum number of query attempts is reached. If the maximum number of query attempts is reached, the certificate request fails.

If the CA server automatically approves certificate requests, the PKI entity can obtain the certificate immediately after it submits a certificate request. In this case, the PKI entity does not send queries to the CA server.

Examples

Set the polling interval to 15 minutes, and the maximum number of query attempts to 40.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] certificate request polling interval 15
[Sysname-pki-domain-aaa] certificate request polling count 40
```

Related commands

display pki certificate request-status

certificate request url

Use **certificate request url** to specify the URL of the certificate request reception authority (CA or RA) to which the device should send SCEP certificate requests.

Use **undo certificate request url** to restore the default.

Syntax

certificate request url *url-string*

undo certificate request url

Default

The URL of the certificate request reception authority is not specified.

Views

PKI domain view

Predefined user roles

network-admin

context-admin

Parameters

url-string: Specifies the URL of the certificate request reception authority, a case-sensitive string of 1 to 511 characters. The URL length is restricted by the CLI string limitation or the *url-string* parameter, whichever is smaller.

Usage guidelines

The certificate request URL contains the location of the certificate request reception authority server and the path of the application script on the server, in the format http*://server_location/cgi_script_location*.

Examples

Set the certificate request URL to **http://169.254.0.1/certsrv/mscep/mscep.dll**.

```
<Sysname> system-view
[Sysname] pki domain a
[Sysname-pki-domain-a] certificate request url
http://169.254.0.1/certsrv/mscep/mscep.dll
```

common-name

Use **common-name** to set the common name for a PKI entity.

Use **undo common-name** to restore the default.

Syntax

common-name *common-name-sting*

undo common-name

Default

No common name is set for a PKI entity.

Views

PKI entity view

Predefined user roles

network-admin

context-admin

Parameters

common-name-sting: Specifies a common name, a case-sensitive string of 1 to 63 characters. No comma can be included. You can set the username of the PKI entity as the common name.

Examples

Set the common name to **test** for PKI entity **en**.

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en] common-name test
```

country

Use **country** to set the country code of a PKI entity.

Use **undo country** to restore the default.

Syntax

country *country-code-string*

undo country

Default

No country code is set for a PKI entity.

Views

PKI entity view

Predefined user roles

network-admin

context-admin

Parameters

country-code-string: Specifies a country code, a case-sensitive string of two characters. For example, CN is the country code for China.

Examples

Set the country code to **CN** for PKI entity **en**.

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en] country CN
```

crl check enable

Use **crl check enable** to enable CRL checking.

Use **undo crl check enable** to disable CRL checking.

Syntax

crl check enable

undo crl check enable

Default

CRL checking is enabled.

Views

PKI domain view

Predefined user roles

network-admin

context-admin

Usage guidelines

A CRL is a list of revoked certificates signed and published by a CA. Revoked certificates should no longer be trusted.

Enable CRL checking to ensure that the device only accepts certificates that have not been revoked by the issuing CA.

Examples

Disable CRL checking.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] undo crl check enable
```

Related commands

pki import

pki retrieve-certificate

pki validate-certificate

crl update-period

Use **crl update-period** to enable automatic CRL update and set the update interval.

Use **undo crl update-period** to restore the default.

Syntax

crl update-period *hours*

undo crl update-period

Default

The device does not update the CRL automatically.

Views

PKI domain view

Predefined user roles

network-admin

context-admin

Parameters

hours: Specifies the CRL update interval, in the range of 1 to 720 hours.

Usage guidelines

In scenarios that require strict certificate verification (such as bank systems), the device must be able to obtain the latest CRL in time. This command enables the device to automatically connect to the CRL repository at the specified intervals to obtain the latest CRL.

The device uses HTTP, LDAP, or SCEP to obtain the CRL, depending on the URL configuration for the CRL repository in the PKI domain (by using the **crl url** command):

- If an HTTP URL is specified for the CRL repository, the device uses HTTP to obtain the CRL.
- If an LDAP URL is specified, the device uses LDAP to obtain the CRL.

  If an LDAP URL is specified, the device must connect to the LDAP server to obtain the CRL. If the LDAP URL does not contain the hostname of the LDAP server, such as **ldap:///CN=8088,OU=test,U=rd,C=cn**, use the **ldap-server** command to configure the server hostname in the PKI domain.
- If no CRL repository URL is specified in the PKI domain, the device looks up the CRL repository from the local certificates and CA certificate in turn. If a CRL repository is found, the device obtains the CRL from the CRL repository. If no CRL repository is found, the device obtains the CRL through SCEP.

  In this case, the CA certificate and the local certificates must have been obtained.

Using automatic CRL update, the device might not be able to update the CRL immediately when the CRL expires. This is because the device must wait for the specified interval of time to perform a next update. Set the CRL update interval to a proper value to ensure the timeliness of CRL update.

You can also execute the **pki retrieve-crl** command to perform an immediate CRL update as needed.

Examples

Set the CRL update interval to 24 hours.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] crl update-period 24
```

Related commands

crl url

ldap server

pki retrieve-crl

crl url

Use **crl url** to specify the URL of the CRL repository.

Use **undo crl url** to restore the default.

Syntax

crl url *url-string*

undo crl url

Default

The URL of the CRL repository is not specified.

Views

PKI domain view

Predefined user roles

network-admin

context-admin

Parameters

url-string: Specifies the URL of the CRL repository, a case-sensitive string of 1 to 511 characters. The URL format is ldap://*server_location* or http://*server_location*, where *server_location* can be the IP address or domain name of the CRL repository server. The URL length is restricted by the CLI string limitation or the *url-string* parameter, whichever is smaller.

Usage guidelines

To use CRL checking, a CRL must be obtained from a CRL repository.

The device selects a CRL repository in the following order:

1. CRL repository specified in the PKI domain by using this command.
2. CRL repository in the certificate that is being verified.
3. CRL repository in the CA certificate or CRL repository in the upper-level CA certificate if the CA certificate is the certificate being verified.

After the previous selection process, if the CRL repository is not found, the device obtains the CRL through SCEP. In this scenario, the CA certificate and the local certificates must have been obtained.

If an LDAP URL is specified, the device must connect to the LDAP server to obtain the CRL. If the LDAP URL does not contain the address of the LDAP server, use the **ldap-server** command to configure the server address in the PKI domain.

Examples

Set the URL of the CRL repository to **http://169.254.0.30**.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] crl url http://169.254.0.30
```

Related commands

ldap-server

pki retrieve-crl

display pki certificate access-control-policy

Use **display pki certificate access-control-policy** to display information about certificate-based access control policies.

Syntax

display pki certificate access-control-policy [*policy-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

policy-name: Specifies a certificate-based access control policy by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

If you do not specify a policy name, this command displays information about all certificate-based access control policies.

Examples

Display information about certificate-based access control policy **mypolicy**.

```
<Sysname> display pki certificate access-control-policy mypolicy
 Access control policy name: mypolicy
     Rule 1  deny    mygroup1
     Rule 2  permit  mygroup2
```

Display information about all certificate-based access control policies.

```
<Sysname> display pki certificate access-control-policy
 Total PKI certificate access control policies: 2
 Access control policy name: mypolicy1
     Rule 1  deny    mygroup1
     Rule 2  permit  mygroup2
 Access control policy name: mypolicy2
     Rule 1  deny    mygroup3
     Rule 2  permit  mygroup4
```

Table 2 Command output

Field	Description
Total PKI certificate access control policies	Total number of certificate-based access control policies.
permit	Permit certificates that match the attribute group in the access control rule.
deny	Deny certificates that match the attribute group in the access control rule.

Related commands

pki certificate access-control-policy

rule

display pki certificate attribute-group

Use **display pki certificate attribute-group** to display information about certificate attribute groups.

Syntax

display pki certificate attribute-group [*group-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

group-name: Specifies a certificate attribute group by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

If you do not specify a certificate attribute group, this command displays information about all certificate attribute groups.

Examples

Display information about certificate attribute group **mygroup**.

```
<Sysname> display pki certificate attribute-group mygroup
 Attribute group name: mygroup
      Attribute  1 subject-name     dn    ctn   abc
      Attribute  2 issuer-name      fqdn  nctn  app
```

Display information about all certificate attribute groups.

```
<Sysname> display pki certificate attribute-group
 Total PKI certificate attribute groups: 2.
 Attribute group name: mygroup1
      Attribute  1 subject-name     dn    ctn   abc
      Attribute  2 issuer-name      fqdn  nctn  app
Attribute group name: mygroup2
      Attribute  1 subject-name     dn    ctn   def
      Attribute  2 issuer-name      fqdn  nctn  fqd
```

Table 3 Command output

Field	Description
Total PKI certificate attribute groups	Total number of certificate attribute groups.
ctn	Contain operation.
nctn	Not-contain operation.
equ	Equal operation.
nequ	Not-equal operation.

Field	Description
Attribute 1 subject-name dn ctn abc	Attribute rule contents: • **alt-subject-name**—Alternative subject name. • **issuer-name**—Certificate issuer name. • **subject-name**—Certificate subject name. • **fqdn**—FQDN of the PKI entity. • **ip**—IP address of the PKI entity. • **dn**—DN of the PKI entity. • **ctn**—Indicates the contain operation. • **equ**—Indicates the equal operation. • **nctn**—Indicates the not-contain operation. • **nequ**—Indicates the not-equal operation.

Related commands

`attribute`

`pki certificate attribute-group`

display pki certificate domain

Use **`display pki certificate domain`** to display information about certificates.

Syntax

`display pki certificate domain` *`domain-name`* { **`ca`** | **`local`** | **`peer`** [**`serial`** *`serial-num`*] }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

`domain-name`: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in Table 4.

Table 4 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

`ca`: Specifies the CA certificate.

`local`: Specifies the local certificates.

peer: Specifies the peer certificates.

serial *serial-num*: Specifies the serial number of a peer certificate.

Usage guidelines

If you specify the **CA** keyword, this command displays information about all CA certificates in the domain. If the domain has RA certificates, the RA certificates are also displayed.

If you specify the **local** keyword, this command displays information about all local certificates in the domain.

If you specify the **peer** keyword without a serial number, this command displays brief information about all peer certificates. If you specify a serial number, this command display detailed information about the specified peer certificate.

Examples

Display information about the CA certificate in PKI domain **aaa**.

```
<Sysname> display pki certificate domain aaa ca
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number:
            5c:72:dc:c4:a5:43:cd:f9:32:b9:c1:90:8f:dd:50:f6
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=cn, O=docm, OU=rnd, CN=rootca
        Validity
            Not Before: Jan  6 02:51:41 2011 GMT
            Not After : Dec  7 03:12:05 2013 GMT
        Subject: C=cn, O=ccc, OU=ppp, CN=rootca
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:c4:fd:97:2c:51:36:df:4c:ea:e8:c8:70:66:f0:
                    28:98:ec:5a:ee:d7:35:af:86:c4:49:76:6e:dd:40:
                    4a:9e:8d:c0:cb:d9:10:9b:61:eb:0c:e0:22:ce:f6:
                    57:7c:bb:bb:1b:1d:b6:81:ad:90:77:3d:25:21:e6:
                    7e:11:0a:d8:1d:3c:8e:a4:17:1e:8c:38:da:97:f6:
                    6d:be:09:e3:5f:21:c5:a0:6f:27:4b:e3:fb:9f:cd:
                    c1:91:18:ff:16:ee:d8:cf:8c:e3:4c:a3:1b:08:5d:
                    84:7e:11:32:5f:1a:f8:35:25:c0:7e:10:bd:aa:0f:
                    52:db:7b:cd:5d:2b:66:5a:fb
                Exponent: 65537 (0x10001)
    Signature Algorithm: sha1WithRSAEncryption
        6d:b1:4e:d7:ef:bb:1d:67:53:67:d0:8f:7c:96:1d:2a:03:98:
        3b:48:41:08:a4:8f:a9:c1:98:e3:ac:7d:05:54:7c:34:d5:ee:
        09:5a:11:e3:c8:7a:ab:3b:27:d7:62:a7:bb:bc:7e:12:5e:9e:
        4c:1c:4a:9f:d7:89:ca:20:46:de:c5:b3:ce:36:ca:5e:6e:dc:
        e7:c6:fe:3f:c5:38:dd:d5:a3:36:ad:f4:3d:e6:32:7f:48:df:
        07:f0:a2:32:89:86:72:22:cd:ed:e5:0f:95:df:9c:75:71:e7:
        fe:34:c5:a0:64:1c:f0:5c:e4:8f:d3:00:bd:fa:90:b6:64:d8:
        88:a6
```

Display information about local certificates in the PKI domain **aaa**.

```
<Sysname> display pki certificate domain aaa local
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            bc:05:70:1f:0e:da:0d:10:16:1e
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=CN, O=sec, OU=software, CN=abdfdc
        Validity
            Not Before: Jan  7 20:05:44 2011 GMT
            Not After : Jan  7 20:05:44 2012 GMT
        Subject: O=OpenCA Labs, OU=Users, CN=fips fips-sec
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:b2:38:ad:8c:7d:78:38:37:88:ce:cc:97:17:39:
                    52:e1:99:b3:de:73:8b:ad:a8:04:f9:a1:f9:0d:67:
                    d8:95:e2:26:a4:0b:c2:8c:63:32:5d:38:3e:fd:b7:
                    4a:83:69:0e:3e:24:e4:ab:91:6c:56:51:88:93:9e:
                    12:a4:30:ad:ae:72:57:a7:ba:fb:bc:ac:20:8a:21:
                    46:ea:e8:93:55:f3:41:49:e9:9d:cc:ec:76:13:fd:
                    a5:8d:cb:5b:45:08:b7:d1:c5:b5:58:89:47:ce:12:
                    bd:5c:ce:b6:17:2f:e0:fc:c0:3e:b7:c4:99:31:5b:
                    8a:f0:ea:02:fd:2d:44:7a:67
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Cert Type:
                SSL Client, S/MIME
            X509v3 Key Usage:
                Digital Signature, Non Repudiation, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Client Authentication, E-mail Protection, Microsoft
Smartcardlogin
            Netscape Comment:
                User Certificate of OpenCA Labs
            X509v3 Subject Key Identifier:
                91:95:51:DD:BF:4F:55:FA:E4:C4:D0:10:C2:A1:C2:99:AF:A5:CB:30
            X509v3 Authority Key Identifier:
                keyid:DF:D2:C9:1A:06:1F:BC:61:54:39:FE:12:C4:22:64:EB:57:3B:11:9F

            X509v3 Subject Alternative Name:
                email:fips@ccc.com
            X509v3 Issuer Alternative Name:
                email:pki@openca.org
            Authority Information Access:
```

```
                CA Issuers - URI:http://titan/pki/pub/cacert/cacert.crt
                OCSP - URI:http://titan:2560/
                1.3.6.1.5.5.7.48.12 - URI:http://titan:830/

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://titan/pki/pub/crl/cacrl.crl

    Signature Algorithm: sha256WithRSAEncryption
        94:ef:56:70:48:66:be:8f:9d:bb:77:0f:c9:f4:65:77:e3:bd:
        ea:9a:b8:24:ae:a1:38:2d:f4:ab:e8:0e:93:c2:30:33:c8:ef:
        f5:e9:eb:9d:37:04:6f:99:bd:b2:c0:e9:eb:b1:19:7e:e3:cb:
        95:cd:6c:b8:47:e2:cf:18:8d:99:f4:11:74:b1:1b:86:92:98:
        af:a2:34:f7:1b:15:ee:ea:91:ed:51:17:d0:76:ec:22:4c:56:
        da:d6:d1:3c:f2:43:31:4f:1d:20:c8:c2:c3:4d:e5:92:29:ee:
        43:c6:d7:72:92:e8:13:87:38:9a:9c:cd:54:38:b2:ad:ba:aa:
        f9:a4:68:b5:2a:df:9a:31:2f:42:80:0c:0c:d9:6d:b3:ab:0f:
        dd:a0:2c:c0:aa:16:81:aa:d9:33:ca:01:75:94:92:44:05:1a:
        65:41:fa:1e:41:b5:8a:cc:2b:09:6e:67:70:c4:ed:b4:bc:28:
        04:50:a6:33:65:6d:49:3c:fc:a8:93:88:53:94:4c:af:23:64:
        cb:af:e3:02:d1:b6:59:5f:95:52:6d:00:00:a0:cb:75:cf:b4:
        50:c5:50:00:65:f4:7d:69:cc:2d:68:a4:13:5c:ef:75:aa:8f:
        3f:ca:fa:eb:4d:d5:5d:27:db:46:c7:f4:7d:3a:b2:fb:a7:c9:
        de:18:9d:c1
```

Display brief information about all peer certificates in the PKI domain **aaa**.

```
<Sysname> display pki certificate domain aaa peer
Total peer certificates: 1

Serial Number: 9a0337eb2156ba1f5476e4d754a5a9f7
Subject  Name: CN=sldsslserver
```

Display detailed information about a peer certificate in the PKI domain **aaa**.

```
<Sysname> display pki certificate domain aaa peer serial 9a0337eb2156ba1f5476e4d754a5a9f7

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            9a:03:37:eb:21:56:ba:1f:54:76:e4:d7:54:a5:a9:f7
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=cn, O=ccc, OU=sec, CN=ssl
        Validity
            Not Before: Oct 15 01:23:06 2010 GMT
            Not After : Jul 26 06:30:54 2012 GMT
        Subject: CN=sldsslserver
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
```

```
                Modulus:
                    00:c2:cf:37:76:93:29:5e:cd:0e:77:48:3a:4d:0f:
                    a6:28:a4:60:f8:31:56:28:7f:81:e3:17:47:78:98:
                    68:03:5b:72:f4:57:d3:bf:c5:30:32:0d:58:72:67:
                    04:06:61:08:3b:e9:ac:53:b9:e7:69:68:1a:23:f2:
                    97:4c:26:14:c2:b5:d9:34:8b:ee:c1:ef:af:1a:f4:
                    39:da:c5:ae:ab:56:95:b5:be:0e:c3:46:35:c1:52:
                    29:9c:b7:46:f2:27:80:2d:a4:65:9a:81:78:53:d4:
                    ca:d3:f5:f3:92:54:85:b3:ab:55:a5:03:96:2b:19:
                    8b:a3:4d:b2:17:08:8d:dd:81
                Exponent: 65537 (0x10001)
            X509v3 extensions:
                X509v3 Authority Key Identifier:
                    keyid:9A:83:29:13:29:D9:62:83:CB:41:D4:75:2E:52:A1:66:38:3C:90:11

                X509v3 Key Usage: critical
                    Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment,
    Key Agreement
                Netscape Cert Type:
                    SSL Server
                X509v3 Subject Alternative Name:
                    DNS:docm.com
                X509v3 Subject Key Identifier:
                    3C:76:95:9B:DD:C2:7F:5F:98:83:B7:C7:A0:F8:99:1E:4B:D7:2F:26
                X509v3 CRL Distribution Points:

                    Full Name:
                      URI:http://s03130.ccc.sec.com:447/ssl.crl

        Signature Algorithm: sha1WithRSAEncryption
            61:2d:79:c7:49:16:e3:be:25:bb:8b:70:37:31:32:e5:d3:e3:
            31:2c:2d:c1:f9:bf:50:ad:35:4b:c1:90:8c:65:79:b6:5f:59:
            36:24:c7:14:63:44:17:1e:e4:cf:10:69:fc:93:e9:70:53:3c:
            85:aa:40:7e:b5:47:75:0f:f0:b2:da:b4:a5:50:dd:06:4a:d5:
            17:a5:ca:20:19:2c:e9:78:02:bd:19:77:da:07:1a:42:df:72:
            ad:07:7d:e5:16:d6:75:eb:6e:06:58:ee:76:31:63:db:96:a2:
            ad:83:b6:bb:ba:4b:79:59:9d:59:6c:77:59:5b:d9:07:33:a8:
            f0:a5
```

Related commands

pki domain

pki retrieve-certificate

display pki certificate renew-status

Use **display pki certificate renew-status** to display the certificate renewal status for a PKI domain.

Syntax

display pki certificate renew-status [**domain** *domain-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in Table 5. If you do not specify a domain name, this command displays the certificate renewal status for all PKI domains.

Table 5 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

Examples

Display the certificate renewal status for all PKI domains.

```
<Sysname> display pki certificate renew-status
Domain Name: domain1
Renew Time : 03:12:05 2016-06-13
Renew public key:
  Key type: RSA
  Time when key pair created: 15:40:48 2016/06/13
  Key code:
    30819F300D06092A864886F70D010101050003818D0030818902818100DAA4AAFEFE04C2C9
    667269BB8226E26331E30F41A8FF922C7338208097E84332610632B49F75DABF6D871B80CE
    C1BA2B75020077C74745C933E2F390DC0B39D35B88283D700A163BB309B19F8F87216A44AB
    FBF6A3D64DEB33E5CEBF2BCF26296778A26A84F4F4C5DBF8B656ACFA62CD96863474899BC1
    2DA4C04EF5AE0835090203010001
```

The command output indicates that the **reuse-public-key** keyword was not configured for PKI domain **domain1** and a new key pair was created for the new certificate.

Display the certificate renewal status for PKI domain **domain1**.

```
<Sysname> display pki certificate renew-status domain domain1
Domain Name: domain1
Renew Time : 03:12:05 2016-06-13
Renew public key:
  Key type: RSA
```

```
Time when  key pair created: 15:40:48 2016/06/13
Key code:
  30819F300D06092A864886F70D010101050003818D0030818902818100DAA4AAFEFE04C2C9
  667269BB8226E26331E30F41A8FF922C7338208097E84332610632B49F75DABF6D871B80CE
  C1BA2B75020077C74745C933E2F390DC0B39D35B88283D700A163BB309B19F8F87216A44AB
  FBF6A3D64DEB33E5CEBF2BCF26296778A26A84F4F4C5DBF8B656ACFA62CD96863474899BC1
  2DA4C04EF5AE0835090203010001
```

Table 6 Command output

Field	Description
Renew Time	Time when a new certificate will be requested.
Renew public key	Information about the new key pair created for the certificate. The renewed public key information is displayed only if the certificate renewal process is slow or has failed.
Key type	Key pair type, which can be RSA, DSA, SM2, or ECDSA.
Time when key pair created	Time when the key pair was created.
Key code	Public key data.

Related commands

`certificate request mode`

`pki domain`

display pki certificate request-status

Use **`display pki certificate request-status`** to display certificate request status.

Syntax

`display pki certificate request-status` [**`domain`** *`domain-name`*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

`domain-name`: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in Table 7.

Table 7 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<

Character name	Symbol	Character name	Symbol
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

Usage guidelines

If you do not specify a PKI domain, this command displays the certificate request status for all PKI domains.

Examples

Display certificate request status for PKI domain **aaa**.

```
<Sysname> display pki certificate request-status domain aaa
Certificate Request Transaction 1
    Domain name: aaa
    Status: Pending
    Key usage: General
    Remain polling attempts: 10
    Next polling attempt after : 1191 seconds
```

Display certificate request statuses for all PKI domains.

```
<Sysname> display pki certificate request-status
Certificate Request Transaction 1
    Domain name: domain1
    Status: Pending
    Key usage: General
    Remain polling attempts: 10
    Next polling attempt after : 1191 seconds
Certificate Request Transaction 2
    Domain name: domain2
    Status: Pending
    Key usage: Signature
    Remain polling attempts: 10
    Next polling attempt after : 188 seconds
```

Table 8 Command output

Field	Description
Certificate Request Transaction *number*	Certificate request transaction number, starting from 1.
Status	Certificate request status, including only the pending status.
Key usage	Certificate purposes: • **General**—Signature and encryption. • **Signature**—Signature only. • **Encryption**—Encryption only.
Remain polling attempts	Remaining number of attempts to query certificate request status.
Next polling attempt after	Remaining seconds before the next request status polling.

Related commands

certificate request polling

pki domain

pki retrieve-certificate

display pki crl domain

Use **display pki crl domain** to display information about the CRL saved at the local for a PKI domain.

Syntax

display pki crl domain *domain-name*

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in Table 9.

Table 9 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

Usage guidelines

Use this command to determine whether a certificate has been revoked.

Examples

Display information about the CRL saved at the local for PKI domain **aaa**.

```
<Sysname> display pki crl domain aaa
Certificate Revocation List (CRL):
        Version 2 (0x1)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: /C=cn/O=docm/OU=sec/CN=therootca
        Last Update: Apr 28 01:42:13 2011 GMT
        Next Update: NONE
        CRL extensions:
            X509v3 CRL Number:
```

```
                6
            X509v3 Authority Key Identifier:
                keyid:49:25:DB:07:3A:C4:8A:C2:B5:A0:64:A5:F1:54:93:69:14:51:11:EF

Revoked Certificates:
    Serial Number: CDE626BF7A44A727B25F9CD81475C004
        Revocation Date: Apr 28 01:37:52 2011 GMT
        CRL entry extensions:
            Invalidity Date:
                Apr 28 01:37:49 2011 GMT
    Serial Number: FCADFA81E1F56F43D3F2D3EF7EB56DE5
        Revocation Date: Apr 28 01:33:28 2011 GMT
        CRL entry extensions:
            Invalidity Date:
                Apr 28 01:33:09 2011 GMT
    Signature Algorithm: sha1WithRSAEncryption
        57:ac:00:3e:1e:e2:5f:59:62:04:05:9b:c7:61:58:2a:df:a4:
        5c:e5:c0:14:af:c8:e7:de:cf:2a:0a:31:7d:32:da:be:cd:6a:
        36:b5:83:e8:95:06:bd:b4:c0:36:fe:91:7c:77:d9:00:0f:9e:
        99:03:65:9e:0c:9c:16:22:ef:4a:40:ec:59:40:60:53:4a:fc:
        8e:47:57:23:e0:75:0a:a4:1c:0e:2f:3d:e0:b2:87:4d:61:8a:
        4a:cb:cb:37:af:51:bd:53:78:76:a1:16:3d:0b:89:01:91:61:
        52:d0:6f:5c:09:59:15:be:b8:68:65:0c:5d:1b:a1:f8:42:04:
        ba:aa
```

Table 10 Command output

Field	Description
Version	CRL version number.
Signature Algorithm	Signature algorithm used by the CA to sign the CRL.
Issuer	Name of the CA that issued the CRL.
Last Update	Most recent CRL update time.
Next Update	Next CRL update time.
X509v3 Authority Key Identifier	X509v3 ID of the CA that issues the CRL.
keyid	Key ID. This field identifies the key pair used to sign the CRL.
Signature Algorithm:	Signature algorithm and signature data.

Related commands

`pki retrieve-crl`

fqdn

Use **`fqdn`** to set the FQDN of an entity.

Use **`undo fqdn`** to restore the default.

Syntax

fqdn *fqdn-name-string*

undo fqdn

Default

No FQDN is set for a PKI entity.

Views

PKI entity view

Predefined user roles

network-admin

context-admin

Parameters

fqdn-name-string: Specifies an FQDN, a case-sensitive string of 1 to 255 characters in the format of *hostname@domainname*.

Usage guidelines

An FQDN uniquely identifies a PKI entity on a network.

Examples

Set the FQDN to **pki.domain-name.com** for PKI entity **en**.

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en] fqdn abc@pki.domain.com
```

ip

Use **ip** to assign an IP address to a PKI entity.

Use **undo ip** to restore the default.

Syntax

ip { *ip-address* | **interface** *interface-type interface-number* }

undo ip

Default

No IP address is assigned to the PKI entity.

Views

PKI entity view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies an IPv4 address.

interface *interface-type interface-number*: Specifies an interface by its type and number. The primary IPv4 address of the interface will be used as the IP address of the PKI entity.

Usage guidelines

Use this command to assign an IP address to a PKI entity or specify an interface for the entity. The interface's primary IPv4 address will be used as the IP address of the PKI entity. If you specify an interface, make sure the interface is assigned an IP address before the PKI entity requests a certificate.

Examples

Assign IP address **192.168.0.2** to PKI entity **en**.

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en] ip 192.168.0.2
```

ldap-server

Use **ldap-server** to specify an LDAP server for a PKI domain.

Use **undo ldap-server** to restore the default.

Syntax

ldap-server host *hostname* [**port** *port-number*] [**vpn-instance** *vpn-instance-name*]

undo ldap-server

Default

No LDAP server is specified for a PKI domain.

Views

PKI domain view

Predefined user roles

network-admin

context-admin

Parameters

host *hostname*: Specifies an LDAP server by its IPv4 address, IPv6 address, or domain name. The domain name is a case-sensitive string of 1 to 255 characters.

port *port-number*: Specifies the port number of the LDAP server. The value range is 1 to 65535, and the default is 389.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If the LDAP server is on the public network, do not specify this option.

Usage guidelines

You must specify an LDAP server for a PKI domain in the following situations:

- The certificate repository uses LDAP for certificate distribution.
- The CRL repository uses LDAP for CRL distribution. However, the CRL repository URL configured for the PKI domain does not contain the IP address or host name of the LDAP server.

You can specify only one LDAP server for a PKI domain. If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify LDAP server **10.0.0.1** for PKI domain **aaa**.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] ldap-server host 10.0.0.1
```

Specify LDAP server **10.0.0.11** in VPN instance **vpn1** for PKI domain **aaa**. Set the port number to **333**.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] ldap-server host 10.0.0.11 port 333 vpn-instance vpn1
```

Related commands

pki retrieve-certificate

pki retrieve-crl

locality

Use **locality** to set the locality of a PKI entity.

Use **undo locality** to restore the default.

Syntax

locality *locality-name*

undo locality

Default

No locality is set for a PKI entity.

Views

PKI entity view

Predefined user roles

network-admin

context-admin

Parameters

locality-name: Specifies a locality, a case-sensitive string of 1 to 63 characters. No comma can be included. You can set a city name as the locality.

Examples

Set the locality to **pukras** for PKI entity **en**.

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en] locality pukras
```

organization

Use **organization** to set an organization name for a PKI entity.

Use **undo organization** to restore the default.

Syntax

organization *org-name*

undo organization

Default

No organization name is set for a PKI entity.

Views

PKI entity view

Predefined user roles

network-admin

context-admin

Parameters

org-name: Specifies an organization name, a case-sensitive string of 1 to 63 characters. No comma can be included.

Examples

Set the organization name to **abc** for PKI entity **en**.

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en] organization abc
```

organization-unit

Use **organization-unit** to set an organization unit name for a PKI entity.

Use **undo organization-unit** to restore the default.

Syntax

organization-unit *org-unit-name*

undo organization-unit

Default

No organization unit name is set for a PKI entity.

Views

PKI entity view

Predefined user roles

network-admin

context-admin

Parameters

org-unit-name: Specifies an organization unit name, a case-sensitive string of 1 to 63 characters. No commas can be included.

Examples

Set the organization unit name to **rdtest** for PKI entity **en**.

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en] organization-unit rdtest
```

pkcs7-encryption-algorithm

Use **pkcs7-encryption-algorithm** to specify the encryption algorithm for certificate files in PKCS#7 format.

Use **undo pkcs7-encryption-algorithm** to restore the default.

Syntax

pkcs7-encryption-algorithm { **3des-cbc** | **aes-cbc-128** | **des-cbc** | **sm4-cbc** }

undo pkcs7-encryption-algorithm

Default

The DES-CBC encryption algorithm is used.

Views

PKI domain view

Predefined user roles

network-admin

context-admin

Parameters

3des-cbc: Specifies the 3DES algorithm in CBC mode, which uses a 168-bit key.

des-cbc: Specifies the DES algorithm in CBC mode, which uses a 56-bit key.

sm4-cbc: Specifies SM4 algorithm in CBC mode, which uses a 128-bit key.

aes-cbc-128: Specifies the AES algorithm in CBC mode, which uses a 128-bit key.

Usage guidelines

During online certificate request, the device uses the specified encryption algorithm to encrypt the certificate signing request in PKCS#7 format before sending the request to the CA. After obtaining the certificate issued by the CA, the device uses the encryption algorithm to decrypt the certificate file in PKCS#7 format. Make sure the specified encryption algorithm is supported on the CA server.

Examples

Specify the 3DES algorithm in CBC mode as the encryption algorithm for certificate files in PKCS#7 format.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] pkcs7-encryption-algorithm 3des-cbc
```

pki abort-certificate-request

Use **pki abort-certificate-request** to abort the certificate request for a PKI domain.

Syntax

pki abort-certificate-request domain *domain-name*

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in Table 11.

Table 11 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

Usage guidelines

You can abort a certificate request and change some parameters, such as common name, country code, or FQDN, in the certificate request before the CA issues the certificate. Use the **display pki certificate request-status** command to display the certificate request status.

Examples

Abort the certificate request for PKI domain 1.

```
<Sysname> system-view
[Sysname] pki abort-certificate-request domain 1
The certificate request is in process.
Confirm to abort it? [Y/N]:y
```

Related commands

display pki certificate request-status

pki request-certificate domain

pki certificate access-control-policy

Use **pki certificate access-control-policy** to create a certificate-based access control policy and enter its view, or enter the view of an existing certificate-based access control policy.

Use **undo pki certificate access-control-policy** to remove a certificate-based access control policy.

Syntax

pki certificate access-control-policy *policy-name*

undo pki certificate access-control-policy *policy-name*

Default

No certificate-based access control policies exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies a policy name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

A certificate-based access control policy contains a set of access control rules that permit or deny access to the device based on the attributes in the requesting client's certificate.

Examples

Create a certificate-based access control policy named **mypolicy** and enter its view.

```
<Sysname> system-view
[Sysname] pki certificate access-control-policy mypolicy
[Sysname-pki-cert-acp-mypolicy]
```

Related commands

display pki certificate access-control-policy

rule

pki certificate attribute-group

Use **pki certificate attribute-group** to create a certificate attribute group and enter its view, or enter the view of an existing certificate attribute group.

Use **undo pki certificate attribute-group** to remove a certificate attribute group.

Syntax

pki certificate attribute-group *group-name*

undo pki certificate attribute-group *group-name*

Default

No certificate attribute groups exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a group name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

A certificate attribute group is a set of attribute rules configured by using the **attribute** command. Each attribute rule defines a matching criterion for an attribute in the issuer name, subject name, or alternative subject name field of certificates.

A certificate attribute group must be associated with an access control rule (a permit or deny statement configured by using the **rule** command). If a certificate attribute group does not have any attribute rules, the system determines that the all certificates match the associated access control rule.

Examples

Create a certificate attribute group named **mygroup** and enter its view.

```
<Sysname> system-view
```

```
[Sysname] pki certificate attribute-group mygroup
[Sysname-pki-cert-attribute-group-mygroup]
```

Related commands

attribute

display pki certificate attribute-group

rule

pki certificate logging enable

Use **pki certificate logging enable** to enable local certificate expiration notification.

Use **undo pki certificate logging enable** to disable local certificate expiration notification.

Syntax

pki certificate logging { **local-will-expire** | **local-has-expired** } **enable**

undo pki certificate logging { **local-will-expire** | **local-has-expired** } **enable**

Default

Local certificate expiration notification is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

local-will-expire: Sends expiration notifications for local certificates every other day starting from 30 days prior to expiration.

local-has-expired: Sends expiration notifications for local certificates every other day starting from the expiration day.

Usage guidelines

After this feature is enabled, the system checks the validity date for local certificates every other hour. When a local certificate is about to expire in 30 days (included) or has expired, the system sends a notification log message for the certificate every other day.

Examples

Enable the device to send expiration notifications for local certificates every other day starting from 30 days prior to expiration.

```
<Sysname> system-view
[Sysname] pki certificate logging local-will-expire enable
```

pki delete-certificate

Use **pki delete-certificate** to remove certificates from a PKI domain.

Syntax

pki delete-certificate domain *domain-name* { **ca** | **local** | **peer** [**serial** *serial-num*] }

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in Table 12.

Table 12 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

ca: Specifies the CA certificate.

local: Specifies the local certificates.

peer: Specifies the peer certificates.

serial *serial-num*: Specifies a peer certificate by its serial number, a case-insensitive string of 1 to 127 characters. If you do not specify a serial number, this command removes all peer certificates in the PKI domain.

Usage guidelines

When you remove the CA certificate in a PKI domain, the system also removes the local certificates, peer certificates, and the CRL in the PKI domain.

To delete a specific peer certificate in a PKI domain, perform the following steps:

1. Execute the **display pki certificate** command to determine the serial number of the peer certificate.
2. Execute the **pki delete-certificate domain** *domain-name* **peer serial** *serial-num* command.

Examples

Remove the CA certificate in PKI domain **aaa**.

```
<Sysname> system-view
[Sysname] pki delete-certificate domain aaa ca
Local certificates, peer certificates and CRL will also be deleted while deleting the CA certificate.
Confirm to delete the CA certificate? [Y/N]:y
[Sysname]
```

Remove the local certificates in PKI domain **aaa**.

```
<Sysname> system-view
[Sysname] pki delete-certificate domain aaa local
[Sysname]
```

Remove all peer certificates in PKI domain **aaa**.

```
<Sysname> system-view
[Sysname] pki delete-certificate domain aaa peer
[Sysname]
```

Display information about all peer certificates in PKI domain **aaa**, and remove a peer certificate with the specified serial number.

```
<Sysname> system-view
[Sysname] display pki certificate domain aaa peer
Total peer certificates: 1

Serial Number: 9a0337eb2156ba1f5476e4d754a5a9f7
Subject  Name: CN=abc
[Sysname] pki delete-certificate domain aaa peer serial 9a0337eb2156ba1f5476e4d754a5a9f7
```

Related commands

display pki certificate

pki domain

Use **pki domain** to create a PKI domain and enter its view, or enter the view of an existing PKI domain.

Use **undo pki domain** to remove a PKI domain.

Syntax

pki domain *domain-name*

undo pki domain *domain-name*

Default

No PKI domains exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

domain-name: Specifies a PKI domain name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in Table 13.

Table 13 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>

Character name	Symbol	Character name	Symbol
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

Usage guidelines

When you remove a PKI domain, the certificates and the CRL in the domain are also removed.

Examples

Create a PKI domain named **aaa** and enter its view.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa]
```

pki entity

Use **pki entity** to create a PKI entity and enter its view, or enter the view of an existing PKI entity.

Use **undo pki entity** to remove a PKI entity.

Syntax

pki entity *entity-name*

undo pki entity *entity-name*

Default

No PKI entities exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

entity-name: Specifies a name for a PKI entity, a case-insensitive string of 1 to 31 characters.

Usage guidelines

A PKI entity includes the identity information that can be used by a CA to identify a certificate applicant. You can configure multiple attributes for a PKI entity, such as common name, organization, organization unit, locality, state, country, FQDN, and IP address. The information will be included as subject contents in the certificate issued by the CA.

Examples

Create a PKI entity named **en** and enter its view.

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en]
```

Related commands

pki domain

pki export

Use **pki export** to export the CA certificate and the local certificates in a PKI domain.

Syntax

pki export domain *domain-name* **der** { **all** | **ca** | **local** } **filename** *filename*

pki export domain *domain-name* **p12** { **all** | **local** } **passphrase** *p12-key* **filename** *filename*

pki export domain *domain-name* **pem** { { **all** | **local** } [{ **3des-cbc** | **aes-128-cbc** | **aes-192-cbc** | **aes-256-cbc** | **des-cbc** } *pem-key*] | **ca** } [**filename** *filename*]

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in Table 14.

Table 14 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

der: Specifies the DER certificate file format, including PKCS#7.

p12: Specifies the PKCS#12 certificate file format.

pem: Specifies the PEM certificate file format.

all: Specifies both CA and local certificates. The RA certificate is excluded.

ca: Specifies the CA certificate.

local: Specifies the local certificates or the local certificates and their private keys.

passphrase *p12-key*: Specifies a password for encrypting the private key of a local PKCS12 certificate.

3des-cbc: Specifies 3DES_CBC for encrypting the private key of a local certificate.

aes-128-cbc: Specifies 128-bit AES_CBC for encrypting the private key of a local certificate.

aes-192-cbc: Specifies 192-bit AES_CBC for encrypting the private key of a local certificate.

aes-256-cbc: Specifies 256-bit AES_CBC for encrypting the private key of a local certificate.

des-cbc: Specifies DES_CBC for encrypting the private key of a local certificate.

pem-key: Specifies a password for encrypting the private key of a local certificate in PEM format.

filename *filename*: Specifies the name of the file for storing the certificate. The file name is a case-insensitive string. If you do not specify a file name when you export certificates in PEM format, this command displays the certificates on the terminal.

Usage guidelines

When you export the CA certificate, the following conditions might exist:

- If the PKI domain has only one CA certificate, this command exports the CA certificate to a file or displays it on the terminal.
- If the PKI domain has a CA certificate chain, this command exports the certificate chain to a file or displays it on the terminal.

When you export a local certificate to a local file, the local file name might be different from the file name specified in the command. The file name depends on the usage of the key pair contained in the certificate.

The following example uses **certificate** as the file name for saving an exported local certificate.

- If the local certificate contains an RSA signing key pair, the local file name is **certificate-signature**.
- If the local certificate contains an RSA encryption key pair, the local file name is **certificate-encryption**.
- If the local certificate contains a general purpose RSA, ECDSA, or DSA key pair, the local file name is **certificate**.

If the PKI domain has two local certificates, the local certificates are exported as follows:

- If you specify a file name, the two local certificates are exported to two different files.
- If you do not specify a file name, the local certificates are displayed on the terminal, separated by system prompts.

When you export all certificates, the following conditions might exist:

- If the PKI domain has only the CA certificate or local certificates, the result is the same as when you export the CA certificate or local certificates separately.
- If the PKI domain has both the CA certificate and local certificates, you get the following results:
  - If you specify a file name, each local certificate is exported to a separate file with their associated CA certificate chain.
  - If you do not specify a file name, the local certificates and CA certificate or CA certificate chain are displayed on the terminal, separated by system prompts.

When you export all certificates in PKCS12 format, the PKI domain must have a local certificate. If the domain does not have a local certificate, the export operation fails. If a local certificate does not have a matching private key, the export of that local certificate fails.

When you export the local certificates or all certificates in PEM format, the local certificates are exported as follows:

- If you do not specify the cryptographic algorithm or password for encrypting a private key, this command does not export the private keys of the local certificates.
- If you specify the cryptographic algorithm and password and the local certificates have matching private keys, this command exports the local certificates with their private keys.
- If you specify the cryptographic algorithm and password but the local certificates do not have matching private keys, the export operation fails.

If the matching private key of a local certificate is an SM2 key created by a crypto device, the certificate cannot be exported in PKCS12 or PEM format.

When you export the local certificates, if the key pair in the PKI domain is changed and no longer matches the key in the local certificates, the export operation fails.

When you export the local certificates or all certificates, if the PKI domain has two local certificates, failure of exporting one local certificate does not affect export of the other.

The specified file name can contain an absolute path. If the specified path does not exist, the export operation fails.

Examples

Export the CA certificate in the PKI domain to a file named **cert-ca.der** in DER format.

```
<Sysname> system-view
[Sysname] pki export domain domain1 der ca filename cert-ca.der
```

Export the local certificates in the PKI domain to a file named **cert-lo.der** in DER format.

```
<Sysname> system-view
[Sysname] pki export domain domain1 der local filename cert-lo.der
```

Export all certificates in the PKI domain to a file named **cert-all.p7b** in DER format.

```
<Sysname> system-view
[Sysname] pki export domain domain1 der all filename cert-all.p7b
```

Export the CA certificate in the PKI domain to a file named **cacert** in PEM format.

```
<Sysname> system-view
[Sysname] pki export domain domain1 pem ca filename cacert
```

Export the local certificates and their private keys in the PKI domain to a file named **local.pem** in PEM format. For the private keys, the cryptographic algorithm is DES_CBC and the password is 111.

```
<Sysname> system-view
[Sysname] pki export domain domain1 pem local des-cbc 111 filename local.pem
```

Export the all certificates in the PKI domain to a file named **all.pem** in PEM format. No cryptographic algorithm or password is specified, and the private keys are not exported.

```
<Sysname> system-view
[Sysname] pki export domain domain1 pem all filename all.pem
```

Display the local certificates and their private keys in the PKI domain on the terminal in PEM format. For the private keys, the cryptographic algorithm is DES_CBC and the password is 111.

```
<Sysname> system-view
[Sysname] pki export domain domain1 pem local des-cbc 111

*** The general usage local certificate: ***
Bag Attributes
    friendlyName:
    localKeyID: 99 0B C2 3B 8B D1 E4 33 42 2B 31 C3 37 C0 1D DF 0D 79 09 1D
subject=/C=CN/O=OpenCA Labs/OU=Users/CN=chktest chktest
issuer=/C=CN/O=OpenCA Labs/OU=software/CN=abcd
-----BEGIN CERTIFICATE-----
MIIEqjCCA5KgAwIBAgILAOhID4rI04kBfYgwDQYJKoZIhvcNAQELBQAwRTELMAkG
A1UEBhMCQ04xFDASBgNVBAoMC09wZW5DQSBMYWJzMREwDwYDVQQLDAhzb2Z0d2Fy
ZTENMAsGA1UEAwwEYWJjZDAeFw0xMTA0MjYxMzMxMjlaFw0xMjA0MjUxMzMxMjla
ME0xCzAJBgNVBAYTAkNOMRQwEgYDVQQKDAtPcGVuQ0EgTGFiczEOMAwGA1UECwwF
VXNlcnMxGDAWBgNVBAMMD2Noa3Rlc3QgY2hrdGVzdDCBnzANBgkqhkiG9w0BAQEF
AAOBjQAwgYkCgYEA54rUZ0Ux2kApceE4ATpQ437CU6ovuHS5eJKZyky8fhMoTHhE
jE2KfBQIzOZSgo2mdgpkccjr9Ek6IUC03ed1lPn0IG/YaAl4Tjgkiv+w1NrlSvAy
cnPaSUko2QbO9sg3ycye1zqpbbqj775ulGpcXyXYD9OY63/Cp5+DRQ92zGsCAwEA
AaOCAhUwggIRMAkGA1UdEwQCMAAwUAYDVR0gBEkwRzAGBgQqAwMEMAYGBCoDAwUw
NQYEKgMDBjAtMCsGCCsGAQUFBwIBFh9odHRwczovL3RpdGFuL3BraS9wdWIvY3Bz
```

```
L2Jhc2ljMBEGCWCGSAGG+EIBAQQEAwIFoDALBgNVHQ8EBAMCBsAwKQYDVR0lBCIw
IAYIKwYBBQUHAwIGCCsGAQUFBwMEBgorBgEEAYI3FAICMC4GCWCGSAGG+EIBDQQh
Fh9Vc2VyIENlcnRpZmljYXRlIG9mIE9wZW5DQSBMYWJzMB0GA1UdDgQWBBTPw8FY
ut7Xr2Ct/23zU/ybgU9dQjAfBgNVHSMEGDAWgBQzEQ58yIC54wxodp6JzZvn/gx0
CDAaBgNVHREEEzARgQ9jaGt0ZXN0QGgzYy5jb20wGQYDVR0SBBIwEIEOcGtpQG9w
ZW5jYS5vcmcwgYEGCCsGAQUFBwEBBHUwczAyBggrBgEFBQcwAoYmaHR0cDovL3Rp
dGFuL3BraS9wdWIvY2FjZXJ0L2NhY2VydC5jcnQwHgYIKwYBBQUHMAGGEmh0dHA6
Ly90aXRhbjoyNTYwLzAdBggrBgEFBQcwDIYRaHR0cDovL3RpdGFuOjgzMC8wPAYD
VR0fBDUwMzAxoC+gLYYraHR0cDovLzE5Mi4xNjguNDAuMTI4L3BraS9wdWIvY3Js
L2NhY3JsLmNybDANBgkqhkiG9w0BAQsFAAOCAQEAGcMeSpBJiuRmsJW0iZK5nygB
tgD8c0b+n4v/F36sJjY1fRFSr4gPLIxZhPWhTrqsCd+QMELRCDNHDxvt3/1NEG12
X6BVjLcKXKH/EQe0fnwK+7PegAJ15P56xDeACHz2oysvNQ0Ot6hGylMqaZ8pKUKv
UDS8c+HgIBrhmxvXztI08N1imYHq27Wy9j6NpSS60mMFmI5whzCWfTSHzqlT2DNd
no0id18SZidApfCZL8zoMWEFI163JZSarv+H5Kbb063dxXfbsqX9Noxggh0gD8dK
7X7/rTJuuhTWVof5gxSUJp+aCCdvSKg0lvJY+tJeXoaznrINVw3SuXJ+Ax8GEw==
-----END CERTIFICATE-----
Bag Attributes
    friendlyName:
    localKeyID: 99 0B C2 3B 8B D1 E4 33 42 2B 31 C3 37 C0 1D DF 0D 79 09 1D
Key Attributes: <No Attributes>
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIICwzA9BgkqhkiG9w0BBQ0wMDAbBgkqhkiG9w0BBQwwDgQIAbfcE+KoYYoCAggA
MBEGBSsOAwIHBAjB+UsJM07JRQSCAoABqtASbjGTQbdxL3n4wNHmyWLxbvL9v27C
Uu6MjYJDCipVzxHU0rExgn+6cQsK5uK99FPBmy4q9/nnyrooTX8BVlXAjenvgyii
WQLwnIg1IuM8j2aPkQ3wbae1+0RACjSLy1u/PCl5sp6CDxI0b9xz6cxIGxKvUOCc
/gxdgk97XZSW/0qnOSZkhgeqBZuxq6Va8iRyho7RCStVxQaeiAZpq/WoZbcS5CKI
/WXEBQd4AX2UxN0Ld/On7Wc6KFToixROTxWTtf8SEsKGPDfrEKq3fSTW1xokB8nM
bkRtU+fUiY27V/mr1RHO6+yEr+/wGGClBy5YDoD4I9xPkGUkmqx+kfYbMo4yxkSi
JdL+X3uEjHnQ/rvnPSKBEU/URwXHxMX9CdCTSqh/SajnrGuB/E4JhOEnS/H9dIM+
DN6iz1IwPFklbcK9KMGwV1bosymXmuEbYCYmSmhZb5FnR/RIyE804Jz9ifin3g0Q
ZrykfG7LHL7Ga4nh0hpEeEDiHGEMcQU+g0EtfpOLTI8cMJf7kdNWDnI0AYCvBAAM
3CY3BElDVjJq3ioyHSJca8C+3lzcueuAF+lO7Y4Zluq3dqWeuJjE+/1BZJbMmaQA
X6NmXKNzmtTPcMtojf+n3+uju0le0d0QYXQz/wPsV+9IYRYasjzoXE5dhZ5sIPOd
u9x9hhp5Ns23bwyNP135qTNjx9i/CZMKvLKywm3Yg+Bgg8Df4bBrFrsH1U0ifmmp
ir2+OuhlC+GbHOxWNeBCa8iAq91k6FGFJ0OLA2oIvhCnh45tM7BjjKTHk+RZdMiA
0TKSWuOyihrwxdUEWh999GKUpkwDHLZJFd21z/kWspqThodEx8ea
-----END ENCRYPTED PRIVATE KEY-----
```

Display all certificates in the PKI domain in PEM format. For the private keys, the cryptographic algorithm is DES_CBC and the password is 111.

```
<Sysname> system-view
[Sysname] pki export domain domain1 pem all des-cbc 111

 %The signature usage local certificate:
Bag Attributes
    friendlyName:
    localKeyID: 99 0B C2 3B 8B D1 E4 33 42 2B 31 C3 37 C0 1D DF 0D 79 09 1D
subject=/C=CN/O=OpenCA Labs/OU=Users/CN=chktest chktest
issuer=/C=CN/O=OpenCA Labs/OU=software/CN=abcd
```

```
-----BEGIN CERTIFICATE-----
MIIEqjCCA5KgAwIBAgILAOhID4rI04kBfYgwDQYJKoZIhvcNAQELBQAwRTELMAkG
A1UEBhMCQ04xFDASBgNVBAoMC09wZW5DQSBMYWJzMREwDwYDVQQLDAhzb2Z0d2Fy
ZTENMAsGA1UEAwwEYWJjZDAeFw0xMTA0MjYxMzMxMjlaFw0xMjA0MjUxMzMxMjla
ME0xCzAJBgNVBAYTAkNOMRQwEgYDVQQKDAtPcGVuQ0EgTGFiczEOMAwGA1UECwwF
VXNlcnMxGDAWBgNVBAMMD2Noa3Rlc3QgY2hrdGVzdDCBnzANBgkqhkiG9w0BAQEF
AAOBjQAwgYkCgYEA54rUZ0Ux2kApceE4ATpQ437CU6ovuHS5eJKZyky8fhMoTHhE
jE2KfBQIzOZSgo2mdgpkccjr9Ek6IUC03ed1lPn0IG/YaAl4Tjgkiv+w1NrlSvAy
cnPaSUko2QbO9sg3ycye1zqpbbqj775ulGpcXyXYD9OY63/Cp5+DRQ92zGsCAwEA
AaOCAhUwggIRMAkGA1UdEwQCMAAwUAYDVR0gBEkwRzAGBgQqAwMEMAYGBCoDAwUw
NQYEKgMDBjAtMCsGCCsGAQUFBwIBFh9odHRwczovL3RpdGFuL3BraS9wdWIvY3Bz
L2Jhc2ljMBEGCWCGSAGG+EIBAQQEAwIFoDALBgNVHQ8EBAMCBsAwKQYDVR0lBCIw
IAYIKwYBBQUHAwIGCCsGAQUFBwMEBgorBgEEAYI3FAICMC4GCWCGSAGG+EIBDQQh
Fh9Vc2VyIENlcnRpZmljYXRlIG9mIE9wZW5DQSBMYWJzMB0GA1UdDgQWBBTPw8FY
ut7Xr2Ct/23zU/ybgU9dQjAfBgNVHSMEGDAWgBQzEQ58yIC54wxodp6JzZvn/gx0
CDAaBgNVHREEEzARgQ9jaGt0ZXN0QGgzYy5jb20wGQYDVR0SBBIwEIEOcGtpQG9w
ZW5jYS5vcmcwgYEGCCsGAQUFBwEBBHUwczAyBggrBgEFBQcwAoYmaHR0cDovL3Rp
dGFuL3BraS9wdWIvY2FjZXJ0L2NhY2VydC5jcnQwHgYIKwYBBQUHMAGGEmh0dHA6
Ly90aXRhbjoyNTYwLzAdBggrBgEFBQcwDIYRaHR0cDovL3RpdGFuOjgzMC8wPAYD
VR0fBDUwMzAxoC+gLYYraHR0cDovLzE5Mi4xNjguNDAuMTI4L3BraS9wdWIvY3Js
L2NhY3JsLmNybDANBgkqhkiG9w0BAQsFAAOCAQEAGcMeSpBJiuRmsJW0iZK5nygB
tgD8c0b+n4v/F36sJjY1fRFSr4gPLIxZhPWhTrqsCd+QMELRCDNHDxvt3/1NEG12
X6BVjLcKXKH/EQe0fnwK+7PegAJ15P56xDeACHz2oysvNQ0Ot6hGylMqaZ8pKUKv
UDS8c+HgIBrhmxvXztI08N1imYHq27Wy9j6NpSS60mMFmI5whzCWfTSHzqlT2DNd
no0id18SZidApfCZL8zoMWEFI163JZSarv+H5Kbb063dxXfbsqX9Noxggh0gD8dK
7X7/rTJuuhTWVof5gxSUJp+aCCdvSKg0lvJY+tJeXoaznrINVw3SuXJ+Ax8GEw==
-----END CERTIFICATE-----
Bag Attributes: <No Attributes>
subject=/C=CN/O=OpenCA Labs/OU=software/CN=abcd
issuer=/C=CN/O=OpenCA Labs/OU=software/CN=abcd
-----BEGIN CERTIFICATE-----
MIIEYTCCA0mgAwIBAgIBFzANBgkqhkiG9w0BAQsFADBFMQswCQYDVQQGEwJDTjEU
MBIGA1UECgwLT3BlbkNBIExhYnMxETAPBgNVBAsMCHNvZnR3YXJlMQ0wCwYDVQQD
DARhYmNkMB4XDTExMDQxODExNDQ0N1oXDTEzMDQxNzExNDQ0N1owRTELMAkGA1UE
BhMCQ04xFDASBgNVBAoMC09wZW5DQSBMYWJzMREwDwYDVQQLDAhzb2Z0d2FyZTEN
MAsGA1UEAwwEYWJjZDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAM1g
vomMF8S4u6q51bOwjKFUBwxyvOy4D897LmOSedaCyDt6Lvp+PBEHfwWBYBpsHhk7
kmnSNhX5dZ6NxunHaARZ2VlcctsYKyvAQapuaThy1tuOcphAB+jQQL9dPoqdk0xp
jvmPDlW+k832Konn9U4dIivS0n+/KMGh0g5UyzHGqUUOo7s9qFuQf5EjQon40TZg
BwUnFYRlvGe7bSQpXjwi8LTyxHPy+dDVjO5CP+rXx5IiToFy1YGWewkyn/WeswDf
Yx7ZludNus5vKWTihgx2Qalgb+sqUMwI/WUET7ghO2dRxPUdUbgIYF0saTndKPYd
4oBgl6M0SMsHhe9nF5UCAwEAAaOCAVowggFWMA8GA1UdEwEB/wQFMAMBAf8wCwYD
VR0PBAQDAgEGMB0GA1UdDgQWBBQzEQ58yIC54wxodp6JzZvn/gx0CDAfBgNVHSME
GDAWgBQzEQ58yIC54wxodp6JzZvn/gx0CDAZBgNVHREEEjAQgQ5wa2lAb3BlbmNh
Lm9yZzAZBgNVHRIEEjAQgQ5wa2lAb3BlbmNhLm9yZzCBgQYIKwYBBQUHAQEEdTBz
MDIGCCsGAQUFBzAChiZodHRwOi8mdcGl0YW4vcGtpL3B1Yi9jYWNlcnQvY2FjZXJ0
LmNydDAeBggrBgEFBQcwAYYSaHR0cDovL3RpdGFuOjI1NjAvMB0GCCsGAQUFBzAM
hhFodHRwOi8mdcGl0YW46ODMwLzA8BgNVHR8ENTAzMDGgL6AthitodHRwOi8vMTky
```

```
LjE2OC40MC4xMjgvcGtpL3B1Yi9jcmwvY2FjcmwuY3JsMA0GCSqGSIb3DQEBCwUA
A4IBAQC0q0SSmvQNfa5ELtRKYF62C/Y8QTLbk6lZDTZuIzN15SGKQcbNM970ffCD
Lk1zosyEVE7PLnii3bZ5khcGO3byyXfluAqRyOGVJcudaw7uIQqgv0AJQ+zaQSHi
d4kQf5QWgYkQ55/C5puOmcMRgCbMpR2lYkqXLDjTIAZIHRZ/sTp6c+ie2bFxi/YT
3xYbO0wDMuGOKJJpsyKTKcbG9NdfbDyFgzEYAobyYqAUB3C0/bMfBduwhQWKSoYE
6vZsPGAEisCmAl3dIp49jPgVkixoShraYF1jLsWzJGlzem8QvWYzOqKEDwq3SV0Z
cXK8gzDBcsobcUMkwIYPAmd1kAPX
-----END CERTIFICATE-----
Bag Attributes
    friendlyName:
    localKeyID: 99 0B C2 3B 8B D1 E4 33 42 2B 31 C3 37 C0 1D DF 0D 79 09 1D
Key Attributes: <No Attributes>
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIICwzA9BgkqhkiG9w0BBQ0wMDAbBgkqhkiG9w0BBQwwDgQIcUSKSW9GVmICAggA
MBEGBSsOAwIHBAi5QZM+lSYWPASCAoBKDYulE5f2BXL9ZhI9zWAJpx2cShz/9PsW
5Qm106D+xSj1eAzkx/m4Xb4xRU8oOAuzu1DlWfSHKXoaa0OoRSiOEX1eg0eo/2vv
CHCvKHfTJr4gVSSa7i4I+aQ6AItrI6q99WlkN/e/IE5U1UE4ZhcsIiFJG+IvG7S8
f9liWQ2CImy/hjgFCD9nqSLN8wUzP7O2SdLVlUb5z4FR6VISZdgTFE8j7ko2HtUs
HVSg0nm114EwPtPMMbHefcuQ6b82y1M+dWfVxBN9K03lN4tZNfPWwLSRrPvjUzBG
dKtjf3/IFdV7/tUMy9JJSpt4iFt1h7SZPcOoGp1ZW+YUR30I7YnFE+9Yp/46KWT8
bk7j0STRnZX/xMy/9E52uHkLdW1ET3TXralLMYt/4jg4M0jUvoi3GS2Kbo+czsUn
gKgqwYnxVfRSvt8d6GBYrpF2tMFS9LEyngPKXExd+m4mAryuT5PhdFTkb1B190Lp
UIBjk3IXnr7AdrhvyLkH0UuQE95emXBD/K0HlD73cMrtmogL8F4yS5B2hpIr/v5/
eW35+1QMnJ9FtHFnVsLx9wl9lX8iNfsoBhg6FQ/hNSioN7rNBe7wwIRzxPVfEhO8
5ajQxWlidRn5RkzfUo6HuAcq02QTpSXI6wf2bzsVmr5sk+fRaELD/cwL6VjtXO6x
ZBLJcUyAwvScrOtTEK7Q5n0I34gQd4qcF0D1x9yQ4sqvTeU/7Jkm6XCPV05/5uiF
RLCfFAwaJMBdIQ6jDQHnpWT67uNDwdEzaPmuTVMme5Woc5zsqE5DY3hWu4oqFdDz
kPLnbX74IZ0gOLki9eIJkVswnF5HkBCKS50ejlW6TgbMNZ+JPk2w
-----END ENCRYPTED PRIVATE KEY-----
```

Display the CA certificate in the PKI domain in PEM format.

```
<Sysname> system-view
[Sysname]pki export domain domain1 pem ca
-----BEGIN CERTIFICATE-----
MIIB+TCCAWICEQDMbgjRKygg3vpGFVY6pa3ZMA0GCSqGSIb3DQEBBQUAMD0xCzAJ
BgNVBAYTAmNuMQwwCgYDVQQKEwNoM2MxETAPBgNVBAsTCGgzYy10ZXN0MQ0wCwYD
VQQDEwQ4MDQzMB4XDTExMDMyMjA0NDQyNFoXDTE0MDMyMzA0MzUyNFowPTELMAkG
A1UEBhMCY24xDDAKBgNVBAoTA2gzYzERMA8GA1UECxMIaDNjLXRlc3QxDTALBgNV
BAMTBDgwNDMwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAOvDAYQhyc++G7h5
eNDzJs22OQjCn/4JqnNKIdKz1BbaJT8/+IueSn9JIsg64Ex2WBeCd/tcmnSW57ag
dCvNIUYXXVOGca2iaSOElqCF4CQfV9zLrBtA7giHD49T+JbxLrrJLmdIQMJ+vYdC
sCxIp3YMAiuCahVLZeXklooqwqIXAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAElm7
W2Lp9Xk4nZVIpVV76CkNe8/C+Id00GCRUUVQFSMvo7Pded76bmYX2KzJSz+DlMqy
TdVrgG9Fp6XTFO80aKJGe6NapsfhJHKS+Q7mL0XpXeMONgK+e3dX7rsDxsY7hF+j
0gwsHrjV7kWvwJvDlhzGW6xbpr4DRmdcao19Cr6o=
-----END CERTIFICATE-----
```

Export the CA certificate in the PKI domain to a file named **cacert** in PEM format.

```
<Sysname> system-view
[Sysname] pki export domain domain1 pem ca filename cacert
```

Display the CA certificate or the CA certificate chain in the PKI domain on the terminal.

```
<Sysname> system-view
[Sysname]pki export domain domain1 pem ca
-----BEGIN CERTIFICATE-----
MIIB7jCCAVcCEQCdSVShJFEMifVG8zRRoSsWMA0GCSqGSIb3DQEBBQUAMDcxCzAJ
BgNVBAYTAmNuMQwwCgYDVQQKEwNoM2MxDDAKBgNVBAsTA2gzYzEMMAoGA1UEAxMD
YWNhMB4XDTExMDEwNjAyNTc0NFoXDTEzMTIwMTAzMTMyMFowODELMAkGA1UEBhMC
Y24xDDAKBgNVBAoTA2gzYzEMMAoGA1UECxMDaDNjMQ0wCwYDVQQDEwRhYWNhMIGf
MA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDcuJsWhAJXEDmowGb5z7VDVms54TKi
xnaNJCWvBOrU64ftvpVB7xQekbkjgAS9FjDyXlLQ8IyIsYIp5ebJr8P+n9i9Pl7j
lBx5mi4XeIldyv2OjfNx5oSQ+gWY9/m1R8uv13RS05r3rxPg+7EvKBjmiy0Giddw
vu3Y3WrjBPp6GQIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAJrQddzVQEiy4AcgtzUL
ltkmlmWoz87+jUsgFB+H+xeyiZE4sancf2UwH8kXWqZ5AuReFCCBC2fkvvQvUGnV
cso7JXAhfw8sUFok9eHz2R+GSoEk5BZFzZ8eCmNyGq9ln6mJsO1hAqMpsCW6G2zh
5mus7FTHhywXpJ22/fnHg61m
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB8DCCAVkCEQD2PBUx/rvslNw9uTrZB3DlMA0GCSqGSIb3DQEBBQUAMDoxCzAJ
BgNVBAYTAmNuMQwwCgYDVQQKEwNoM2MxDDAKBgNVBAsTA2gzYzEPMA0GA1UEAxMG
cm9mdcGNhMB4XDTExMDEwNjAyNTY1OFoXDTEzMTIwNDAzMTMxMFowNzELMAkGA1UE
BhMCY24xDDAKBgNVBAoTA2gzYzEMMAoGA1UECxMDaDNjMQwwCgYDVQQDEwNhY2Ew
gZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAOeklR7DpeEV72N1OLz+dydIDTx0
zVZDdPxF1gQYWSfIBwwFKJEyQ/4y8VIfDIm0EGTM4dsOX/QFwudhl/Czkio3dWLh
Q1y5XCJy68vQKrB82WZ2mah5Nuekus3LSZZBoZKTAOY5MCCMFcULM858dtSq15Sh
xF7tKSeAT7ARlJxTAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEADJQCo6m0RNup0ewa
ItX4XK/tYcJXAQWMA0IuwaWpr+ofqVVgYBPwVpYglhJDOuIZxKdR2pfQOA4f35wM
Vz6kAujLATsEA1GW9ACUWa5PHwVgJk9BDEXhKSJ2e7odmrg/iROhJjc1NMV3pvIs
CuFiCLxRQcMGhCNHlOn4wuydssc=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB8jCCAVsCEFxy3MSlQ835MrnBkI/dUPYwDQYJKoZIhvcNAQEFBQAwOjELMAkG
A1UEBhMCY24xDDAKBgNVBAoTA2gzYzEMMAoGA1UECxMDaDNjMQ8wDQYDVQQDEwZy
b290Y2EwHhcNMTEwMTA2MDI1MTQxWhcNMTMxMjA3MDMxMjA1WjA6MQswCQYDVQQG
EwJjbjEMMAoGA1UEChMDaDNjMQwwCgYDVQQLEwNoM2MxDzANBgNVBAMTBnJvb3Rj
YTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAxP2XLFE230zq6MhwZvAomOxa
7tc1r4bESXZu3UBKno3Ay9kQm2HrDOAizvZXfLu7Gx22ga2Qdz0lIeZ+EQrYHTyO
pBcejDjal/ZtvgnjXyHFoG8nS+P7n83BkRj/Fu7Yz4zjTKMbCF2EfhEyXxr4NSXA
fhC9qg9S23vNXStmWvsCAwEAATANBgkqhkiG9w0BAQUFAAOBgQBtsU7X77sdZ1Nn
0I98lh0qA5g7SEEIpI+pwZjjrH0FVHw01e4JWhHjyHqrOyfXYqe7vH4SXp5MHEqf
14nKIEbexbPONspebtznxv4/xTjd1aM2rfQ95jJ/SN8H8KIyiYZyIs3t5Q+V35x1
cef+NMWgZBzwXOSP0wC9+pC2ZNiIpg==
-----END CERTIFICATE-----
```

Export the local certificates and their private keys in the PKI domain to a file named **cert-lo.der** in PKCS12 format. The password for the private keys is 123.

```
<Sysname> system-view
[Sysname] pki export domain domain1 p12 local passphrase 123 filename cert-lo.der
```

Export all certificates in the PKI domain to a file named **cert-all.p7b** in PKCS12 format.

```
<Sysname> system-view
```

```
[Sysname] pki export domain domain1 p12 all passphrase 123 filename cert-all.p7b
```

Related commands

pki domain

pki import

Use **pki import** to import the CA certificate, local certificates, or peer certificates for a PKI domain.

Syntax

pki import domain *domain-name* { **der** { **ca** | **local** | **peer** } **filename** *filename* | **p12 local filename** *filename* | **pem** { **ca** | **local** | **peer** } [**filename** *filename*] }

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in Table 15.

Table 15 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

der: Specifies the DER certificate file format, including PKCS#7.

p12: Specifies the PKCS#12 certificate file format.

pem: Specifies the PEM certificate file format.

ca: Specifies the CA certificate.

local: Specifies the local certificates.

peer: Specifies the peer certificates.

filename *filename*: Specifies a certificate file name, a case-insensitive string. For a certificate in PEM format, you can also choose to copy and paste the certificate contents on the terminal instead of importing from a file.

Usage guidelines

Use this command to import a certificate in the following situations:

- The CRL repository is not specified or the CA server does not support SCEP.
- The certificate is packed with the server generated key pair in a single file. Only certificate files in PKCS12 or PEM format can contain key pairs.

Before you import certificates, complete the following tasks:

- Use FTP or TFTP to upload the certificate files to the storage media of the device. If FTP or TFTP is not available, display and copy the contents of a certificate to a file on the device. Make sure the certificate is in PEM format because only certificates in PEM format can be imported by this means.
- For the local certificates or peer certificates to be imported, the correct CA certificate chain must exist. The CA certificate chain can be stored on the device, or carried in the local certificates or peer certificates. If the PKI domain, the local certificates, or the peer certificates do not have the CA certificate chain, you must import the CA certificate first.

When you import the local or peer certificates:

- If the local or peer certificates contain the CA certificate chain, you can import the CA certificate and the local or peer certificates at the same time. If the CA certificate already exists in a PKI domain, the system prompts you whether to overwrite the existing CA certificate.
- If the local or peer certificates do not contain the CA certificate chain, but the CA certificate already exists in a PKI domain, you can directly import the certificates.

You can import the CA certificate to a PKI domain when either of the following conditions is met:

- The CA certificate to be imported is the root CA certificate or contains the certificate chain with the root certificate.
- The CA certificate contains a certificate chain without the root certificate, but can form a complete certificate chain with an existing CA certificate on the device.

Contact the CA administrator to get information as prompted in the following scenarios:

- The system prompts you to confirm the certificate's fingerprint in the following situation:
  - The certificate file to be imported contains the root certificate, but the root certificate does not exist in any PKI domains on the device.
  - The **root-certificate fingerprint** command is not configured in the PKI domain to which the certificate file is to be imported.
- The system prompts you to enter the challenge password used for encrypting the private key if the local certificate to be imported contains a key pair.

When you import a local certificate file that contains a key pair to a PKI domain, you can choose to update the domain with the key pair. Depending on the purpose of the key pair, the following conditions might apply:

- If the purpose of the key pair is general, the device uses the key pair to replace the local key pair that is found in this order:
  a. General-purpose key pair.
  b. Signature key pair.
  c. Encryption key pair.
- If the purpose of the key pair is signature, the device uses the key pair to replace the local key pair that is found in this order:
  a. General-purpose key pair.
  b. Signature key pair.
- If the purpose of the key pair is encryption, the device searches the PKI domain for an encryption key pair.

If a matching key pair is found, the device asks whether you want to overwrite the existing key pair on the device. If no match is found, the device asks you to enter a key pair name, which must be different from the names of any local key pairs of the same algorithm on the device. Then, it generates the key pair according to the key algorithm and the purpose defined in the certificate file. If you do not specify a key pair name, the PKI domain name will be used as the key pair name.

The import operation automatically updates or generates the correct key pair. When you perform the import operation, be sure to save the configuration file to avoid data loss.

Examples

Import CA certificate file **rootca_pem.cer** in PEM format to PKI domain **aaa**. The certificate file contains the root certificate.

```
<Sysname> system-view
[Sysname] pki import domain aaa pem ca filename rootca_pem.cer
The trusted CA's finger print is:
    MD5  fingerprint:FFFF 3EFF FFFF 37FF FFFF 137B FFFF 7535
    SHA1 fingerprint:FFFF FF7F FF2B FFFF 7618 FF4C FFFF 0A7D FFFF FF69
Is the finger print correct?(Y/N):y
[Sysname]
```

Import CA certificate file **aca_pem.cer** in PEM format to PKI domain **bbb**. The certificate file does not contain the root certificate.

```
<Sysname> system-view
[Sysname] pki import domain bbb pem ca filename aca_pem.cer
[Sysname]
```

Import local certificate file **local-ca.p12** in PKCS12 format to PKI domain **bbb**. The certificate file contains a key pair.

```
<Sysname> system-view
[Sysname] pki import domain bbb p12 local filename local-ca.p12
Please input challenge password:
******
[Sysname]
```

Import the local certificate in PEM format to PKI domain **bbb** by copying and pasting the contents of the certificate. The certificate contains the key pair and the CA certificate chain.

```
<Sysname> system-view
[Sysname] pki import domain bbb pem local
Enter PEM-formatted certificates.
End with a Ctrl+C on a line by itself.
Bag Attributes
localKeyID: 01 00 00 00
friendlyName: {F7619D96-3AC2-40D4-B6F3-4EAB73DEED73}
Microsoft CSP Name: Microsoft Enhanced Cryptographic Provider v1.0
Key Attributes
X509v3 Key Usage: 10
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,8DCE37F0A61A4B8C

k9C3KHY5S3EtnF5iQymvHYYrVFy5ZdjSasU5y4XFubjdcvmpFHQteMjD0GKX6+xO
kuKbvpyCnWsPVg56sL/PDRyrRmqLmtUV3bpyQsFXgnc7p+Snj3CG2Ciow9XApybW
Ec1TDCD75yuQckpVQdhguTvoPQXf9zHmiGu5jLkySp2k7ec/Mc97Ef+qqpfnHpQp
GDmMqnFpp59ZzB21OGlbGzlPcsjoT+EGpZg6B1KrPiCyFim95L9dWVwX9sk+U1s2
+8wqac8jETwwM0UZ1NGJ50JJz1QYIzMbcrw+S5WlPxACTIz1cldlBlb1kpc+7mcX
4W+MxFzsL88IJ99T72eu4iUNsy26g0BZMAcc1sJA3A4w9RNhfs9hSG43S3hAh5li
JPp720LfYBlkQHn/MgMCZASWDJ5G0eSXQt9QymHAth4BiT9v7zetnQqf4q8plfd/
Xqd9zEFlBPpoJFtJqXwxHUCKgw6kJeC4CxHvi9ZCJU/upg9IpiguFPoaDOPia+Pm
GbRqSyy55clVde5GOccGN1DZ94DW7AypazgLpBbrkIYAdjFPRmq+zMOdyqsGMTNj
jnheI5l784pNOAKuGi0i/uXmRRcfoMh6qAnK6YZGS7rOLC9CfPmy8fgY+/Sl9d9x
```

```
Q00ruO1psxzh9c2YfuaiXFIx0auKl6o5+ZZYn7Rg/xy2Y0awVP+dO925GoAcHO40
cCl6jA/HsGAU9HkpwKHL35lmBDRLEzQeBFcaGwSm1JvRfE4tkJM7+Uz2QHJOfP10
0VLqMgxMlpk3TvBWgzHGJDe7TdzFCDPMPhod8pi4P8gGXmQd01PbyQ==
-----END RSA PRIVATE KEY-----
Bag Attributes
localKeyID: 01 00 00 00
subject=/CN=sldsslserver
issuer=/C=cn/O=ccc/OU=sec/CN=ssl
-----BEGIN CERTIFICATE-----
MIICjzCCAfigAwIBAgIRAJoDN+shVrofVHbk11SlqfcwDQYJKoZIhvcNAQEFBQAw
NzELMAkGA1UEBhMCY24xDDAKBgNVBAoTA2gzYzEMMAoGA1UECxMDc2VjMQwwCgYD
VQQDEwNzc2wwHhcNMTAxMDE1MDEyMzA2WhcNMTIwNzI2MDYzMDU0WjAXMRUwEwYD
VQQDEwxzbGRzc2xzZXJ2ZXIwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMLP
N3aTKV7NDndIOk0PpiikYPgxVih/geMXR3iYaANbcvRX07/FMDINWHJnBAZhCDvp
rFO552loGiPyl0wmFMK12TSL7sHvrxr0OdrFrqtWlbW+DsNGNcFSKZy3RvIngC2k
ZZqBeFPUytP185JUhbOrVaUDlisZi6NNshcIjd2BAgMBAAGjgbowgbcwHwYDVR0j
BBgwFoAUmoMpEynZYoPLQdR1LlKhZjg8kBEwDgYDVR0PAQH/BAQDAgP4MBEGCWCG
SAGG+EIBAQQEAwIGQDASBgNVHREECzAJggdoM2MuY29tMB0GA1UdDgQWBBQ8dpWb
3cJ/X5iDt8eg+JkeS9cvJjA+BgNVHR8ENzA1MDOgMaAvhi1odHRwOi8vczAzMTMw
LmgzYy5odWF3ZWktM2NvbS5jb206NDQ3L3NzbC5jcmwwDQYJKoZIhvcNAQEFBQAD
gYEAYS15x0kW474lu4twNzEy5dPjMSwtwfm/UK01S8GQjGV5tl9ZNiTHFGNEFx7k
zxBp/JPpcFM8hapAfrVHdQ/wstq0pVDdBkrVF6XKIBks6XgCvRl32gcaQt9yrQd9
5RbWdetuBljudjFj25airYO2u7pLeVmdWWx3WVvZBzOo8KU=
-----END CERTIFICATE-----
Bag Attributes: <Empty Attributes>
subject=/C=cn/O=ccc/OU=sec/CN=ssl
issuer=/C=cn/O=ccc/OU=sec/CN=ssl
-----BEGIN CERTIFICATE-----
MIIB7DCCAVUCEG+jJTPxxiE67pl2ff0SnOMwDQYJKoZIhvcNAQEFBQAwNzELMAkG
A1UEBhMCY24xDDAKBgNVBAoTA2gzYzEMMAoGA1UECxMDc2VjMQwwCgYDVQQDEwNz
c2wwHhcNMDkwNzMxMDY0ODQ2WhcNMTIwNzI5MDYyODU4WjA3MQswCQYDVQQGEwJj
bjEMMAoGA1UEChMDaDNjMQwwCgYDVQQLEwNzZWMxDDAKBgNVBAMTA3NzbDCBnzAN
BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAt8QSMetQ70GONiFh7iJkvGQ8nC15zCF1
cqC/RcJhE/88LkKyQcu9j+Tz8Bk9Qj2UPaZdrk8fOrgtBsa7lZ+UO3j3l30q84l+
HjWq8yxVLRQahU3gqJze6pGR2l0s76u6GRyCX/zizGrHKqYlNnxK44NyRZx2klQ2
tKQAfpXCPIkCAwEAATANBgkqhkiG9w0BAQUFAAOBgQBWsaMgRbBMtYNrrYCMjY6g
c7PBjvajVOKNUMxaDalePmXfKCxl91+PKM7+i8I/zLcoQO+sHbva26a2/C4sNvoJ
2QZs6GtAOahP6CDqXC5VuNBU6eTKNKjL+mf6uuDeMxrlDNha0iymdrXXVIp5cuIu
fl7xgArs8Ks6aXDXM1o4DQ==
-----END CERTIFICATE-----


Please input the password:********
Local certificate already exist, confirm to overwrite it? [Y/N]:y
The PKI domain already has a CA certificate. If it is overwritten, local certificates,
peer certificates and CRL of this domain will also be deleted.
Overwrite it? [Y/N]:y
```

```
The system is going to save the key pair. You must specify a key pair name, which is a
case-insensitive string of 1 to 64 characters. Valid characters include a to z, A to Z,
0 to 9, and hyphens (-).
Please enter the key pair name [default name: bbb]:

The key pair already exists.
Please enter the key pair name:
import-key
```

Related commands

display pki certificate

public-key dsa

public-key ecdsa

public-key rsa

pki request-certificate

Use **pki request-certificate** to submit a local certificate request or generate a certificate request in PKCS#10 format.

Syntax

pki request-certificate domain *domain-name* [**password** *password*] [**pkcs10** [**filename** *filename*]]

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in Table 16.

Table 16 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

password *password*: Sets the password for certificate revocation, a case-sensitive string of 1 to 31 characters. The password is contained in the certificate request and must be provided if the certificate is revoked.

pkcs10: Displays BASE64-encoded PKCS#10 certificate request information, which can be used to request a certificate by an out-of-band means, like phone, disk, or email.

filename *filename*: Specifies a local file for saving the certificate request in PKCS#10 format. The *filename* argument is case-insensitive.

Usage guidelines

If SCEP fails, you can perform one of the following tasks:

- Use the **pkcs10** keyword to print the BASE64-encoded request information.
- Use the **pkcs10 filename** *filename* option to save the request information to a local file and transfer the file to the CA by using an out-of-band means. The file name can contain an absolute path. If the specified path does exist, the request information cannot be saved.

This command is not saved in the configuration file.

Examples

Display information about the certificate request in PKCS#10 format.

```
<Sysname> system-view
[Sysname] pki request-certificate domain aaa pkcs10

*** Request for general certificate ***
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBTDCBtgIBADANMQswCQYDVQQDEwJqajCBnzANBgkqhkiG9w0BAQEFAAOBjQAw
gYkCgYEAw5Drj8ofs9THA4ezkDcQPBy8pvH1kumampPsJmx8sGG52NFtbrDTnTT5
ALx3LJijB3d/ndKpcHT/DfbJVDCn5gdw32tBZyCkEwMHZN3ol2z7Nmdcu5TED6iN8
4m+hfp1QWoV6lty3o9pxAXuQl8peUDcfN6WV3LBXYyl1WCtkLkECAwEAAaAAMA0G
CSqGSIb3DQEBBAUAA4GBAA8E7BaIdmT6NVCZgv/I/1tqZH3TS4e4H9Qo5NiCKiEw
R8owVmA0XVtGMbyqBNcDTG0f5NbHrXZQT5+MbFJOnm5K/mn1ro5TJKMTKV46PlCZ
JUjsugaY02GBY0BVcylpC9iIXLuXNIqjh1MBIqVsa1lQOHS7YMvnop6hXAQlkM4c
-----END NEW CERTIFICATE REQUEST-----
```

Request the local certificates.

```
[Sysname] pki request-certificate domain openca
Start to request certificate ...
…
Request certificate of domain openca successfully
```

Related commands

display pki certificate

pki retrieve-certificate

Use **pki retrieve-certificate** to obtain a certificate from the certificate distribution server.

Syntax

pki retrieve-certificate domain *domain-name* { **ca** | **local** | **peer** *entity-name* }

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in Table 17.

Table 17 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

ca: Specifies the CA certificate.

local: Specifies the local certificates.

peer *entity-name*: Specifies a peer entity by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

In online mode:

- You can obtain the CA certificate through the SCEP protocol. If a CA certificate already exists locally, do not obtain the CA certificate again. To obtain a new CA certificate, use the **pki delete-certificate** command to remove the CA certificate and local certificates, and then obtain the CA certificate again.
- You can obtain local certificates or peer certificates through the LDAP protocol. If a PKI domain already has local certificates or peer certificates, you can still perform the obtain operation and the obtained local certificates or peer certificates overwrite the existing ones. If RSA or SM2 is used, a PKI domain can have two local certificates, one for signing and the other for encryption. Certificates for different purposes do not overwrite each other.

The obtained CA certificate, local certificates, and peer certificates are automatically verified before they are saved locally. If the verification fails, they are not saved.

This command is not saved in the configuration file.

Examples

Obtain the CA certificate from the certificate distribution server. (This operation requires the user to confirm the fingerprint of the root CA certificate.)

```
<Sysname> system-view
[Sysname] pki retrieve-certificate domain aaa ca
The trusted CA's finger print is:
    MD5  fingerprint:5C41 E657 A0D6 ECB4 6BD6 1823 7473 AABC
    SHA1 fingerprint:1616 E7A5 D89A 2A99 9419 1C12 D696 8228 87BC C266
Is the finger print correct?(Y/N):y
```

Obtain the local certificates from the certificate distribution server.

```
<Sysname> system-view
[Sysname] pki retrieve-certificate domain aaa local
```

Obtain the certificate of the peer entity **en1** from the certificate distribution server.

```
<Sysname> system-view
[Sysname] pki retrieve-certificate domain aaa peer en1
```

Related commands

display pki certificate

pki delete-certificate

pki retrieve-crl

Use **pki retrieve-crl** to obtain CRLs and save them locally.

Syntax

pki retrieve-crl domain *domain-name*

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in Table 18.

Table 18 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

Usage guidelines

CRLs are used to verify the validity of the local certificates and the peer certificates in a PKI domain. To obtain CRLs, a PKI domain must have the correct CA certificate.

The URL of the CRL repository is specified by using the **crl url** command.

The device can obtain CRLs from the CRL repository through the HTTP, LDAP, or SCEP protocol. Which protocol is used depends on the configuration of the CRL repository in the PKI domain:

- If the specified URL of the CRL repository is in HTTP format, the device obtains CRLs through the HTTP protocol.
- If the specified URL of the CRL repository is in LDAP format, the device obtains CRLs through the LDAP protocol. If the specified URL does not have a host name, for example, **ldap:///CN=8088,OU=test,U=rd,C=cn**, you must specify the LDAP server's URL for the PKI domain by using the **ldap server** command. The device can obtain the complete URL of the LDAP repository by combining the URLs of the LDAP server and of the CRL repository.
- If the PKI domain is not configured with the CRL repository, the device looks up the local certificates and then the CA certificate for the CRL repository. If a CRL repository is found, the device obtains CRLs from the CRL repository. If no CRL repository is found, the device obtains CRLs through the SCEP protocol.

Examples

Obtain CRLs from the CRL repository.

```
<Sysname> system-view
[Sysname] pki retrieve-crl domain aaa
```

Related commands

crl url

ldap server

pki storage

Use **pki storage** to specify the storage path for the certificates or CRLs.

Use **undo pki storage** to restore the default.

Syntax

pki storage { **certificates** | **crls** } *dir-path*

undo pki storage { **certificates** | **crls** }

Default

Certificates and CRLs are stored in the **PKI** directory on the storage media of the device. The **PKI** directory is automatically created when a certificate is successfully requested, obtained, or imported for the first time.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

certificates: Specifies a storage path for certificates.

crls: Specifies a storage path for CRLs.

dir-path: Specifies a storage path, a case-sensitive string, which cannot start with a slash (/) or contain two dots plus a slash (../). The *dir-path* argument specifies an absolute path or a relative path, and the path must exist.

Usage guidelines

The specified storage path must be on the master device.

If the path to be specified does not exist, use the **mkdir** command to create the path first.

Certificate files use the .cer or .p12 file extension. CRL files use the .crl file extension. After you change the storage path for certificates or CRLs, the certificate files and CRL files in the original path are moved to the new path.

Examples

Specifies **flash:/pki-new** as the storage path for certificates.

```
<Sysname> system-view
[Sysname] pki storage certificates flash:/pki-new
```

Specifies **pki-new** as the storage path for CRLs.

```
<Sysname> system-view
```

```
[Sysname] pki storage crls pki-new
```

pki validate-certificate

Use **pki validate-certificate** to verify the validity of certificates.

Syntax

pki validate-certificate domain *domain-name* { **ca** | **local** }

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in Table 19.

Table 19 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

ca: Specifies the CA certificate.

local: Specifies the local certificates.

Usage guidelines

Generally, certificates are automatically verified when you request, obtain, or import them, or when an application uses PKI.

You can also use this command to manually verify a certificate in the following aspects:

- Whether the certificate is issued by a trusted CA.
- Whether the certificate has expired.
- Whether the certificate is revoked. This check is performed only if CRL checking is enabled.

When CRL checking is enabled:

- To verify the local certificates, if the PKI domain has no CRLs, the device looks up the locally saved CRLs. If a correct CRL is found, the device loads the CRL to the PKI domain. If no correct CRL is found locally, the device obtains a correct CRL from the CA server and saves it locally.
- To verify the CA certificate, CRL checking is performed for the CA certificate chain from the current CA to the root CA.

Examples

Verify the validity of the CA certificate in PKI domain **aaa**.

```
<Sysname> system-view
[Sysname] pki validate-certificate domain aaa ca
```

```
Verifying certificates......
        Serial Number:
            f6:3c:15:31:fe:bb:ec:94:dc:3d:b9:3a:d9:07:70:e5
        Issuer:
            C=cn
            O=ccc
            OU=ppp
            CN=rootca
        Subject:
            C=cn
            O=abc
            OU=test
            CN=aca

Verify result: OK
Verifying certificates......
        Serial Number:
            5c:72:dc:c4:a5:43:cd:f9:32:b9:c1:90:8f:dd:50:f6
        Issuer:
            C=cn
            O=ccc
            OU=ppp
            CN=rootca
        Subject:
            C=cn
            O=ccc
            OU=ppp
            CN=rootca

Verify result: OK
```

Verify the local certificates in PKI domain **aaa**.

```
<Sysname> system-view
[Sysname] pki validate-certificate domain aaa local
Verifying certificates......
        Serial Number:
            bc:05:70:1f:0e:da:0d:10:16:1e
        Issuer:
            C=CN
            O=sec
            OU=software
            CN=bca
        Subject:
            O=OpenCA Labs
            OU=Users
            CN=fips fips-sec

Verify result: OK
```

Related commands

crl check

pki domain

public-key dsa

Use **public-key dsa** to specify a DSA key pair for certificate request.

Use **undo public-key** to restore the default.

Syntax

public-key dsa name *key-name* [**length** *key-length*]

undo public-key

Default

No key pair is specified for certificate request.

Views

PKI domain view

Predefined user roles

network-admin

context-admin

Parameters

name *key-name*: Specifies a key pair by its name, a case-insensitive string of 1 to 64 characters. The key pair name can contain only letters, digits, and hyphens (-).

length *key-length*: Specifies the key length, in bits. The value range is 512 to 2048, and the default is 1024. A longer key means higher security but more public key calculation time.

Usage guidelines

You can specify a nonexistent key pair in this command. A key pair can be obtained in any of the following ways:

- Use the **public-key local create** command to generate a key pair.
- An application, like IKE using digital signature authentication, triggers the device to generate a key pair.
- Use the **pki import** command to import a certificate containing a key pair.

A PKI domain can have key pairs using only one type of cryptographic algorithm (DSA, ECDSA, RSA, or SM2).

- If DSA or ECDSA is used, a PKI domain can have only one key pair. If you configure a DSA or ECDSA key pair multiple times, the most recent configuration takes effect.
- If RSA or SM2 is used, a PKI domain can have two key pairs of different purposes: one is the signing key pair, and the other is the encryption key pair.

  If you configure an RSA signing key pair or RSA encryption key pair multiple times, the most recent configuration takes effect. The RSA signing key pair and encryption key pair do not overwrite each other. The same is true for SM2 key pairs.

The **length** *key-length* option takes effect only if you specify a nonexistent key pair. The device will automatically create the key pair by using the specified name and length before submitting a certificate request. The **length** *key-length* option is ignored if the specified key pair already exists or is already contained in an imported certificate.

Examples

Specify 2048-bit DSA key pair **abc** for certificate request.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] public-key dsa name abc length 2048
```

Related commands

pki import

public-key local create

public-key ecdsa

Use **public-key ecdsa** to specify an ECDSA key pair for certificate request.

Use **undo public-key** to restore the default.

Syntax

public-key ecdsa name *key-name* [**secp192r1** | **secp256r1** | **secp384r1** | **secp521r1**]

undo public-key

Default

No key pair is specified for certificate request.

Views

PKI domain view

Predefined user roles

network-admin

context-admin

Parameters

name *key-name*: Specifies a key pair by its name, a case-insensitive string of 1 to 64 characters. The key pair name can contain only letters, digits, and hyphens (-).

secp192r1: Uses the secp192r1 curve to generate the key pair.

secp256r1: Uses the secp256r1 curve to generate the key pair.

secp384r1: Uses the secp384r1 curve to generate the key pair.

secp521r1: Uses the secp521r1 curve to generate the key pair.

Usage guidelines

You can specify a nonexistent key pair for a PKI domain.

A key pair can be obtained in any of the following ways:

- Use the **public-key local create** command to generate a key pair.
- An application, like IKE using digital signature authentication, triggers the device to generate a key pair.
- Use the **pki import** command to import a certificate containing a key pair.

A PKI domain can have key pairs using only one type of cryptographic algorithm (DSA, ECDSA, RSA, or SM2).

- If DSA or ECDSA is used, a PKI domain can have only one key pair. If you configure a DSA or ECDSA key pair multiple times, the most recent configuration takes effect.
- If RSA or SM2 is used, a PKI domain can have two key pairs of different purposes: one is the signing key pair, and the other is the encryption key pair.

  If you configure an RSA signing key pair or RSA encryption key pair multiple times, the most recent configuration takes effect. The RSA signing key pair and encryption key pair do not overwrite each other. The same is true for SM2 key pairs.

The specified elliptic curve takes effect only if you specify a nonexistent key pair. The device will automatically create the key pair by using the specified name and curve before submitting a certificate request. The curve parameter is ignored if the specified key pair already exists or is already contained in an imported certificate.

If you do not specify an elliptic curve, the secp192r1 curve is used by default.

Examples

Specify 384-bit ECDSA key pair **abc** for certificate request.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] public-key ecdsa name abc secp384r1
```

Related commands

pki import

public-key local create

public-key rsa

Use **public-key rsa** to specify an RSA key pair for certificate request.

Use **undo public-key** to restore the default.

Syntax

public-key rsa { { **encryption name** *encryption-key-name* [**length** *key-length*] | **signature name** *signature-key-name* [**length** *key-length*] } * | **general name** *key-name* [**length** *key-length*] }

undo public-key

Default

No key pair is specified for certificate request.

Views

PKI domain view

Predefined user roles

network-admin

context-admin

Parameters

encryption: Specifies a key pair for encryption.

name *encryption-key-name*: Specifies a key pair name, a case-insensitive string of 1 to 64 characters. The key pair name can contain only letters, digits, and hyphens (-).

signature: Specifies a key pair for signing.

name *signature-key-name*: Specifies a key pair name, a case-insensitive string of 1 to 64 characters. The key pair name can contain only letters, digits, and hyphens (-).

general: Specifies a key pair for both signing and encryption.

name *key-name*: Specifies a key pair name, a case-insensitive string of 1 to 64 characters. The key pair name can contain only letters, digits, and hyphens (-).

length *key-length*: Specifies the key length, in bits. The value range is 512 to 2048, and the default is 1024. A longer key means higher security but more public key calculation time.

Usage guidelines

You can specify a nonexistent key pair in this command. You can get a key pair in any of the following ways:

- Use the **public-key local create** command to generate a key pair.
- An application, like IKE using digital signature authentication, triggers the device to generate a key pair.
- Use the **pki import** command to import a certificate containing a key pair.

A PKI domain can have key pairs using only one type of cryptographic algorithm (DSA, ECDSA, RSA, or SM2).

- If DSA or ECDSA is used, a PKI domain can have only one key pair. If you configure a DSA or ECDSA key pair multiple times, the most recent configuration takes effect.
- If RSA or SM2 is used, a PKI domain can have two key pairs of different purposes: one is the signing key pair, and the other is the encryption key pair.

  If you configure an RSA signing key pair or RSA encryption key pair multiple times, the most recent configuration takes effect. The RSA signing key pair and encryption key pair do not overwrite each other. The same is true for SM2 key pairs.

If you specify a signing key pair and an encryption key pair separately, their key lengths can be different.

The **length** *key-length* option takes effect only if you specify a nonexistent key pair. The device will automatically create the key pair by using the specified name and length before submitting a certificate request. The **length** *key-length* option is ignored if the specified key pair already exists or is already contained in an imported certificate.

Examples

Specify 2048-bit general purpose RSA key pair **abc** for certificate request.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] public-key rsa general name abc length 2048
```

Specify the following RSA key pairs for certificate request:

- 2048-bit RSA encryption key pair **rsa1**.
- 2048-bit RSA signing key pair **sig1**.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] public-key rsa encryption name rsa1 length 2048
[Sysname-pki-domain-aaa] public-key rsa signature name sig1 length 2048
```

Related commands

pki import

public-key local create

public-key sm2

Use **public-key sm2** to specify an SM2 key pair for certificate request.

Use **undo public-key** to restore the default.

Syntax

public-key sm2 { { **encryption name** *encryption-key-name* | **signature name** *signature-key-name* } * | **general name** *key-name* }

undo public-key

Default

No key pair is specified for certificate request.

Views

PKI domain view

Predefined user roles

network-admin

context-admin

Parameters

encryption name *encryption-key-name*: Specifies a key pair for encryption by its name, a case-insensitive string of 1 to 64 characters. The key pair name can contain only letters, digits, and hyphens (-).

signature name *signature-key-name*: Specifies a key pair for signing by its name, a case-insensitive string of 1 to 64 characters. The key pair name can contain only letters, digits, and hyphens (-).

general name *key-name*: Specifies a key pair for both signing and encryption. The **name** *key-name* option specifies the key pair name, a case-insensitive string of 1 to 64 characters. The key pair name can contain only letters, digits, and hyphens (-).

Usage guidelines

You can specify a nonexistent key pair in this command. You can get a key pair in any of the following ways:

- Use the **public-key local create** command to generate a key pair.
- An application, like IKE using digital signature authentication, triggers the device to generate a key pair.

A PKI domain can have key pairs using only one type of cryptographic algorithm (DSA, ECDSA, RSA, or SM2).

If you configure an SM2 key pair for a PKI domain multiple times, the most recent configuration takes effect.

A CA server that uses double certificate templates always issues both a signing certificate and an encryption certificate to a requesting applicant. When such a CA server is used, follow these guidelines when you specify SM2 key pairs for certificate request:

- Specify different names for the encryption key pair and the signing key pair. If you specify the same name for the two key pairs, request of the signing certificate will fail.
- If you do not specify an encryption key pair, the device will save the key pair in the issued encryption certificate with the PKI domain name. Do not use the PKI domain name as the name of the SM2 signing key pair.

If you configure this command for a PKI domain multiple times, the most recent configuration takes effect.

Examples

Specify SM2 signing key pair **sm21** and SM2 encryption key pair **sm22** for certificate request.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] public-key sm2 signature name sm21 encryption name sm22
```

Related commands

pki import

public-key local create

revocation-check method

Use **revocation-check method** to specify the certificate revocation checking methods.

Use **undo revocation-check method** to restore the default.

Syntax

revocation-check method *method1* [*method2*]

undo revocation-check method

Default

The CRL is used for certificate revocation checking.

Views

PKI domain view

Predefined user roles

network-admin

context-admin

Parameters

method1 [*method2*]: Specifies an ordered list of certificate revocation checking methods. Supported methods are:

- **crl**: Uses the CRL for certificate revocation checking.
- **none**: Performs no revocation checking and treats all certificates as not revoked. If you specify **none** as method 1, you cannot specify method 2 because no revocation checking is required.

Usage guidelines

If you configure the **revocation-check method crl none** command, the device will first check the CRL to identify whether the certificate has been revoked during certificate verification. If the device cannot obtain a CRL, it will treat the certificate as not revoked.

The CRL method takes effect only if CRL checking is enabled in the PKI domain (by using the **crl check enable** command). If CRL checking is disabled in the PKI domain, no CRL checking will be performed and all certificates will be treated as not revoked.

If the **revocation-check method none** command is configured in the PKI domain, the **crl check enable** command does not take effect.

Examples

Specify the CRL certificate revocation checking method for PKI domain **abc**.

```
<Sysname> system
[Sysname] pki domain abc
[Sysname-pki-domain-abc] revocation-check method crl
```

Related commands

crl check enable

root-certificate fingerprint

Use **root-certificate fingerprint** to set the fingerprint for verifying the root CA certificate.

Use **undo root-certificate fingerprint** to restore the default.

Syntax

root-certificate fingerprint { **md5** | **sha1** } *string*

undo root-certificate fingerprint

Default

No fingerprint is set for verifying the root CA certificate.

Views

PKI domain view

Predefined user roles

network-admin

context-admin

Parameters

md5: Sets an MD5 fingerprint.

sha1: Sets an SHA1 fingerprint.

string: Sets the fingerprint in hexadecimal notation. If you specify the **MD5** keyword, the fingerprint is a string of 32 characters. If you specify the **SHA1** keyword, the fingerprint is a string of 40 characters.

Usage guidelines

If you set the certificate request mode to auto for a PKI domain that does not have a CA certificate, you must configure the fingerprint for root CA certificate verification. When an application (for example, IKE) triggers the device to request local certificates, the device automatically performs the following operations:

1. Obtains the CA certificate from the CA server.
2. Compares the fingerprint contained in the root CA certificate with the fingerprint configured in the PKI domain, if either of the following conditions exists:
   - The obtained CA certificate is a root certificate.
   - The obtained CA certificate is a certificate chain and contains a root certificate that does not exist on the device.

   If the two fingerprints do not match, or if no fingerprint is configured in the PKI domain, the device rejects the CA certificate and the local certificate request fails.

The fingerprint configured by this command is also used for root CA certificate verification when the device performs the following operations:

- Imports the CA certificate as requested by the **pki import** command.
- Obtains the CA certificate as requested by the **pki retrieve-certificate** command.

The device compares the fingerprint contained in the root CA certificate with the fingerprint configured in the PKI domain, if either of the following conditions exists:

- The CA certificate to be imported or obtained is a root certificate that does not exist on the device.
- The CA certificate to be imported or obtained is a certificate chain and contains a root certificate that does not exist on the device.

If the two fingerprints do not match, the device rejects the CA certificate. If no fingerprint is configured in the PKI domain, the device prompts you to manually verify the fingerprint of the root CA certificate.

Examples

Specify an MD5 fingerprint for verifying the root CA certificate.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] root-certificate fingerprint md5
12EF53FA355CD23E12EF53FA355CD23E
```

Specify an SHA1 fingerprint for verifying the root CA certificate.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] root-certificate fingerprint sha1
D1526110AAD7527FB093ED7FC037B0B3CDDDAD93
```

Related commands

certificate request mode

pki import

pki retrieve-certificate

rule

Use **rule** to create an access control rule.

Use **undo rule** to remove an access control rule.

Syntax

rule [*id*] { **deny** | **permit** } *group-name*

undo rule *id*

Default

No access control rules exist.

Views

Certificate-based access control policy view

Predefined user roles

network-admin

context-admin

Parameters

id: Assigns an ID to the access control rule, in the range of 1 to 16. The default setting is the smallest unused ID in this range.

deny: Denies the certificates that match the associated attribute group.

permit: Permits the certificates that match the associated attribute group.

group-name: Specifies a certificate attribute group by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

When you create an access control rule, you can associate it with a nonexistent certificate attribute group.

The system determines that a certificate matches an access control rule when either of the following conditions exists:

- The associated certificate attribute group does not exist.
- The associated certificate attribute group does not contain any attribute rules.
- The certificate matches all attribute rules in the associated certificate attribute group.

You can configure multiple access control rules for an access control policy. A certificate matches the rules one by one, starting with the rule with the smallest ID. When a match is found, the match process stops, and the system performs the access control action defined in the access control rule.

Examples

Create rule 1 to permit all certificates that match certificate attribute group **mygroup**.

```
<Sysname> system-view
[Sysname] pki certificate access-control-policy mypolicy
[Sysname-pki-cert-acp-mypolicy] rule 1 permit mygroup
```

Related commands

attribute

display pki certificate access-control-policy

pki certificate attribute-group

source

Use **source** to specify the source IP address for PKI protocol packets.

Use **undo source** to restore the default.

Syntax

source { **ip** | **ipv6** } { *ip-address* | **interface** *interface-type interface-number* }

undo source

Default

The source IP address of PKI protocol packets is the IP address of their outgoing interface.

Views

PKI domain view

Predefined user roles

network-admin

context-admin

Parameters

ip *ip-address*: Specifies a source IPv4 address.

ipv6 *ip-address*: Specifies a source IPv6 address.

interface *interface-type interface-number*: Specifies an interface by its type and number. The interface's primary IP address or the lowest IPv6 address will be used as the source IP address for PKI protocol packets.

Usage guidelines

Use this command to specify the source IP address for PKI protocol packets. You can also specify a source interface if the IP address is dynamically obtained.

Make sure there is a route between the source IP address and the CA server.

You can specify only one source IP address in a PKI domain. If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify **111.1.1.8** as the source IP address for PKI protocol packets.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] source ip 111.1.1.8
```

Specify **1::8** as the source IPv6 address for PKI protocol packets.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] source ipv6 1::8
```

Use the IP address of GigabitEthernet 1/0/1 as the source IP address for PKI protocol packets.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] source ip interface gigabitethernet 1/0/1
```

Use the IPv6 address of GigabitEthernet 1/0/1 as the source IPv6 address for PKI protocol packets.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] source ipv6 interface gigabitethernet 1/0/1
```

state

Use **state** to set the state or province name for a PKI entity.

Use **undo state** to restore the default.

Syntax

state *state-name*

undo state

Default

No state name or province name is set for a PKI entity.

Views

PKI entity view

Predefined user roles

network-admin

context-admin

Parameters

state-name: Specifies a state or province by its name, a case-sensitive string of 1 to 63 characters. No comma can be included.

Examples

Set the state name to **countryA** for PKI entity **en**.

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en] state countryA
```

subject-dn

Use **subject-dn** to configure the DN for a PKI entity.

Use **undo subject-dn** to restore the default.

Syntax

subject-dn *dn-string*

undo subject-dn

Default

No DN is configured for a PKI entity.

Views

PKI entity view

Default command level

network-admin

context-admin

Parameters

dn-string: Specifies the DN for the PKI entity, a case-insensitive string of 1 to 255 characters.

Usage guidelines

The subject DN string is a sequence of *attribute=value* pairs separated by commas. Each attribute can be specified multiple times with different values. Supported DN attributes are:

- **CN**—Common-name.
- **C**—Country code.
- **L**—Locality.
- **O**—Organization.
- **OU**—Organization unit.
- **ST**—State or province.

After this command is configured, the following commands do not take effect:

- **common-name**
- **country**
- **locality**
- **organization**
- **organization-unit**
- **state**

If you configure this command multiple times, the most recent configuration takes effect.

Examples

Configure the DN for PKI entity **en**.

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en] subject-dn
CN=test,C=CN,O=abc,OU=rdtest,OU=rstest,ST=countryA,L=pukras
```

Related commands

common-name

country

locality

organization

organization-unit

state

usage

Use **usage** to specify the extensions for certificates.

Use **undo usage** to remove certificate extensions.

Syntax

usage { **ike** | **ssl-client** | **ssl-server** } *

undo usage [**ike** | **ssl-client** | **ssl-server**] *

Default

No extensions for certificates are specified. A certificate can be used by IKE, SSL clients, and SSL servers.

Views

PKI domain view

Predefined user roles

network-admin

context-admin

Parameters

ike: Specifies the IKE certificate extension so IKE peers can use the certificates.

ssl-client: Specifies the SSL client certificate extension so the SSL client can use the certificates.

ssl-server: Specifies the SSL server certificate extension so the SSL server can use the certificates.

Usage guidelines

If you do not specify any keywords for the **undo usage** command, this command removes all certificate extensions.

The extension options contained in a certificate depends on the CA policy, and might be different from those specified in the PKI domain.

Examples

Specify the SSL client certificate extension.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] usage ssl-client
```

vpn-instance

Use **vpn-instance** to specify the VPN instance where the certificate request reception authority and the CRL repository belong.

Use **undo vpn-instance** to restore the default.

Syntax

vpn-instance *vpn-instance-name*

undo vpn-instance

Default

The certificate request reception authority and the CRL repository belong to the public network.

Views

PKI domain view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance-name: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters.

Examples

Specify **vpn1** as the VPN instance where the certificate request reception authority and the CRL repository belong.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] vpn-instance vpn1
```

Contents

SSH commands

SSH server commands

display ssh server

Use **display ssh server** on an SSH server to display the SSH server status or sessions.

Syntax

display ssh server { **session** [**slot** *slot-number*] | **status** }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

session: Specifies the SSH server sessions.

status: Specifies the SSH server status.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays SSH server session information for the master device.

Examples

Display the SSH server status.

```
<Sysname> display ssh server status
 Stelnet server: Disable
 SSH version : 2.0
 SSH authentication-timeout : 60 second(s)
 SSH server key generating interval : 0 hour(s)
 SSH authentication retries : 3 time(s)
 SFTP server: Disable
 SFTP server Idle-Timeout: 10 minute(s)
 NETCONF server: Disable
 SCP server: Disable
 SSH Server PKI domain name: aaa
```

Table 1 Command output

Field	Description
Stelnet server	Whether the Stelnet server is enabled.
SSH version	SSH protocol version. When the SSH supports SSH1, the protocol version is 1.99. Otherwise, the protocol version is 2.

Field	Description
SSH authentication-timeout	Authentication timeout timer.
SSH server key generating interval	Minimum interval for updating the RSA server key pair.
SSH authentication retries	Maximum number of authentication attempts for SSH users.
SFTP server	Whether the SFTP server is enabled.
SFTP server Idle-Timeout	SFTP connection idle timeout timer.
NETCONF server	Whether NETCONF over SSH is enabled.
SCP server	Whether the SCP server is enabled.
SSH Server PKI domain name	Name of the PKI domain specified for the SSH server.

Display the SSH server sessions.

```
<Sysname> display ssh server session
UserPid   SessID Ver   Encrypt    State          Retries  Serv     Username   Idx
 184      0     2.0   aes128-cbc Established    1        Stelnet  abc@123
```

Table 2 Command output

Field	Description
UserPid	User process ID.
SessID	Session ID.
Ver	Protocol version of the SSH server.
Encrypt	Encryption algorithm used on the SSH server.
State	Session state: • **Init**—Initialization. • **Ver-exchange**—Version negotiation. • **Keys-exchange**—Key exchange. • **Auth-request**—Authentication request. • **Serv-request**—Session service request. • **Established**—The session is established. • **Disconnected**—The session is terminated.
Retries	Number of authentication failures.
Serv	Service type: • SCP. • SFTP. • Stelnet. • NETCONF.
Username	Username that the client uses to log in to the server.
Idx	Absolute number of the user line. The value for this field is empty if the SSH connection for the user is not redirected.

display ssh user-information

Use **display ssh user-information** to display information about SSH users on an SSH server.

Syntax

display ssh user-information [*username*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

username: Specifies an SSH username, a case-sensitive string of 1 to 80 characters. If you do not specify an SSH user, this command displays information about all SSH users.

Usage guidelines

This command displays information only about SSH users that are configured by using the **ssh user** command on the SSH server.

Examples

Display information about all SSH users.

```
<Sysname> display ssh user-information
 Total ssh users:2
 Username            Authentication-type  User-public-key-name  Service-type
 yemx                password                                   Stelnet|SFTP
 test                publickey            pubkey                SFTP
```

Table 3 Command output

Field	Description
Total ssh users	Total number of SSH users.
Authentication-type	Authentication methods: • Password authentication. • Publickey authentication. • Password-publickey authentication. • Any authentication.
User-public-key-name	Public key name of the user. This field is empty if the authentication method is password authentication.
Service-type	Service types: • Stelnet. • SFTP. • SCP. • NETCONF. If multiple service types are available for an SSH user, they are separated by vertical bars (|).

Related commands

ssh user

scp server enable

Use **scp server enable** to enable the SCP server.

Use **undo scp server enable** to disable the SCP server.

Syntax

scp server enable

undo scp server enable

Default

The SCP server is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Examples

Enable the SCP server.

```
<Sysname> system-view
[Sysname] scp server enable
```

Related commands

display ssh server

sftp server enable

Use **sftp server enable** to enable the SFTP server.

Use **undo sftp server enable** to disable the SFTP server.

Syntax

sftp server enable

undo sftp server enable

Default

The SFTP server is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Examples

Enable the SFTP server.

```
<Sysname> system-view
[Sysname] sftp server enable
```

Related commands

display ssh server

sftp server idle-timeout

Use **sftp server idle-timeout** to set the idle timeout timer for SFTP connections on an SFTP server.

Use **undo sftp server idle-timeout** to restore the default.

Syntax

sftp server idle-timeout *time-out-value*

undo sftp server idle-timeout

Default

The idle timeout timer is 10 minutes for SFTP connections.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

time-out-value: Specifies an idle timeout timer in the range of 1 to 35791 minutes.

Usage guidelines

If an SFTP connection is idle when the idle timeout timer expires, the system automatically terminates the connection. To promptly release connection resources, set the idle timeout timer to a small value when many SFTP connections concurrently exist.

Examples

Set the idle timeout timer to 500 minutes for SFTP connections.

```
<Sysname> system-view
[Sysname] sftp server idle-timeout 500
```

Related commands

display ssh server

ssh server acl

Use **ssh server acl** to specify an ACL to control IPv4 SSH connections to the server.

Use **undo ssh server acl** to restore the default.

Syntax

ssh server acl { *advanced-acl-number* | *basic-acl-number* | **mac** *mac-acl-number* }

undo ssh server acl

Default

No ACLs are specified and all IPv4 SSH clients can initiate SSH connections to the server.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

advanced-acl-number: Specifies an IPv4 advanced ACL number in the range of 3000 to 3999.

basic-acl-number: Specifies an IPv4 basic ACL number in the range of 2000 to 2999.

mac *mac-acl-number:* Specifies a Layer 2 ACL by its number in the range of 4000 to 4999.

Usage guidelines

The ACL specified in this command filters IPv4 SSH clients' connection requests. Only the IPv4 SSH clients that the ACL permits can access the device. If the specified ACL does not exist or contains no rules, IPv4 SSH clients are not allowed to access the device.

If the **vpn-instance** keyword is specified in an ACL rule, the rule applies only to VPN packets. If the **vpn-instance** keyword is not specified in an ACL rule, the rule applies only to public network packets.

This command takes effect only on SSH connections that are initiated after the configuration of this command.

This command does not take effect on NETCONF-over-SSH connections initiated by IPv4 SSH clients. To control IPv4 clients to establish NETCONF-over-SSH connections to the server, use the **netconf ssh acl** command. For more information about the **netconf ssh acl** command, see NETCONF commands in *Network Management and Monitoring Command Reference*.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure ACL 2001 and permit only the users at 1.1.1.1 to initiate SSH connections to the server.

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] ssh server acl 2001
```

Related commands

display ssh server

ssh server acl-deny-log enable

Use **ssh server acl-deny-log enable** to enable logging for SSH login attempts that are denied by the SSH login control ACL.

Use **undo ssh server acl-deny-log enable** to disable logging for SSH login attempts that are denied by the SSH login control ACL.

Syntax

ssh server acl-deny-log enable

undo ssh server acl-deny-log enable

Default

Logging is disabled for SSH login attempts that are denied by the SSH login control ACL.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

Only SSH clients permitted by the SSH login control ACL can access the SSH server. The logging feature generates log messages for SSH login attempts that are denied by the SSH login control ACL, and sends the messages to the information center.

For information about log message output, see the information center in *Network Management and Monitoring Configuration Guide*. For information about configuring an SSH login control ACL, see the **ssh server acl** or **ssh server ipv6 acl** command.

Examples

Enable logging for SSH login attempts that are denied by the SSH login control ACL.

```
<Sysname> system-view
[Sysname] ssh server acl-deny-log enable
```

Related commands

ssh server acl

ssh server ipv6 acl

ssh server authentication-retries

Use **ssh server authentication-retries** to set the maximum number of authentication attempts for SSH users.

Use **undo ssh server authentication-retries** to restore the default.

Syntax

ssh server authentication-retries *retries*

undo ssh server authentication-retries

Default

The maximum number of authentication attempts is 3 for SSH users.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

retries: Specifies the maximum number of authentication attempts for SSH users, in the range of 1 to 5.

Usage guidelines

Setting the maximum number of authentication attempts prevents malicious hacking of usernames and passwords.

If the total number of authentication attempts exceeds the upper limit specified in this command, further authentication is not allowed.

- For **any** authentication, an authentication attempt is a publickey or password authentication process.
- For **password-publickey** authentication, an authentication attempt contains both a publickey authentication process and a password authentication process. The server first uses publickey authentication, and then uses password authentication to authenticate the SSH user.

This configuration does not affect logged-in users. It affects only users that attempt to log in after the configuration.

Examples

Set the maximum number of authentication attempts to 4 for SSH users.

```
<Sysname> system-view
[Sysname] ssh server authentication-retries 4
```

Related commands

display ssh server

ssh server authentication-timeout

Use **ssh server authentication-timeout** to set the SSH user authentication timeout timer on the SSH server.

Use **undo ssh server authentication-timeout** to restore the default.

Syntax

ssh server authentication-timeout *time-out-value*

undo ssh server authentication-timeout

Default

The SSH user authentication timeout timer is 60 seconds.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

time-out-value: Specifies an authentication timeout timer in the range of 1 to 120 seconds.

Usage guidelines

If a user does not finish the authentication when the timeout timer expires, the connection cannot be established.

To prevent malicious occupation of TCP connections, set the authentication timeout timer to a small value.

Examples

Set the authentication timeout timer to 10 seconds for SSH users.

```
<Sysname> system-view
[Sysname] ssh server authentication-timeout 10
```

Related commands

display ssh server

ssh server compatible-ssh1x enable

Use **ssh server compatible-ssh1x enable** to enable the SSH server to support SSH1 clients.

Use **undo ssh server compatible-ssh1x** [**enable**] to restore the default.

Syntax

ssh server compatible-ssh1x enable

undo ssh server compatible-ssh1x [**enable**]

Default

The SSH server does not support SSH1 clients.

Views

System view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Usage guidelines

The **undo** form of this command restores the default setting whether you specify the **enable** keyword or not.

This configuration does not affect logged-in users. It affects only users that attempt to log in after the configuration.

Examples

Enable the SSH server to support SSH1 clients.

```
<Sysname> system-view
[Sysname] ssh server compatible-ssh1x enable
```

Related commands

display ssh server

ssh server dscp

Use **ssh server dscp** to set the DSCP value in the IPv4 SSH packets that the SSH server sends to SSH clients.

Use **undo ssh server dscp** to restore the default.

Syntax

ssh server dscp *dscp-value*

undo ssh server dscp

Default

The DSCP value is 48 in IPv4 SSH packets.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

dscp-value: Specifies the DSCP value in the IPv4 SSH packets, in the range of 0 to 63. A bigger DSCP value represents a higher priority.

Usage guidelines

The DSCP value of a packet specifies the priority of the packet and affects the transmission priority of the packet.

Examples

Set the DSCP value to 30 for IPv4 SSH packets.

```
<Sysname> system-view
[Sysname] ssh server dscp 30
```

ssh server enable

Use **ssh server enable** to enable the Stelnet server.

Use **undo ssh server enable** to disable the Stelnet server.

Syntax

ssh server enable

undo ssh server enable

Default

The Stelnet server is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Examples

Enable the Stelnet server.

```
<Sysname> system-view
[Sysname] ssh server enable
```

Related commands

display ssh server

ssh server ipv6 acl

Use **ssh server ipv6 acl** to specify an ACL to control IPv6 SSH connections to the server.

Use **undo ssh server ipv6 acl** to restore the default.

Syntax

ssh server ipv6 acl { **ipv6** { *advanced-acl-number* | *basic-acl-number* } | **mac** *mac-acl-number* }

undo ssh server ipv6 acl

Default

No ACLs are specified and all IPv6 SSH clients can initiate SSH connections to the server.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ipv6: Specifies the IPv6 ACL type.

advanced-acl-number: Specifies an IPv6 advanced ACL number in the range of 3000 to 3999.

basic-acl-number: Specifies an IPv6 basic ACL number in the range of 2000 to 2999.

mac *mac-acl-number:* Specifies a Layer 2 ACL by its number in the range of 4000 to 4999.

Usage guidelines

The ACL specified in this command filters IPv6 SSH clients' connection requests. Only the IPv6 SSH clients that the ACL permits can access the device. If the specified ACL does not exist or contains no rules, IPv6 SSH clients are not allowed to access the device.

If the **vpn-instance** keyword is specified in an ACL rule, the rule applies only to VPN packets. If the **vpn-instance** keyword is not specified in an ACL rule, the rule applies only to public network packets.

This command takes effect only on SSH connections that are initiated after the configuration of this command.

This command does not take effect on NETCONF-over-SSH connections initiated by IPv6 SSH clients.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure ACL 2001 and permit only the users on the subnet 1::1/64 to initiate SSH connections to the server.

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2001
[Sysname-acl-ipv6-basic-2001] rule permit source 1::1 64
[Sysname-acl-ipv6-basic-2001] quit
[Sysname] ssh server ipv6 acl ipv6 2001
```

Related commands

display ssh server

ssh server ipv6 dscp

Use **ssh server ipv6 dscp** to set the DSCP value in the IPv6 SSH packets that the SSH server sends to SSH clients.

Use **undo ssh server ipv6 dscp** to restore the default.

Syntax

ssh server ipv6 dscp *dscp-value*

undo ssh server ipv6 dscp

Default

The DSCP value is 48 in IPv6 SSH packets.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

dscp-value: Specifies the DSCP value in the IPv6 SSH packets, in the range of 0 to 63. A bigger DSCP value represents a higher priority.

Usage guidelines

The DSCP value of an IPv6 packet specifies the priority of the packet and affects the transmission priority of the packet.

Examples

Set the DSCP value to 30 for IPv6 SSH packets.

```
<Sysname> system-view
[Sysname] ssh server ipv6 dscp 30
```

ssh server pki-domain

Use **ssh server pki-domain** to specify a PKI domain for an SSH server.

Use **undo ssh server pki-domain** to restore the default.

Syntax

ssh server pki-domain *domain-name*

undo ssh server pki-domain

Default

No PKI domain is specified for an SSH server.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

domain-name: Specifies the name of the PKI domain used to verify the SSH server. The PKI domain name is a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes (').

Examples

Specify PKI domain **serverpkidomain** for the SSH server.

```
<Sysname> system-view
[Sysname] ssh server pki-domain serverpkidomain
```

ssh server port

Use **ssh server port** to specify the SSH service port.

Use **undo ssh server port** to restore the default.

Syntax

ssh server port *port-number*

undo ssh server port

Default

The SSH service port is 22.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

port-number: Specifies a port number in the range of 1 to 65535.

Usage guidelines

CAUTION:

- If you modify the SSH port number when the SSH server is enabled, the SSH service is restarted and all SSH connections are terminated after the modification. SSH users must reconnect to the SSH server to access the server.
- If you set the SSH port to a well-known port number, the service that uses the well-known port number might fail to start. Well-known port numbers are in the range of 1 to 1024.

When the device acts as an SSH redirect server, modifying the SSH service port on the device affects existing SSH redirect connections as follows:

- If an SSH user accesses the destination device by specifying the SSH redirect listening port, modifying the SSH service port does not affect the existing SSH redirect connection.
- If an SSH user accesses the destination device by specifying the absolute number of the user line, modifying the SSH service port terminates the SSH redirect connection. The SSH user must reconnect to the SSH redirect server to access the destination device.

Examples

Set the SSH service port to 1025.

```
<Sysname> system-view
```

```
[Sysname] ssh server port 1025
```

ssh server rekey-interval

Use **ssh server rekey-interval** to set the minimum interval for updating the RSA server key pair.

Use **undo ssh server rekey-interval** to restore the default.

Syntax

ssh server rekey-interval *interval*

undo ssh server rekey-interval

Default

The minimum interval for updating the RSA server key pair is 0 hours. The system does not update the RSA server key pair.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies the minimum interval for updating the RSA server key pair, in the range of 1 to 24 hours.

Usage guidelines

Periodically updating the RSA server key pair prevents malicious hacking to the key pair and enhances security of the SSH connections.

The system starts to count down the configured minimum update interval after the first SSH1 user logs in to the server. If a new SSH1 user logs in to the server after the interval, the system performs the following operations:

1. Updates the RSA server key pair.
2. Uses the updated RSA server key pair for key pair negotiation with the new user.
3. Resets the interval and starts to count down the interval again.

This command takes effect only on SSH1 clients.

Examples

Set the minimum interval to 3 hours for updating the RSA server key pair.

```
<Sysname> system-view
[Sysname] ssh server rekey-interval 3
```

Related commands

display ssh server

ssh user

Use **ssh user** to create an SSH user and specify the service type and authentication method.

Use **undo ssh user** to delete an SSH user.

Syntax

ssh user *username* **service-type** { **all** | **netconf** | **scp** | **sftp** | **stelnet** } **authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } [**assign** { **pki-domain** *domain-name* | **publickey** *keyname* }] }

undo ssh user *username*

Default

No SSH users exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

username: Specifies an SSH username, a case-sensitive string of 1 to 80 characters. The username cannot be **a**, **al**, or **all**. In addition, the username cannot include vertical bars (|), colons (:), asterisks (*), question marks (?), or angle brackets (< >). The at sign (@), slash (/), and backslash (\) can only be used to append ISP domain names to usernames in the *pureusername@domain*, *pureusername*/*domain*, and *domain**pureusername* format. Do not include hyphens (-) in the username of an SCP user. Otherwise, SCP logins using that username will fail.

service-type: Specifies a service type for the SSH user.

- **all**: Specifies service types Stelnet, SFTP, SCP, and NETCONF.
- **scp**: Specifies the service type SCP.
- **sftp**: Specifies the service type SFTP.
- **stelnet**: Specifies the service type Stelnet.
- **netconf**: Specifies the service type NETCONF.

authentication-type: Specifies an authentication method for the SSH user.

- **password**: Specifies password authentication. This authentication method provides easy and fast encryption, but it is vulnerable. It can work with AAA to implement user authentication, authorization, and accounting.
- **any**: Specifies either password authentication or publickey authentication.
- **password-publickey**: Specifies both password authentication and publickey authentication for SSH2 clients. In SSH2, the password-publickey authentication method provides higher security. If the client runs SSH1, this keyword specifies either password authentication or publickey authentication.
- **publickey**: Specifies publickey authentication. This authentication method has complicated and slow encryption, but it provides strong authentication that can defend against brute-force attacks. This authentication method is easy to use. If this method is configured, the authentication process completes automatically without entering any password.

assign: Specifies parameters used for client verification.

- **pki-domain** *domain-name*: Specifies the PKI domain that verifies the client's digital certificate. The *domain-name* argument is a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes ('). The server uses the CA certificate that is saved in the PKI domain to verify the client's digital certificate. In this scenario, the server does not need to save clients' public keys in advance.

- **publickey** *keyname*: Specifies the public key of the SSH client. The *keyname* argument represents the name of the SSH client's public key configured on the server. It is a case-insensitive string of 1 to 64 characters. The server uses the client's public key to check the validity of the client. If the public key file of the client is changed, you must update the client's public key on the server promptly.

Usage guidelines

Use this command to configure an SSH user depending on the authentication method.

- If the authentication method is **publickey**, you must create an SSH user and a local user on the SSH server. The two users must have the same username, so that the SSH user can be assigned the correct working directory and user role.
- If the authentication method is **password**, you must perform one of the following tasks:
  - For local authentication, configure a local user on the SSH server.
  - For remote authentication, configure an SSH user on a remote authentication server, for example, a RADIUS server.

  You do not need to create an SSH user by using the **ssh user** command. However, if you want to display all SSH users, including the password-only SSH users, for centralized management, you can use this command to create them. If such an SSH user has been created, make sure you have specified the correct service type and authentication method.
- If the authentication method is **password-publickey** or **any**, you must create an SSH user on the SSH server and perform one of the following tasks:
  - For local authentication, configure a local user on the SSH server.
  - For remote authentication, configure an SSH user on a remote authentication server, for example, a RADIUS server.

  In either case, the local user or the SSH user configured on the remote authentication server must have the same username as the SSH user.

For an SFTP or SCP user, the working directory depends on the authentication method.

- If the authentication method is **publickey** or **password-publickey**, the working directory is specified by the **authorization-attribute** command in the associated local user view.
- If the authentication method is **password**, the working directory is authorized by AAA.

For an SSH user, the user role also depends on the authentication method.

- If the authentication method is **publickey** or **password-publickey**, the user role is specified by the **authorization-attribute** command in the associated local user view.
- If the authentication method is **password**, the user role is authorized by AAA.

If you use this command to specify a host public key or a PKI domain for a user multiple times, the most recent configuration takes effect. If neither a host public key nor a PKI domain is specified for the user, the user uses certificate authentication for login. The server uses the PKI domain of its own certificate to verify the client's certificate.

The command configuration does not affect logged-in users. It affects only users that attempt to log in after the configuration.

Examples

Create an SSH user named **user1**. Specify the service type as **sftp** and the authentication method as **password-publickey** for the user. Assign the host public key **key1** to the user.

```
<Sysname> system-view
[Sysname] ssh user user1 service-type sftp authentication-type password-publickey assign publickey key1
```

Create a local device management user named **user1**. Specify the password as **123456TESTplat&!** in plain text and the service type as **ssh** for the user. Assign the working directory **flash:** and the **network-admin** user role to the user.

```
[Sysname] local-user user1 class manage
[Sysname-luser-manage-user1] password simple 123456TESTplat&!
[Sysname-luser-manage-user1] service-type ssh
[Sysname-luser-manage-user1] authorization-attribute work-directory flash: user-role
network-admin
```

Related commands

authorization-attribute

display ssh user-information

local-user

pki domain

SSH client commands

bye

Use **bye** to terminate the connection with the SFTP server and return to user view.

Syntax

bye

Views

SFTP client view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command has the same function as the **exit** and **quit** commands.

Examples

Terminate the connection with the SFTP server.

```
sftp> bye
<Sysname>
```

cd

Use **cd** to change the working directory on the SFTP server.

Syntax

cd [*remote-path*]

Views

SFTP client view

Predefined user roles

network-admin

context-admin

Parameters

remote-path: Specifies the name of a directory on the server.

Usage guidelines

You can use the **cd ..** command to return to the upper-level directory.

You can use the **cd /** command to return to the root directory of the system.

Examples

Change the working directory to **new1**.

```
sftp> cd new1
Current Directory is:/new1
sftp> pwd
Remote working directory: /new1
sftp>
```

cdup

Use **cdup** to return to the upper-level directory.

Syntax

cdup

Views

SFTP client view

Predefined user roles

network-admin

context-admin

Example

Return to the upper-level directory from the current working directory **/test1**.

```
sftp> cd test1
Current Directory is:/test1
sftp> pwd
Remote working directory: /test1
sftp> cdup
Current Directory is:/
sftp> pwd
Remote working directory: /
sftp>
```

delete

Use **delete** to delete a file from the SFTP server.

Syntax

delete *remote-file*

Views

SFTP client view

Predefined user roles

network-admin

context-admin

Parameters

remote-file: Specifies a file by its name.

Usage guidelines

This command has the same function as the **remove** command.

Examples

Delete file **temp.c** from the SFTP server.

```
sftp> delete temp.c
Removing /temp.c
```

dir

Use **dir** to display information about the files and subdirectories under a directory.

Syntax

dir [**-a** | **-l**] [*remote-path*]

Views

SFTP client view

Predefined user roles

network-admin

context-admin

Parameters

-a: Displays detailed information about files and subdirectories under a directory in a list, including the files and subdirectories with names starting with dots (.).

-l: Displays detailed information about the files and subdirectories under a directory in a list, excluding the files and subdirectories with names starting with dots (.).

remote-path: Specifies the name of the directory to be queried. If you do not specify this argument, the command displays information about the files and subdirectories under the current working directory.

Usage guidelines

If you do not specify both of the **-a** and **-l** keywords, this command displays the names of the files and subdirectories under a directory.

This command has the same function as the **ls** command.

Examples

Display detailed information about the files and subdirectories under the current directory, including the files and subdirectories with names starting with dots (.).

```
sftp> dir -a
drwxrwxrwx    2 1        1               512 Dec 18 14:12 .
drwxrwxrwx    2 1        1               512 Dec 18 14:12 ..
-rwxrwxrwx    1 1        1               301 Dec 18 14:11 010.pub
-rwxrwxrwx    1 1        1               301 Dec 18 14:12 011.pub
-rwxrwxrwx    1 1        1               301 Dec 18 14:12 012.pub
```

Display detailed information about the files and subdirectories under the current directory, excluding the files and subdirectories with names starting with dots (.).

```
sftp> dir -l
-rwxrwxrwx    1 1        1               301 Dec 18 14:11 010.pub
-rwxrwxrwx    1 1        1               301 Dec 18 14:12 011.pub
-rwxrwxrwx    1 1        1               301 Dec 18 14:12 012.pub
```

display sftp client source

Use **display sftp client source** to display the source IP address configuration of the SFTP client.

Syntax

display sftp client source

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display the source IP address configuration of the SFTP client.

```
<Sysname> display sftp client source
The source IP address of the SFTP client is 192.168.0.1
The source IPv6 address of the SFTP client is 2:2::2:2.
```

Related commands

sftp client ipv6 source

sftp client source

display ssh client source

Use **display ssh client source** to display the source IP address configuration of the Stelnet client.

Syntax

display ssh client source

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display the source IP address configuration of the Stelnet client.

```
<Sysname> display ssh client source
The source IP address of the SSH client is 192.168.0.1
The source IPv6 address of the SSH client is 2:2::2:2.
```

Related commands

ssh client ipv6 source

ssh client source

exit

Use **exit** to terminate the SFTP connection and return to user view.

Syntax

exit

Views

SFTP client view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Usage guidelines

This command has the same function as the **bye** and **quit** commands.

Examples

Terminate the SFTP connection.

```
sftp> exit
<Sysname>
```

get

Use **get** to download a file from the SFTP server and save it locally.

Syntax

get *remote-file* [*local-file*]

Views

SFTP client view

Predefined user roles

network-admin

context-admin

Parameters

remote-file: Specifies the name of a file on the SFTP server.

local-file: Specifies the name for the local file. If you do not specify this argument, the file will be saved locally with the same name as the file on the SFTP server.

Examples

Download file **temp1.c** and save it as **temp.c** locally.

```
sftp> get temp1.c temp.c
Fetching /temp1.c to temp.c
/temp.c                                                100% 1424     1.4KB/s   00:00
```

help

Use **help** to display help information on the SFTP client.

Syntax

help

Views

SFTP client view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command has the same function as entering the question mark (?).

Examples

Display help information on the SFTP client.

```
sftp> help
Available commands:
  bye                          Quit sftp
  cd [path]                    Change remote directory to 'path'
  cdup                         Change remote directory to the parent directory
  delete path                  Delete remote file
  dir [-a|-l][path]            Display remote directory listing
       -a                        List all filenames
       -l                        List filename including the specific
                                 information of the file
  exit                         Quit sftp
  get remote-path [local-path] Download file
  help                         Display this help text
  ls [-a|-l][path]             Display remote directory
       -a                          List all filenames
       -l                          List filename including the specific
                                   information of the file
  mkdir path                   Create remote directory
  put local-path [remote-path] Upload file
  pwd                          Display remote working directory
  quit                         Quit sftp
  rename oldpath newpath       Rename remote file
  remove path                  Delete remote file
```

```
rmdir path                    Delete remote empty directory
?                             Synonym for help
```

ls

Use **ls** to display information about the files and subdirectories under a directory.

Syntax

ls [**-a** | **-l**] [*remote-path*]

Views

SFTP client view

Predefined user roles

network-admin

context-admin

Parameters

-a: Displays detailed information about files and subdirectories under a directory in a list, including the files and subdirectories with names starting with dots (.).

-l: Displays detailed information about the files and subdirectories under a directory in a list, excluding the files and subdirectories with names starting with dots (.).

remote-path: Specifies the name of the directory to be queried. If you do not specify this argument, the command displays information about the files and subdirectories under the current working directory.

Usage guidelines

If you do not specify both of the **-a** and **-l** keywords, this command displays the names of the files and subdirectories under a directory.

This command has the same function as the **dir** command.

Examples

Display detailed information about the files and subdirectories under the current directory, including the files and subdirectories with names starting with dots (.).

```
sftp> ls -a
drwxrwxrwx    2 1        1               512 Dec 18 14:12 .
drwxrwxrwx    2 1        1               512 Dec 18 14:12 ..
-rwxrwxrwx    1 1        1               301 Dec 18 14:11 010.pub
-rwxrwxrwx    1 1        1               301 Dec 18 14:12 011.pub
-rwxrwxrwx    1 1        1               301 Dec 18 14:12 012.pub
```

Display detailed information about the files and subdirectories under the current working directory, excluding the files and subdirectories with names starting with dots (.).

```
sftp> ls -l
-rwxrwxrwx    1 1        1               301 Dec 18 14:11 010.pub
-rwxrwxrwx    1 1        1               301 Dec 18 14:12 011.pub
-rwxrwxrwx    1 1        1               301 Dec 18 14:12 012.pub
```

mkdir

Use **mkdir** to create a directory on the SFTP server.

Syntax

mkdir *remote-path*

Views

SFTP client view

Predefined user roles

network-admin

context-admin

Parameters

remote-path: Specifies the name of a directory.

Examples

Create a directory named **test** on the SFTP server.

```
sftp> mkdir test
```

put

Use **put** to upload a local file to the SFTP server.

Syntax

put *local-file* [*remote-file*]

Views

SFTP client view

Predefined user roles

network-admin

context-admin

Parameters

local-file: Specifies the name of a local file.

remote-file: Specifies the name of a file on an SFTP server. If you do not specify this argument, the file will be remotely saved with the same name as the local file.

Examples

Upload the local file **startup.bak** to the SFTP server and save it as **startup01.bak**.

```
sftp> put startup.bak startup01.bak
Uploading startup.bak to /startup01.bak
startup01.bak                                 100% 1424     1.4KB/s   00:00
```

pwd

Use **pwd** to display the current working directory of the SFTP server.

Syntax

pwd

Views

SFTP client view

Predefined user roles

network-admin

context-admin

Examples

Display the current working directory of the SFTP server.

```
sftp> pwd
Remote working directory: /
```

The output shows that the current working directory is the root directory.

quit

Use **quit** to terminate the SFTP connection and return to user view.

Syntax

quit

Views

SFTP client view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command has the same function as the **bye** and **exit** commands.

Examples

Terminate the SFTP connection.

```
sftp> quit
<Sysname>
```

remove

Use **remove** to delete a file from the SFTP server.

Syntax

remove *remote-file*

Views

SFTP client view

Predefined user roles

network-admin

context-admin

Parameters

remote-file: Specifies a file by its name.

Usage guidelines

This command has the same function as the **delete** command.

Examples

Delete file **temp.c** from the SFTP server.

```
sftp> remove temp.c
Removing /temp.c
```

rename

Use **rename** to change the name of a file or directory on the SFTP server.

Syntax

rename *old-name new-name*

Views

SFTP client view

Predefined user roles

network-admin

context-admin

Parameters

oldname: Specifies the name of an existing file or directory.

newname: Specifies a new name for the existing file or directory.

Examples

Change the name of a file on the SFTP server from **temp1.c** to **temp2.c**.

```
sftp> dir
aa.pub  temp1.c
sftp> rename temp1.c temp2.c
sftp> dir
aa.pub  temp2.c
```

rmdir

Use **rmdir** to delete a directory from the SFTP server.

Syntax

rmdir *remote-path*

Views

SFTP client view

Predefined user roles

network-admin

context-admin

Parameters

remote-path: Specifies a directory.

Examples

Delete subdirectory **temp1** under the current directory on the SFTP server.

```
sftp> rmdir temp1
```

scp

Use **scp** to establish a connection to an IPv4 SCP server and transfer files with the server.

Syntax

scp *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] { **get** | **put** } *source-file-name* [*destination-file-name*] [**identity-key** { **dsa** | **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** | { **x509v3-ecdsa-sha2-nistp256** | **x509v3-ecdsa-sha2-nistp384** } **pki-domain** *domain-name* } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [{ **public-key** *keyname* | **server-pki-domain** *domain-name* } | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] *

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

server: Specifies a server by its IPv4 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range of 1 to 65535. The default is 22.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

get: Downloads the file.

put: Uploads the file.

source-file-name: Specifies the name of the source file, a case-sensitive string of 1 to 255 characters.

destination-file-name: Specifies the name of the target file, a case-sensitive string of 1 to 255 characters. If you do not specify this argument, the target file uses the same file name as the source file.

identity-key: Specifies a public key algorithm for publickey authentication of the client. The default is DSA. If the server uses publickey authentication, you must specify this keyword. The client generates the digital signature or certificate by using the local private key that is associated with the specified algorithm.

- **dsa**: Specifies public key algorithm DSA.
- **ecdsa-sha2-nistp256**: Specifies the ECDSA algorithm with 256-bit key strength.
- **ecdsa-sha2-nistp384**: Specifies the ECDSA algorithm with 384-bit key strength.
- **rsa**: Specifies public key algorithm RSA.

- **x509v3-ecdsa-sha2-nistp256**: Specifies public key algorithm x509v3-ecdsa-sha2-nistp256.
- **x509v3-ecdsa-sha2-nistp384**: Specifies public key algorithm x509v3-ecdsa-sha2-nistp384.
- **pki-domain** *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument is a case-insensitive string of 1 to 31 characters. When the x509v3 public key algorithm is used, you must specify this option for the client to get the correct local certificate.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies compression algorithm zlib.

prefer-ctos-cipher: Specifies the preferred client-to-server encryption algorithm. The default is AES128-CTR. Supported algorithms are DES-CBC, 3DES-CBC, AES128-CBC, AES128-CTR, AES128-GCM, AES192-CTR, AES256-CBC, AES256-CTR, and AES256-GCM, in ascending order of security strength and computation time.

- **3des-cbc**: Specifies encryption algorithm 3DES-CBC.
- **aes128-cbc**: Specifies encryption algorithm AES128-CBC.
- **aes128-ctr**: Specifies encryption algorithm AES128-CTR.
- **aes128-gcm**: Specifies encryption algorithm AES128-GCM.
- **aes192-ctr**: Specifies encryption algorithm AES192-CTR.
- **aes256-cbc**: Specifies encryption algorithm AES256-CBC.
- **aes256-ctr**: Specifies encryption algorithm AES256-CTR.
- **aes256-gcm**: Specifies encryption algorithm AES256-GCM.
- **des-cbc**: Specifies encryption algorithm DES-CBC.

prefer-ctos-hmac: Specifies the preferred client-to-server HMAC algorithm. The default is SHA2-256. Supported algorithms are MD5, MD5-96, SHA1, SHA1-96, SHA2-256, and SHA2-512, in ascending order of security strength and computation time.

- **md5**: Specifies HMAC algorithm HMAC-MD5.
- **md5-96**: Specifies HMAC algorithm HMAC-MD5-96.
- **sha1**: Specifies HMAC algorithm HMAC-SHA1.
- **sha1-96**: Specifies HMAC algorithm HMAC-SHA1-96.
- **sha2-256**: Specifies HMAC algorithm HMAC-SHA2-256.
- **sha2-512**: Specifies HMAC algorithm HMAC-SHA2-512.

prefer-kex: Specifies the preferred key exchange algorithm. The default is ecdh-sha2-nistp256. Supported algorithms are diffie-hellman-group-exchange-sha1, diffie-hellman-group1-sha1, diffie-hellman-group14-sha1, ecdh-sha2-nistp256, and ecdh-sha2-nistp384, in ascending order of security strength and computation time.

- **dh-group-exchange-sha1**: Specifies key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1-sha1**: Specifies key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14-sha1**: Specifies key exchange algorithm diffie-hellman-group14-sha1.
- **ecdh-sha2-nistp256**: Specifies key exchange algorithm ecdh-sha2-nistp256.
- **ecdh-sha2-nistp384**: Specifies key exchange algorithm ecdh-sha2-nistp384.

prefer-stoc-cipher: Specifies the preferred server-to-client encryption algorithm. The default is AES128-CTR. Supported algorithms are the same as the client-to-server encryption algorithms (see the **prefer-ctos-cipher** keyword).

prefer-stoc-hmac: Specifies the preferred server-to-client HMAC algorithm. The default is SHA2-256. Supported algorithms are the same as the client-to-server HMAC algorithms (see the **prefer-ctos-hmac** keyword).

public-key *keyname*: Specifies the server's host public key that the client uses to authenticate the server. The *keyname* argument is a case-insensitive string of 1 to 64 characters.

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes (').

source: Specifies a source IPv4 address or source interface for SCP packets. By default, the device uses the primary IPv4 address of the output interface in the routing entry as the source address of SCP packets. As a best practice to ensure successful SCP connections, specify a loopback interface as the source interface or specify the IPv4 address of a loopback or dialer interface as the source address.

- **interface** *interface-type interface-number*: Specifies a source interface by its type and number. The IPv4 address of this interface is the source IPv4 address of the SCP packets.
- **ip** *ip-address*: Specifies a source IPv4 address.

Usage guidelines

If the client uses certificate authentication, the client must verify the server's certificate. For the client to correctly get the server's certificate, use the **server-pki-domain** *domain-name* option to specify the server's PKI domain on the client. The client uses the CA certificate stored in the specified PKI domain to verify the server's certificate and does not need to save the server's public key before authentication. If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

Examples

Connect the SCP client to SCP server **200.1.1.1**. Specify the public key of the server as **svkey**, and download file **abc.txt** from the server. The SCP client uses publickey authentication. Use the following algorithms:

- Preferred key exchange algorithm: **dh-group14-sha1**.
- Preferred server-to-client encryption algorithm: **aes128-cbc**.
- Preferred client-to-server HMAC algorithm: **sha1**.
- Preferred server-to-client HMAC algorithm: **sha1-96**.
- Preferred compression algorithm: **zlib**.

```
<Sysname> scp 200.1.1.1 get abc.txt prefer-kex dh-group14-sha1 prefer-stoc-cipher
aes128-cbc prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key
svkey
Username:
```

scp ipv6

Use **scp ipv6** to establish a connection to an IPv6 SCP server and transfer files with the server.

Syntax

scp ipv6 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**-i** *interface-type interface-number*] { **get** | **put** } *source-file-name*

[*destination-file-name*] [**identity-key** { **dsa** | **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** | { **x509v3-ecdsa-sha2-nistp256** | **x509v3-ecdsa-sha2-nistp384** } **pki-domain** *domain-name* } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [{ **public-key** *keyname* | **server-pki-domain** *domain-name* } | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

server: Specifies a server by its IPv6 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range of 1 to 65535. The default is 22.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

-i *interface-type interface-number:* Specifies an output interface by its type and number for SCP packets. This option is used only when the server uses a link-local address to provide the SCP service for the client. The specified output interface on the SCP client must have a link-local address.

get: Downloads the file.

put: Uploads the file.

source-file-name: Specifies the name of the source file, a case-sensitive string of 1 to 255 characters.

destination-file-name: Specifies the name of the target file, a case-sensitive string of 1 to 255 characters. If you do not specify this argument, the target file uses the same file name as the source file.

identity-key: Specifies a public key algorithm for publickey authentication of the client. The default is DSA. If the server uses publickey authentication, you must specify this keyword. The client generates the digital signature or certificate by using the local private key that is associated with the specified algorithm.

- **dsa**: Specifies public key algorithm DSA.
- **ecdsa-sha2-nistp256**: Specifies the ECDSA algorithm with 256-bit key strength.
- **ecdsa-sha2-nistp384**: Specifies the ECDSA algorithm with 384-bit key strength.
- **rsa**: Specifies public key algorithm RSA.
- **x509v3-ecdsa-sha2-nistp256**: Specifies public key algorithm x509v3-ecdsa-sha2-nistp256.

x509v3-ecdsa-sha2-nistp384: Specifies public key algorithm x509v3-ecdsa-sha2-nistp384.

- **pki-domain** *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument is a case-insensitive string of 1 to 31 characters. When the x509v3 public key algorithm is used, you must specify this option for the client to get the correct local certificate.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies compression algorithm zlib.

prefer-ctos-cipher: Specifies the preferred client-to-server encryption algorithm. The default is AES128-CTR. Supported algorithms are DES-CBC, 3DES-CBC, AES128-CBC, AES128-CTR, AES128-GCM, AES192-CTR, AES256-CBC, AES256-CTR, and AES256-GCM, in ascending order of security strength and computation time.

- **3des-cbc**: Specifies encryption algorithm 3DES-CBC.
- **aes128-cbc**: Specifies encryption algorithm AES128-CBC.
- **aes128-ctr**: Specifies encryption algorithm AES128-CTR.
- **aes128-gcm**: Specifies encryption algorithm AES128-GCM.
- **aes192-ctr**: Specifies encryption algorithm AES192-CTR.
- **aes256-cbc**: Specifies encryption algorithm AES256-CBC.
- **aes256-ctr**: Specifies encryption algorithm AES256-CTR.
- **aes256-gcm**: Specifies encryption algorithm AES256-GCM.
- **des-cbc**: Specifies encryption algorithm DES-CBC.

prefer-ctos-hmac: Specifies the preferred client-to-server HMAC algorithm. The default is SHA2-256. Supported algorithms are MD5, MD5-96, SHA1, SHA1-96, SHA2-256, and SHA2-512 in ascending order of security strength and computation time.

- **md5**: Specifies HMAC algorithm HMAC-MD5.
- **md5-96**: Specifies HMAC algorithm HMAC-MD5-96.
- **sha1**: Specifies HMAC algorithm HMAC-SHA1.
- **sha1-96**: Specifies HMAC algorithm HMAC-SHA1-96.
- **sha2-256**: Specifies HMAC algorithm HMAC-SHA2-256.
- **sha2-512**: Specifies HMAC algorithm HMAC-SHA2-512.

prefer-kex: Specifies the preferred key exchange algorithm. The default is ecdh-sha2-nistp256. Supported algorithms are diffie-hellman-group-exchange-sha1, diffie-hellman-group1-sha1, diffie-hellman-group14-sha1, ecdh-sha2-nistp256, and ecdh-sha2-nistp384, in ascending order of security strength and computation time.

- **dh-group-exchange-sha1**: Specifies key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1-sha1**: Specifies key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14-sha1**: Specifies key exchange algorithm diffie-hellman-group14-sha1.
- **ecdh-sha2-nistp256**: Specifies key exchange algorithm ecdh-sha2-nistp256.
- **ecdh-sha2-nistp384**: Specifies key exchange algorithm ecdh-sha2-nistp384.

prefer-stoc-cipher: Specifies the preferred server-to-client encryption algorithm. The default is AES128-CTR. Supported algorithms are the same as the client-to-server encryption algorithms (see the **prefer-ctos-cipher** keyword).

prefer-stoc-hmac: Specifies the preferred server-to-client HMAC algorithm. The default is SHA2-256. Supported algorithms are the same as the client-to-server HMAC algorithms (see the **prefer-ctos-hmac** keyword).

public-key *keyname*: Specifies the server's host public key that the client uses to authenticate the server. The *keyname* argument is a case-insensitive string of 1 to 64 characters.

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes (').

source: Specifies a source IPv6 address or source interface for IPv6 SCP packets. By default, the device automatically selects a source address for IPv6 SCP packets in compliance with RFC 3484. As a best practice to ensure successful SCP connections, specify a loopback interface as the source interface or specify the IPv6 address of a loopback or dialer interface as the source address.

- **interface** *interface-type interface-number*: Specifies a source interface by its type and number. The IPv6 address of this interface is the source IPv6 address of the IPv6 SCP packets.
- **ipv6** *ipv6-address*: Specifies a source IPv6 address.

Usage guidelines

If the client uses certificate authentication, the client must verify the server's certificate. For the client to correctly get the server's certificate, use the **server-pki-domain** *domain-name* option to specify the server's PKI domain on the client. The client uses the CA certificate stored in the specified PKI domain to verify the server's certificate and does not need to save the server's public key before authentication. If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

Examples

Connect an SCP client to SCP server **2000::1**. Specify the public key of the server as **svkey**, and download file **abc.txt** from the server. The SCP client uses publickey authentication. Use the following algorithms:

- Preferred key exchange algorithm: **dh-group14-sha1**.
- Preferred server-to-client encryption algorithm: **aes128-cbc**.
- Preferred client-to-server HMAC algorithm: **sha1**.
- Preferred server-to-client HMAC algorithm: **sha1-96**.
- Preferred compression algorithm: **zlib**.

```
<Sysname> scp ipv6 2000::1 get abc.txt prefer-kex dh-group14-sha1 prefer-stoc-cipher
aes128-cbc prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key
svkey
Username:
```

scp ipv6 suite-b

Use **scp ipv6 suite-b** to establish a connection to an IPv6 SCP server based on Suite B algorithms and transfer files with the server.

Syntax

scp ipv6 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**-i** *interface-type interface-number*] { **get** | **put** } *source-file-name* [*destination-file-name*] **suite-b** [**128-bit** | **192-bit**] **pki-domain** *domain-name* [**server-pki-domain** *domain-name*] [**prefer-compress zlib**] [**source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

server: Specifies a server by its IPv6 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range of 1 to 65535. The default is 22.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

-i *interface-type interface-number:* Specifies an output interface by its type and number for SCP packets. Specify this option when the server uses a link-local address to provide the SCP service for the client. The specified output interface on the SCP client must have a link-local address.

get: Downloads the file.

put: Uploads the file.

source-file-name: Specifies the name of the source file, a case-sensitive string of 1 to 255 characters.

destination-file-name: Specifies the name of the target file, a case-sensitive string of 1 to 255 characters. If you do not specify this argument, the target file uses the same file name as the source file.

suite-b: Specifies the Suite B algorithms. If neither the 128-bit keyword nor the 192-bit keyword is specified, all algorithms in Suite B are used. For more information about the Suite B algorithms, see Table 4.

128-bit: Specifies the 128-bit Suite B security level.

192-bit: Specifies the 192-bit Suite B security level.

pki-domain *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes (').

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes ('). If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies compression algorithm zlib.

source: Specifies a source IPv6 address or source interface for IPv6 SCP packets. By default, the device automatically selects a source address for IPv6 SCP packets in compliance with RFC 3484. As a best practice to ensure successful SCP connections, specify a loopback interface as the source interface or specify the IPv6 address of a loopback or dialer interface as the source address.

- **interface** *interface-type interface-number*: Specifies a source interface by its type and number. The IPv6 address of this interface is the source IPv6 address of the IPv6 SCP packets.
- **ipv6** *ipv6-address*: Specifies a source IPv6 address.

Usage guidelines

Table 4 Suite B algorithms

Security level	Key exchange algorithm	Encryption algorithm and HMAC algorithm	Public key algorithm
128-bit	ecdh-sha2-nistp256	AES128-GCM	x509v3-ecdsa-sha2-nistp256
192-bit	ecdh-sha2-nistp384	AES256-GCM	x509v3-ecdsa-sha2-nistp384
Both	ecdh-sha2-nistp256 ecdh-sha2-nistp384	AES128-GCM AES256-GCM	x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384

Examples

Use the 192-bit Suite B algorithms to establish a connection to SCP server **2000::1** and download the file **abc.txt** from the server. Specify the client's PKI domain and the server's PKI domain as **clientpkidomain** and **serverpkidomain**, respectively.

```
<Sysname> scp ipv6 2000::1 get abc.txt suite-b 192-bit pki-domain clientpkidomain
server-pki-domain serverpkidomain
Username:
```

scp suite-b

Use **scp suite-b** to establish a connection to an SCP server based on Suite B algorithms and transfer files with the server.

Syntax

scp *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] { **get** | **put** } *source-file-name* [*destination-file-name*] **suite-b** [**128-bit** | **192-bit**] **pki-domain** *domain-name* [**server-pki-domain** *domain-name*] [**prefer-compress zlib**] [**source** { **interface** *interface-type interface-number* | **ip** *ip-address* }]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

server: Specifies a server by its IPv4 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range of 1 to 65535. The default is 22.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

get: Downloads the file.

put: Uploads the file.

source-file-name: Specifies the name of the source file, a case-sensitive string of 1 to 255 characters.

destination-file-name: Specifies the name of the target file, a case-sensitive string of 1 to 255 characters. If you do not specify this argument, the target file uses the same file name as the source file.

suite-b: Specifies the Suite B algorithms. If neither the 128-bit keyword nor the 192-bit keyword is specified, all algorithms in Suite B are used. For more information about the Suite B algorithms, see Table 5.

128-bit: Specifies the 128-bit Suite B security level.

192-bit: Specifies the 192-bit Suite B security level.

pki-domain *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes (').

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes ('). If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies compression algorithm zlib.

source: Specifies a source IP address or source interface for SCP packets. By default, the device uses the primary IPv4 address of the output interface in the routing entry as the source address of SCP packets. As a best practice to ensure successful SCP connections, specify a loopback interface as the source interface or specify the IPv4 address of a loopback or dialer interface as the source address.

- **interface** *interface-type interface-number*: Specifies a source interface by its type and number. The IPv4 address of this interface is the source IPv4 address of the SCP packets.
- **ip** *ip-address*: Specifies a source IPv4 address.

Usage guidelines

Table 5 Suite B algorithms

Security level	Key exchange algorithm	Encryption algorithm and HMAC algorithm	Public key algorithm
128-bit	ecdh-sha2-nistp256	AES128-GCM	x509v3-ecdsa-sha2-nistp256
192-bit	ecdh-sha2-nistp384	AES256-GCM	x509v3-ecdsa-sha2-nistp384
Both	ecdh-sha2-nistp256 ecdh-sha2-nistp384	AES128-GCM AES256-GCM	x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384

Examples

Use the 128-bit Suite B algorithms to establish a connection to SCP server **200.1.1.1** and download the file **abc.txt** from the server. Specify the client's PKI domain and the server's PKI domain as **clientpkidomain** and **serverpkidomain**, respectively.

```
<Sysname> scp 200.1.1.1 get abc.txt suite-b 128-bit pki-domain clientpkidomain
server-pki-domain serverpkidomain
Username
```

sftp

Use **sftp** to establish a connection to an IPv4 SFTP server and enter SFTP client view.

Syntax

sftp *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key** { **dsa** | **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** | { **x509v3-ecdsa-sha2-nistp256** | **x509v3-ecdsa-sha2-nistp384** } **pki-domain** *domain-name* } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [**dscp** *dscp-value* | { **public-key** *keyname* | **server-pki-domain** *domain-name* } | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] *

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

server: Specifies a server by its IPv4 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range of 1 to 65535. The default is 22.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

identity-key: Specifies a public key algorithm for publickey authentication of the client. The default is DSA. If the server uses publickey authentication, you must specify this keyword. The client generates the digital signature or certificate by using the local private key that is associated with the specified algorithm.

- **dsa**: Specifies public key algorithm DSA.
- **ecdsa-sha2-nistp256**: Specifies the ECDSA algorithm with 256-bit key strength.
- **ecdsa-sha2-nistp384**: Specifies the ECDSA algorithm with 384-bit key strength.
- **rsa**: Specifies public key algorithm RSA.
- **x509v3-ecdsa-sha2-nistp256**: Specifies public key algorithm x509v3-ecdsa-sha2-nistp256.
- **x509v3-ecdsa-sha2-nistp384**: Specifies public key algorithm x509v3-ecdsa-sha2-nistp384.

- **pki-domain** *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument is a case-insensitive string of 1 to 31 characters. When the x509v3 public key algorithm is used, you must specify this option for the client to get the correct local certificate.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies compression algorithm zlib.

prefer-ctos-cipher: Specifies the preferred client-to-server encryption algorithm. The default is AES128-CTR. Supported algorithms are DES-CBC, 3DES-CBC, AES128-CBC, AES128-CTR, AES128-GCM, AES192-CTR, AES256-CBC, AES256-CTR, and AES256-GCM, in ascending order of security strength and computation time.

- **3des-cbc**: Specifies encryption algorithm 3DES-CBC.
- **aes128-cbc**: Specifies encryption algorithm AES128-CBC.
- **aes128-ctr**: Specifies encryption algorithm AES128-CTR.
- **aes128-gcm**: Specifies encryption algorithm AES128-GCM.
- **aes192-ctr**: Specifies encryption algorithm AES192-CTR.
- **aes256-cbc**: Specifies encryption algorithm AES256-CBC.
- **aes256-ctr**: Specifies encryption algorithm AES256-CTR.
- **aes256-gcm**: Specifies encryption algorithm AES256-GCM.
- **des-cbc**: Specifies encryption algorithm DES-CBC.

prefer-ctos-hmac: Specifies the preferred client-to-server HMAC algorithm. The default is SHA2-256. Supported algorithms are MD5, MD5-96, SHA1, SHA1-96, SHA2-256, and SHA2-512 in ascending order of security strength and computation time.

- **md5**: Specifies HMAC algorithm HMAC-MD5.
- **md5-96**: Specifies HMAC algorithm HMAC-MD5-96.
- **sha1**: Specifies HMAC algorithm HMAC-SHA1.
- **sha1-96**: Specifies HMAC algorithm HMAC-SHA1-96.
- **sha2-256**: Specifies HMAC algorithm HMAC-SHA2-256.
- **sha2-512**: Specifies HMAC algorithm HMAC-SHA2-512.

prefer-kex: Specifies the preferred key exchange algorithm. The default is ecdh-sha2-nistp256. Supported algorithms are diffie-hellman-group-exchange-sha1, diffie-hellman-group1-sha1, diffie-hellman-group14-sha1, ecdh-sha2-nistp256, and ecdh-sha2-nistp384, in ascending order of security strength and computation time.

- **dh-group-exchange-sha1**: Specifies key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1-sha1**: Specifies key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14-sha1**: Specifies key exchange algorithm diffie-hellman-group14-sha1.
- **ecdh-sha2-nistp256**: Specifies key exchange algorithm ecdh-sha2-nistp256.
- **ecdh-sha2-nistp384**: Specifies key exchange algorithm ecdh-sha2-nistp384.

prefer-stoc-cipher: Specifies the preferred server-to-client encryption algorithm. The default is AES128-CTR. Supported algorithms are the same as the client-to-server encryption algorithms (see the **prefer-ctos-cipher** keyword).

prefer-stoc-hmac: Specifies the preferred server-to-client HMAC algorithm. The default is SHA2-256. Supported algorithms are the same as the client-to-server HMAC algorithms (see the **prefer-ctos-hmac** keyword).

dscp *dscp-value*: Specifies the DSCP value in the IPv4 SFTP packets. The value range for the *dscp-value* argument is 0 to 63, and the default value is 48. The DSCP value determines the transmission priority of the packet.

public-key *keyname*: Specifies the server's host public key that the client uses to authenticate the server. The *keyname* argument is a case-insensitive string of 1 to 64 characters.

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes (').

source: Specifies a source IPv4 address or source interface for the SFTP packets. By default, the device uses the primary IPv4 address of the output interface in the routing entry as the source address of SFTP packets. As a best practice to ensure successful SFTP connections, specify a loopback interface as the source interface or specify the IPv4 address of a loopback or dialer interface as the source address.

- **interface** *interface-type interface-number*: Specifies a source interface by its type and number. The primary IPv4 address of this interface is the source IPv4 address of the SFTP packets.
- **ip** *ip-address*: Specifies a source IPv4 address.

Usage guidelines

If the client uses certificate authentication, the client must verify the server's certificate. For the client to correctly get the server's certificate, use the **server-pki-domain** *domain-name* option to specify the server's PKI domain on the client. The client uses the CA certificate stored in the specified PKI domain to verify the server's certificate and does not need to save the server's public key before authentication. If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

Examples

Connect an SFTP client to SFTP server **10.1.1.2** and specify the public key of the server as **svkey**. The SFTP client uses publickey authentication. Use the following algorithms:

- Preferred key exchange algorithm: **dh-group14-sha1**.
- Preferred server-to-client encryption algorithm: **aes128-cbc**.
- Preferred client-to-server HMAC algorithm: **sha1**.
- Preferred server-to-client HMAC algorithm: **sha1-96**.
- Preferred compression algorithm: **zlib**.

```
<Sysname> sftp 10.1.1.2 prefer-kex dh-group14-sha1 prefer-stoc-cipher aes128-cbc
prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key svkey
```

sftp client ipv6 source

Use **sftp client ipv6 source** to configure the source IPv6 address for SFTP packets that are sent by the SFTP client.

Use **undo sftp client ipv6 source** to restore the default.

Syntax

sftp client ipv6 source { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }

undo sftp client ipv6 source

Default

The source IPv6 address for outgoing SFTP packets is not configured. The SFTP client automatically selects an IPv6 address for outgoing SFTP packets in compliance with RFC 3484.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interface *interface-type interface-number*: Specifies a source interface by its type and number. The SFTP client selects the interface's address that most specifically matches the destination address of outgoing SFTP packets as the source address of the SFTP packets.

ipv6 *ipv6-address*: Specifies a source IPv6 address.

Usage guidelines

This command takes effect on all IPv6 SFTP connections. The source IPv6 address specified in the **sftp ipv6** command takes effect only on the current IPv6 SFTP connection. If you specify the source IPv6 address both in this command and the **sftp ipv6** command, the source IPv6 address specified in the **sftp ipv6** command takes effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify **2:2::2:2** as the source IPv6 address for SFTP packets.

```
<Sysname> system-view
[Sysname] sftp client ipv6 source ipv6 2:2::2:2
```

Related commands

display sftp client source

sftp client source

Use **sftp client source** to configure the source IPv4 address for SFTP packets that are sent by the SFTP client.

Use **undo sftp client source** to restore the default.

Syntax

sftp client source { **interface** *interface-type interface-number* | **ip** *ip-address* }

undo sftp client source

Default

The source IPv4 address for outgoing SFTP packets is not configured. The SFTP client uses the primary IPv4 address of the output interface in the matching route as the source IPv4 address of outgoing SFTP packets.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interface *interface-type interface-number*: Specifies a source interface by its type and number. The SFTP client uses the primary IPv4 address of the interface as the source address of outgoing SFTP packets.

ip *ip-address*: Specifies a source IPv4 address.

Usage guidelines

This command takes effect on all SFTP connections. The source IPv4 address specified in the **sftp** command takes effect only on the current SFTP connection. If you specify the source IPv4 address both in this command and the **sftp** command, the source IPv4 address specified in the **sftp** command takes effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify **192.168.0.1** as the source IPv4 address for SFTP packets.

```
<Sysname> system-view
[Sysname] sftp client source ip 192.168.0.1
```

Related commands

display sftp client source

sftp ipv6

Use **sftp ipv6** to connect an SFTP client to an IPv6 SFTP server and enter SFTP client view.

Syntax

sftp ipv6 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**-i** *interface-type interface-number*] [**identity-key** { **dsa** | **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** | { **x509v3-ecdsa-sha2-nistp256** | **x509v3-ecdsa-sha2-nistp384** } **pki-domain** *domain-name* } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [**dscp** *dscp-value* | { **public-key** *keyname* | **server-pki-domain** *domain-name* } | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

server: Specifies a server by its IPv6 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range of 1 to 65535. The default is 22.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

-i *interface-type interface-number:* Specifies an output interface by its type and number for IPv6 SFTP packets. This option is used only when the server uses a link-local address to provide the SFTP service for the client. The specified output interface on the SFTP client must have a link-local address.

identity-key: Specifies a public key algorithm for publickey authentication of the client. The default is DSA. If the server uses publickey authentication, you must specify this keyword. The client generates the digital signature or certificate by using the local private key that is associated with the specified algorithm.

- **dsa**: Specifies public key algorithm DSA.
- **ecdsa-sha2-nistp256**: Specifies the ECDSA algorithm with 256-bit key strength.
- **ecdsa-sha2-nistp384**: Specifies the ECDSA algorithm with 384-bit key strength.
- **rsa**: Specifies public key algorithm RSA.
- **x509v3-ecdsa-sha2-nistp256**: Specifies public key algorithm x509v3-ecdsa-sha2-nistp256.
- **x509v3-ecdsa-sha2-nistp384**: Specifies public key algorithm x509v3-ecdsa-sha2-nistp384.
- **pki-domain** *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument is a case-insensitive string of 1 to 31 characters. When the x509v3 public key algorithm is used, you must specify this option for the client to get the correct local certificate.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies compression algorithm zlib.

prefer-ctos-cipher: Specifies the preferred client-to-server encryption algorithm. The default is AES128-CTR. Supported algorithms are DES-CBC, 3DES-CBC, AES128-CBC, AES128-CTR, AES128-GCM, AES192-CTR, AES256-CBC, AES256-CTR, and AES256-GCM, in ascending order of security strength and computation time.

- **3des-cbc**: Specifies encryption algorithm 3DES-CBC.
- **aes128-cbc**: Specifies encryption algorithm AES128-CBC.
- **aes128-ctr**: Specifies encryption algorithm AES128-CTR.
- **aes128-gcm**: Specifies encryption algorithm AES128-GCM.
- **aes192-ctr**: Specifies encryption algorithm AES192-CTR.
- **aes256-cbc**: Specifies encryption algorithm AES256-CBC.
- **aes256-ctr**: Specifies encryption algorithm AES256-CTR.
- **aes256-gcm**: Specifies encryption algorithm AES256-GCM.
- **des-cbc**: Specifies encryption algorithm DES-CBC.

prefer-ctos-hmac: Specifies the preferred client-to-server HMAC algorithm. The default is SHA2-256. Supported algorithms are MD5, MD5-96, SHA1, SHA1-96, SHA2-256, and SHA2-512 in ascending order of security strength and computation time.

- **md5**: Specifies HMAC algorithm HMAC-MD5.
- **md5-96**: Specifies HMAC algorithm HMAC-MD5-96.
- **sha1**: Specifies HMAC algorithm HMAC-SHA1.
- **sha1-96**: Specifies HMAC algorithm HMAC-SHA1-96.
- **sha2-256**: Specifies HMAC algorithm HMAC-SHA2-256.
- **sha2-512**: Specifies HMAC algorithm HMAC-SHA2-512.

prefer-kex: Specifies the preferred key exchange algorithm. The default is ecdh-sha2-nistp256. Supported algorithms are diffie-hellman-group-exchange-sha1, diffie-hellman-group1-sha1, diffie-hellman-group14-sha1, ecdh-sha2-nistp256, and ecdh-sha2-nistp384, in ascending order of security strength and computation time.

- **dh-group-exchange-sha1**: Specifies key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1-sha1**: Specifies key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14-sha1**: Specifies key exchange algorithm diffie-hellman-group14-sha1.
- **ecdh-sha2-nistp256**: Specifies key exchange algorithm ecdh-sha2-nistp256.
- **ecdh-sha2-nistp384**: Specifies key exchange algorithm ecdh-sha2-nistp384.

prefer-stoc-cipher: Specifies the preferred server-to-client encryption algorithm. The default is AES128-CTR. Supported algorithms are the same as the client-to-server encryption algorithms (see the **prefer-ctos-cipher** keyword).

prefer-stoc-hmac: Specifies the preferred server-to-client HMAC algorithm. The default is SHA2-256. Supported algorithms are the same as the client-to-server HMAC algorithms (see the **prefer-ctos-hmac** keyword).

dscp *dscp-value*: Specifies the DSCP value in the IPv6 SFTP packets. The value range for the *dscp-value* argument is 0 to 63, and the default value is 48. The DSCP value determines the transmission priority of the packet.

public-key *keyname*: Specifies the host public key of the server that the client uses to authenticate the server. The *keyname* argument is a case-insensitive string of 1 to 64 characters.

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes (').

source: Specifies a source IPv6 address or source interface for IPv6 SFTP packets. By default, the device automatically selects a source address for IPv6 SFTP packets in compliance with RFC 3484. As a best practice to ensure successful SFTP connections, specify a loopback interface as the source interface or specify the IPv6 address of a loopback or dialer interface as the source address.

- **interface** *interface-type interface-number*: Specifies a source interface by its type and number. The IPv6 address of this interface is the source IPv6 address of the IPv6 SFTP packets.
- **ipv6** *ipv6-address*: Specifies a source IPv6 address.

Usage guidelines

If the client uses certificate authentication, the client must verify the server's certificate. For the client to correctly get the server's certificate, use the **server-pki-domain** *domain-name* option to specify the server's PKI domain on the client. The client uses the CA certificate stored in the

specified PKI domain to verify the server's certificate and does not need to save the server's public key before authentication. If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

Examples

Connect an SFTP client to SFTP server **2000::1** and specify the public key of the server as **svkey**. The SFTP client uses publickey authentication. Use the following algorithms:

- Preferred key exchange algorithm: **dh-group14-sha1**.
- Preferred server-to-client encryption algorithm: **aes128-cbc**.
- Preferred client-to-server HMAC algorithm: **sha1**.
- Preferred server-to-client HMAC algorithm: **sha1-96**.
- Preferred compression algorithm: **zlib**.

```
<Sysname> sftp ipv6 2000::1 prefer-kex dh-group14-sha1 prefer-stoc-cipher aes128-cbc
prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key svkey
Username:
```

sftp ipv6 suite-b

Use **sftp ipv6 suite-b** to establish a connection to an IPv6 SFTP server based on Suite B algorithms and enter SFTP client view.

Syntax

sftp ipv6 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**-i** *interface-type interface-number*] **suite-b** [**128-bit** | **192-bit**] **pki-domain** *domain-name* [**server-pki-domain** *domain-name*] [**prefer-compress zlib**] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

server: Specifies a server by its IPv6 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range of 1 to 65535. The default is 22.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

-i *interface-type interface-number:* Specifies an output interface by its type and number for IPv6 SFTP packets. The specified outgoing interface must have a link-local address. This option is used only when the server uses a link-local address to provide the SFTP service for the client.

suite-b: Specifies the Suite B algorithms. If neither the 128-bit keyword nor the 192-bit keyword is specified, all algorithms in Suite B are used. For more information about the Suite B algorithms, see Table 6.

128-bit: Specifies the 128-bit Suite B security level.

192-bit: Specifies the 192-bit Suite B security level.

pki-domain *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes (').

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes ('). If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies compression algorithm zlib.

dscp *dscp-value*: Specifies the DSCP value in the IPv6 SFTP packets. The value range for the *dscp-value* argument is 0 to 63, and the default value is 48. The DSCP value determines the transmission priority of the packet.

source: Specifies a source IP address or source interface for IPv6 SFTP packets. By default, the device automatically selects a source address for IPv6 SFTP packets in compliance with RFC 3484. As a best practice to ensure successful SFTP connections, specify a loopback interface as the source interface or specify the IPv6 address of a loopback or dialer interface as the source address.

- **interface** *interface-type interface-number*: Specifies a source interface by its type and number. The IPv6 address of this interface is the source IP address of the IPv6 SFTP packets.
- **ipv6** *ipv6-address*: Specifies a source IPv6 address.

Usage guidelines

Table 6 Suite B algorithms

Security level	Key exchange algorithm	Encryption algorithm and HMAC algorithm	Public key algorithm
128-bit	ecdh-sha2-nistp256	AES128-GCM	x509v3-ecdsa-sha2-nistp256
192-bit	ecdh-sha2-nistp384	AES256-GCM	x509v3-ecdsa-sha2-nistp384
Both	ecdh-sha2-nistp256 ecdh-sha2-nistp384	AES128-GCM AES256-GCM	x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384

Examples

Use the 192-bit Suite B algorithms to establish a connection to SFTP server **2000::1**. Specify the client's PKI domain and the server's PKI domain as **clientpkidomain** and **serverpkidomain**, respectively.

```
<Sysname> sftp ipv6 2000::1 suite-b 192-bit pki-domain clientpkidomain server-pki-domain
serverpkidomain
Username:
```

sftp suite-b

Use **sftp suite-b** to establish a connection to an IPv4 SFTP server based on Suite B algorithms and enter SFTP client view.

Syntax

sftp *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] **suite-b** [**128-bit** | **192-bit**] **pki-domain** *domain-name* [**server-pki-domain** *domain-name*] [**prefer-compress** **zlib**] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] *

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

server: Specifies a server by its IPv4 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range of 1 to 65535. The default is 22.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

suite-b: Specifies the Suite B algorithms. If neither the 128-bit keyword nor the 192-bit keyword is specified, all algorithms in Suite B are used. For more information about the Suite B algorithms, see Table 7.

128-bit: Specifies the 128-bit Suite B security level.

192-bit: Specifies the 192-bit Suite B security level.

pki-domain *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes (').

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes ('). If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies compression algorithm zlib.

dscp *dscp-value*: Specifies the DSCP value in the IPv4 SFTP packets. The value range for the *dscp-value* argument is 0 to 63, and the default value is 48. The DSCP value determines the transmission priority of the packet.

source: Specifies a source IP address or source interface for the SFTP packets. By default, the device uses the primary IPv4 address of the output interface in the routing entry as the source address of SFTP packets. As a best practice to ensure successful SFTP connections, specify a loopback interface as the source interface or specify the IPv4 address of a loopback or dialer interface as the source address.

- **interface** *interface-type interface-number*: Specifies a source interface by its type and number. The primary IPv4 address of this interface is the source IPv4 address of the SFTP packets.

- **ip** *ip-address*: Specifies a source IPv4 address.

Usage guidelines

Table 7 Suite B algorithms

Security level	Key exchange algorithm	Encryption algorithm and HMAC algorithm	Public key algorithm
128-bit	ecdh-sha2-nistp256	AES128-GCM	x509v3-ecdsa-sha2-nistp256
192-bit	ecdh-sha2-nistp384	AES256-GCM	x509v3-ecdsa-sha2-nistp384
Both	ecdh-sha2-nistp256 ecdh-sha2-nistp384	AES128-GCM AES256-GCM	x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384

Examples

Use the 128-bit Suite B algorithms to establish a connection to SFTP server **10.1.1.2**. Specify the client's PKI domain and the server's PKI domain as **clientpkidomain** and **serverpkidomain**, respectively.

```
<Sysname> sftp 10.1.1.2 suite-b 128-bit pki-domain clientpkidomain server-pki-domain
serverpkidomain
Username
```

ssh client ipv6 source

Use **ssh client ipv6 source** to configure the source IPv6 address for SSH packets that are sent by the Stelnet client.

Use **undo ssh client ipv6 source** to restore the default.

Syntax

ssh client ipv6 source { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }

undo ssh client ipv6 source

Default

The source IPv6 address for outgoing SSH packets is not configured. The Stelnet client automatically selects an IPv6 address for outgoing SSH packets in compliance with RFC 3484.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interface *interface-type interface-number*: Specifies a source interface by its type and number. The Stelnet client selects the interface's address that most specifically matches the destination address of outgoing SSH packets as the source address of the SSH packets.

ipv6 *ipv6-address*: Specifies a source IPv6 address.

Usage guidelines

This command takes effect on all IPv6 Stelnet connections. The source IPv6 address specified in the **ssh2 ipv6** command takes effect only on the current IPv6 Stelnet connection. If you specify the

source IPv6 address both in this command and the **ssh2 ipv6** command, the source IPv6 address specified in the **ssh2 ipv6** command takes effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify **2:2::2:2** as the source IPv6 address for SSH packets that are sent by the Stelnet client.

```
<Sysname> system-view
[Sysname] ssh client ipv6 source ipv6 2:2::2:2
```

Related commands

display ssh client source

ssh client source

Use **ssh client source** to configure the source IPv4 address for SSH packets that are sent by the Stelnet client.

Use **undo ssh client source** to restore the default.

Syntax

ssh client source { **interface** *interface-type interface-number* | **ip** *ip-address* }

undo ssh client source

Default

The source IPv4 address for outgoing SSH packets is not configured. The Stelnet client uses the primary IPv4 address of the output interface in the matching route as the source address of outgoing SSH packets.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interface *interface-type interface-number*: Specifies a source interface by its type and number. The Stelnet client uses the primary IPv4 address of the interface as the source address of outgoing SSH packets.

ip *ip-address*: Specifies a source IPv4 address.

Usage guidelines

This command takes effect on all Stelnet connections. The source IPv4 address specified in the **ssh2** command takes effect only on the current Stelnet connection. If you specify the source IPv4 address both in this command and the **ssh2** command, the source IPv4 address specified in the **ssh2** command takes effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify **192.168.0.1** as the source IPv4 address for SSH packets.

```
<Sysname> system-view
[Sysname] ssh client source ip 192.168.0.1
```

Related commands

display ssh client source

ssh2

Use **ssh2** to establish a connection to an IPv4 Stelnet server.

Syntax

ssh2 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key** { **dsa** | **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** | { **x509v3-ecdsa-sha2-nistp256** | **x509v3-ecdsa-sha2-nistp384** } **pki-domain** *domain-name* } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [**dscp** *dscp-value* | **escape** *character* | { **public-key** *keyname* | **server-pki-domain** *domain-name* } | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] *

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

server: Specifies a server by its IPv4 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range 1 to 65535. The default is 22.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

identity-key: Specifies a public key algorithm for publickey authentication of the client. The default is DSA. If the server uses publickey authentication, you must specify this keyword. The client generates the digital signature or certificate by using the local private key that is associated with the specified algorithm.

- **dsa**: Specifies public key algorithm DSA.
- **ecdsa-sha2-nistp256**: Specifies the ECDSA algorithm with 256-bit key strength.
- **ecdsa-sha2-nistp384**: Specifies the ECDSA algorithm with 384-bit key strength.
- **rsa**: Specifies public key algorithm RSA.
- **x509v3-ecdsa-sha2-nistp256**: Specifies public key algorithm x509v3-ecdsa-sha2-nistp256.
- **x509v3-ecdsa-sha2-nistp384**: Specifies public key algorithm x509v3-ecdsa-sha2-nistp384.

- **pki-domain** *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument is a case-insensitive string of 1 to 31 characters. When the x509v3 public key algorithm is used, you must specify this option for the client to get the correct local certificate.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies compression algorithm zlib.

prefer-ctos-cipher: Specifies the preferred client-to-server encryption algorithm. The default is AES128-CTR. Supported algorithms are DES-CBC, 3DES-CBC, AES128-CBC, AES128-CTR, AES128-GCM, AES192-CTR, AES256-CBC, AES256-CTR, and AES256-GCM, in ascending order of security strength and computation time.

- **3des-cbc**: Specifies encryption algorithm 3DES-CBC.
- **aes128-cbc**: Specifies encryption algorithm AES128-CBC.
- **aes128-ctr**: Specifies encryption algorithm AES128-CTR.
- **aes128-gcm**: Specifies encryption algorithm AES128-GCM.
- **aes192-ctr**: Specifies encryption algorithm AES192-CTR.
- **aes256-cbc**: Specifies encryption algorithm AES256-CBC.
- **aes256-ctr**: Specifies encryption algorithm AES256-CTR.
- **aes256-gcm**: Specifies encryption algorithm AES256-GCM.
- **des-cbc**: Specifies encryption algorithm DES-CBC.

prefer-ctos-hmac: Specifies the preferred client-to-server HMAC algorithm. The default is SHA2-256. Supported algorithms are MD5, MD5-96, SHA1, SHA1-96, SHA2-256, and SHA2-512 in ascending order of security strength and computation time.

- **md5**: Specifies HMAC algorithm HMAC-MD5.
- **md5-96**: Specifies HMAC algorithm HMAC-MD5-96.
- **sha1**: Specifies HMAC algorithm HMAC-SHA1.
- **sha1-96**: Specifies HMAC algorithm HMAC-SHA1-96.
- **sha2-256**: Specifies HMAC algorithm HMAC-SHA2-256.
- **sha2-512**: Specifies HMAC algorithm HMAC-SHA2-512.

prefer-kex: Specifies the preferred key exchange algorithm. The default is ecdh-sha2-nistp256. Supported algorithms are diffie-hellman-group-exchange-sha1, diffie-hellman-group1-sha1, diffie-hellman-group14-sha1, ecdh-sha2-nistp256, and ecdh-sha2-nistp384, in ascending order of security strength and computation time.

- **dh-group-exchange-sha1**: Specifies key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1-sha1**: Specifies key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14-sha1**: Specifies key exchange algorithm diffie-hellman-group14-sha1.
- **ecdh-sha2-nistp256**: Specifies key exchange algorithm ecdh-sha2-nistp256.
- **ecdh-sha2-nistp384**: Specifies key exchange algorithm ecdh-sha2-nistp384.

prefer-stoc-cipher: Specifies the preferred server-to-client encryption algorithm. The default is AES128-CTR. Supported algorithms are the same as the client-to-server encryption algorithms (see the **prefer-ctos-cipher** keyword).

prefer-stoc-hmac: Specifies the preferred server-to-client HMAC algorithm. The default is SHA2-256. Supported algorithms are the same as the client-to-server HMAC algorithms (see the **prefer-ctos-hmac** keyword).

dscp *dscp-value*: Specifies the DSCP value in the IPv4 SSH packets. The value range for the *dscp-value* argument is 0 to 63, and the default value is 48. The DSCP value determines the transmission priority of the packet.

escape *character*: Specifies a case-sensitive escape character. By default, the escape character is a tilde (~).

public-key *keyname*: Specifies the host public key of the server that the client uses to authenticate the server. The *keyname* argument is a case-insensitive string of 1 to 64 characters.

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes (').

source: Specifies a source IPv4 address or source interface for SSH packets. By default, the device uses the primary IPv4 address of the output interface in the routing entry as the source address of SSH packets. As a best practice to ensure successful Stelnet connections, specify a loopback interface as the source interface or specify the IPv4 address of a loopback or dialer interface as the source address.

- **interface** *interface-type interface-number*: Specifies a source interface by its type and number. The primary IPv4 address of this interface is the source IPv4 address of the SSH packets.
- **ip** *ip-address*: Specifies a source IPv4 address.

Usage guidelines

The combination of an escape character and a dot (.) works as an escape sequence. This escape sequence is typically used to quickly terminate an SSH connection when the server reboots or malfunctions.

For the escape sequence to take effect, you must enter it at the very beginning of a line. If you have entered other characters or performed operations in a line, enter the escape sequence in the next line.

As a best practice, use the default escape character (~). Do not use any character in SSH usernames as the escape character.

If the client uses certificate authentication, the client must verify the server's certificate. For the client to correctly get the server's certificate, use the **server-pki-domain** *domain-name* option to specify the server's PKI domain on the client. The client uses the CA certificate stored in the specified PKI domain to verify the server's certificate and does not need to save the server's public key before authentication. If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

Examples

Establish a connection to Stelnet server **3.3.3.3** and specify the public key of the server as **svkey**. The Stelnet client uses publickey authentication. Specify the dollar sign ($) as the escape character. Use the following algorithms:

- Preferred key exchange algorithm: **dh-group14-sha1**.
- Preferred server-to-client encryption algorithm: **aes128-cbc**.
- Preferred client-to-server HMAC algorithm: **sha1**.
- Preferred server-to-client HMAC algorithm: **sha1-96**.
- Preferred compression algorithm: **zlib**.

```
<Sysname> ssh2 3.3.3.3 prefer-kex dh-group14-sha1 prefer-stoc-cipher aes128-cbc
prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key svkey
escape $
```

ssh2 ipv6

Use **ssh2 ipv6** to establish a connection to an IPv6 Stelnet server.

Syntax

ssh2 ipv6 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**-i** *interface-type interface-number*] [**identity-key** { **dsa** | **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** | { **x509v3-ecdsa-sha2-nistp256** | **x509v3-ecdsa-sha2-nistp384** } **pki-domain** *domain-name* } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [**dscp** *dscp-value* | **escape** *character* | { **public-key** *keyname* | **server-pki-domain** *domain-name* } | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

server: Specifies a server by its IPv6 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range 1 to 65535. The default is 22.

vpn-instance *vpn-instance-name:* Specifies the MPLS L3VPN instance to which the server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

-i *interface-type interface-number:* Specifies an output interface by its type and number for IPv6 SSH packets. This option is used only when the server uses a link-local address to provide the Stelnet service for the client. The specified output interface on the Stelnet client must have a link-local address.

identity-key: Specifies a public key algorithm for publickey authentication of the client. The default is DSA. If the server uses publickey authentication, you must specify this keyword. The client generates the digital signature or certificate by using the local private key that is associated with the specified algorithm.

- **dsa**: Specifies public key algorithm DSA.
- **ecdsa-sha2-nistp256**: Specifies the ECDSA algorithm with 256-bit key strength.
- **ecdsa-sha2-nistp384**: Specifies the ECDSA algorithm with 384-bit key strength.
- **rsa**: Specifies public key algorithm RSA.

- **x509v3-ecdsa-sha2-nistp256**: Specifies public key algorithm x509v3-ecdsa-sha2-nistp256.
- **x509v3-ecdsa-sha2-nistp384**: Specifies public key algorithm x509v3-ecdsa-sha2-nistp384.
- **pki-domain** *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument is a case-insensitive string of 1 to 31 characters. When the x509v3 public key algorithm is used, you must specify this option for the client to get the correct local certificate.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies compression algorithm zlib.

prefer-ctos-cipher: Specifies the preferred client-to-server encryption algorithm. The default is AES128-CTR. Supported algorithms are DES-CBC, 3DES-CBC, AES128-CBC, AES128-CTR, AES128-GCM, AES192-CTR, AES256-CBC, AES256-CTR, and AES256-GCM, in ascending order of security strength and computation time.

- **3des-cbc**: Specifies encryption algorithm 3DES-CBC.
- **aes128-cbc**: Specifies encryption algorithm AES128-CBC.
- **aes128-ctr**: Specifies encryption algorithm AES128-CTR.
- **aes128-gcm**: Specifies encryption algorithm AES128-GCM.
- **aes192-ctr**: Specifies encryption algorithm AES192-CTR.
- **aes256-cbc**: Specifies encryption algorithm AES256-CBC.
- **aes256-ctr**: Specifies encryption algorithm AES256-CTR.
- **aes256-gcm**: Specifies encryption algorithm AES256-GCM.
- **des-cbc**: Specifies encryption algorithm DES-CBC.

prefer-ctos-hmac: Specifies the preferred client-to-server HMAC algorithm. The default is SHA2-256. Supported algorithms are MD5, MD5-96, SHA1, SHA1-96, SHA2-256, and SHA2-512 in ascending order of security strength and computation time.

- **md5**: Specifies HMAC algorithm HMAC-MD5.
- **md5-96**: Specifies HMAC algorithm HMAC-MD5-96.
- **sha1**: Specifies HMAC algorithm HMAC-SHA1.
- **sha1-96**: Specifies HMAC algorithm HMAC-SHA1-96.
- **sha2-256**: Specifies HMAC algorithm HMAC-SHA2-256.
- **sha2-512**: Specifies HMAC algorithm HMAC-SHA2-512.

prefer-kex: Specifies the preferred key exchange algorithm. The default is ecdh-sha2-nistp256. Supported algorithms are diffie-hellman-group-exchange-sha1, diffie-hellman-group1-sha1, diffie-hellman-group14-sha1, ecdh-sha2-nistp256, and ecdh-sha2-nistp384, in ascending order of security strength and computation time.

- **dh-group-exchange-sha1**: Specifies key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1-sha1**: Specifies key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14-sha1**: Specifies key exchange algorithm diffie-hellman-group14-sha1.
- **ecdh-sha2-nistp256**: Specifies key exchange algorithm ecdh-sha2-nistp256.
- **ecdh-sha2-nistp384**: Specifies key exchange algorithm ecdh-sha2-nistp384.

prefer-stoc-cipher: Specifies the preferred server-to-client encryption algorithm. The default is AES128-CTR. Supported algorithms are the same as the client-to-server encryption algorithms (see the **prefer-ctos-cipher** keyword).

prefer-stoc-hmac: Specifies the preferred server-to-client HMAC algorithm. The default is SHA2-256. Supported algorithms are the same as the client-to-server HMAC algorithms (see the **prefer-ctos-hmac** keyword).

dscp *dscp-value*: Specifies the DSCP value in the IPv6 SSH packets. The value range for the *dscp-value* argument is 0 to 63, and the default value is 48. The DSCP value determines the transmission priority of the packet.

escape *character*: Specifies a case-sensitive escape character. By default, the escape character is a tilde (~).

public-key *keyname*: Specifies the server by its host public key that the client uses to authenticate the server. The *keyname* argument is a case-insensitive string of 1 to 64 characters.

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes (').

source: Specifies a source IPv6 address or source interface for IPv6 SSH packets. By default, the device automatically selects a source address for IPv6 SSH packets in compliance with RFC 3484. As a best practice to ensure successful Stelnet connections, specify a loopback interface as the source interface or specify the IPv6 address of a loopback or dialer interface as the source address.

- **interface** *interface-type interface-number*: Specifies a source interface by its type and number. The IPv6 address of this interface is the source IPv6 address of the IPv6 SSH packets.
- **ipv6** *ipv6-address*: Specifies a source IPv6 address.

Usage guidelines

The combination of an escape character and a dot (.) works as an escape sequence. This escape sequence is typically used to quickly terminate an SSH connection when the server reboots or malfunctions.

For the escape sequence to take effect, you must enter it at the very beginning of a line. If you have entered other characters or performed operations in a line, enter the escape sequence in the next line.

As a best practice, use the default escape character (~). Do not use any characters in SSH usernames as the escape character.

If the client uses certificate authentication, the client must verify the server's certificate. For the client to correctly get the server's certificate, use the **server-pki-domain** *domain-name* option to specify the server's PKI domain on the client. The client uses the CA certificate stored in the specified PKI domain to verify the server's certificate and does not need to save the server's public key before authentication. If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

Examples

Establish a connection to Stelnet server **2000::1** and specify the public key of the server as **svkey**. The SSH client uses publickey authentication. Specify the dollar sign ($) as the escape character. Use the following algorithms:

- Preferred key exchange algorithm: **dh-group14-sha1**.
- Preferred server-to-client encryption algorithm: **aes128-cbc**.
- Preferred client-to-server HMAC algorithm: **sha1**.
- Preferred server-to-client HMAC algorithm: **sha1-96**.

- Preferred compression algorithm: **zlib**.

```
<Sysname> ssh2 ipv6 2000::1 prefer-kex dh-group14-sha1 prefer-stoc-cipher aes128-cbc
prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key svkey
escape $
```

ssh2 ipv6 suite-b

Use **ssh2 ipv6 suite-b** to establish a connection to an IPv6 Stelnet server based on Suite B algorithms.

Syntax

ssh2 ipv6 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**-i** *interface-type interface-number*] **suite-b** [**128-bit** | **192-bit**] **pki-domain** *domain-name* [**server-pki-domain** *domain-name*] [**prefer-compress zlib**] [**dscp** *dscp-value* | **escape** *character* | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

server: Specifies a server by its IPv6 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range 1 to 65535. The default is 22.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

-i *interface-type interface-number:* Specifies an output interface by its type and number for IPv6 SSH packets. Specify this option when the server uses a link-local address to provide the Stelnet service for the client. The specified output interface on the Stelnet client must have a link-local address.

suite-b: Specifies the Suite B algorithms. If neither the 128-bit keyword nor the 192-bit keyword is specified, all algorithms in Suite B are used. For more information about the Suite B algorithms, see Table 8.

128-bit: Specifies the 128-bit Suite B security level.

192-bit: Specifies the 192-bit Suite B security level.

pki-domain *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes (').

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes ('). If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies compression algorithm zlib.

dscp *dscp-value*: Specifies the DSCP value in the IPv6 SSH packets. The value range for the *dscp-value* argument is 0 to 63, and the default value is 48. The DSCP value determines the transmission priority of the packet.

escape *character*: Specifies a case-sensitive escape character. By default, the escape character is a tilde (~).

source: Specifies a source IP address or source interface for IPv6 SSH packets. By default, the device automatically selects a source address for IPv6 SSH packets in compliance with RFC 3484. As a best practice to ensure successful Stelnet connections, specify a loopback interface as the source interface or specify the IPv6 address of a loopback or dialer interface as the source address.

- **interface** *interface-type interface-number*: Specifies a source interface by its type and number. The IPv6 address of this interface is the source IP address of the IPv6 SSH packets.
- **ipv6** *ipv6-address*: Specifies a source IPv6 address.

Usage guidelines

Table 8 Suite B algorithms

Security level	Key exchange algorithm	Encryption algorithm and HMAC algorithm	Public key algorithm
128-bit	ecdh-sha2-nistp256	AES128-GCM	x509v3-ecdsa-sha2-nistp256
192-bit	ecdh-sha2-nistp384	AES256-GCM	x509v3-ecdsa-sha2-nistp384
Both	ecdh-sha2-nistp256 ecdh-sha2-nistp384	AES128-GCM AES256-GCM	x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384

The combination of an escape character and a dot (.) works as an escape sequence. This escape sequence is typically used to quickly terminate an SSH connection when the server reboots or malfunctions.

For the escape sequence to take effect, you must enter it at the very beginning of a line. If you have entered other characters or performed operations in a line, enter the escape sequence in the next line. As a best practice, use the default escape character (~). Do not use any character in SSH usernames as the escape character.

Examples

Use the 192-bit Suite B algorithms to establish a connection to Stelnet server **2000::1**. Specify the client's PKI domain and the server's PKI domain as **clientpkidomain** and **serverpkidomain**, respectively.

```
<Sysname> ssh2 ipv6 2000::1 suite-b 192-bit pki-domain clientpkidomain server-pki-domain
serverpkidomain
Username
```

ssh2 suite-b

Use **ssh2 suite-b** to establish a connection to an IPv4 Stelnet server based on Suite B algorithms.

Syntax

ssh2 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] **suite-b** [**128-bit** | **192-bit**] **pki-domain** *domain-name* [**server-pki-domain** *domain-name*] [**prefer-compress** **zlib**] [**dscp** *dscp-value* | **escape** *character* | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] *

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

server: Specifies a server by its IPv4 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range 1 to 65535. The default is 22.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

suite-b: Specifies the Suite B algorithms. If neither the 128-bit keyword nor the 192-bit keyword is specified, all algorithms in Suite B are used. For more information about the Suite B algorithms, see Table 9.

128-bit: Specifies the 128-bit Suite B security level.

192-bit: Specifies the 192-bit Suite B security level.

pki-domain *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes (').

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes ('). If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies compression algorithm zlib.

dscp *dscp-value*: Specifies the DSCP value in the IPv4 SSH packets. The value range for the *dscp-value* argument is 0 to 63, and the default value is 48. The DSCP value determines the transmission priority of the packet.

escape *character*: Specifies a case-sensitive escape character. By default, the escape character is a tilde (~).

source: Specifies a source IP address or source interface for SSH packets. By default, the device uses the primary IPv4 address of the output interface in the routing entry as the source address of SSH packets. As a best practice to ensure successful Stelnet connections, specify a loopback interface as the source interface or specify the IPv4 address of a loopback or dialer interface as the source address.

- **interface** *interface-type interface-number*: Specifies a source interface by its type and number. The primary IPv4 address of this interface is the source IPv4 address of the SSH packets.
- **ip** *ip-address*: Specifies a source IPv4 address.

Usage guidelines

Table 9 Suite B algorithms

Security level	Key exchange algorithm	Encryption algorithm and HMAC algorithm	Public key algorithm
128-bit	ecdh-sha2-nistp256	AES128-GCM	x509v3-ecdsa-sha2-nistp256
192-bit	ecdh-sha2-nistp384	AES256-GCM	x509v3-ecdsa-sha2-nistp384
Both	ecdh-sha2-nistp256 ecdh-sha2-nistp384	AES128-GCM AES256-GCM	x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384

The combination of an escape character and a dot (.) works as an escape sequence. This escape sequence is typically used to quickly terminate an SSH connection when the server reboots or malfunctions.

For the escape sequence to take effect, you must enter it at the very beginning of a line. If you have entered other characters or performed operations in a line, enter the escape sequence in the next line. As a best practice, use the default escape character (~). Do not use any character in SSH usernames as the escape character.

Examples

Use the 128-bit Suite B algorithms to establish a connection to Stelnet server **3.3.3.3**. Specify the client's PKI domain and the server's PKI domain as **clientpkidomain** and **serverpkidomain**, respectively.

```
<Sysname> ssh2 3.3.3.3 suite-b 128-bit pki-domain clientpkidomain server-pki-domain
serverpkidomain
Username
```

SSH2 commands

display ssh2 algorithm

Use **display ssh2 algorithm** to display algorithms used by SSH2 in the algorithm negotiation stage.

Syntax

display ssh2 algorithm

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display algorithms used by SSH2 in the algorithm negotiation stage.

```
<Sysname> display ssh2 algorithm
 Key exchange algorithms: ecdh-sha2-nistp256 ecdh-sha2-nistp384 dh-group-exchange-sha1
dh-group14-sha1 dh-group1-sha1
 Public key algorithms: x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384
ecdsa-sha2-nistp256 ecdsa-sha2-nistp384 rsa dsa
 Encryption algorithms: aes128-ctr aes192-ctr aes256-ctr aes128-gcm aes256-gcm aes128-cbc
3des-cbc aes256-cbc des-cbc
 MAC algorithms: sha2-256 sha2-512 sha1 md5 sha1-96 md5-96
```

Table 10 Command output

Field	Description
Key exchange algorithms	Key exchange algorithms in descending order of priority for algorithm negotiation.
Public key algorithms	Public key algorithms in descending order of priority for algorithm negotiation.
Encryption algorithms	Encryption algorithms in descending order of priority for algorithm negotiation.
MAC algorithms	HMAC algorithms in descending order of priority for algorithm negotiation.

Related commands

ssh2 algorithm cipher

ssh2 algorithm key-exchange

ssh2 algorithm mac

ssh2 algorithm public-key

ssh2 algorithm cipher

Use **ssh2 algorithm cipher** to specify encryption algorithms for SSH2.

Use **undo ssh2 algorithm cipher** to restore the default.

Syntax

ssh2 algorithm cipher { **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } *

undo ssh2 algorithm cipher

Default

SSH2 uses encryption algorithms AES128-CTR, AES192-CTR, AES256-CTR, AES128-GCM, AES256-GCM, AES128-CBC, 3DES-CBC, AES256-CBC, and DES-CBC in descending order of priority for algorithm negotiation.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

3des-cbc: Specifies encryption algorithm 3DES-CBC.

aes128-cbc: Specifies encryption algorithm AES128-CBC.

aes128-ctr: Specifies encryption algorithm AES128-CTR.

aes128-gcm: Specifies encryption algorithm AES128-GCM.

aes192-ctr: Specifies encryption algorithm AES192-CTR.

aes256-cbc: Specifies encryption algorithm AES256-CBC.

aes256-ctr: Specifies encryption algorithm AES256-CTR.

aes256-gcm: Specifies encryption algorithm AES256-GCM.

des-cbc: Specifies encryption algorithm DES-CBC.

Usage guidelines

If you specify the encryption algorithms, SSH2 uses only the specified algorithms for algorithm negotiation. The algorithm specified earlier has a higher priority during negotiation.

Examples

Specify algorithm **aes256-cbc** as the encryption algorithm for SSH2.

```
<Sysname> system-view
[Sysname] ssh2 algorithm cipher aes256-cbc
```

Related commands

display ssh2 algorithm

ssh2 algorithm key-exchange

ssh2 algorithm mac

ssh2 algorithm public-key

ssh2 algorithm key-exchange

Use **ssh2 algorithm key-exchange** to specify key exchange algorithms for SSH2.

Use **undo ssh2 algorithm key-exchange** to restore the default.

Syntax

ssh2 algorithm key-exchange { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } *

undo ssh2 algorithm key-exchange

Default

SSH2 uses key exchange algorithms ecdh-sha2-nistp256, ecdh-sha2-nistp384, diffie-hellman-group-exchange-sha1, diffie-hellman-group14-sha1, and diffie-hellman-group1-sha1 in descending order of priority for algorithm negotiation.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

dh-group-exchange-sha1: Specifies key exchange algorithm diffie-hellman-group-exchange-sha1.

dh-group1-sha1: Specifies key exchange algorithm diffie-hellman-group1-sha1.

dh-group14-sha1: Specifies key exchange algorithm diffie-hellman-group14-sha1.

ecdh-sha2-nistp256: Specifies key exchange algorithm ecdh-sha2-nistp256.

ecdh-sha2-nistp384: Specifies key exchange algorithm ecdh-sha2-nistp384.

Usage guidelines

If you specify the key exchange algorithms, SSH2 uses only the specified algorithms for algorithm negotiation. The algorithm specified earlier has a higher priority during negotiation.

Examples

Specify algorithm **dh-group1-sha1** as the key exchange algorithm for SSH2.

```
<Sysname> system-view
[Sysname] ssh2 algorithm key-exchange dh-group1-sha1
```

Related commands

display ssh2 algorithm

ssh2 algorithm cipher

ssh2 algorithm mac

ssh2 algorithm public-key

ssh2 algorithm mac

Use **ssh2 algorithm mac** to specify HMAC algorithms for SSH2.

Use **undo ssh2 algorithm mac** to restore the default.

Syntax

ssh2 algorithm mac { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } *

undo ssh2 algorithm mac

Default

SSH2 uses HMAC algorithms SHA2-256, SHA2-512, SHA1, MD5, SHA1-96, and MD5-96 in descending order of priority for algorithm negotiation.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

md5: Specifies HMAC algorithm HMAC-MD5.

md5-96: Specifies HMAC algorithm HMAC-MD5-96.

sha1: Specifies HMAC algorithm HMAC-SHA1.

sha1-96: Specifies HMAC algorithm HMAC-SHA1-96.

sha2-256: Specifies HMAC algorithm HMAC-SHA2-256.

sha2-512: Specifies HMAC algorithm HMAC-SHA2-512.

Usage guidelines

If you specify the HMAC algorithms, SSH2 uses only the specified algorithms for algorithm negotiation. The algorithm specified earlier has a higher priority during negotiation.

Examples

Specify algorithm **md5** as the HMAC algorithm for SSH2.

```
<Sysname> system-view
[Sysname] ssh2 algorithm mac md5
```

Related commands

display ssh2 algorithm

ssh2 algorithm cipher

ssh2 algorithm key-exchange

ssh2 algorithm public-key

ssh2 algorithm public-key

Use **ssh2 algorithm public-key** to specify public key algorithms for SSH2.

Use **undo ssh2 algorithm public-key** to restore the default.

Syntax

ssh2 algorithm public-key { **dsa** | **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** | **x509v3-ecdsa-sha2-nistp256** | **x509v3-ecdsa-sha2-nistp384** } *

undo ssh2 algorithm public-key

Default

SSH2 uses public key algorithms x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, RSA, and DSA in descending order of priority for algorithm negotiation.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

dsa: Specifies public key algorithm DSA.

ecdsa-sha2-nistp256: Specifies the ECDSA algorithm with 256-bit key strength.

ecdsa-sha2-nistp384: Specifies the ECDSA algorithm with 384-bit key strength.

rsa: Specifies public key algorithm RSA.

x509v3-ecdsa-sha2-nistp256: Specifies public key algorithm x509v3-ecdsa-sha2-nistp256.

x509v3-ecdsa-sha2-nistp384: Specifies public key algorithm x509v3-ecdsa-sha2-nistp384.

Usage guidelines

If you specify the public key algorithms, SSH2 uses only the specified algorithms for algorithm negotiation. The algorithm specified earlier has a higher priority during negotiation.

Examples

Specify algorithm **dsa** as the public key algorithm for SSH2.

```
<Sysname> system-view
[Sysname] ssh2 algorithm public-key dsa
```

Related commands

display ssh2 algorithm

ssh2 algorithm cipher

ssh2 algorithm key-exchange

ssh2 algorithm mac

Contents

SSL commands

certificate-chain-sending enable

Use **certificate-chain-sending enable** to enable the SSL server to send the complete certificate chain to the client during SSL negotiation.

Use **undo certificate-chain-sending enable** to restore the default.

Syntax

certificate-chain-sending enable

undo certificate-chain-sending enable

Default

During SSL negotiation, the SSL server sends the server certificate rather than the complete certificate chain to the client.

Views

SSL server policy view

Predefined user roles

network-admin

context-admin

Usage guidelines

This feature causes additional overheads in the SSL negotiation process. Enable it only when the SSL client does not have the complete certificate chain to verify the server certificate.

Examples

Enable the SSL server to send the complete certificate chain to the client during SSL negotiation.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] certificate-chain-sending enable
```

ciphersuite

Use **ciphersuite** to specify the cipher suites supported by an SSL server policy.

Use **undo ciphersuite** to restore the default.

Syntax

ciphersuite { dhe_rsa_aes_128_cbc_sha | dhe_rsa_aes_128_cbc_sha256 | dhe_rsa_aes_256_cbc_sha | dhe_rsa_aes_256_cbc_sha256 | ecc_sm2_sm1_sm3 | ecc_sm2_sm4_sm3 | ecdhe_ecdsa_aes_128_cbc_sha256 | ecdhe_ecdsa_aes_128_gcm_sha256 | ecdhe_ecdsa_aes_256_cbc_sha384 | ecdhe_ecdsa_aes_256_gcm_sha384 | ecdhe_rsa_aes_128_cbc_sha256 | ecdhe_rsa_aes_128_gcm_sha256 | ecdhe_rsa_aes_256_cbc_sha384 | ecdhe_rsa_aes_256_gcm_sha384 | ecdhe_sm2_sm1_sm3 | ecdhe_sm2_sm4_sm3 | exp_rsa_des_cbc_sha | rsa_3des_ede_cbc_sha | rsa_aes_128_cbc_sha | rsa_aes_128_cbc_sha256 | rsa_aes_128_gcm_sha256 | rsa_aes_256_cbc_sha | rsa_aes_256_cbc_sha256 | rsa_aes_256_gcm_sha384 | rsa_des_cbc_sha | rsa_sm1_sha | rsa_sm1_sm3 | rsa_sm4_sha | rsa_sm4_sm3

| **tls_aes_128_ccm_8_sha256** | **tls_aes_128_ccm_sha256** | **tls_aes_128_gcm_sha256** | **tls_aes_256_gcm_sha384** | **tls_chacha20_poly1305_sha256** }*<1-11>

undo ciphersuite

Default

An SSL server policy supports cipher suites ECC_SM2_SM1_SM3, ECC_SM2_SM4_SM3, ECDHE_SM2_SM1_SM3, ECDHE_SM2_SM4_SM3, RSA_SM1_SHA, RSA_SM1_SM3, RSA_SM4_SHA, RSA_SM4_SM3, RSA_AES_128_CBC_SHA, RSA_AES_256_CBC_SHA, DHE_RSA_AES_128_CBC_SHA, DHE_RSA_AES_256_CBC_SHA, RSA_AES_128_CBC_SHA256, RSA_AES_256_CBC_SHA256, DHE_RSA_AES_128_CBC_SHA256, DHE_RSA_AES_256_CBC_SHA256, ECDHE_RSA_AES_128_CBC_SHA256, ECDHE_RSA_AES_256_CBC_SHA384, ECDHE_RSA_AES_128_GCM_SHA256, ECDHE_RSA_AES_256_GCM_SHA384, ECDHE_ECDSA_AES_128_CBC_SHA256, ECDHE_ECDSA_AES_256_CBC_SHA384, ECDHE_ECDSA_AES_128_GCM_SHA256, ECDHE_ECDSA_AES_256_GCM_SHA384, RSA_AES_128_GCM_SHA256, RSA_AES_256_GCM_SHA384, TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384, TLS_CHACHA20_POLY1305_SHA256, TLS_AES_128_CCM_SHA256, and TLS_AES_128_CCM_8_SHA256.

Views

SSL server policy view

Predefined user roles

network-admin

context-admin

Parameters

dhe_rsa_aes_128_cbc_sha: Specifies the cipher suite that uses key exchange algorithm DHE RSA, data encryption algorithm 128-bit AES_CBC, and MAC algorithm SHA.

dhe_rsa_aes_128_cbc_sha256: Specifies the cipher suite that uses key exchange algorithm DHE RSA, data encryption algorithm 128-bit AES_CBC, and MAC algorithm SHA256.

dhe_rsa_aes_256_cbc_sha: Specifies the cipher suite that uses key exchange algorithm DHE RSA, data encryption algorithm 256-bit AES_CBC, and MAC algorithm SHA.

dhe_rsa_aes_256_cbc_sha256: Specifies the cipher suite that uses key exchange algorithm DHE RSA, data encryption algorithm 256-bit AES_CBC, and MAC algorithm SHA256.

ecc_sm2_sm1_sm3: Specifies the cipher suite that uses key exchange algorithm ECC SM2, data encryption algorithm 128-bit SM1, and MAC algorithm SM3.

ecc_sm2_sm4_sm3: Specifies the cipher suite that uses key exchange algorithm ECC SM2, data encryption algorithm SM4, and MAC algorithm SM3.

ecdhe_ecdsa_aes_128_cbc_sha256: Specifies the cipher suite that uses key exchange algorithm ECDHE ECDSA, data encryption algorithm 128-bit AES_CBC, and MAC algorithm SHA256.

ecdhe_ecdsa_aes_128_gcm_sha256: Specifies the cipher suite that uses key exchange algorithm ECDHE ECDSA, data encryption algorithm 128-bit AES_GCM, and MAC algorithm SHA256.

ecdhe_ecdsa_aes_256_cbc_sha384: Specifies the cipher suite that uses key exchange algorithm ECDHE ECDSA, data encryption algorithm 256-bit AES_CBC, and MAC algorithm SHA384.

ecdhe_ecdsa_aes_256_gcm_sha384: Specifies the cipher suite that uses key exchange algorithm ECDHE ECDSA, data encryption algorithm 256-bit AES_GCM, and MAC algorithm SHA384.

ecdhe_rsa_aes_128_cbc_sha256: Specifies the cipher suite that uses key exchange algorithm ECDHE RSA, data encryption algorithm 128-bit AES_CBC, and MAC algorithm SHA256.

ecdhe_rsa_aes_128_gcm_sha256: Specifies the cipher suite that uses key exchange algorithm ECDHE RSA, data encryption algorithm 128-bit AES_GCM, and MAC algorithm SHA256.

ecdhe_rsa_aes_256_cbc_sha384: Specifies the cipher suite that uses key exchange algorithm ECDHE RSA, data encryption algorithm 256-bit AES_CBC, and MAC algorithm SHA384.

ecdhe_rsa_aes_256_gcm_sha384: Specifies the cipher suite that uses key exchange algorithm ECDHE RSA, data encryption algorithm 256-bit AES_GCM, and MAC algorithm SHA384.

ecdhe_sm2_sm1_sm3: Specifies the cipher suite that uses key exchange algorithm ECDHE SM2, data encryption algorithm 128-bit SM1, and MAC algorithm SM3.

ecdhe_sm2_sm4_sm3: Specifies the cipher suite that uses key exchange algorithm ECDHE SM2, data encryption algorithm SM4, and MAC algorithm SM3.

exp_rsa_des_cbc_sha: Specifies the export cipher suite that uses key exchange algorithm RSA, data encryption algorithm DES_CBC, and MAC algorithm SHA.

rsa_3des_ede_cbc_sha: Specifies the cipher suite that uses key exchange algorithm RSA, data encryption algorithm 3DES_EDE_CBC, and MAC algorithm SHA.

rsa_aes_128_cbc_sha: Specifies the cipher suite that uses key exchange algorithm RSA, data encryption algorithm 128-bit AES_CBC, and MAC algorithm SHA.

rsa_aes_128_cbc_ sha256: Specifies the cipher suite that uses key exchange algorithm RSA, data encryption algorithm 128-bit AES_CBC, and MAC algorithm SHA256.

rsa_aes_128_gcm_sha256: Specifies the cipher suite that uses key exchange algorithm RSA, data encryption algorithm 128-bit AES_GCM, and MAC algorithm SHA256.

rsa_aes_256_cbc_sha: Specifies the cipher suite that uses key exchange algorithm RSA, data encryption algorithm 256-bit AES_CBC, and MAC algorithm SHA.

rsa_aes_256_cbc_ sha256: Specifies the cipher suite that uses key exchange algorithm RSA, data encryption algorithm 256-bit AES_CBC, and MAC algorithm SHA256.

rsa_aes_256_gcm_sha384: Specifies the cipher suite that uses key exchange algorithm RSA, data encryption algorithm 256-bit AES_GCM, and MAC algorithm SHA384.

rsa_des_cbc_sha: Specifies the cipher suite that uses key exchange algorithm RSA, data encryption algorithm DES_CBC, and MAC algorithm SHA.

rsa_sm1_sha: Specifies the cipher suite that uses key exchange algorithm RSA, data encryption algorithm 128-bit SM1, and MAC algorithm SHA.

rsa_sm1_sm3: Specifies the cipher suite that uses key exchange algorithm RSA, data encryption algorithm 128-bit SM1, and MAC algorithm SM3.

rsa_sm4_sha: Specifies the cipher suite that uses key exchange algorithm RSA, data encryption algorithm SM4, and MAC algorithm SHA.

rsa_sm4_sm3: Specifies the cipher suite that uses key exchange algorithm RSA, data encryption algorithm SM4, and MAC algorithm SM3.

tls_aes_128_ccm_sha256: Specifies the cipher suite that uses data encryption algorithm AES 128 CCM and MAC algorithm SHA256. This cipher suite is exclusive to TLS 1.3 and is supported only by SSL VPN.

tls_aes_128_ccm_8_sha256: Specifies the cipher suite that uses data encryption algorithm AES 128 CCM 8 and MAC algorithm SHA256. This cipher suite is exclusive to TLS 1.3 and is supported only by SSL VPN.

tls_aes_128_gcm_sha256: Specifies the cipher suite that uses data encryption algorithm 128-bit AES_GCM and MAC algorithm SHA256. This cipher suite is exclusive to TLS 1.3 and is supported only by SSL VPN.

tls_aes_256_gcm_sha384: Specifies the cipher suite that uses data encryption algorithm 256-bit AES_GCM and MAC algorithm SHA384. This cipher suite is exclusive to TLS 1.3 and is supported only by SSL VPN.

tls_chacha20_poly1305_sha256: Specifies the cipher suite that uses data encryption algorithm CHACHA20 POLY1305 and MAC algorithm SHA256. This cipher suite is exclusive to TLS 1.3 and is supported only by SSL VPN.

<1-11>: Specifies a maximum of 11 cipher suites.

Usage guidelines

SSL employs the following algorithms:

- **Data encryption algorithms**—Encrypt data to ensure privacy. Commonly used data encryption algorithms are symmetric key algorithms. When a symmetric key algorithm is used, the SSL server and the SSL client must use the same key.
- **Message Authentication Code (MAC) algorithms**—Calculate the MAC value for data to ensure integrity. Commonly used MAC algorithms include MD5 and SHA. When a MAC algorithm is used, the SSL server and the SSL client must use the same key.
- **Key exchange algorithms**—Implement secure exchange of the keys used by the symmetric key algorithm and the MAC algorithm. Commonly used key exchange algorithms are usually asymmetric key algorithms, such as RSA.

After the SSL server receives cipher suites from a client, the server compares the received cipher suites with the cipher suites it supports. If a match is found, the cipher suite negotiation succeeds. If no match is found, the negotiation fails. The cipher suite matching can use the server-preferred order or the client-preferred order, depending on the configuration of the **ciphersuite server-preferred enable** command.

The earlier a cipher suite is configured, the higher priority it has during the cipher suite negotiation.

When executing the **ciphersuite** command, you can specify a maximum of 11 cipher suites at a time. If you execute this command multiple times, the SSL server policy supports all the specified cipher suites.

Examples

Configure SSL server policy **policy1** to support the following cipher suites:

- Key exchange algorithm DHE RSA, data encryption algorithm 128-bit AES, and MAC algorithm SHA.
- Key exchange algorithm RSA, data encryption algorithm 128-bit AES, and MAC algorithm SHA.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] ciphersuite dhe_rsa_aes_128_cbc_sha
rsa_aes_128_cbc_sha
```

Related commands

display ssl server-policy

prefer-cipher

ciphersuite server-preferred enable

ciphersuite server-preferred enable

Use **ciphersuite server-preferred enable** to enable the server-preferred order for the cipher suite negotiation between the SSL server and SSL client.

Use **undo ciphersuite server-preferred enable** to restore the default.

Syntax

ciphersuite server-preferred enable

undo ciphersuite server-preferred enable

Default

The SSL server uses the client-preferred order to choose a cipher suite during the cipher suite negotiation.

Views

SSL server policy view

Predefined user roles

network-admin

context-admin

Usage guidelines

During the SSL connection negotiation process, the SSL server and client present a list of cipher suites that they each support, in order of preference. By default, the SSL server uses the order of cipher suites presented by the client to negotiate the cipher suite. That is, the SSL server chooses the first cipher suite in the client's list that matches any one of the server's cipher suites. If no match is found, the negotiation fails.

After this command is executed, the server-preferred order is used for cipher suite negotiation. That is, the SSL server chooses the first cipher suite in its list that matches any one of the client's cipher suites. If no match is found, the negotiation fails.

The earlier a cipher suite is configured, the higher priority it has during the cipher suite negotiation.

Examples

Enable the server-preferred order for cipher suite negotiation.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] ciphersuite server-preferred enable
```

Related commands

ciphersuite

display ssl server-policy

prefer-cipher

client-verify

Use **client-verify** to enable mandatory or optional SSL client authentication.

Use **undo client-verify** to restore the default.

Syntax

client-verify { **enable** | **optional** }

undo client-verify

Default

SSL client authentication is disabled. The SSL server does not authenticate SSL clients based on digital certificates.

Views

SSL server policy view

Predefined user roles

network-admin

context-admin

Parameters

`enable`: Enables mandatory SSL client authentication.

`optional`: Enables optional SSL client authentication.

Usage guidelines

SSL uses digital certificates to authenticate communicating parties. For more information about digital certificates, see *Security Configuration Guide*.

Mandatory SSL client authentication—The SSL server requires an SSL client to submit its digital certificate for identity authentication. The SSL client can access the SSL server only after it passes identity authentication.

Optional SSL client authentication—The SSL server does not require an SSL client to submit its digital certificate for identity authentication.

- If an SSL client submits its certificate to the SSL server, the server authenticates the client identity. The client must pass authentication to access the server.
- If an SSL client does not submit its certificate to the SSL server, the server does not authenticate the client identity. The client can access the SSL server without authentication.

If SSL client authentication is disabled, the SSL server does not authenticate SSL clients regardless of whether the clients submit digital certificates or not. SSL clients can access the SSL server without authentication.

When authenticating a client by using the digital certificate, the SSL server performs the following operations:

- Verifies the certificate chain presented by the client.
- Checks that the certificates in the certificate chain (except the root CA certificate) are not revoked.

Examples

Enable mandatory SSL client authentication.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] client-verify enable
```

Enable optional SSL client authentication.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] client-verify optional
```

Disable SSL client authentication.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] undo client-verify
```

Related commands

display ssl server-policy

display ssl client-policy

Use **display ssl client-policy** to display SSL client policy information.

Syntax

display ssl client-policy [*policy-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

policy-name: Specifies an SSL client policy by its name, a case-insensitive string of 1 to 31 characters. If you do not specify a policy name, this command displays information about all SSL client policies.

Examples

Display information about the SSL client policy **policy1**.

```
<Sysname> display ssl client-policy policy1
 SSL client policy: policy1
     SSL version: SSL 3.0
     PKI domain: client-domain
     Preferred ciphersuite:
         RSA_AES_128_CBC_SHA
     Server-verify: enabled
```

Display information about the SSL client policy **policy2**.

```
<Sysname> display ssl client-policy policy2
 SSL client policy: policy2
     SSL version: TLS 1.3
     PKI domain:
     Preferred ciphersuite:
         TLS_AES_128_GCM_SHA256
         TLS_CHACHA20_POLY1305_SHA256
         TLS_AES_256_GCM_SHA384
         TLS_AES_128_CCM_8_SHA256
         TLS_AES_128_CCM_SHA256
     Server-verify: enable
```

Table 1 Command output

Field	Description
Server-verify	Indicates whether the client is enabled to use digital certificates to authenticate servers.
SSL version	SSL protocol version in the SSL client policy. Possible versions include: • SSL 3.0. • TLS 1.0. • TLS 1.1. • TLS 1.2. • TLS 1.3. TLS 1.3 is supported only by SSL VPN. • GM-TLS 1.1.

display ssl server-policy

Use **display ssl server-policy** to display SSL server policy information.

Syntax

display ssl server-policy [*policy-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

policy-name: Specifies an SSL server policy by its name, a case-insensitive string of 1 to 31 characters. If you do not specify a policy name, this command displays information about all SSL server policies.

Examples

Display information about the SSL server policy **policy1**.

```
<Sysname> display ssl server-policy policy1
 SSL server policy: policy1
     Version info:
         SSL3.0: Disabled
         TLS1.0: Enabled
         TLS1.1: Disabled
         TLS1.2: Enabled
         TLS1.3: Enabled
         GM-TLS1.1: Disabled
     PKI domains: server-domain
     Ciphersuites:
         DHE_RSA_AES_128_CBC_SHA
         RSA_AES_128_CBC_SHA
         TLS_AES_128_GCM_SHA256
```

```
        TLS_CHACHA20_POLY1305_SHA256
        TLS_AES_256_GCM_SHA384
        TLS_AES_128_CCM_8_SHA256
        TLS_AES_128_CCM_SHA256
    Session cache size: 600
    Caching timeout: 3600 seconds
    Client-verify: Enabled
    Ciphersuite server-perferred: Disabled
```

Table 2 Command output

Field	Description
Version info	Enabling status of the SSL protocol versions in the SSL server policy. The SSL server can use only the enabled SSL protocol versions for session negotiation. Possible SSL protocol versions include: • SSL 3.0. • TLS 1.0. • TLS 1.1. • TLS 1.2. • TLS 1.3. TLS 1.3 is supported only by SSL VPN. • GM-TLS 1.1.
Caching timeout	Session cache timeout time in seconds.
Client-verify	SSL client authentication mode, including: • **Disabled**—SSL client authentication is disabled. • **Enabled**—SSL client authentication is mandatory. • **Optional**—SSL client authentication is optional.
Ciphersuite server-preferred	Enabling status of using the server-preferred order during the cipher suite negotiation between the SSL server and SSL client: • **Enabled**—The server-preferred order is used. • **Disabled**—The client-preferred order is used.

pki-domain (SSL client policy view)

Use **pki-domain** to specify a PKI domain for an SSL client policy.

Use **undo pki-domain** to restore the default.

Syntax

pki-domain *domain-name*

undo pki-domain

Default

No PKI domain is specified for an SSL client policy.

Views

SSL client policy view

Predefined user roles

network-admin

context-admin

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

If you specify a PKI domain for an SSL client policy, the SSL client that uses the SSL client policy will obtain its digital certificate through the specified PKI domain.

Examples

Specify PKI domain **client-domain** for SSL client policy **policy1**.

```
<Sysname> system-view
[Sysname] ssl client-policy policy1
[Sysname-ssl-client-policy-policy1] pki-domain client-domain
```

Related commands

display ssl client-policy

pki domain

pki-domain (SSL server policy view)

Use **pki-domain** to specify a PKI domain for an SSL server policy.

Use **undo pki-domain** to restore the default.

Syntax

pki-domain *domain-name*

undo pki-domain

Default

No PKI domain is specified for an SSL server policy.

Views

SSL server policy view

Predefined user roles

network-admin

context-admin

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. You must specify a minimum of one domain name. A maximum of two domain names are supported.

Usage guidelines

If you specify a PKI domain for an SSL server policy, the SSL server that uses the SSL server policy will obtain its digital certificate through the specified PKI domain.

Some services (such as SSL VPN, load balancing, and proxy policy) might require using two digital certificates on the server. To meet the requirement, you can use this command to specify two PKI domains in the SSL server policy at a time. If the two digital certificates obtained through the specified PKI domains are of the same type, only the digital certificate obtained through the first PKI domain takes effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify PKI domain **server-domain** for SSL server policy **policy1**.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] pki-domain server-domain
```

Related commands

display ssl server-policy

pki domain

prefer-cipher

Use **prefer-cipher** to specify a preferred cipher suite for an SSL client policy.

Use **undo prefer-cipher** to restore the default.

Syntax

prefer-cipher { **dhe_rsa_aes_128_cbc_sha** | **dhe_rsa_aes_128_cbc_sha256** | **dhe_rsa_aes_256_cbc_sha** | **dhe_rsa_aes_256_cbc_sha256** | **ecc_sm2_sm1_sm3** | **ecc_sm2_sm4_sm3** | **ecdhe_ecdsa_aes_128_cbc_sha256** | **ecdhe_ecdsa_aes_128_gcm_sha256** | **ecdhe_ecdsa_aes_256_cbc_sha384** | **ecdhe_ecdsa_aes_256_gcm_sha384** | **ecdhe_rsa_aes_128_cbc_sha256** | **ecdhe_rsa_aes_128_gcm_sha256** | **ecdhe_rsa_aes_256_cbc_sha384** | **ecdhe_rsa_aes_256_gcm_sha384** | **ecdhe_sm2_sm1_sm3** | **ecdhe_sm2_sm4_sm3** | **exp_rsa_des_cbc_sha** | **rsa_3des_ede_cbc_sha** | **rsa_aes_128_cbc_sha** | **rsa_aes_128_cbc_sha256** | **rsa_aes_128_gcm_sha256** | **rsa_aes_256_cbc_sha** | **rsa_aes_256_cbc_sha256** | **rsa_aes_256_gcm_sha384** | **rsa_des_cbc_sha** | **rsa_sm1_sha** | **rsa_sm1_sm3** | **rsa_sm4_sha** | **rsa_sm4_sm3**

tls_aes_128_ccm_8_sha256 | **tls_aes_128_ccm_sha256** | **tls_aes_128_gcm_sha256** | **tls_aes_256_gcm_sha384** | **tls_chacha20_poly1305_sha256** } *<1-11>

undo prefer-cipher

Default

The preferred cipher suites of an SSL client policy are **dhe_rsa_aes_256_cbc_sha, rsa_aes_256_cbc_sha**, **dhe_rsa_aes_128_cbc_sha**, , and **rsa_aes_128_cbc_sha**.

Views

SSL client policy view

Predefined user roles

network-admin

context-admin

Parameters

dhe_rsa_aes_128_cbc_sha: Specifies the cipher suite that uses key exchange algorithm DHE RSA, data encryption algorithm 128-bit AES_CBC, and MAC algorithm SHA.

dhe_rsa_aes_128_cbc_sha256: Specifies the cipher suite that uses key exchange algorithm DHE RSA, data encryption algorithm 128-bit AES_CBC, and MAC algorithm SHA256.

dhe_rsa_aes_256_cbc_sha: Specifies the cipher suite that uses key exchange algorithm DHE RSA, data encryption algorithm 256-bit AES_CBC, and MAC algorithm SHA.

dhe_rsa_aes_256_cbc_sha256: Specifies the cipher suite that uses key exchange algorithm DHE RSA, data encryption algorithm 256-bit AES_CBC, and MAC algorithm SHA256.

ecc_sm2_sm1_sm3: Specifies the cipher suite that uses key exchange algorithm ECC SM2, data encryption algorithm 128-bit SM1, and MAC algorithm SHA256.

ecc_sm2_sm4_sm3: Specifies the cipher suite that uses key exchange algorithm ECC SM2, data encryption algorithm SM4, and MAC algorithm SM3.

ecdhe_ecdsa_aes_128_cbc_sha256: Specifies the cipher suite that uses key exchange algorithm ECDHE ECDSA, data encryption algorithm 128-bit AES_CBC, and MAC algorithm SHA256.

ecdhe_ecdsa_aes_128_gcm_sha256: Specifies the cipher suite that uses key exchange algorithm ECDHE ECDSA, data encryption algorithm 128-bit AES_GCM, and MAC algorithm SHA256.

ecdhe_ecdsa_aes_256_cbc_sha384: Specifies the cipher suite that uses key exchange algorithm ECDHE ECDSA, data encryption algorithm 256-bit AES_CBC, and MAC algorithm SHA384.

ecdhe_ecdsa_aes_256_gcm_sha384: Specifies the cipher suite that uses key exchange algorithm ECDHE ECDSA, data encryption algorithm 256-bit AES_GCM, and MAC algorithm SHA384.

ecdhe_rsa_aes_128_cbc_sha256: Specifies the cipher suite that uses key exchange algorithm ECDHE RSA, data encryption algorithm 128-bit AES_CBC, and MAC algorithm SHA256.

ecdhe_rsa_aes_128_gcm_sha256: Specifies the cipher suite that uses key exchange algorithm ECDHE RSA, data encryption algorithm 128-bit AES_GCM, and MAC algorithm SHA256.

ecdhe_rsa_aes_256_cbc_sha384: Specifies the cipher suite that uses key exchange algorithm ECDHE RSA, data encryption algorithm 256-bit AES_CBC, and MAC algorithm SHA384.

ecdhe_rsa_aes_256_gcm_sha384: Specifies the cipher suite that uses key exchange algorithm ECDHE RSA, data encryption algorithm 256-bit AES_GCM, and MAC algorithm SHA384.

ecdhe_sm2_sm1_sm3: Specifies the cipher suite that uses key exchange algorithm ECDHE SM2, data encryption algorithm 128-bit SM1, and MAC algorithm SM3.

ecdhe_sm2_sm4_sm3: Specifies the cipher suite that uses key exchange algorithm ECDHE SM2, data encryption algorithm SM4, and MAC algorithm SM3.

exp_rsa_des_cbc_sha: Specifies the export cipher suite that uses key exchange algorithm RSA, data encryption algorithm DES_CBC, and MAC algorithm SHA.

rsa_3des_ede_cbc_sha: Specifies the cipher suite that uses key exchange algorithm RSA, data encryption algorithm 3DES_EDE_CBC, and MAC algorithm SHA.

rsa_aes_128_cbc_sha: Specifies the cipher suite that uses key exchange algorithm RSA, data encryption algorithm 128-bit AES_CBC, and MAC algorithm SHA.

rsa_aes_128_cbc_ sha256: Specifies the cipher suite that uses key exchange algorithm RSA, data encryption algorithm 128-bit AES_CBC, and MAC algorithm SHA256.

rsa_aes_128_gcm_sha256: Specifies the cipher suite that uses key exchange algorithm RSA, data encryption algorithm 128-bit AES_CBC, and MAC algorithm SHA256.

rsa_aes_256_cbc_sha: Specifies the cipher suite that uses key exchange algorithm RSA, data encryption algorithm 256-bit AES_CBC, and MAC algorithm SHA.

rsa_aes_256_cbc_ sha256: Specifies the cipher suite that uses key exchange algorithm RSA, data encryption algorithm 256-bit AES_CBC, and MAC algorithm SHA256.

rsa_aes_256_gcm_sha384: Specifies the cipher suite that uses key exchange algorithm RSA, data encryption algorithm 256-bit AES_GCM, and MAC algorithm SHA384.

rsa_des_cbc_sha: Specifies the cipher suite that uses key exchange algorithm RSA, data encryption algorithm DES_CBC, and MAC algorithm SHA.

rsa_sm1_sha: Specifies the cipher suite that uses key exchange algorithm RSA, data encryption algorithm 128-bit SM1, and MAC algorithm SHA.

rsa_sm1_sm3: Specifies the cipher suite that uses key exchange algorithm RSA, data encryption algorithm 128-bit SM1, and MAC algorithm SM3.

rsa_sm4_sha: Specifies the cipher suite that uses key exchange algorithm RSA, data encryption algorithm SM4, and MAC algorithm SHA.

rsa_sm4_sm3: Specifies the cipher suite that uses key exchange algorithm RSA, data encryption algorithm SM4, and MAC algorithm SM3.

tls_aes_128_ccm_sha256: Specifies the cipher suite that uses data encryption algorithm AES 128 CCM and MAC algorithm SHA256. This cipher suite is exclusive to TLS 1.3 and is supported only by SSL VPN.

tls_aes_128_ccm_8_sha256: Specifies the cipher suite that uses data encryption algorithm AES 128 CCM 8 and MAC algorithm SHA256. This cipher suite is exclusive to TLS 1.3 and is supported only by SSL VPN.

tls_aes_128_gcm_sha256: Specifies the cipher suite that uses data encryption algorithm 128-bit AES_GCM and MAC algorithm SHA256. This cipher suite is exclusive to TLS 1.3 and is supported only by SSL VPN.

tls_aes_256_gcm_sha384: Specifies the cipher suite that uses data encryption algorithm 256-bit AES_GCM and MAC algorithm SHA384. This cipher suite is exclusive to TLS 1.3 and is supported only by SSL VPN.

tls_chacha20_poly1305_sha256: Specifies the cipher suite that uses data encryption algorithm CHACHA20 POLY1305 and MAC algorithm SHA256. This cipher suite is exclusive to TLS 1.3 and is supported only by SSL VPN.

<1-11>: Specifies a maximum of 11 cipher suites.

Usage guidelines

SSL employs the following algorithms:

- **Data encryption algorithms**—Encrypt data to ensure privacy. Commonly used data encryption algorithms are usually symmetric key algorithms. When using a symmetric key algorithm, the SSL server and the SSL client must use the same key.
- **Message Authentication Code (MAC) algorithms**—Calculate the MAC value for data to ensure integrity. Commonly used MAC algorithms include MD5 and SHA. When using a MAC algorithm, the SSL server and the SSL client must use the same key.
- **Key exchange algorithms**—Implement secure exchange of the keys used by the symmetric key algorithm and MAC algorithm. Commonly used key exchange algorithms are asymmetric key algorithms, such as RSA.

The SSL client sends the preferred cipher suites to the SSL server. The server compares the received cipher suites with the cipher suites it supports. If a match is found, the cipher suite negotiation succeeds. If no match is found, the negotiation fails. The cipher suite matching can use the server-preferred order or the client-preferred order, depending on the configuration of the **ciphersuite server-preferred enable** command.

The earlier a cipher suite is configured, the higher priority it has during the cipher suite negotiation.

When executing the **prefer-cipher** command, you can specify a maximum of 11 cipher suites at a time. If you execute this command multiple times, the SSL client policy supports all the specified cipher suites.

Examples

Configure SSL client policy **policy1** to support the key exchange algorithm RSA, data encryption algorithm 128-bit AES_CBC, and MAC algorithm SHA.

```
<Sysname> system-view
```

```
[Sysname] ssl client-policy policy1
[Sysname-ssl-client-policy-policy1] prefer-cipher rsa_aes_128_cbc_sha
```

Related commands

ciphersuite

display ssl client-policy

server-preferred ciphersuite

server-verify enable

Use **server-verify enable** to enable the SSL client to use digital certificates to authenticate the SSL server.

Use **undo server-verify enable** to disable SSL server authentication. The SSL client does not authenticate the SSL server.

Syntax

server-verify enable

undo server-verify enable

Default

The SSL client uses digital certificates to authenticate the SSL server.

Views

SSL client policy view

Predefined user roles

network-admin

context-admin

Usage guidelines

SSL uses digital certificates to authenticate communicating parties. For more information about digital certificates, see *Security Configuration Guide*.

If you execute the **server-verify enable** command, the SSL server must send its digital certificate to the SSL client for authentication. The client can access the SSL server only after the server passes the authentication.

Examples

Enable the SSL client to use digital certificates to authenticate the SSL server.

```
<Sysname> system-view
[Sysname] ssl client-policy policy1
[Sysname-ssl-client-policy-policy1] server-verify enable
```

Related commands

display ssl client-policy

session

Use **session** to set the maximum number of sessions that the SSL server can cache and the timeout time for cached sessions.

Use **undo session** to restore the default.

Syntax

session { **cachesize** *size* | **timeout** *time* } *

undo session { **cachesize** | **timeout** } *

Default

The SSL server can cache a maximum of 500 sessions, and the timeout time for cached sessions is 3600 seconds.

Views

SSL server policy view

Predefined user roles

network-admin

context-admin

Parameters

cachesize *size*: Sets the maximum number of cached sessions, in the range of 100 to 20480.

timeout *time*: Sets the session cache timeout in the range of 1 to 4294967295 seconds.

Usage guidelines

The SSL server caches SSL sessions to reuse negotiated session parameters to simplify SSL handshake. Use this command to limit the maximum number and timeout time for cached sessions. When the number of cached sessions reaches the maximum, SSL does not cache new sessions. When the timeout timer for a cached session expires, SSL deletes the session.

Examples

Set the maximum number of cached sessions to 600, and the timeout time for cached sessions to 1800 seconds.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] session cachesize 600 timeout 1800
```

Related commands

display ssl server-policy

ssl client-policy

Use **ssl client-policy** to create an SSL client policy and enter its view, or enter the view of an existing SSL client policy.

Use **undo ssl client-policy** to delete an SSL client policy.

Syntax

ssl client-policy *policy-name*

undo ssl client-policy *policy-name*

Default

No SSL client policies exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies an SSL client policy by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

This command creates an SSL client policy for which you can configure SSL parameters that the client uses to establish a connection to the server. The parameters include a PKI domain and a preferred cipher suite. An SSL client policy takes effect only after it is associated with an application such as DDNS.

Examples

Create an SSL client policy named **policy1** and enter its view.

```
<Sysname> system-view
[Sysname] ssl client-policy policy1
[Sysname-ssl-client-policy-policy1]
```

Related commands

display ssl client-policy

ssl renegotiation disable

Use **ssl renegotiation disable** to disable SSL session renegotiation.

Use **undo ssl renegotiation disable** to restore the default.

Syntax

ssl renegotiation disable

undo ssl renegotiation disable

Default

SSL session renegotiation is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

The SSL session renegotiation feature enables the SSL client and server to reuse a previously negotiated SSL session for an abbreviated handshake.

Disabling session renegotiation causes more computational overhead to the system but it can avoid potential risks. Disable SSL session renegotiation only when explicitly required.

Examples

#Disable SSL session renegotiation.

```
<Sysname> system-view
[Sysname] ssl renegotiation disable
```

ssl server-policy

Use **ssl server-policy** to create an SSL server policy and enter its view, or enter the view of an existing SSL server policy.

Use **undo ssl server-policy** to delete an SSL server policy.

Syntax

ssl server-policy *policy-name*

undo ssl server-policy *policy-name*

Default

No SSL server policies exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies a name for the SSL server policy, a case-insensitive string of 1 to 31 characters.

Usage guidelines

This command creates an SSL server policy for which you can configure SSL parameters such as a PKI domain and supported cipher suits. An SSL server policy takes effect only after it is associated with an application such as HTTPS.

Examples

Create an SSL server policy named **policy1** and enter its view.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1]
```

Related commands

display ssl server-policy

ssl version disable

Use **ssl version disable** to disable the SSL server from using specific SSL protocol versions for session negotiation.

Use **undo ssl version disable** restore the default.

Syntax

ssl version { **gm-tls1.1** | **ssl3.0** | **tls1.0** | **tls1.1** | **tls1.2** | **tls1.3** } * **disable**

undo ssl version { **gm-tls1.1** | **ssl3.0** | **tls1.0** | **tls1.1** | **tls1.2** | **tls1.3** } * **disable**

Default

The SSL server supports TLS 1.1 and TLS 1.2.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

gm-tls1.1: Specifies GM-TLS 1.1.

ssl3.0: Specifies SSL 3.0.

tls1.0: Specifies TLS 1.0.

tls1.1: Specifies TLS 1.1.

tls1.2: Specifies TLS 1.2.

tls1.3: Specifies TLS 1.3. TLS 1.3 is supported only by SSL VPN.

Usage guidelines

To enhance security, you can disable the SSL server from using specific SSL protocol versions.

This command allows you to disable SSL protocol versions in system view. You can also enable or disable an SSL protocol version in SSL server policy view by using the **version disable** command. An SSL server policy prefers the policy-specific setting over the system global setting.

Make sure the SSL server is allowed to use a minimum of one SSL protocol version for session negotiation.

Disabling an SSL protocol version does not affect the availability of earlier SSL protocol versions. For example, if you execute the **ssl version tls1.1 disable** command, TLS 1.1 is disabled but TLS 1.0 is still available for the SSL server.

Examples

Disable TLS 1.0.

```
<Sysname> system-view
[Sysname] ssl version tls1.0 disable
```

Related commands

version disable

version

Use **version** to specify an SSL protocol version for an SSL client policy.

Use **undo version** to restore the default.

Syntax

version { **gm-tls1.1** | **ssl3.0** | **tls1.0** | **tls1.1** | **tls1.2** | **tls1.3** }

undo version

Default

An SSL client policy uses SSL protocol version TLS 1.2.

Views

SSL client policy view

Predefined user roles

network-admin

context-admin

Parameters

gm-tls1.1: Specifies GM-TLS 1.1.

ssl3.0: Specifies SSL 3.0.

tls1.0: Specifies TLS 1.0.

tls1.1: Specifies TLS 1.1.

tls1.2: Specifies TLS 1.2.

tls1.3: Specifies TLS 1.3. TLS 1.3 is supported only by SSL VPN.

Usage guidelines

To ensure security, do not specify SSL 3.0 for an SSL client policy.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the SSL protocol version to TLS 1.0 for SSL client policy **policy1**.

```
<Sysname> system-view
[Sysname] ssl client-policy policy1
[Sysname-ssl-client-policy-policy1] version tls1.0
```

Related commands

display ssl client-policy

version disable

Use **version disable** to disable SSL protocol versions for the SSL server in an SSL server policy.

Use **undo version disable** restore the default.

Syntax

version { **gm-tls1.1** | **ssl3.0** | **tls1.0** | **tls1.1** | **tls1.2** | **tls1.3** } * **disable**

undo version { **gm-tls1.1** | **ssl3.0** | **tls1.0** | **tls1.1** | **tls1.2** | **tls1.3** } * **disable**

Default

An SSL protocol version is enabled in an SSL sever policy unless it is explicitly disabled in system view by using the **ssl version disable** command.

Views

SSL server policy view

Predefined user roles

network-admin

context-admin

Parameters

gm-tls1.1: Specifies GM-TLS 1.1.

ssl3.0: Specifies SSL 3.0.

tls1.0: Specifies TLS 1.0.

tls1.1: Specifies TLS 1.1.

tls1.2: Specifies TLS 1.2.

tls1.3: Specifies TLS 1.3. TLS 1.3 is supported only by SSL VPN.

Usage guidelines

You can enable or disable an SSL protocol version in system view or in SSL server policy view. An SSL server can use an SSL protocol version for session negotiation only when the status of the SSL protocol version in the SSL server policy is **Enabled**. The status of an SSL protocol version in an SSL server policy is determined in the following sequence:

1. Configuration of the **version disable** command in SSL server policy view.
2. Configuration of the **ssl version disable** command in system view.
3. Default setting (**Enabled**).

Make sure the SSL server is allowed to use a minimum of one SSL protocol version for session negotiation.

Disabling an SSL protocol version does not affect the availability of earlier SSL protocol versions. For example, if you execute the **version tls1.1 disable** command in SSL server policy view, TLS 1.1 is disabled but TLS 1.0 is still available for the SSL server.

Examples

Disable TLS 1.0 in SSL server policy **policy1**.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] version tls1.0 disable
```

Related commands

ssl version disable

Contents

Connection limit commands

connection-limit

Use **connection-limit** to create a connection limit policy and enter its view, or enter the view of an existing connection limit policy.

Use **undo connection-limit** to delete a connection limit policy.

Syntax

connection-limit { **ipv6-policy** | **policy** } *policy-id*

undo connection-limit { **ipv6-policy** | **policy** } *policy-id*

Default

No connection limit policies exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-policy: Specifies an IPv6 connection limit policy.

policy: Specifies an IPv4 connection limit policy.

policy-id: Specifies the ID of a connection limit policy, in the range of 1 to 32. An IPv4 or IPv6 connection limit policy has its own number.

Examples

Create IPv4 connection limit policy 1 and enter its view.

```
<Sysname> system-view
[Sysname] connection-limit policy 1
[Sysname-connlmt-policy-1]
```

Create IPv6 connection limit policy 12 and enter its view.

```
<Sysname> system-view
[Sysname] connection-limit ipv6-policy 12
[Sysname-connlmt-ipv6-policy-12]
```

Related commands

connection-limit apply

connection-limit apply global

display connection-limit

limit

connection-limit apply

Use **connection-limit apply** to apply a connection limit policy to an interface.

Use **undo connection-limit apply** to remove a connection limit policy from an interface.

Syntax

connection-limit apply { **ipv6-policy** | **policy** } *policy-id*

undo connection-limit apply { **ipv6-policy** | **policy** }

Default

No connection limit policy is applied to an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-policy: Specifies an IPv6 connection limit policy.

policy: Specifies an IPv4 connection limit policy.

policy-id: Specifies the ID of a connection limit policy, in the range of 1 to 32.

Usage guidelines

Only one IPv4 connection limit policy and one IPv6 connection limit policy can be applied to an interface. A new IPv4 or IPv6 connection limit policy overwrites the old one.

Related commands

connection-limit

limit

connection-limit apply global

Use **connection-limit apply global** to apply a connection limit policy globally.

Use **undo connection-limit apply global** to remove the application.

Syntax

connection-limit apply global { **ipv6-policy** | **policy** } *policy-id*

undo connection-limit apply global { **ipv6-policy** | **policy** }

Default

No connection limit policy is applied globally.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-policy: Specifies an IPv6 connection limit policy.

policy: Specifies an IPv4 connection limit policy.

policy-id: Specifies the ID of a connection limit policy, in the range of 1 to 32.

Usage guidelines

Only one IPv4 connection limit policy and one IPv6 connection limit policy can be applied globally. A new IPv4 or IPv6 connection limit policy overwrites the old one.

Examples

Apply IPv4 connection limit policy 1 globally.

```
<Sysname> system-view
[Sysname] connection-limit apply global policy 1
```

Apply IPv6 connection limit policy 12 globally.

```
<Sysname> system-view
[Sysname] connection-limit apply global ipv6-policy 12
```

Related commands

connection-limit

limit

description

Use **description** to configure a description for a connection limit policy.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

A connection limit policy does not have a description.

Views

IPv4 connection limit policy view

IPv6 connection limit policy view

Predefined user roles

network-admin

context-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 127 characters.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure the description as **CenterToA** for IPv4 connection limit policy 1.

```
<Sysname> system-view
[Sysname] connection-limit policy 1
[Sysname-connlmt-policy-1] description CenterToA
```

Related commands

display connection-limit

display connection-limit

Use **display connection-limit** to display information about connection limit policies.

Syntax

display connection-limit { **ipv6-policy** | **policy** } { *policy-id* | **all** }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ipv6-policy: Specifies an IPv6 connection limit policy.

policy: Specifies an IPv4 connection limit policy.

policy-id: Specifies the ID of a connection limit policy, in the range of 1 to 32.

all: Specifies all connection limit policies.

Examples

Display information about all IPv4 connection limit policies.

```
<Sysname> display connection-limit policy all
3 policies in total:
 Policy  Rule     Stat Type  HiThres  LoThres  Rate     PermitNew   ACL
--------------------------------------------------------------------------------
      1     2      Dst-Port      800       70     0           Yes   3010
            3       Src-Dst      100       90     0            No   3000
           10  Src-Dst-Port       50       45     0            No   3003
           11           Src      200      200     0            No   3004
          200            --    500000   498000     0            No   2002
     28     4          Port     1500     1400     0            No   3100
            5           Dst     3000      280     0            No   3101
           21       Src-Dst      200      180     0            No   3102
           25      Src-Port       50       35     0            No   3200

Description list:
 Policy      Description
--------------------------------------------------------------------------------
      1       IPv4Description1
     28      Description for IPv4 28
```

Display information about IPv4 connection limit policy 1.

```
<Sysname> display connection-limit policy 1
IPv4 connection limit policy 1 has been applied 5 times, and has 5 limit rules.
Description: IPv4Description1
Limit rule list:
```

```
 Policy  Rule     Stat Type  HiThres  LoThres     Rate   PermitNew   ACL
------------------------------------------------------------------------------
      1     2      Dst-Port      800       70     0          Yes   3010
            3       Src-Dst      100       90     0           No   3000
           10  Src-Dst-Port       50       45     0           No   3003
           11           Src      200      200     0           No   3004
          200            --    500000   498000     0           No   2002
 Application list:
     GigabitEthernet1/0/1
     GigabitEthernet1/0/2
     Vlan-interface2
     Global
```

Display information about all IPv6 connection limit policies.

```
<Sysname> display connection-limit ipv6-policy all
2 policies in total:
 Policy  Rule     Stat Type  HiThres  LoThres  Rate     PermitNew   ACL
------------------------------------------------------------------------------
      3     1       Src-Dst     1000      800    10           Yes   3010
            2           Dst      500      450     0           Yes   3001
      4     2  Src-Dst-Port      800      700     0           No    3010
            3           Src      100       90     0           No    3020
          200            --   100000    89000     0           No    2005

Description list:
 Policy      Description
------------------------------------------------------------------------------
      3      IPv6Description3
      4      Description for IPv6 4
```

Display information about IPv6 connection limit policy 3.

```
<Sysname> display connection-limit ipv6-policy 3
IPv6 connection limit policy 3 has been applied 3 times, and has 2 limit rules.
Description: IPv6Description3
Limit rule list:
 Policy  Rule     Stat Type  HiThres  LoThres  Rate     PermitNew   ACL
------------------------------------------------------------------------------
     3     1       Src-Dst     1000      800     0           Yes   3010
           2           Dst      500      450     0           No    3001
Application list:
    GigabitEthernet1/0/1
    Vlan-interface2
```

Table 1 Command output

Field	Description
Limit rule list	Connection limit policy information.
Policy	Number of the connection limit policy.
Rule	Number of the connection limit rule.

Field	Description
Stat Type	Statistics types: • **Src-Dst-Port**—Limits connections by source IP, destination IP, and service combination. • **Src-Dst**—Limits connections by source IP address and destination IP address combination. • **Src-Port**—Limits connections by source IP and service combination. • **Dst-Port**—Limits connections by destination IP and service combination. • **Src**—Limits connections by source IP address. • **Dst**—Limits connections by destination IP address. • **Port**—Limits connections by service. • **Dslite**—Limits connections by B4 device of a DS-Lite tunnel. • **--**—Limits connections not by a specific IP address or service. All connections that match the ACL used by the rule are limited.
HiThres	Upper limit of the connections.
LoThres	Lower limit of the connections.
Rate	Maximum number of connections established per second.
ACL	Number or name of the ACL used by the rule.
PermitNew	Permit new connections when the connection count or connection rate exceeds the threshold.
Application list	Application list of the connection limit policy, including interface name and **Global**. **Global** indicates that the connection limit policy is applied globally.
Description	Connection limit policy description.
Description list	List of connection limit policy descriptions.

Related commands

connection-limit

connection-limit apply

connection-limit apply global

limit

display connection-limit ipv6-stat-nodes

Use **display connection-limit ipv6-stat-nodes** to display statistics about IPv6 connections that match connection limit rules globally or on an interface.

Syntax

display connection-limit ipv6-stat-nodes { **global** | **interface** *interface-type interface-number* } [**slot** *slot-number*] [{ **deny-new** | **permit-new** } | **destination** *destination-ip* | **service-port** *port-number* | **source** *source-ip*] * [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

global: Displays statistics about IPv6 connections that match connection limit rules globally.

interface *interface-type interface-number*: Specifies an interface by its type and number.

slot *slot-number*: Specifies an IRF member device by its member ID. This option is available only when you specify the **global** keyword or specify a virtual interface, such as a VLAN-interface and tunnel interface.

deny-new: Displays limit rule-based statistics sets of which new connections are rejected.

permit-new: Displays limit rule-based statistics sets of which new connections are allowed.

destination *destination-ip*: Specifies a destination by its IP address.

service-port *port-number*: Specifies a service port by its port number.

source *source-ip*: Specifies a source by its IP address.

count: Displays only the number of limit rule-based statistics sets. Detailed information about the specified IPv6 connections is not displayed. If you do not specify this keyword, the command displays detailed information about the specified IPv6 connections that match connection limit rules.

Usage guidelines

The statistics for this command include the following information:

- Connection information, including the source/destination IP address, service port, and transport layer protocol of connections.
- Matching connection limit rules.
- Number of current connections.
- Whether or not new connections can be created.

To further filter the output statistics, specify the following options in the command:

- **source** *source-ip*.
- **destination** *destination-ip*.
- **service-port** *port-number*.
- **permit-new**.
- **deny-new**.

For example, if you specify the **source** *source-ip* and **destination** *destination-ip* combination, this command displays statistics about IPv6 connections that match connection limit rules by source IP address and destination IP address.

If you specify none of the previously mentioned parameters, this command displays statistics about all IPv6 connections that match connection limit rules.

Deleting or modifying an IPv6 connection limit policy will not delete the effective IPv6 connection limit rule-based statistics sets. An IPv6 connection limit rule-based statistics set will be automatically deleted after all the IPv6 connections for the set are disconnected.

Examples

Display statistics about IPv6 connections that match the connection limit rule on IRF member device 2.

```
<Sysname> display connection-limit ipv6-stat-nodes global slot 2
```

```
Slot 2:
 Src IP address          : Any
     VPN instance        : --
 Dst IP address          : Any
     VPN instance        : --
 DS-Lite tunnel peer     : --
 Service                 : icmp/0
 Limit rule ID           : 22(ACL: 3666)
 Sessions threshold Hi/Lo: 3500/3000
 Sessions count          : 3100
 Sessions limit rate     : 0
 New session flag        : Permit
```

Display the number of limit rule-based statistics sets on IRF member device 2.

```
<Sysname> display connection-limit ipv6-stat-nodes global slot 2 count
Slot 2:
       Current limit statistic nodes count is 0.
```

Table 2 Command output

Field	Description
Src IP address	Source IP address.
Dst IP address	Destination IP address.
VPN instance	MPLS L3VPN instance to which the IP address belongs. Two hyphens (--) indicates that the IP address is on the public network.
DS-Lite tunnel peer	Peer IP address of the DS-Lite tunnel to which the connection belongs. Two hyphens (--) indicates that the connection does not belong to a DS-Lite tunnel.
Service	Protocol name and service port number. For an unwell-known protocol, this field displays **unknown(xx)**.The cross signs (xx) indicates the protocol number. For the ICMP protocol, the protocol number is the decimal digits that are converted from the hexadecimal contents of the type and code fields.
Limit rule ID	ID of the matched rule. The ACL number of the rule is enclosed in parentheses.
Sessions threshold Hi/Lo	Upper and lower connection limits.
Sessions count	Number of current connections.
Sessions limit rate	Maximum number of connections established per second.
New session flag	Whether or not new connections can be created: • **Permit**—New connections can be created. • **Deny**—New connections cannot be created. **NOTE:** When the number of connections reaches the upper limit, this field displays **Permit** although new connections are not allowed. This field displays **Deny** only when the number of connections exceeds the upper limit.

Related commands

connection-limit apply global ipv6-policy

connection-limit apply ipv6-policy

connection-limit ipv6-policy

limit

display connection-limit statistics

Use **display connection-limit statistics** to display the connection limit statistics globally or on an interface.

Syntax

display connection-limit statistics { **global** | **interface** *interface-type interface-number* } [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

global: Displays the global connection limit statistics.

interface *interface-type interface-number*: Specifies an interface by its type and number.

slot *slot-number*: Specifies an IRF member device by its member ID. This option is available only when you specify the **global** keyword or specify a virtual interface, such as a VLAN interface or tunnel interface.

Examples

Display the global connection limit statistics on IRF member device 2.

```
<Sysname> display connection-limit statistics global slot 2
Connection limit statistics (Global, slot 2):
    Dropped IPv4 packets:   74213
    Dropped IPv6 packets:   58174
```

Table 3 Command output

Field	Description
Dropped IPv4 packet	Number of IPv4 packets that are dropped because the upper connection limit is exceeded for the IPv4 connection limit policy that is configured globally or on an interface.
Dropped IPv6 packet	Number of IPv6 packets that are dropped because the upper connection limit is exceeded for the IPv6 connection limit policy that is configured globally or on an interface.

Related commands

connection-limit

connection-limit apply

connection-limit apply global

limit

display connection-limit stat-nodes

Use **display connection-limit stat-nodes** to display statistics about IPv4 connections that match connection limit rules globally or on an interface.

Syntax

display connection-limit stat-nodes { **global** | **interface** *interface-type interface-number* } [**slot** *slot-number*] [{ **deny-new** | **permit-new** } | **destination** *destination-ip* | **service-port** *port-number* | **source** *source-ip*] * [**count**]

display connection-limit stat-nodes { **global** | **interface** *interface-type interface-number* } [**slot** *slot-number*] **dslite-peer** *b4-address* [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

global: Displays statistics about IPv4 connections that match connection limit rules globally.

interface *interface-type interface-number*: Specifies an interface by its type and number.

slot *slot-number*: Specifies an IRF member device by its member ID. This option is available only when you specify the **global** keyword or specify a virtual interface, such as a VLAN-interface and tunnel interface.

deny-new: Displays limit rule-based statistics sets of which new connections are rejected.

permit-new: Displays limit rule-based statistics sets of which new connections are allowed.

destination *destination-ip*: Specifies a destination by its IP address.

service-port *port-number*: Specifies a service port by its port number.

source *source-ip*: Specifies a source by its IP address.

dslite-peer *b4-address*: Specifies a B4 device on a DS-Lite tunnel. The *b4-address* argument specifies the IPv6 address of the B4 device.

count: Displays only the number of limit rule-based statistics sets. Detailed information about the specified IPv4 connections is not displayed. If you do not specify this keyword, the command displays detailed information about the specified IPv4 connections that match connection limit rules.

Usage guidelines

The statistics for this command include the following information:

- Connection information, including the source/destination IP address, service port, and transport layer protocol of connections.
- Matching connection limit rules.
- Number of current connections.
- Whether or not new connections can be created.

To further filter the output statistics, specify the following options in the command:

- **source** *source-ip*.
- **destination** *destination-ip*.
- **service-port** *port-number*.
- **permit-new**.
- **deny-new**.

For example, if you specify the **source** *source-ip* and **destination** *destination-ip* combination, this command displays statistics about IPv4 connections that match connection limit rules by source IP address and destination IP address.

If you specify none of the previously mentioned parameters, this command displays statistics about all IPv4 connections that match connection limit rules.

Deleting or modifying an IPv4 connection limit policy will not delete the effective IPv4 connection limit rule-based statistics sets. An IPv4 connection limit rule-based statistics set will be automatically deleted after all the IPv4 connections for the set are disconnected.

Examples

Display statistics about IPv4 connections that match the connection limit rule on IRF member device 2.

```
<Sysname> display connection-limit stat-nodes global slot 2
Slot 2:
 Src IP address          : Any
     VPN instance        : Vpn1
 Dst IP address          : 202.113.16.117
     VPN instance        : Vpn2
 DS-Lite tunnel peer     : --
 Service                 : icmp/0
 Limit rule ID           : 7(ACL: 3102)
 Sessions threshold Hi/Lo: 4000/3800
 Sessions count          : 1001
 Sessions limit rate     : 0
 New session flag        : Permit
```

Display the number of limit rule-based statistics sets on IRF member device 2 by source IP address 1.1.1.1.

```
<Sysname> display connection-limit stat-nodes global slot 2 source 1.1.1.1 count
Slot 2:
       Current limit statistic nodes count is 0.
```

Table 4 Command output

Field	Description
Src IP address	Source IP address.
Dst IP address	Destination IP address.
VPN instance	MPLS L3VPN instance to which the IP address belongs. Two hyphens (--) indicates that the IP address is on the public network.
DS-Lite tunnel peer	Peer IP address of the DS-Lite tunnel to which the connection belongs. Two hyphens (--) indicates that the connection does not belong to a DS-Lite tunnel.

Field	Description
Service	Protocol name and service port number. For an unwell-known protocol, this field displays **unknown(xx)**. The cross signs (xx) represents the protocol number. For the ICMP protocol, the protocol number is the decimal digits that are converted from the hexadecimal contents of the type and code fields.
Sessions threshold Hi/Lo	Upper and lower connection limits.
Sessions count	Number of current connections.
Sessions limit rate	Maximum number of connections established per second.
New session flag	Whether or not new connections can be created: • **Permit**—New connections can be created. • **Deny**—New connections cannot be created. **NOTE:** When the number of connections reaches the upper limit, this field displays **Permit** although new connections are not allowed. This field displays **Deny** only when the number of connections exceeds the upper limit.

Related commands

connection-limit apply global policy

connection-limit apply policy

connection-limit policy

limit

limit

Use **limit** to configure a connection limit rule.

Use **undo limit** to delete a connection limit rule.

Syntax

In IPv4 connection limit policy view:

limit *limit-id* **acl** { *acl-number* | **name** *acl-name* } [**per-destination** | **per-service** | **per-source**] * { **amount** *max-amount min-amount* | **rate** *rate* } * [**description** *text* | **permit-new**] *

limit *limit-id* **acl ipv6** { *acl-number* | **name** *acl-name* } **per-dslite-b4** { **amount** *max-amount min-amount* | **rate** *rate* } * [**description** *text* | **permit-new**] *

undo limit *limit-id*

In IPv6 connection limit policy view:

limit *limit-id* **acl ipv6** { *acl-number* | **name** *acl-name* } [**per-destination** | **per-service** | **per-source**] * { **amount** *max-amount min-amount* | **rate** *rate* } * [**description** *text* | **permit-new**] *

undo limit *limit-id*

Default

No connection limit rules exist.

Views

IPv4 connection limit policy view

IPv6 connection limit policy view

Predefined user roles

network-admin

context-admin

Parameters

limit-id: Specifies a connection limit rule by its ID in the range of 1 to 256.

acl: Specifies the ACL that matches the user range. Only the user connections that match the ACL are limited.

ipv6: Specifies an IPv6 ACL. If you do not specify this keyword, an IPv4 ACL is used.

acl-number: Specifies an ACL by its number in the range of 2000 to 3999.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters. It must start with an English letter. To avoid confusion, it cannot be **all**.

per-destination: Limits connections by destination IP address.

per-service: Limits connections by service depending on transport layer protocol and service port.

per-source: Limits connections by source IP address.

per-dslite-b4: Limits connections by IPv6 address of a B4 device on a DS-Lite tunnel. This keyword is available only in IPv4 connection limit policy view.

amount: Limits the number of connections.

max-amount: Specifies the upper connection limit in the range of 1 to 4294967294. If the **permit-new** parameter is not specified, when user connections in a range or of a type exceed the upper limit, new connections cannot be created until the connection count drops below *min-amount*.

min-amount: Specifies the lower connection limit in the range of 1 to 4294967294. The lower connection limit cannot be greater than the upper connection limit. New connections cannot be created until the connection number goes below the lower connection limit.

rate: Limits the connection establishment rate.

rate: Specifies the maximum number of connections established per second. The value range is 5 to 10000000. If the permit-new parameter is not specified, when user connections in a range or of a type exceed this rate, new connections cannot be created until the connection rate drops below this rate.

description *text*: Specifies a description for the connection limit rule, a case-sensitive string of 1 to 127 characters. By default, a connection limit rule does not have a description.

permit-new: Permits new connections when the connection count or connection rate exceeds the threshold and generates alarm logs.

Usage guidelines

Each connection limit policy can define multiple rules, and each rule must specify the used ACL, rule type, and either of upper/lower connection limit and connection establishment rate limit. In one rule, you can specify one or multiple of the keywords **per-destination**, **per-source**, and **per-service**, but you cannot specify the **per-dslite-b4** keyword together with other keywords. For example, if the **per-destination** and **per-source** combination is specified,

connections are limited by the source IP address and destination IP address. Connections with the same source IP address and destination IP address are the same type.

When you configure a connection limit rule, follow these guidelines:

- Different rules in the same connection limit policy must use different ACLs.
- If you specify none of the **per-destination**, **per-source**, and **per-service** keywords, all connections that match the specified ACL are limited by the specified value.
- When the connections established on a device are matched against a connection limit policy, the limit rules in the policy are matched in ascending order of rule ID.
- When the specified ACL changes, the connections that have been established are limited by the new connection limit policy.
- A rule that has the **per-dslite-b4** keyword limits IPv4 connections of the DS-Lite tunnel B4 device that matches the specified IPv6 ACL in the rule. On a DS-Lite tunnel network, if the AFTR device uses the Endpoint-Independent Mapping-based NAT configuration, you must limit connections from external IPv4 networks to access the internal IPv4 network. To implement B4 device-based connection limits, perform the following tasks:
  - Add a rule that has the **per-dslite-b4** keyword to a connection limit policy.
  - Apply the policy globally or on the DS-Lite tunnel interface.

Examples

Configure connection limit rule 1 for IPv4 connection limit policy 1:

1. Configure ACL 3000.

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule permit ip source 192.168.0.0 0.0.0.255
[Sysname-acl-ipv4-adv-3000] quit
```

2. Limit connections that match ACL 3000 by the source and destination IP addresses, with the upper limit 2000, lower limit 1800, and establishment rate 10 per second.

```
[Sysname] connection-limit policy 1
[Sysname-connlmt-policy-1] limit 1 acl 3000 per-destination per-source amount 2000
1800 rate 10
```

3. Verify that when the connection number exceeds 2000, new connections cannot be established until the connection number goes below 1800. (Details not shown.)

Configure connection limit rule 1 for IPv4 connection limit policy 1:

1. Configure ACL 3000.

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule permit ip source 192.168.0.0 0.0.0.255
[Sysname-acl-ipv4-adv-3000] quit
```

2. Limit connections that match ACL 3000 by the source and destination IP addresses, with the upper limit 2000, lower limit 1800, and establishment rate 10 per second. Specify the **permit-new** keyword.

```
[Sysname] connection-limit policy 1
[Sysname-connlmt-policy-1] limit 1 acl 3000 per-destination per-source amount 2000
1800 rate 10 permit-new
```

3. Verify that when the connection number exceeds 2000 or the connection rate exceeds 10 per second, new connections can be established but alarm logs are generated. (Details not shown.)

Configure connection limit rule 2 for IPv6 connection limit policy 12:

1. Configure ACL 2001.

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2001
[Sysname-acl-ipv6-basic-2001] rule permit source 2:1::/96
[Sysname-acl-ipv6-basic-2001] quit
```

2. Limit connections that match ACL 2001 by the source and destination IP addresses, with the upper limit 200, lower limit 100, and establishment rate 10 per second.

```
[Sysname] connection-limit ipv6-policy 12
[Sysname-connlmt-ipv6-policy-12] limit 2 acl ipv6 2001 per-destination amount 200 100 rate 10
```

3. Verify that when the connection number exceeds 200, new connections cannot be established until the connection number goes below 100. (Details not shown.)

Configure connection limit rule 2 for IPv6 connection limit policy 12:

1. Configure ACL 2001.

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2001
[Sysname-acl-ipv6-basic-2001] rule permit source 2:1::/96
[Sysname-acl-ipv6-basic-2001] quit
```

2. Limit connections that match ACL 2001 by the destination IP addresses, with the upper limit 200, lower limit 100, and establishment rate 10 per second. Specify the **permit-new** keyword.

```
[Sysname] connection-limit ipv6-policy 12
[Sysname-connlmt-ipv6-policy-12] limit 2 acl ipv6 2001 per-destination amount 200 100 rate 10
```

3. Verify that when the connection number exceeds 200 or the connection rate exceeds 10 per second, new connections can be established but alarm logs are generated. (Details not shown.)

Related commands

connection-limit

display connection-limit

reset connection-limit statistics

Use **reset connection-limit statistics** to clear the connection limit statistics globally or on an interface.

Syntax

reset connection-limit statistics { **global** | **interface** *interface-type interface-number* } [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

global: Clears the global connection limit statistics.

interface *interface-type interface-number*: Specifies an interface by its type and number.

slot *slot-number*: Specifies an IRF member device by its member ID. The *slot-number* argument represents the ID of the IRF member device. This option is available only when you specify the **global** keyword or specify a virtual interface, such as a VLAN interface or tunnel interface.

Examples

Clear the global connection limit statistics on IRF member device 2.

```
<Sysname> reset connection-limit statistics global slot 2
```

Related commands

display connection-limit statistics

Contents

Attack detection and prevention commands

ack-flood action

Use **ack-flood action** to specify global actions against ACK flood attacks.

Use **undo ack-flood action** to restore the default.

Syntax

ack-flood action { **client-verify** | **drop** | **logging** } *

undo ack-flood action

Default

No global action is specified for ACK flood attacks.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

client-verify: Adds the victim IP addresses to the protected IP list for TCP client verification. If TCP client verification is enabled, the device provides proxy services for protected servers. This keyword does not take effect on source-based flood attack prevention.

drop: Drops subsequent ACK packets destined for the victim IP addresses in destination-based flood attack prevention, or drops subsequent ACK packets originating from the attacker IP addresses in source-based flood attack prevention.

logging: Enables logging for ACK flood attack events. The log messages will be sent to the log system.

Usage guidelines

For the ACK flood attack detection to collaborate with the TCP client verification, make sure the **client-verify** keyword is specified and the TCP client verification is enabled. To enable TCP client verification, use the **client-verify tcp enable** command.

The **logging** keyword enables the attack detection and prevention module to log ACK flood attack events and send log messages to the information center.

With the information center, you can set log message filtering and output rules, including output destinations.

The information center can output ACK flood attack logs to any destinations except the console and the monitor terminal. If you configure the console or monitor terminal as an output destination, the output destination setting will not take effect.

To view ACK flood attack logs stored on the device, use the **display logbuffer** command. Make sure you do not disable log output to the log buffer, which is enabled by default.

For more information about configuring the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Specify **drop** as the global action against ACK flood attacks in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] ack-flood action drop
```

Related commands

ack-flood detect

ack-flood detect non-specific

ack-flood source-threshold

ack-flood threshold

client-verify tcp enable

ack-flood detect

Use **ack-flood detect** to configure IP address-specific ACK flood attack detection.

Use **undo ack-flood detect** to remove IP address-specific ACK flood attack detection configuration.

Syntax

ack-flood detect { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**threshold** *threshold-value*] [**action** { { **client-verify** | **drop** | **logging** } * | **none** }]

undo ack-flood detect { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]

Default

IP address-specific ACK flood attack detection is not configured.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

ip *ipv4-address*: Specifies the IPv4 address to be protected. The *ip-address* argument cannot be 255.255.255.255 or 0.0.0.0.

ipv6 *ipv6-address*: Specifies the IPv6 address to be protected. The IPv6 address cannot be a multicast address or ::.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the protected IP address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the protected IP address is on the public network.

threshold *threshold-value*: Specifies the maximum receiving rate in pps for ACK packets that are destined for the protected IP address. The value range is 1 to 1000000.

action: Specifies the actions against a detected ACK flood attack. If no action is specified, the global actions set by the **ack-flood action** command apply.

client-verify: Adds the victim IP addresses to the protected IP list for TCP client verification. If TCP client verification is enabled, the device provides proxy services for protected servers.

drop: Drops subsequent ACK packets destined for the protected IP address.

logging: Enables logging for ACK flood attack events. The log messages will be sent to the log system.

none: Takes no action.

Usage guidelines

With ACK flood attack detection configured for an IP address, the device is in attack detection state. When the receiving rate of ACK packets destined for the IP address keeps reaching or exceeding the threshold, the device enters prevention state and takes the specified actions. When the rate drops below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

You can configure ACK flood attack detection for multiple IP addresses in one attack defense policy.

The **logging** keyword enables the attack detection and prevention module to log ACK flood attack events and send log messages to the information center.

With the information center, you can set log message filtering and output rules, including output destinations.

The information center can output ACK flood attack logs to any destinations except the console and the monitor terminal. If you configure the console or monitor terminal as an output destination, the output destination setting will not take effect.

To view ACK flood attack logs stored on the device, use the **display logbuffer** command. Make sure you do not disable log output to the log buffer, which is enabled by default.

For more information about configuring the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Configure ACK flood attack detection for 192.168.1.2 in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] ack-flood detect ip 192.168.1.2 threshold 2000
```

Related commands

ack-flood action

ack-flood detect non-specific

ack-flood threshold

client-verify tcp enable

ack-flood detect non-specific

Use **ack-flood detect non-specific** to enable global ACK flood attack detection.

Use **undo ack-flood detect non-specific** to disable global ACK flood attack detection.

Syntax

ack-flood detect non-specific

undo ack-flood detect non-specific

Default

Global ACK flood attack detection is disabled.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Usage guidelines

The device supports the following ACK flood attack prevention types:

- **Source-based ACK flood attack prevention**—Monitors the receiving rate of ACK packets on a per-source IP basis.
- **Destination-based ACK flood attack prevention**—Monitors the receiving rate of ACK packets on a per-destination IP basis.

The global ACK flood attack detection applies to all IP addresses except those specified by the **ack-flood detect** command. The global detection uses the global trigger threshold set by the **ack-flood threshold** or **ack-flood source-threshold** command and global actions specified by the **ack-flood action** command.

Examples

Enable global ACK flood attack detection in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] ack-flood detect non-specific
```

Related commands

ack-flood action

ack-flood detect

ack-flood source-threshold

ack-flood threshold

ack-flood threshold

Use **ack-flood threshold** to set the global threshold for triggering destination-based ACK flood attack prevention.

Use **undo ack-flood threshold** to restore the default.

Syntax

ack-flood threshold *threshold-value*

undo ack-flood threshold

Default

The global threshold is 40000 for triggering destination-based ACK flood attack prevention.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

threshold-value: Specifies the maximum receiving rate in pps for ACK packets that are destined for an IP address. The value range is 0 to 1000000. If you set the threshold value to 0, the destination-based ACK flood attack prevention is disabled.

Usage guidelines

With global ACK flood attack detection configured, the device is in attack detection state. When the receiving rate of ACK packets destined for an IP address keeps reaching or exceeding the threshold, the device enters prevention state and takes the specified actions. When the rate drops below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

The global threshold applies to global ACK flood attack detection. Adjust the threshold according to the application scenarios.

- If the number of ACK packets sent to a protected server, such as an HTTP or FTP server, is normally large, set a high threshold. A low threshold might affect the server services.
- For a network that is unstable or susceptible to attacks, set a low threshold.

Examples

Set the global threshold to 100 for triggering destination-based ACK flood attack prevention in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] ack-flood threshold 100
```

Related commands

ack-flood action

ack-flood detect

ack-flood detect non-specific

ack-flood source-threshold

Use **ack-flood source-threshold** to set the global threshold for triggering source-based ACK flood attack prevention.

Use **undo ack-flood source-threshold** to restore the default.

Syntax

ack-flood source-threshold *threshold-value*

undo ack-flood source-threshold

Default

The global threshold is 40000 for triggering source-based ACK flood attack prevention.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

threshold-value: Specifies the maximum receiving rate in pps for ACK packets that originate from an IP address. The value range is 0 to 1000000. If you set the threshold value to 0, the source-based ACK flood attack prevention is disabled.

Usage guidelines

With global ACK flood attack detection configured, the device is in attack detection state. When the receiving rate of ACK packets originating from an IP address keeps reaching or exceeding the threshold, the device enters prevention state and takes the specified actions. When the rate drops below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

Examples

Set the global threshold to 100 for triggering source-based ACK flood attack prevention in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] ack-flood source-threshold 100
```

Related commands

ack-flood action

ack-flood detect

ack-flood detect non-specific

attack-defense apply policy

Use **attack-defense apply policy** to apply an attack defense policy to a security zone.

Use **undo attack-defense apply policy** to restore the default.

Syntax

attack-defense apply policy *policy-name*

undo attack-defense apply policy

Default

No attack defense policy is applied to a security zone.

Views

Security zone view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies an attack defense policy by its name. The policy name is a case-insensitive string of 1 to 31 characters. Valid characters include uppercase and lowercase letters, digits, underscores (_), and hyphens (-).

Usage guidelines

A security zone can have only one attack defense policy applied. If you execute this command multiple times, the most recent configuration takes effect.

An attack defense policy can be applied to multiple security zones.

Examples

Apply attack defense policy **atk-policy-1** to security zone **DMZ**.

```
<Sysname> system-view
[Sysname] security-zone name DMZ
[Sysname-security-zone-DMZ] attack-defense apply policy atk-policy-1
```

Related commands

attack-defense policy

display attack-defense policy

attack-defense cpu-core action

Use **attack-defense cpu-core action** to specify an attack prevention action for CPU core protection.

Use **undo attack-defense cpu-core action** to restore the default.

Syntax

attack-defense cpu-core action { **drop** | **isolate** | **per-packet-balance** }

undo attack-defense cpu-core action

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX5-HD6480	Yes
NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB680, NFNX3-HDB1080	No

Default

The attack prevention action for a CPU core is **drop**.

Views

System view

Predefined user roles

network-admin

Parameters

drop: Drops subsequent packets sent to a CPU core when the CPU core is attacked.

isolate: Isolates the flow that uses the most CPU time to lower its priority when a CPU core is attacked. This parameter takes effect on only one flow at a time.

The following compatibility matrixes show the support of hardware platforms for the **isolate** keyword:

Models	Parameter compatibility
NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280	Yes
NFNX5-HD6480, NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB680,	No

Models	Parameter compatibility
NFNX3-HDB1080	

per-packet-balance: Distributes subsequent packets across CPU cores on a per-packet basis when a CPU core is attacked.

Usage guidelines

After the usage of a CPU core reaches the specified threshold and the shared queue of the driver is full, the system determines that an attack risk is present on the CPU core. Then, it processes the subsequent packets sent to the CPU core as follows:

- **Drop**—The CPU core uses all its available processing capability to process packets. The driver drops the packets beyond the maximum processing capability to decrease the CPU core usage. This action affects normal service processing.
- **Per-packet balance**—The CPU core uses all its available processing capability to process packets. Packets exceeding the maximum processing capability are sent to other CPU cores for load sharing on a per-packet basis. This action ensures normal service processing to some extent, but leads to risk of attacks on other CPU cores.
- **Isolate**—The driver isolates the flow that uses the most CPU time to lower the flow's processing priority. It sends the isolated packets to the CPU core for processing after the shared queue has no packets to process. This action ensures normal service processing to some extent, but it cannot significantly decrease the CPU usage because the packets in the public queue are still sent to the CPU core for processing.

To set CPU usage threshold per CPU core, execute the **context-capability inbound unicast total** command. For more information about this command, see context commands in *Virtual Technologies Command Reference*.

Examples

Specify **per-packet balance** as the attack prevention action for CPU core protection.

```
<Sysname> system-view
[Sysname] attack-defense cpu-core action per-packet-balance
```

Related commands

context-capability inbound unicast total (*Virtual Technologies Command Reference*)

display attack-defense cpu-core flow info

attack-defense ipcar action

Use **attack-defense ipcar action** to set defense actions upon threshold violations for monitored sessions.

Use **undo attack-defense ipcar action** to restore the default settings for a rate limit type.

Syntax

attack-defense ipcar { **destination** | **source** } { **ip** | **ipv6** } [**threshold** *threshold*] **action** { { **drop** | **logging** } * | **none** }

undo attack-defense ipcar { **destination** | **source** } { **ip** | **ipv6** }

Default

The packet receiving rate threshold is 5000 pps for each monitored session, and no defense actions are set.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

destination: Limits session creation rate on a per-destination basis.

source: Limits session creation rate on a per-source basis.

ip: Specifies IPv4 sessions.

ipv6: Specifies IPv6 sessions.

threshold *threshold*: Sets the packet receiving rate threshold, in pps. The value range is 1 to 500000, and the default is 5000.

logging: Enables logging upon threshold violations.

drop: Drops subsequent packets of sessions encountering threshold violations.

none: Takes no action.

Usage guidelines

The device supports limiting session creation rate based on the following criteria:

- Source IPv4 addresses.
- Source IPv6 addresses.
- Destination IPv4 addresses.
- Destination IPv6 addresses.

Make sure you define the same criteria as those defined in the **attack-defense ipcar session-rate-limit enable** command. Otherwise, the **attack-defense ipcar action** command does not take effect.

Examples

Limit sessions on a per-source IPv4 address, set the packet receiving rate threshold to 5000 pps, and set the **drop** action.

```
<Sysname> system-view
[Sysname] attack-defense ipcar source ip threshold 5000 action drop
```

Related commands

attack-defense ipcar session-rate-limit enable

attack-defense ipcar session-rate-limit enable

Use **attack-defense ipcar session-rate-limit enable** to enable session creation rate limit.

Use **undo attack-defense ipcar session-rate-limit enable** to disable session creation rate limit.

Syntax

attack-defense ipcar { destination | source } { ip | ipv6 } session-rate-limit enable

undo attack-defense ipcar { **destination** | **source** } { **ip** | **ipv6** } **session-rate-limit enable**

Default

Session creation rate limit is disabled.

Views

Layer 3 Ethernet interface view

Layer 3 Ethernet subinterface view

Layer 3 Reth interface view

Layer 3 aggregate interface view

Layer 3 aggregate subinterface view

VLAN interface view

Predefined user roles

network-admin

context-admin

Parameters

destination: Limits session creation rate on a per-destination basis.

source: Limits session creation rate on a per-source basis.

ip: Specifies IPv4 sessions.

ipv6: Specifies IPv6 sessions.

Usage guidelines

The device supports limiting session creation rate based on the following criteria:

- Source IPv4 addresses.
- Source IPv6 addresses.
- Destination IPv4 addresses.
- Destination IPv6 addresses.

With this feature enabled, the device enters attack detection state. It monitors the receiving rate of IP packets originating from or destined for an IP address. If the receiving rate reaches or exceeds the threshold, the device enters prevention state and takes defense actions. When the rate drops below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state. To set the threshold, execute the **attack-defense ipcar action** command.

You cannot enable session creation rate limit based on both source and destination IP addresses on the same interface.

Examples

Enable session creation rate limit based on source IPv4 addresses on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] attack-defense ipcar destination ip session-rate-limit enable
```

Related commands

attack-defense ipcar action

attack-defense login block-timeout

Use **attack-defense login block-timeout** to set the block period during which a login attempt is blocked.

Use **undo attack-defense login block-timeout** to restore the default.

Syntax

attack-defense login block-timeout *minutes*

undo attack-defense login block-timeout

Default

The block period is 60 minutes.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

minutes: Specifies the block period in minutes, in the range of 1 to 2880.

Usage guidelines

After a user fails the maximum number of login attempts, login attack prevention triggers the blacklist module to add the user's IP address to the blacklist. The block period determines how long the user is on the blacklist. During the period, login attempts from the user are blocked.

Examples

Set the block period to 5 minutes.

```
<Sysname> system-view
[Sysname] attack-defense login block-timeout 5
```

attack-defense login enable

Use **attack-defense login enable** to enable login attack prevention.

Use **undo attack-defense login enable** to disable login attack prevention.

Syntax

attack-defense login enable

undo attack-defense login enable

Default

Login attack prevention is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

After a user fails the maximum number of login attempts, login attack prevention uses the blacklist to block the user from logging in during the block period.

For login attack prevention to take effect, you must enable the global blacklist feature.

Examples

Enable login attack prevention.

```
<Sysname> system-view
[Sysname] attack-defense login enable
```

Related commands

blacklist global enable

attack-defense login max-attempt

Use **attack-defense login max-attempt** to set the maximum number of successive login failures for each user.

Use **undo attack-defense login max-attempt** to restore the default.

Syntax

attack-defense login max-attempt *max-attempt*

undo attack-defense login max-attempt

Default

Login attack prevention detects a login attack if a user fails three successive login attempts.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

max-attempt: Specifies the maximum number of login failures. The value range is 1 to 60.

Usage guidelines

After a user fails the maximum number of login attempts, login attack prevention uses the blacklist to block the user from logging in during the block period.

For login attack prevention to take effect, you must enable the global blacklist feature.

The login failure counter for a user is reset after the user logs in successfully. If the device reboots, all login failure counters are reset.

Examples

Set the maximum number of successive login failures to five.

```
<Sysname> system-view
[Sysname] attack-defense login max-attempt 5
```

Related commands

attack-defense login enable

attack-defense login reauthentication-delay

Use **attack-defense login reauthentication-delay** to enable the login delay feature and set the delay period.

Use **undo attack-defense login reauthentication-delay** to restore the default.

Syntax

attack-defense login reauthentication-delay *seconds*

undo attack-defense login reauthentication-delay

Default

The login delay feature is disabled. The device does not delay accepting a login request from a user who has failed a login attempt.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies the delay period in seconds, in the range of 4 to 60.

Usage guidelines

The login delay feature delays the device to accept a login request from a user after the user fails a login attempt. This feature can slow down login dictionary attacks.

The login delay feature is independent of the login attack prevention feature.

Examples

Enable the login delay feature and set the delay period to 5 seconds.

```
<Sysname> system-view
[Sysname] attack-defense login reauthentication-delay 5
```

attack-defense malformed-packet defend enable

Use **attack-defense malformed-packet defend enable** to enable malformed packet attack detection and prevention.

Use **undo attack-defense malformed-packet defend enable** to disable malformed packet attack detection and prevention.

Syntax

attack-defense malformed-packet defend enable

undo attack-defense malformed-packet defend enable

Default

Malformed packet attack detection and prevention is enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This feature improves the single-packet attack prevention efficiency because it drops malformed packets of the following attacks without an attack defense policy match:

- IP impossible packet attack.
- TCP packet attacks that use TCP packets with different flag settings (all flags set, only the FIN flag set, invalid flags, no flags set, and both SYN and FIN flags set).
- Land attack and WinNuke attack.
- UDP fraggle attack, UDP bomb attack, and UDP snork attack.

For a single-packet attack that cannot be detected by this feature, you can use the **`signature detect`** command to enable detection and prevention specific to that attack.

Examples

Enable malformed packet attack detection and prevention.

```
<Sysname> system-view
[Sysname] attack-defense malformed-packet defend enable
```

Related commands

`signature detect`

attack-defense policy

Use **`attack-defense policy`** to create an attack defense policy and enter its view, or enter the view of an existing attack defense policy.

Use **`undo attack-defense policy`** to delete an attack defense policy.

Syntax

`attack-defense policy` *`policy-name`*

`undo attack-defense policy` *`policy-name`*

Default

No attack defense policies exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

`policy-name`: Assigns a name to the attack defense policy. The policy name is a case-insensitive string of 1 to 31 characters. Valid characters include uppercase and lowercase letters, digits, underscores (_), and hyphens (-).

Usage guidelines

CAUTION:

The default thresholds for triggering attack prevention might not be appropriate for your network. Set appropriate thresholds according to the actual application scenarios. Small thresholds might affect the Internet or webpage access speed. Large thresholds might make your network vulnerable to attacks.

Examples

Create attack defense policy **atk-policy-1** and enter its view.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1]
```

Related commands

attack-defense apply policy

display attack-defense policy

attack-defense signature log non-aggregate

Use **attack-defense signature log non-aggregate** to enable log non-aggregation for single-packet attack events.

Use **undo attack-defense signature log non-aggregate** to restore the default.

Syntax

attack-defense signature log non-aggregate

undo attack-defense signature log non-aggregate

Default

Log non-aggregation is disabled for single-packet attack events.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

Log aggregation aggregates multiple logs generated during a period of time and sends one log. Logs that are aggregated must have the following attributes in common:

- Location where the attacks are detected: security zone.
- Attack type.
- Attack prevention action.
- Source and destination IP addresses.
- VPN instance to which the victim IP address belongs.

As a best practice, do not disable log aggregation. A large number of logs will consume the display resources of the console.

Examples

Enable log non-aggregation for single-packet attack events.

```
<Sysname> system-view
[Sysname] attack-defense signature log non-aggregate
```

Related commands

signature detect

attack-defense top-attack-statistics enable

Use **attack-defense top-attack-statistics enable** to enable the top attack statistics ranking feature.

Use **undo attack-defense top-attack-statistics enable** to disable the top attack statistics ranking feature.

Syntax

attack-defense top-attack-statistics enable

undo attack-defense top-attack-statistics enable

Default

The top attack statistics ranking feature is disabled.

Views

System view.

Predefined user roles

network-admin

context-admin

Usage guidelines

This feature collects statistics about number of dropped attack packets based on attacker, victim, and attack type and ranks the statistics by attacker and victim.

To display the top attack statistics, use the **display attack-defense top-attack-statistics** command.

Examples

Enable the top attack statistics ranking feature.

```
<Sysname> system-view
[Sysname] attack-defense top-attack-statistics enable
```

Related commands

display attack-defense top-attack-statistics

blacklist destination-ip

Use **blacklist destination-ip** to add a destination IPv4 blacklist entry.

Use **undo blacklist destination-ip** to delete a destination IPv4 blacklist entry.

Syntax

blacklist destination-ip *destination-ip-address* [**vpn-instance** *vpn-instance-name*] [**timeout** *minutes*]

undo blacklist destination-ip *destination-ip-address* [**vpn-instance** *vpn-instance-name*]

Default

No destination IPv4 blacklist entries exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

destination-ip-address Specifies an IPv4 address for the destination blacklist entry. Packets destined for this address will be dropped.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the blacklist belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the blacklist is on the public network.

timeout *minutes*: Specifies the aging time for the destination blacklist entry, in the range of 1 to 10080 minutes. If you do not specify this option, the blacklist entry never ages out. You must delete it manually.

Usage guidelines

The **undo blacklist destination-ip** command deletes only manually added destination IPv4 blacklist entries. To delete dynamically added destination IPv4 blacklist entries, use the **reset blacklist destination-ip** command.

A destination blacklist entry with an aging time is not saved to the configuration file and cannot survive a reboot.

You can use the **display blacklist destination-ip** command to display all effective destination IPv4 blacklist entries.

Examples

Add a destination blacklist entry for IPv4 address 192.168.1.2 and set the aging time to 20 minutes for the entry.

```
<Sysname> system-view
[Sysname] blacklist ip 192.168.1.2 timeout 20
```

Related commands

blacklist enable

blacklist global enable

display blacklist destination-ip

blacklist destination-ipv6

Use **blacklist destination-ipv6** to add a destination IPv6 blacklist entry.

Use **undo blacklist destination-ipv6** to delete a destination IPv6 blacklist entry.

Syntax

blacklist destination-ipv6 *destination-ipv6-address* [**vpn-instance** *vpn-instance-name*] [**timeout** *minutes*]

undo blacklist destination-ipv6 *destination-ipv6-address* [**vpn-instance** *vpn-instance-name*]

Default

No destination IPv6 blacklist entries exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

destination-ipv6-address: Specifies an IPv6 address for the blacklist entry. Packets destined for this address will be dropped.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the blacklist belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the blacklist is on the public network.

timeout *minutes*: Specifies the aging time for the blacklist entry, in the range of 1 to 10080 minutes. If you do not specify this option, the blacklist entry never ages out. You must delete it manually.

Usage guidelines

The **undo blacklist destination-ipv6** command deletes only manually added destination IPv6 blacklist entries. To delete dynamically added destination IPv6 blacklist entries, use the **reset blacklist ipv6** command.

A destination blacklist entry with an aging time is not saved to the configuration file and cannot survive a reboot.

You can use the **display blacklist destination-ipv6** command to display all effective destination IPv6 blacklist entries.

Examples

Add a destination blacklist entry for IPv6 address 2012::12:25 and set the aging time to 10 minutes for the entry.

```
<Sysname> system-view
[Sysname] blacklist ipv6 2012::12:25 timeout 10
```

Related commands

blacklist enable

blacklist global enable

blacklist destination-ipv6

blacklist enable

Use **blacklist enable** to enable the blacklist feature on a security zone.

Use **undo blacklist enable** to disable the blacklist feature on a security zone.

Syntax

blacklist enable

undo blacklist enable

Default

The blacklist feature is disabled on a security zone.

Views

Security zone view

Predefined user roles

network-admin

context-admin

Usage guidelines

If the global blacklist feature is enabled, the blacklist feature is enabled on all security zones. If the global blacklist feature is disabled, you can use this command to enable blacklist on individual security zones.

Examples

Enable the blacklist feature on security zone **Untrust**.

```
<Sysname> system-view
[Sysname] security-zone name untrust
[Sysname-security-zone-Untrust] blacklist enable
```

Related commands

blacklist ip

blacklist ipv6

blacklist global enable

Use **blacklist global enable** to enable the global blacklist feature.

Use **undo blacklist global enable** to disable the global blacklist feature.

Syntax

blacklist global enable

undo blacklist global enable

Default

The global blacklist feature is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

If you enable the global blacklist feature, the blacklist feature is enabled on all security zones.

Examples

Enable the global blacklist feature.

```
<Sysname> system-view
[Sysname] blacklist global enable
```

Related commands

blacklist enable

blacklist ip

blacklist ip

Use **blacklist ip** to add a source IPv4 blacklist entry.

Use **undo blacklist ip** to delete a source IPv4 blacklist entry.

Syntax

blacklist ip *source-ip-address* [**vpn-instance** *vpn-instance-name*] [**ds-lite-peer** *ds-lite-peer-address*] [**timeout** *minutes*]

undo blacklist ip *source-ip-address* [**vpn-instance** *vpn-instance-name*] [**ds-lite-peer** *ds-lite-peer-address*]

Default

No source IPv4 blacklist entries exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

source-ip-address: Specifies an IPv4 address for the source blacklist entry. Packets sourced from this address will be dropped.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the blacklist belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the blacklist is on the public network.

ds-lite-peer *ds-lite-peer-address*: Specifies the IPv6 address of the B4 element of the DS-Lite tunnel that transmits packets from the blacklisted IPv4 address.

timeout *minutes*: Specifies the aging time in minutes for the source blacklist entry, in the range of 1 to 10080. If you do not specify this option, the blacklist entry never ages out. You must delete it manually.

Usage guidelines

The **undo blacklist ip** command deletes only manually added source IPv4 blacklist entries. To delete dynamically added source IPv4 blacklist entries, use the **reset blacklist ip** command.

A source blacklist entry with an aging time is not saved to the configuration file and cannot survive a reboot.

You can use the **display blacklist ip** command to display all effective source IPv4 blacklist entries.

Examples

Add a source blacklist entry for IPv4 address 192.168.1.2 and set the aging time to 20 minutes for the entry.

```
<Sysname> system-view
[Sysname] blacklist ip 192.168.1.2 timeout 20
```

Related commands

blacklist enable

blacklist global enable

display blacklist ip

blacklist ipv6

Use **blacklist ipv6** to add a source IPv6 blacklist entry.

Use **undo blacklist ipv6** to delete a source IPv6 blacklist entry.

Syntax

blacklist ipv6 *source-ipv6-address* [**vpn-instance** *vpn-instance-name*] [**timeout** *minutes*]

undo blacklist ipv6 *source-ipv6-address* [**vpn-instance** *vpn-instance-name*]

Default

No source IPv6 blacklist entries exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

source-ipv6-address: Specifies an IPv6 address for the source blacklist entry. Packets sourced from this address will be dropped.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the blacklist belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the blacklist is on the public network.

timeout *minutes*: Specifies the aging time in minutes for the source blacklist entry, in the range of 1 to 10080. If you do not specify this option, the blacklist entry never ages out. You must delete it manually.

Usage guidelines

The **undo blacklist ipv6** command deletes only manually added source IPv6 blacklist entries. To delete dynamically added source IPv6 blacklist entries, use the **reset blacklist ipv6** command.

A source blacklist entry with an aging time is not saved to the configuration file and cannot survive a reboot.

You can use the **display blacklist ipv6** command to display all effective source IPv6 blacklist entries.

Examples

Add a source blacklist entry for IPv6 address 2012::12:25 and set the aging time to 10 minutes for the entry.

```
<Sysname> system-view
[Sysname] blacklist ipv6 2012::12:25 timeout 10
```

Related commands

blacklist enable

blacklist global enable

blacklist ip

blacklist logging enable

Use **blacklist logging enable** to enable logging for the blacklist feature.

Use **undo blacklist logging enable** to disable logging for the blacklist feature.

Syntax

blacklist logging enable

undo blacklist logging enable

Default

Logging is disabled for the blacklist feature.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

With logging enabled for the blacklist feature, the system outputs logs in the following situations:

- A blacklist entry is manually added.
- A blacklist entry is dynamically added by the scanning attack detection feature.
- A blacklist entry is manually deleted.
- A blacklist entry ages out.

A blacklist log records the following information:

- Source IP address of the blacklist entry.
- Remote IP address of the DS-Lite tunnel.
- VPN instance name.
- Reason for adding or deleting the blacklist entry.
- Aging time for the blacklist entry.

This command enables the attack detection and prevention module to log blacklist events and send log messages to the information center.

With the information center, you can set log message filtering and output rules, including output destinations.

The information center can output blacklist logs to any destinations except the console and the monitor terminal. If you configure the console or monitor terminal as an output destination, the output destination setting will not take effect.

To view blacklist logs stored on the device, use the **display logbuffer** command. Make sure you do not disable log output to the log buffer, which is enabled by default.

For more information about configuring the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Enable logging for the blacklist feature.

```
<Sysname> system-view
[Sysname] blacklist logging enable
```

Add 192.168.1.2 to the blacklist. A log is output for the adding event.

```
[Sysname] blacklist ip 192.168.100.12
%Mar 13 03:47:49:736 2013 Sysname BLS/5/BLS_ENTRY_ADD:SrcIPAddr(1003)=192.168.100.12;
DSLiteTunnelPeer(1040)=--; RcvVPNInstance(1041)=--; TTL(1051)=;
Reason(1052)=Configuration.
```

Delete 192.168.1.2 from the blacklist. A log is output for the deletion event.

```
[Sysname] undo blacklist ip 192.168.100.12
%Mar 13 03:49:52:737 2013 Sysname BLS/5/BLS_ENTRY_DEL:SrcIPAddr(1003)=192.168.100.12;
DSLiteTunnelPeer(1040)=--; RcvVPNInstance(1041)=--; Reason(1052)=Configuration.
```

Related commands

blacklist ip

blacklist ipv6

blacklist object-group

Use **blacklist object-group** to add an address object group to the blacklist.

Use **undo blacklist object-group** to restore the default.

Syntax

blacklist object-group *object-group-name*

undo blacklist object-group

Default

No address object group is on the blacklist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

object-group-name: Specifies an address object group by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

This command must be used together with the address object group feature. For more information about address object groups, see object group configuration in *Security Configuration Guide*.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Add address object group **object-group1** to the blacklist.

```
<Sysname> system-view
[Sysname] blacklist object-group object-group1
```

blacklist user

Use **blacklist user** to add a user blacklist entry.

Use **undo blacklist user** to delete a user blacklist entry.

Syntax

blacklist user *user-name* [**domain** *domain-name*] [**timeout** *minutes*]

undo blacklist user *user-name* [**domain** *domain-name*]

Default

No user blacklist entries exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

user-name: Specifies a user by the username, a case-sensitive string of 1 to 55 characters. Packets sourced from this user will be dropped.

domain *domain-name*: Specifies a user identification domain by its name, a case-insensitive string of 1 to 255 characters. The user identification domain name cannot include question marks (?). If you do not specify a user identification domain, the user does not belong to any user identification domain.

timeout *minutes*: Specifies the aging time for the blacklist entry, in the range of 1 to 1000 minutes. If you do not specify this option, the blacklist entry never ages out. You must delete it manually.

Usage guidelines

The user blacklist feature must be used together with the user identification feature. For more information about user identification, see "Configuring user identification."

Examples

Add a user blacklist entry for user **usera** and set the aging time to 20 minutes for the entry.

```
<Sysname> system-view
[Sysname] blacklist user usera timeout 20
```

Add a user blacklist entry for user **usera** in user identification domain **domaina** and set the aging time to 20 minutes for the entry.

```
<Sysname> system-view
[Sysname] blacklist user usera domain domaina timeout 20
```

Related commands

blacklist global enable

display blacklist user

client-verify dns enable

Use **client-verify dns enable** to enable DNS client verification on a security zone.

Use **undo client-verify dns enable** to disable DNS client verification on a security zone.

Syntax

client-verify dns enable

undo client-verify dns enable

Default

DNS client verification is disabled on a security zone.

Views

Security zone view

Predefined user roles

network-admin

context-admin

Usage guidelines

Enable DNS client verification on the security zone that is connected to the external network. This feature protects internal DNS servers against DNS flood attacks.

For the DNS client verification to collaborate with DNS flood attack prevention, specify **client-verify** as the DNS flood attack prevention action. During collaboration, the device adds the victim IP address to the protected IP list and verifies the untrusted sources if it detects a DNS flood attack. You can use the **display client-verify dns protected ip** command to display the protected IP list for DNS client verification.

Examples

Enable DNS client verification on security zone **DMZ**.

```
<Sysname> system-view
[Sysname] security-zone name DMZ
[Sysname-security-zone-DMZ] client-verify dns enable
```

Related commands

client-verify dns protected ip

display client-verify dns protected ip

client-verify dns-reply enable

Use **client-verify dns-reply enable** to enable DNS response verification on a security zone.

Use **undo client-verify dns-reply enable** to disable DNS response verification on a security zone.

Syntax

client-verify dns-reply enable

undo client-verify dns-reply enable

Default

DNS response verification is disabled on a security zone.

Views

Security zone view

Predefined user roles

network-admin

context-admin

Usage guidelines

Enable DNS response verification on the security zone that is connected to the external network. This feature protects internal DNS clients against DNS response flood attacks.

For the DNS response verification to collaborate with DNS response flood attack prevention, specify **client-verify** as the DNS response flood attack prevention action. During collaboration, the device adds the victim IP address to the protected IP list and verifies the untrusted servers if it detects a DNS response flood attack. You can use the **display client-verify dns-reply protected ip** command to display the protected IP list for DNS response verification.

Examples

Enable DNS response verification on security zone **DMZ**.

```
<Sysname> system-view
[Sysname] security-zone name dmz
[Sysname-security-zone-DMZ] client-verify dns-reply enable
```

Related commands

client-verify dns-reply protected ip

display client-verify dns-reply protected ip

client-verify http enable

Use **client-verify http enable** to enable HTTP client verification on a security zone.

Use **undo client-verify http enable** to disable HTTP client verification on a security zone.

Syntax

client-verify http enable

undo client-verify http enable

Default

HTTP client verification is disabled on a security zone.

Views

Security zone view

Predefined user roles

network-admin

context-admin

Usage guidelines

Enable HTTP client verification on the security zone that is connected to the external network. This feature protects internal servers against HTTP flood attacks.

For the HTTP client verification to collaborate with HTTP flood attack prevention, specify **client-verify** as the HTTP flood attack prevention action. During collaboration, the device adds the victim IP address to the protected IP list and verifies the untrusted sources if it detects an HTTP flood attack. You can use the **display client-verify http protected ip** command to display the protected IP list for HTTP client verification.

Examples

Enable HTTP client verification on security zone **DMZ**.

```
<Sysname> system-view
[Sysname] security-zone name DMZ
[Sysname- security-zone-DMZ] client-verify http enable
```

Related commands

client-verify http protected ip

display client-verify http protected ip

client-verify sip enable

Use **client-verify sip enable** to enable SIP client verification on a security zone.

Use **undo client-verify sip enable** to disable SIP client verification on a security zone.

Syntax

client-verify sip enable

undo client-verify sip enable

Default

SIP client verification is disabled on a security zone.

Views

Security zone view

Predefined user roles

network-admin

context-admin

Usage guidelines

Enable SIP client verification on the security zone that is connected to the external network. This feature protects internal servers against SIP flood attacks.

For the SIP client verification to collaborate with SIP flood attack prevention, specify **client-verify** as the SIP flood attack prevention action. During collaboration, the device adds the victim IP address to the protected IP list and verifies the untrusted sources if it detects an SIP flood attack. You can use the **display client-verify sip protected ip** command to display the protected IP list for SIP client verification.

Examples

Enable SIP client verification on security zone **DMZ**.

```
<Sysname> system-view
[Sysname] security-zone name DMZ
[Sysname-security-zone-DMZ] client-verify sip enable
```

Related commands

client-verify sip protected ip

display client-verify sip protected ip

client-verify protected ip

Use **client-verify protected ip** to specify an IPv4 address to be protected by the client verification feature.

Use **undo client-verify protected ip** to remove an IPv4 address protected by the client verification feature.

Syntax

client-verify { **dns** | **dns-reply** | **http** | **sip** | **tcp** } **protected ip** *destination-ip-address* [**vpn-instance** *vpn-instance-name*] [**port** *port-number*]

undo client-verify { **dns** | **dns-reply** | **http** | **sip** | **tcp** } **protected ip** *destination-ip-address* [**vpn-instance** *vpn-instance-name*] [**port** *port-number*]

Default

The client verification feature does not protect any IPv4 addresses.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

dns: Specifies the DNS client verification feature.

dns-reply: Specifies the DNS response verification feature.

http: Specifies the HTTP client verification feature.

sip: Specifies the SIP client verification feature.

tcp: Specifies the TCP client verification feature.

destination-ip-address: Specifies the IPv4 address to be protected. All connection requests destined for this address are verified by the client verification feature.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the specified IPv4 address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the IPv4 address is on the public network.

port *port-number*: Specifies the port to be protected, in the range of 1 to 65535. If you do not specify this option, the verification feature protects ports for different protocols as follows:

- DNS client or DNS response verification protects port 53.
- HTTP client verification protects port 80.
- SIP client verification protects port 5060.
- TCP client verification protects all ports.

Usage guidelines

You can specify multiple protected IP addresses by using this command multiple times.

Examples

Configure TCP client verification to protect IPv4 address 2.2.2.5 and port 25.

```
<Sysname> system-view
[Sysname] client-verify tcp protected ip 2.2.2.5 port 25
```

Configure DNS client verification to protect IPv4 address 2.2.2.5 and port 50.

```
<Sysname> system-view
[Sysname] client-verify dns protected ip 2.2.2.5 port 50
```

Related commands

display client-verify protected ip

client-verify protected ipv6

Use **client-verify protected ipv6** to specify an IPv6 address to be protected by the client verification feature.

Use **undo client-verify protected ipv6** to remove an IPv6 address protected by the client verification feature.

Syntax

client-verify { **dns** | **dns-reply** | **http** | **sip** | **tcp** } **protected ipv6** *destination-ipv6-address* [**vpn-instance** *vpn-instance-name*] [**port** *port-number*]

undo client-verify { **dns** | **dns-reply** | **http** | **sip** | **tcp** } **protected ipv6** *destination-ipv6-address* [**vpn-instance** *vpn-instance-name*] [**port** *port-number*]

Default

The client verification feature does not protect any IPv6 addresses.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

dns: Specifies the DNS client verification feature.

dns-reply: Specifies the DNS response verification feature.

http: Specifies the HTTP client verification feature.

sip: Specifies the SIP client verification feature.

tcp: Specifies the TCP client verification feature.

destination-ipv6-address: Specifies the IPv6 address to be protected. All connection requests destined for this address are verified by the client verification feature.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the specified IPv6 address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the IPv6 address is on the public network.

port *port-number*: Specifies the port to be protected, in the range of 1 to 65535. If you do not specify this option, the verification feature for different protocols protects ports as follows:

- DNS client or DNS response verification protects port 53.
- HTTP client verification protects port 80.
- SIP client verification protects port 5060.
- TCP client verification protects all ports.

Usage guidelines

You can specify multiple protected IPv6 addresses by using this command multiple times.

Examples

Configure TCP client verification to protect IPv6 address 2013::12 and port 23.

```
<Sysname> system-view
```

```
[Sysname] client-verify tcp protected ipv6 2013::12 port 23
```

Configure HTTP client verification to protect IPv6 address 2013::12.

```
<Sysname> system-view
[Sysname] client-verify http protected ipv6 2013::12
```

Related commands

display client-verify protected ipv6

client-verify tcp enable

Use **client-verify tcp enable** to enable TCP client verification on a security zone.

Use **undo client-verify tcp enable** to disable TCP client verification on a security zone.

Syntax

client-verify tcp enable [**mode** { **syn-cookie** | **safe-reset** }]

undo client-verify tcp enable

Default

TCP client verification is disabled on a security zone.

Views

Security zone view

Predefined user roles

network-admin

context-admin

Parameters

mode: Specifies a working mode for TCP client verification. If you do not specify this keyword, the SYN cookie mode is used.

syn-cookie: Specifies the SYN cookie mode. In this mode, bidirectional TCP proxy is enabled.

safe-reset: Specifies the safe reset mode. In this mode, unidirectional TCP proxy is enabled.

Usage guidelines

Enable TCP client verification on the security zone that is connected to the external network. This feature protects internal servers against TCP flood attacks, including SYN flood attacks, SYN-ACK flood attacks, RST flood attacks, FIN flood attacks, and ACK flood attacks.

For TCP client verification to collaborate with TCP flood attack prevention, specify **client-verify** as the TCP flood attack prevention action. During collaboration, the device adds the victim IP address to the protected IP list and verifies the untrusted sources if it detects a TCP flood attack. You can use the **display client-verify tcp protected ip** command to display the protected IP list for TCP client verification.

TCP client verification supports the following modes:

- **Safe reset**—Enables unidirectional TCP proxy for packets only from TCP connection initiators.
- **SYN cookie**—Enables bidirectional TCP proxy for packets from both TCP clients and TCP servers.

Choose a TCP proxy mode according to the network scenarios. If packets from clients pass through the TCP proxy device, but packets from servers do not, specify the safe reset mode. If packets from clients and servers both pass through the TCP proxy device, specify either safe reset or SYN cookie. TCP proxy must be enabled on input security zones. Otherwise, TCP connections cannot be established correctly.

Examples

Enable TCP client verification in safe reset mode on security zone **DMZ**.

```
<Sysname> system-view
[Sysname] security-zone name DMZ
[Sysname-security-zone-DMZ] client-verify tcp enable mode safe-reset
```

Related commands

client-verify tcp protected ip

display client-verify tcp protected ip

display attack-defense cpu-core flow info

Use **display attack-defense cpu-core flow info** to display the attack flow information for CPU cores.

Syntax

display attack-defense cpu-core flow info slot *slot-number*

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX5-HD6480	Yes
NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB680, NFNX3-HDB1080	No

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID.

Examples

Display the attack flow information for the CPU cores on CPU 1 in slot 2.

```
<Sysname> display attack-defense cpu-core flow info slot 2 cpu 1
Hardware Buffer Full: Yes
TimeStamp: 2018-09-19 08:59:07
CPU ID: 10
SMAC: 02:1c:2b:3c:4d:5f DMAC: 0a:bc:2c:3d:4f:5e
VLAN ID: 0 Interface: GiabitEthernet1/0/1
SIP: 1.1.1.1 DIP: 2.2.2.2
Pro: 17
SPort: 1223 DPort: 2668
CPU Usage: 60% IfIsolate: true

SMAC: 03:11:22:33:44:55 DMAC: 04:aa:bb:cc:dd:5e
```

```
VLAN ID: 0 Interface: GiabitEthernet1/0/1
SIP: 1::1 DIP: 2::2
Pro: 132
CPU Usage: 40% IfIsolate: false

TimeStamp: 2018-09-19 08:59:07
CPU ID: 12
SMAC: 02:1c:2b:3c:4d:5f DMAC: 0a:bc:2c:3d:4f:5e
VLAN ID: 0 Interface: GiabitEthernet1/0/1
SIP: 1.1.1.1 DIP: 2.2.2.2
Pro: 17
SPort: 1223 DPort: 2668
CPU Usage: 70% IfIsolate: false

SMAC: 03:11:22:33:44:55 DMAC: 04:aa:bb:cc:dd:5e
VLAN ID: 0 Interface: GiabitEthernet1/0/1
SIP: 1::1 DIP: 2::2
Pro: 132
CPU Usage: 30% IfIsolate: false
```

Table 1 Command output

Field	Description
Hardware Buffer Full	Whether the shared hardware queue of the driver is full. • **Yes**. • **No**.
TimeStamp	Time when information collection finishes.
CPU ID	ID of the CPU core to which the flow was sent.
SMAC	Source MAC address of the attack flow.
DMAC	Destination MAC address of the attack flow.
VLAN ID	ID of the VLAN to which the attack flow belongs.
Interface	Ingress interface of the attack flow.
SIP	Source IP address of the attack flow.
DIP	Destination IP address of the attack flow.
Pro	Protocol type of the attack flow.
SPort	Source port of the attack flow. This field is available only when the protocol type is TCP or UDP.
DPort	Destination port of the attack flow. This field is available only when the protocol type is TCP or UDP.
CPU Usage	Percentage of the CPU time used by the attack flow.
IfIsolate	Whether the isolation entry has been deployed to the hardware successfully. • **True**—Deployment succeeded. • **False**—Deployment failed.

Related commands

attack-defense cpu-core action

display attack-defense flood statistics ip

Use **display attack-defense flood statistics ip** to display IPv4 flood attack detection and prevention statistics.

Syntax

display attack-defense { **ack-flood** | **dns-flood** | **dns-reply-flood** | **fin-flood** | **flood** | **icmp-flood** | **rst-flood** | **sip-flood** | **syn-flood** | **syn-ack-flood** | **udp-flood** } **statistics ip** [*ip-address* [**vpn** *vpn-instance-name*]] [**security-zone** *zone-name*] [**slot** *slot-number*] [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ack-flood: Specifies ACK flood attack.

dns-flood: Specifies DNS flood attack.

dns-reply-flood: Specifies DNS response flood attack.

fin-flood: Specifies FIN flood attack.

flood: Specifies all IPv4 flood attacks.

http-flood: Specifies HTTP flood attack.

icmp-flood: Specifies ICMP flood attack.

rst-flood: Specifies RST flood attack.

sip-flood: Specifies SIP flood attack.

syn-ack-flood: Specifies SYN-ACK flood attack.

syn-flood: Specifies SYN flood attack.

udp-flood: Specifies UDP flood attack.

ip-address: Specifies a protected IPv4 address. If you do not specify an IPv4 address, this command displays flood attack detection and prevention statistics for all protected IPv4 addresses.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the protected IPv4 address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the protected IPv4 address is on the public network.

security-zone *zone-name*: Specifies a security zone by its name. The *zone-name* argument is a case-insensitive string of 1 to 31 characters. It cannot contain hyphens (-).

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv4 flood attack detection and prevention statistics for all member devices.

count: Displays the number of flood attack prevention entries.

Usage guidelines

The device collects statistics about protected IP addresses for flood attack detection and prevention. The attackers' IP addresses are not recorded.

Examples

Display all IPv4 flood attack detection and prevention statistics.

```
<Sysname> display attack-defense flood statistics ip
Slot 1:
Dest IP         VPN         Detected on  Detect type   State    PPS    Dropped
201.55.7.45     --          Trust1       SYN-ACK-FLOOD Normal   1000   111111111
192.168.11.5    --          Trust2       ACK-FLOOD     Normal   1000   222222222
Src IP          VPN         Detected on  Detect type   State    PPS    Dropped
10.118.21.14    --          Trust4       SIP-FLOOD     Normal   1000   265387945
Slot 2:
Dest IP         VPN         Detected on  Detect type   State    PPS    Dropped
IP address      VPN         Detected on  Detect type   State    PPS    Dropped
201.55.1.10     --          Trust1       ACK-FLOOD     Normal   1000   222222222
Src IP          VPN         Detected on  Detect type   State    PPS    Dropped
192.168.100.30  --          Trust3       DNS-FLOOD     Normal   1000   333333333
192.168.100.66  --          Trust4       SYN-ACK-FLOOD Normal   1000   165467998
```

Display the number of flood attack prevention entries.

```
<Sysname> display attack-defense flood statistics ip count
Slot 1:
Totally 2 flood destination entries.
Totally 1 flood source entries.
Slot 2:
Totally 1 flood destination entries.
Totally 2 flood source entries.
```

Table 2 Command output

Field	Description
Dest IP	Destination IPv4 address in attack packets.
Src IP	Source IPv4 address in attack packets.
VPN	MPLS L3VPN instance to which the protected IPv4 address belongs. If the protected IPv4 address is on the public network, this field displays hyphens (--).
Detected on	Name of the security zone where the attack is detected.
Detect type	Type of the detected flood attack: • ACK flood. • DNS flood. • DNS reply flood. • FIN flood. • ICMP flood. • ICMPv6 flood.

Field	Description
	• SYN flood. • SYN-ACK flood. • UDP flood. • RST flood. • HTTP flood. • SIP flood.
State	Whether the security zone is attacked: • **Attacked**. • **Normal**.
PPS	Number of packets sent to the IPv4 address per second.
Dropped	Number of attack packets dropped by the security zone.
Totally 2 flood destination entries	Total number of IPv4 destination-based flood attack prevention entries.
Totally 2 flood source entries	Total number of IPv4 source-based flood attack prevention entries.

display attack-defense flood statistics ipv6

Use **display attack-defense flood statistics ipv6** to display IPv6 flood attack detection and prevention statistics.

Syntax

display attack-defense { **ack-flood** | **dns-flood** | **dns-reply-flood** | **fin-flood** |**flood** | **http-flood** | **icmpv6-flood** | **rst-flood** | **sip-flood** | **syn-flood** | **syn-ack-flood** | **udp-flood** } **statistics ipv6** [*ipv6-address* [**vpn** *vpn-instance-name*]] [**security-zone** *zone-name*] [**slot** *slot-number*] [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ack-flood: Specifies ACK flood attack.

dns-flood: Specifies DNS flood attack.

dns-reply-flood: Specifies DNS response flood attack.

fin-flood: Specifies FIN flood attack.

flood: Specifies all IPv6 flood attacks.

http-flood: Specifies HTTP flood attack.

icmpv6-flood: Specifies ICMPv6 flood attack.

rst-flood: Specifies RST flood attack.

sip-flood: Specifies SIP flood attack.

syn-ack-flood: Specifies SYN-ACK flood attack.

syn-flood: Specifies SYN flood attack.

udp-flood: Specifies UDP flood attack.

ipv6-address: Specifies a protected IPv6 address. If you do not specify an IPv6 address, this command displays flood attack detection and prevention statistics for all protected IPv6 addresses.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the protected IPv6 address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the protected IPv6 address is on the public network.

security-zone *zone-name*: Specifies a security zone by its name. The *zone-name* argument is a case-insensitive string of 1 to 31 characters. It cannot contain hyphens (-).

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv6 flood attack detection and prevention statistics for all member devices.

count: Displays the number of flood attack prevention entries.

Usage guidelines

The device collects statistics about protected IP addresses for flood attack detection and prevention. The attackers' IP addresses are not recorded.

Examples

Display all IPv6 flood attack detection and prevention statistics.

```
<Sysname> display attack-defense flood statistics ipv6
Slot 1:
Dest IPv6       VPN         Detected on  Detect type   State    PPS    Dropped
1::2            --          Trust1       DNS-FLOOD     Normal   1000   111111111
1::3            --          Trust2       SYN-ACK-FLOOD Normal   1000   222222222
Src IPv6        VPN         Detected on  Detect type   State    PPS    Dropped
17::14          --          Trust4       SIP-FLOOD     Normal   1000   266649789
Slot 2:
Dest IPv6       VPN         Detected on  Detect type   State    PPS    Dropped
1::2            --          Trust1       SYN-FLOOD     Normal   1000   468792363
1::5            --          Trust2       ACK-FLOOD     Normal   1000   452213396
Src IPv6        VPN         Detected on  Detect type   State    PPS    Dropped
1::6            --          Trust4       DNS-FLOOD     Normal   1000   12569985
```

Display the number of flood attack prevention entries.

```
<Sysname> display attack-defense flood statistics ipv6 count
Slot 1:
Totally 1 flood destination entries.
Totally 2 flood source entries
Slot 2:
Totally 2 flood destination entries.
Totally 1 flood source entries
```

Table 3 Command output

Field	Description
Dest IPv6	Destination IPv6 address in attack packets.

Field	Description
Src IPv6	Source IPv6 address in attack packets.
VPN	MPLS L3VPN instance to which the protected IPv6 address belongs. If the protected IPv6 address is on the public network, this field displays hyphens (--).
Detected on	Name of the security zone where the attack is detected.
Detect type	Type of the detected flood attack: • ACK flood. • DNS flood. • DNS reply flood. • FIN flood. • ICMPv6 flood. • SYN flood. • SYN-ACK flood. • UDP flood. • RST flood. • HTTP flood. • SIP flood.
State	Whether the security zone is attacked: • **Attacked**. • **Normal**.
PPS	Number of packets sent to the IPv6 address per second.
Dropped	Number of attack packets dropped by the security zone.
Totally 2 flood destination entries	Total number of IPv6 destination-based flood attack prevention entries.
Totally 2 flood source entries	Total number of IPv6 source-based flood attack prevention entries.

display attack-defense http-slow-attack statistics ip

Use **display attack-defense http-slow-attack statistics ip** to display statistics about IPv4 HTTP slow attack detection and prevention.

Syntax

display attack-defense http-slow-attack statistics ip [*ip-address* [**vpn-instance** *vpn-instance-name*]] [[**interface** { *interface-type interface-number* | *interface-name* } | **local**] [**slot** *slot-number*]] [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ip-address: Specifies a destination IPv4 address.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the destination IPv4 address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the destination IPv4 address is on the public network.

interface { *interface-type interface-number* | *interface-name* }: Specifies an interface. The *interface-type* argument specifies the interface type. The *interface-number* argument specifies the interface number, and the *interface-name* argument specifies the interface name.

local: Specifies the local device.

slot *slot-number*: Specifies an IRF member device by its member ID. This option is available only when you specify the local device or a global interface, such as a VLAN interface or tunnel interface. If you do not specify a member device, this command displays statistics about IPv4 HTTP slow attack detection and prevention for all member devices.

count: Displays the number of IPv4 HTTP slow attack prevention entries for matching protected IPv4 addresses.

Usage guidelines

If you do not specify the **interface** or **local** parameter, this command displays statistics about IPv4 HTTP slow attack detection and prevention for all interfaces and the local device.

Examples

Display statistics about IPv4 HTTP slow attack detection and prevention.

```
<Sysname> display attack-defense http-slow-attack statistics ip
Slot 1:
IP address       VPN              Detected on          State
192.168.11.4     asd              Local                Normal
201.55.7.44      --               GE1/0/2              Normal
Slot 2:
IP address       VPN              Detected on          State
192.168.11.4     asd              Local                Normal
201.55.7.44      --               GE1/0/2              Normal
```

Display the number of IPv4 HTTP slow attack prevention entries for protected IPv4 addresses.

```
<Sysname> display attack-defense http-slow-attack statistics ip count
Slot 1:
Totally 2 HTTP slow attack entries.
Slot 2:
Totally 1 HTTP slow attack entries.
```

Display the number of IPv4 HTTP slow attack prevention entries for protected IPv4 addresses.

```
<Sysname> display attack-defense http-slow-attack statistics ip count
Slot 1:
Totally 2 HTTP slow attack entries.
Slot 2:
Totally 3 HTTP slow attack entries.
```

Table 4 Command output

Field	Description
IP address	Destination IPv4 address.
VPN	MPLS L3VPN instance to which the destination IPv6 address belongs. If the destination IPv6 address is on the public network, this field displays hyphens (**--**).
Detected on	Where the attack is detected: the device (**Local**) or an interface.
State	Whether the interface or device is attacked: • **Attacked**—It is being attacked. • **Normal**—It is not attacked.
Totally 2 http slow attack entries	Total number of IPv4 HTTP slow attack prevention entries.

display attack-defense http-slow-attack statistics ip

Use **display attack-defense http-slow-attack statistics ip** to display statistics about IPv4 HTTP slow attack detection and prevention.

Syntax

display attack-defense http-slow-attack statistics ip [*ip-address* [**vpn-instance** *vpn-instance-name*]] [**security-zone** *zone-name*] [**slot** *slot-number*] [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ip-address: Specifies a destination IPv4 address.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the destination IPv4 address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the destination IPv4 address is on the public network.

security-zone *zone-name*: Specifies a security zone by its name. The *zone-name* argument is a case-insensitive string of 1 to 31 characters. It cannot contain hyphens (-).

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays statistics about IPv4 HTTP slow attack detection and prevention for all member devices.

count: Displays the number of IPv4 HTTP slow attack prevention entries for matching protected IPv4 addresses.

Examples

Display statistics about IPv4 HTTP slow attack detection and prevention.

```
<Sysname> display attack-defense http-slow-attack statistics ip
```

```
Slot 1:
IP address       VPN             Detected on          State
192.168.11.4     asd             Trust1               Normal
201.55.7.44      --              Trust4               Normal
Slot 2:
IP address       VPN             Detected on          State
192.168.11.4     asd             Trust1               Normal
201.55.7.44      --              Trust4               Normal
```

Display the number of IPv4 HTTP slow attack prevention entries for protected IPv4 addresses.

```
<Sysname> display attack-defense http-slow-attack statistics ip count
Slot 1:
Totally 2 HTTP slow attack entries.
Slot 2:
Totally 1 HTTP slow attack entries.
```

Table 5 Command output

Field	Description
IP address	Destination IPv4 address.
VPN	MPLS L3VPN instance to which the destination IPv6 address belongs. If the destination IPv6 address is on the public network, this field displays hyphens (--).
Detected on	Name of the security zone where the attack is detected.
State	Whether the security zone is attacked: • **Attacked**—It is being attacked. • **Normal**—It is not attacked.
Totally 2 HTTP slow attack entries	Total number of IPv4 HTTP slow attack prevention entries.

display attack-defense http-slow-attack statistics ipv6

Use **display attack-defense http-slow-attack statistics ipv6** to display statistics about IPv6 HTTP slow attack detection and prevention.

Syntax

display attack-defense http-slow-attack statistics ipv6 [*ipv6-address* [**vpn-instance** *vpn-instance-name*]] [[**interface** { *interface-type interface-number* | *interface-name* } | **local**] [**slot** *slot-number*]] [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ipv6-address: Specifies a destination IPv6 address.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the destination IPv6 address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the destination IPv6 address is on the public network.

interface { *interface-type interface-number* | *interface-name* }: Specifies an interface. The *interface-type* argument specifies the interface type. The *interface-number* argument specifies the interface number, and the *interface-name* argument specifies the interface name.

local: Specifies the local device.

slot *slot-number*: Specifies an IRF member device by its member ID. This option is available only when you specify the local device or a global interface, such as a VLAN interface or tunnel interface. If you do not specify a member device, this command displays statistics about IPv6 HTTP slow attack detection and prevention for all member devices.

count: Displays the number of IPv6 HTTP slow attack prevention entries for matching protected IPv6 addresses.

Usage guidelines

If you do not specify the **interface** or **local** parameter, this command displays statistics about IPv6 HTTP slow attack detection and prevention for all interfaces and the local device.

Examples

Display statistics about IPv6 HTTP slow attack detection and prevention.

```
<Sysname> display attack-defense http-slow-attack statistics ipv6
Slot 1:
IPv6 address     VPN             Detected on          State
1::5             asd             Local                Normal
17::14           --              GE1/0/2              Normal
Slot 2:
IPv6 address     VPN             Detected on          State
1::5             asd             Local                Normal
17::14           --              GE1/0/2              Normal
```

Display the number of IPv6 HTTP slow attack prevention entries for protected IPv6 addresses.

```
<Sysname> display attack-defense http-slow-attack statistics ipv6 count
Slot 1:
Totally 5 HTTP slow attack entries.
Slot 2:
Totally 3 HTTP slow attack entries.
```

Table 6 Command output

Field	Description
IPv6 address	Destination IPv6 address.
VPN	MPLS L3VPN instance to which the destination IPv6 address belongs. If the destination IPv6 address is on the public network, this field displays hyphens (--).
Detected on	Where the attack is detected: the device (**Local**) or an interface.

Field	Description
State	Whether the interface or local device is attacked: • **Attacked**—It is being attacked. • **Normal**—It is not attacked.
Totally 2 HTTP slow attack entries	Total number of IPv6 HTTP slow attack prevention entries.

display attack-defense http-slow-attack statistics ipv6

Use **display attack-defense http-slow-attack statistics ipv6** to display statistics about IPv6 HTTP slow attack detection and prevention.

Syntax

display attack-defense http-slow-attack statistics ipv6 [*ipv6-address* [**vpn-instance** *vpn-instance-name*]] [**security-zone** *zone-name*] [**slot** *slot-number*] [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ipv6-address: Specifies a destination IPv6 address.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the destination IPv6 address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the destination IPv6 address is on the public network.

security-zone *zone-name*: Specifies a security zone by its name. The *zone-name* argument is a case-insensitive string of 1 to 31 characters. It cannot contain hyphens (-).

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays statistics about IPv6 HTTP slow attack detection and prevention for all member devices.

count: Displays the number of IPv6 HTTP slow attack prevention entries for matching protected IPv6 addresses.

Examples

Display statistics about IPv6 HTTP slow attack detection and prevention.

```
<Sysname> display attack-defense http-slow-attack statistics ipv6
Slot 1:
IPv6 address     VPN             Detected on          State
2000::1011       asd             Trust1               Normal
1::4             --              Trust4               Normal
Slot 2:
IPv6 address     VPN             Detected on          State
```

```
2000::1011       asd             Trust1               Normal
1::4             --              Trust4               Normal
```

Display the number of IPv6 HTTP slow attack prevention entries for protected IPv6 addresses.

```
<Sysname> display attack-defense http-slow-attack statistics ipv6 count
Slot 1:
Totally 5 HTTP slow attack entries.
Slot 2:
Totally 3 HTTP slow attack entries.
```

Table 7 Command output

Field	Description
IPv6 address	Destination IPv6 address.
VPN	MPLS L3VPN instance to which the destination IPv6 address belongs. If the destination IPv6 address is on the public network, this field displays hyphens (--).
Detected on	Name of the security zone where the attack is detected.
State	Whether the security zone is attacked: • **Attacked**. • **Normal**.
Totally 5 HTTP slow attack entries	Total number of IPv6 HTTP slow attack prevention entries.

display attack-defense malformed-packet statistics

Use **display attack-defense malformed-packet statistics** to display statistics about malformed packets.

Syntax

display attack-defense malformed-packet statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays statistics about malformed packets for all member devices.

Examples

Display statistics about malformed packets.

```
<Sysname> display attack-defense malformed-packet statistics
Slot 1:
Malformed packets dropped: 10000
Slot 2:
```

```
Malformed packets dropped: 1000
```

Table 8 Command output

Field	Description
Malformed packets dropped	Number of dropped malformed packets.

Related commands

`reset attack-defense malformed-packet statistics`

display attack-defense policy

Use **`display attack-defense policy`** to display attack defense policy configuration.

Syntax

`display attack-defense policy` [*`policy-name`*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

`policy-name`: Specifies an attack defense policy by its name. The policy name is a case-insensitive string of 1 to 31 characters. Valid characters include uppercase and lowercase letters, digits, underscores (_), and hyphens (-). If no attack defense policy is specified, this command displays brief information about all attack defense policies.

Usage guidelines

This command output includes the following configuration information about an attack defense policy:

- Whether attack detection is enabled.
- Attack prevention actions.
- Attack prevention trigger thresholds.

Examples

Display the configuration of attack defense policy **abc**.

```
<Sysname> display attack-defense policy abc
          Attack-defense Policy Information
------------------------------------------------------------------------
Policy name                       : abc
Applied list                      : Trust
------------------------------------------------------------------------
Exempt IPv4 ACL:                 : Not configured
Exempt IPv6 ACL:                 : vip
------------------------------------------------------------------------
  Actions: CV-Client verify  BS-Block source  L-Logging  D-Drop  N-None
```

Signature attack defense configuration:

Signature name	Defense	Level	Actions
Fragment	Enabled	Info	L
Impossible	Enabled	Info	L
Teardrop	Disabled	Info	L
Tiny fragment	Disabled	Info	L
IP option abnormal	Disabled	Info	L
Smurf	Disabled	Info	N
Traceroute	Disabled	Medium	L,D
Ping of death	Disabled	Low	L
Large ICMP	Disabled	Medium	L,D
Max length	4000 bytes		
Large ICMPv6	Disabled	Low	L
Max length	4000 bytes		
TCP invalid flags	Disabled	medium	L,D
TCP null flag	Disabled	Low	L
TCP all flags	Enabled	Info	L
TCP SYN-FIN flags	Disabled	Info	L
TCP FIN only flag	Enabled	Info	L
TCP Land	Disabled	Info	L
Winnuke	Disabled	Info	L
UDP Bomb	Disabled	Info	L
UDP Snork	Disabled	Info	L
UDP Fraggle	Enabled	Info	L
IP option record route	Disabled	Info	L
IP option internet timestamp	Enabled	Info	L
IP option security	Disabled	Info	L
IP option loose source routing	Enabled	Info	L
IP option stream ID	Disabled	Info	L
IP option strict source routing	Disabled	Info	L
IP option route alert	Disabled	Info	L
ICMP echo request	Disabled	Info	L
ICMP echo reply	Disabled	Info	L
ICMP source quench	Disabled	Info	L
ICMP destination unreachable	Enabled	Info	L
ICMP redirect	Enabled	Info	L
ICMP time exceeded	Enabled	Info	L
ICMP parameter problem	Disabled	Info	L
ICMP timestamp request	Disabled	Info	L
ICMP timestamp reply	Disabled	Info	L
ICMP information request	Disabled	Info	L
ICMP information reply	Disabled	Medium	L,D
ICMP address mask request	Disabled	Medium	L,D
ICMP address mask reply	Disabled	Medium	L,D
ICMPv6 echo request	Enabled	Medium	L,D
ICMPv6 echo reply	Disabled	Medium	L,D
ICMPv6 group membership query	Disabled	Medium	L,D

```
ICMPv6 group membership report     Disabled     Medium           L,D
ICMPv6 group membership reduction  Disabled     Medium           L,D
ICMPv6 destination unreachable     Enabled      Medium           L,D
ICMPv6 time exceeded               Enabled      Medium           L,D
ICMPv6 parameter problem           Disabled     Medium           L,D
ICMPv6 packet too big              Disabled     Medium           L,D
IPv6 extension header abnormal     Disabled     Info             L
IPv6 extension header exceeded     Disabled     Info             L
  Limit                            7
```

```
Scan attack defense configuration:
  Preset defense:
  Defense: Disabled
  User-defined defense:
    Port scan defense: Enabled
    Port scan defense threshold: 5000 packets
    IP sweep defense: Enabled
    IP sweep defense threshold: 8000 packets
    Period: 100s
    Actions: L
```

```
Flood type  Global dest/src thres(pps)  Global actions Service ports  Non-specific
DNS flood         1000/1000             -              53             Disabled
DNS reply flood   1000/1000             -              -              Disabled
HTTP flood        1000/1000             80             -              Disabled
SIP flood         1000/1000             50             -              Enabled
SYN flood         1000/1000             -              -              Disabled
ACK flood         1000/1000             -              -              Disabled
SYN-ACK flood     1000/1000             -              -              Disabled
RST flood         1000/1000             -              -              Disabled
FIN flood         1000/1000             -              -              Disabled
UDP flood         1000/1000             -              -              Disabled
ICMP flood        1000/1000             -              -              Disabled
ICMPv6 flood      1000/1000             -              -              Enabled
```

```
Flood attack defense for protected IP addresses:
 Address                 VPN instance Flood type    Thres(pps)  Actions Ports
 1::1                    --           FIN-FLOOD     10          L,D     -
 192.168.1.1             --           SYN-ACK-FLOOD 10          -       -
 1::1                    --           FIN-FLOOD     -           L       -
 2013:2013:2013:2013:    --           DNS-FLOOD     100         L,CV    53
 2013:2013:2013:2013
 10::13:                 A0123458589  SIP-FLOOD     100         L,CV    5060
```

```
HTTP slow attack defense configuration:
  Non-specific: Enabled
  Global threshold:
    Alert-number: 1200000
```

```
    Content-length: 100000000
    Payload-length: 1000
    Packet-number: 1000
  Global period: 1200 seconds
  Global action: L, BS (1000)
  Ports: 80, 8000 to 8001

Threshold: AN-Alert number, CL-Content length, PL-Payload length, PN-Packet number
HTTP slow attack defense configuration for protected IP addresses:
Address          VPN instance  Threshold (AN/CL/PL/PN)      Period  Actions  Ports
1111:2222:3333:4 abcdefghigkl 1200000,100000000,1000,1000  1000    L,BS(10) 80
444::8888        mnopqrstuvwx
                 yz
```

Table 9 Command output

Field	Description
Policy name	Name of the attack defense policy.
Applied list	Locations to which the attack defense policy is applied.
Exempt IPv4 ACL	IPv4 ACL used for attack detection exemption.
Exempt IPv6 ACL	IPv6 ACL used for attack detection exemption.
Actions	Attack prevention actions: • **CV**—Client verification. • **BS**—Blocking sources. • **L**—Logging. • **D**—Dropping packets. • **N**—No action.
Signature attack defense configuration	Configuration information about single-packet attack detection and prevention.
Signature name	Type of the single-packet attack.
Defense	Whether attack detection is enabled.
Level	Level of the single-packet attack, **info**, **low**, **medium**, or **high**. Currently, no high-level single-packet attacks exist.
Actions	Prevention actions against the scanning attack: • **L**—Logging. • **D**—Dropping packets. • **N**—No action.
Large ICMPv6	Large ICMPv6 attack.
ICMPv6 echo request	ICMPv6 echo request attack.
ICMPv6 echo reply	ICMPv6 echo reply attack.
ICMPv6 group membership query	ICMPv6 group membership query attack.
ICMPv6 group membership report	ICMPv6 group membership report attack.
ICMPv6 group membership reduction	ICMPv6 group membership reduction attack.

Field	Description
ICMPv6 destination unreachable	ICMPv6 destination unreachable attack.
ICMPv6 time exceeded	ICMPv6 time exceeded attack.
ICMPv6 parameter problem	ICMPv6 parameter problem attack.
ICMPv6 packet too big	ICMPv6 packet too big attack.
IPv6 extension header abnormal	Abnormal IPv6 extension header attack.
IPv6 extension header exceeded	IPv6 extension header exceeded attack.
Limit	Upper limit of IPv6 extension headers.
Scan attack defense configuration	Configuration information about scanning attack detection and prevention.
Preset defense	Configuration information about predefined scanning attack detection and prevention.
Defense	Whether scanning attack detection is enabled.
Level	Level of the scanning attack detection, **low**, **medium**, or **high**.
User-defined defense	Configuration information about user-defined scanning attack detection and prevention.
Port scan defense	Status of port scan attack prevention, which can be **Enabled** or **Disabled**.
Port scan defense threshold	Threshold for triggering port scan attack prevention.
IP sweep defense	Status of IP sweep attack prevention, which can be **Enabled** or **Disabled**.
IP sweep defense threshold	Threshold for triggering IP sweep attack prevention.
Period	Scanning attack detection cycle in seconds.
Actions	Scanning attack prevention actions: • **BS**—Blocking sources. • **D**—Dropping packets. • **L**—Logging.
Flood attack defense configuration	Configuration information about flood attack detection and prevention.
Flood type	Type of the flood attack: • ACK flood. • DNS flood. • DNS reply flood. • FIN flood. • ICMP flood. • ICMPv6 flood. • SYN flood. • SYN-ACK flood. • UDP flood. • RST flood. • HTTP flood. • SIP flood.
Global dest/src thres(pps)	Global thresholds for triggering the destination-based and source-based flood attack prevention. The default is 1000 pps.

Field	Description
Global actions	Global prevention actions against the flood attack: • **D**—Dropping packets. • **L**—Logging. • **CV**—Client verification. If no actions are configured, this field displays a hyphen (**-**).
Service ports	Ports that are protected against the flood attack. This field displays port numbers only for the DNS and HTTP flood attacks. For other flood attacks, this field displays a hyphen (-).
Non-specific	Whether the global flood attack detection is enabled.
Flood attack defense for protected IP addresses	Configuration of the IP address-specific flood attack detection and prevention.
Address	Protected IP address.
VPN instance	MPLS L3VPN instance to which the protected IP address belongs. If no MPLS L3VPN instance is specified, this field does not display.
Thres(pps)	Threshold for triggering the flood attack prevention, in units of packets sent to the IP address per second. If no threshold is specified, this field displays **1000**.
Actions	Flood attack prevention actions: • **CV**—Client verification. • **BS**—Blocking sources. • **D**—Dropping packets. • **L**—Logging. • **N**—No action.
Ports	Ports that are protected against the flood attack. This field displays port numbers only for the DNS and HTTP flood attacks. For other flood attacks, this field displays a hyphen (-).
HTTP slow attack defense configuration	Configuration information about the global HTTP slow attack detection and prevention.
Non-specific	Whether global HTTP slow attack detection is enabled.
Global threshold	Global threshold settings: • **Alert-number**—HTTP concurrent connection threshold. If this threshold is not specified, the field displays **5000**. • **Content-length**—Threshold for the **Content-Length** field value. If this threshold is not specified, the field displays **10000**. • **Payload-length**—Payload size threshold. If this threshold is not specified, the field displays **50**. • **Packet-number**—Threshold of abnormal packets. If this threshold is not specified, the field displays **10**.
Global period	Global HTTP slow attack detection period.
Global action	Global HTTP slow attack prevention actions: • **BS**—Blocking sources. • **L**—Logging.
Ports	Ports protected by the global HTTP slow attack prevention. If protected no ports are specified, the field displays **80**.
HTTP slow attack defense configuration for protected IP addresses	Configuration of the IP address-specific HTTP slow attack detection and prevention.

Field	Description
Address	Protected IP address.
VPN instance	VPN instance to which the protected IP address belongs. If no VPN instance is specified, this field does not display.
Threshold (AN/CL/PL/PN)	Threshold parameter settings for IP address-specific HTTP slow attack detection. Full spellings for threshold parameters are as follows: • **AN**—Alert number. • **CL**—Content length. • **PL**—Payload length. • **PN**—Packet number. If a parameter threshold is not specified, the global threshold for this parameter is displayed.
Period	IP address-specific HTTP slow attack detection period. If this period is not specified, the field displays the global detection period.
Actions	IP address-specific HTTP slow attack prevention actions: • **BS**—Blocking sources. • **L**—Logging. If no actions are specified, this field displays the global prevention actions.
Ports	Ports protected by the IP address-specific HTTP slow attack prevention. If no ports are specified, the field displays ports protected by the global HTTP slow attack prevention.

Display brief information about all attack defense policies.

```
<Sysname> display attack-defense policy
           Attack-defense Policy Brief Information
------------------------------------------------------------
Policy Name                         Applied list
Atk-policy-1                        Trust1
P2                                  Trust2
P123                                Trust3
```

Table 10 Command output

Field	Description
Policy name	Name of the attack defense policy.
Applied list	Locations to which the attack defense policy is applied.

Related commands

attack-defense policy

display attack-defense policy ip

Use **display attack-defense policy ip** to display information about IPv4 addresses protected by flood attack detection and prevention.

Syntax

display attack-defense policy *policy-name* { **ack-flood** | **dns-flood** | **dns-reply-flood** | **fin-flood** | **flood** | **http-flood** | **icmp-flood** | **rst-flood** |

sip-flood | **syn-ack-flood** | **syn-flood** | **udp-flood** } **ip** [*ip-address* [**vpn** *vpn-instance-name*]] [**slot** *slot-number*] [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

policy-name: Specifies an attack defense policy by its name. The policy name is a case-insensitive string of 1 to 31 characters. Valid characters include uppercase and lowercase letters, digits, underscores (_), and hyphens (-).

ack-flood: Specifies ACK flood attack.

dns-flood: Specifies DNS flood attack.

dns-reply-flood: Specifies DNS response flood attack.

fin-flood: Specifies FIN flood attack.

flood: Specifies all IPv4 flood attacks.

http-flood: Specifies HTTP flood attack.

icmp-flood: Specifies ICMP flood attack.

rst-flood: Specifies RST flood attack.

sip-flood: Specifies SIP flood attack.

syn-ack-flood: Specifies SYN-ACK flood attack.

syn-flood: Specifies SYN flood attack.

udp-flood: Specifies UDP flood attack.

ip-address: Specifies a protected IPv4 address. If you do not specify an IPv4 address, this command displays information about all protected IPv4 addresses.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the IPv4 address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the IPv4 address is on the public network.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about IPv4 addresses protected by flood attack detection and prevention for all IRF member devices.

count: Displays the number of matching IPv4 addresses protected by flood attack detection and prevention.

Examples

Display information about all IPv4 addresses protected by flood attack detection and prevention in attack defense policy **abc**.

```
<Sysname> display attack-defense policy abc flood ip
Slot 1:
IP address      VPN instance     Type          Rate threshold(PPS) Dropped
123.123.123.123 --               SYN-ACK-FLOOD 100                 4294967295
```

```
201.55.7.45     --              ICMP-FLOOD    100                10
192.168.11.5    --              DNS-FLOOD     23                 100
10.168.200.5    --              SIP-FLOOD     100                102556
Slot 2:
IP address      VPN instance    Type          Rate threshold(PPS) Dropped
123.123.123.123 --              SYN-ACK-FLOOD 100                2543
201.55.7.45     --              ICMP-FLOOD    100                122
192.168.11.5    --              DNS-FLOOD     23                 0
```

Display the number of IPv4 addresses protected by flood attack detection and prevention in attack defense policy **abc**.

```
<Sysname> display attack-defense policy abc flood ip count
Slot 1:
Totally 3 flood protected IP addresses.
Slot 2:
Totally 0 flood protected IP addresses.
```

Table 11 Command output

Field	Description
Totally 3 flood protected IP addresses	Total number of the IPv4 addresses protected by flood attack detection and prevention.
IP address	Protected IPv4 address.
VPN instance	MPLS L3VPN instance to which the protected IPv4 address belongs. If the protected IPv4 address is on the public network, this field does not display.
Type	Type of the flood attack.
Rate threshold(PPS)	Threshold for triggering the flood attack prevention, in units of packets sent to the IP address per second. If no rate threshold is set, this field displays **1000**.
Dropped	Number of dropped attack packets. If the prevention action is logging, this field displays **0**.

display attack-defense policy ipv6

Use **display attack-defense policy ipv6** to display information about IPv6 addresses protected by flood attack detection and prevention.

Syntax

display attack-defense policy *policy-name* { **ack-flood** | **dns-flood** | **dns-reply-flood** | **fin-flood** | **flood** | **http-flood** | **icmpv6-flood** | **rst-flood** | **sip-flood** | **syn-ack-flood** | **syn-flood** | **udp-flood** } **ipv6** [*ipv6-address* [**vpn** *vpn-instance-name*]] [**slot** *slot-number*]] [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

policy-name: Specifies an attack defense policy by its name. The policy name is a case-insensitive string of 1 to 31 characters. Valid characters include uppercase and lowercase letters, digits, underscores (_), and hyphens (-).

ack-flood: Specifies ACK flood attack.

dns-flood: Specifies DNS flood attack.

dns-reply-flood: Specifies DNS response flood attack.

fin-flood: Specifies FIN flood attack.

flood: Specifies all IPv6 flood attacks.

http-flood: Specifies HTTP flood attack.

icmpv6-flood: Specifies ICMPv6 flood attack.

rst-flood: Specifies RST flood attack.

sip-flood: Specifies SIP flood attack.

syn-ack-flood: Specifies SYN-ACK flood attack.

syn-flood: Specifies SYN flood attack.

udp-flood: Specifies UDP flood attack.

ipv6-address: Specifies a protected IPv6 address. If you do not specify an IPv6 address, this command displays information about all protected IPv6 addresses.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the IPv6 address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the IPv6 address is on the public network.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about IPv6 addresses protected by flood attack detection and prevention for all IRF member devices.

count: Displays the number of matching IPv6 addresses protected by flood attack detection and prevention.

Examples

Display information about all IPv6 addresses protected by flood attack detection and prevention in attack defense policy **abc**.

```
<Sysname> display attack-defense policy abc flood ipv6
Slot 1:
IPv6 address    VPN instance     Type          Rate threshold(PPS) Dropped
2013::127f      --               SYN-ACK-FLOOD 100                 4294967295
2::5            --               ACK-FLOOD     100                 10
1::5            --               ACK-FLOOD     100                 23
10::15          --               SIP-FLOOD     100                 1002
Slot 2:
IPv6 address    VPN instance     Type          Rate threshold(PPS) Dropped
2013::127f      --               SYN-ACK-FLOOD 100                 5465
2::5            --               ACK-FLOOD     100                 0
1::5            --               ACK-FLOOD     100                 122
```

Display the number of IPv6 addresses protected by flood attack detection and prevention in attack defense policy **abc**.

```
<Sysname> display attack-defense policy abc flood ipv6 count
Slot 1:
Totally 3 flood protected IP addresses.
Slot 2:
Totally 0 flood protected IP addresses.
```

Table 12 Command output

Field	Description
Totally 3 flood protected IP addresses	Total number of the IPv6 addresses protected by flood attack detection and prevention.
IPv6 address	Protected IPv6 address.
VPN instance	MPLS L3VPN instance to which the protected IPv6 address belongs. If the protected IPv6 address is on the public network, this field does not display.
Type	Type of the flood attack.
Rate threshold(PPS)	Threshold for triggering the flood attack prevention, in units of packets sent to the IPv6 address per second. If no rate threshold is set, this field displays **1000**.
Dropped	Number of dropped attack packets. If the prevention action is logging, this field displays **0**.

display attack-defense scan attacker ip

Use **display attack-defense scan attacker ip** to display information about IPv4 scanning attackers.

Syntax

display attack-defense scan attacker ip [**security-zone** *zone-name* [**slot** *slot-number*]] [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

security-zone *zone-name*: Specifies a security zone by its name. The *zone-name* argument is a case-insensitive string of 1 to 31 characters. It cannot contain hyphens (-).

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about IPv4 scanning attackers for all member devices.

count: Displays the number of matching IPv4 scanning attackers.

Usage guidelines

If you do not specify any parameters, this command displays information about all IPv4 scanning attackers.

Examples

Display information about all IPv4 scanning attackers.

```
<Sysname> display attack-defense scan attacker ip
Slot 1:
IP addr(DslitePeer) VPN instance     Protocol         Detected on  Duration(min)
192.168.31.2(--)    --               TCP              DMZ          1284
2.2.2.3(--)         --               UDP              DMZ          23
Slot 2:
IP addr(DslitePeer) VPN instance     Protocol         Detected on  Duration(min)
192.168.1.100(--)   --               TCP              DMZ          1586
202.2.1.172(--)     --               UDP              DMZ          258
```

Display the number of IPv4 scanning attackers.

```
<Sysname> display attack-defense scan attacker ip count
Slot 1:
Totally 3 attackers.
Slot 2:
Totally 0 attackers.
```

Table 13 Command output

Field	Description
Totally 3 attackers	Total number of IPv4 scanning attackers.
IP addr(DslitePeer)	The **IP addr** field displays the IPv4 address of the attacker. The **DslitePeer** field displays the DS-Lite tunnel source IPv6 address of the attacker in a DS-Lite network. In other situations, this field displays hyphens (**--**).
VPN instance	MPLS L3VPN instance to which the attacker's IPv4 address belongs. If the IPv4 address is on the public network, this field does not display.
Protocol	Name of the protocol.
Detected on	Name of the security zone where the attack is detected.
Duration(min)	The amount of time the attack lasts, in minutes.

Related commands

scan detect

display attack-defense scan attacker ipv6

Use **display attack-defense scan attacker ipv6** to display information about IPv6 scanning attackers.

Syntax

display attack-defense scan attacker ipv6 [**security-zone** *zone-name* [**slot** *slot-number*]] [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

security-zone *zone-name*: Specifies a security zone by its name. The *zone-name* argument is a case-insensitive string of 1 to 31 characters. It cannot contain hyphens (-).

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about IPv6 scanning attackers for all member devices.

count: Displays the number of matching IPv6 scanning attackers.

Usage guidelines

If you do not specify any parameters, this command displays information about all IPv6 scanning attackers.

Examples

Display information about all IPv6 scanning attackers.

```
<Sysname> display attack-defense scan attacker ipv6
Slot 1:
IPv6 address        VPN instance     Protocol         Detected on  Duration(min)
2013::2             --               TCP              DMZ          1234
1230::22            --               UDP              DMZ          10
Slot 2:
IPv6 address        VPN instance     Protocol         Detected on  Duration(min)
2004::4             --               TCP              DMZ          1122
1042::2             --               UDP              DMZ          24
```

Display the number of IPv6 scanning attackers.

```
<Sysname> display attack-defense scan attacker ipv6 count
Slot 1:
Totally 3 attackers.
Slot 2:
Totally 0 attackers.
```

Table 14 Command output

Field	Description
Totally 3 attackers	Total number of IPv6 scanning attackers.
IPv6 address	IPv6 address of the attacker.
VPN instance	MPLS L3VPN instance to which the attacker IPv6 address belongs. If the attacker IPv6 address is on the public network, this field does not display.
Protocol	Name of the protocol.
Detected on	Name of the security zone where the attack is detected.
Duration(min)	The amount of time the attack lasts, in minutes.

Related commands

scan detect

display attack-defense statistics security-zone

Use **display attack-defense statistics security-zone** to display attack detection and prevention statistics on a security zone.

Syntax

display attack-defense statistics security-zone *zone-name* [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

zone-name: Specifies a security zone by its name. The *zone-name* argument is a case-insensitive string of 1 to 31 characters. It cannot contain hyphens (-).

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this commands displays attack detection and prevention statistics for all member devices.

Examples

Display attack detection and prevention statistics on security zone **Untrust** for the specified slot.

```
<Sysname> display attack-defense statistics security-zone untrust slot 1
Slot 1:
Attack policy name: abc
Scanning attack defense statistics:
 AttackType                      AttackTimes Dropped
 Port scan                       2           23
 IP sweep                        3           33
 Distribute port scan            1           10
Flood attack defense statistics:
 AttackType                      AttackTimes Dropped
 SYN flood                       1           0
 ACK flood                       1           0
 SYN-ACK flood                   3           5000
 RST flood                       2           0
 FIN flood                       2           0
 UDP flood                       1           0
 ICMP flood                      1           0
 ICMPv6 flood                    1           0
 DNS flood                       1           0
 DNS reply flood                 1           0
 HTTP flood                      1           0
 SIP flood                       1           1000
HTTP slow attack defense statistics:
```

```
 AttackType                          AttackTimes
 HTTP slow attack                    1
Signature attack defense statistics:
 AttackType                          AttackTimes Dropped
 IP option record route              1           100
 IP option security                  2           0
 IP option stream ID                 3           0
 IP option internet timestamp        4           1
 IP option loose source routing      5           0
 IP option strict source routing     6           0
 IP option route alert               3           0
 Fragment                            1           0
 Impossible                          1           1
 Teardrop                            1           1
 Tiny fragment                       1           0
 IP options abnormal                 3           0
 Smurf                               1           0
 Ping of death                       1           0
 Traceroute                          1           0
 Large ICMP                          1           0
 TCP NULL flag                       1           0
 TCP all flags                       1           0
 TCP SYN-FIN flags                   1           0
 TCP FIN only flag                   1           0
 TCP invalid flag                    1           0
 TCP Land                            1           0
 Winnuke                             1           0
 UDP Bomb                            1           0
 Snork                               1           0
 Fraggle                             1           0
 Large ICMPv6                        1           0
 ICMP echo request                   1           0
 ICMP echo reply                     1           0
 ICMP source quench                  1           0
 ICMP destination unreachable        1           0
 ICMP redirect                       2           0
 ICMP time exceeded                  3           0
 ICMP parameter problem              4           0
 ICMP timestamp request              5           0
 ICMP timestamp reply                6           0
 ICMP information request            7           0
 ICMP information reply              4           0
 ICMP address mask request           2           0
 ICMP address mask reply             1           0
 ICMPv6 echo request                 1           1
 ICMPv6 echo reply                   1           1
 ICMPv6 group membership query       1           0
 ICMPv6 group membership report      1           0
```

```
ICMPv6 group membership reduction   1           0
ICMPv6 destination unreachable      1           0
ICMPv6 time exceeded                1           0
ICMPv6 parameter problem            1           0
ICMPv6 packet too big               1           0
IPv6 extension header abnormal      1           0
IPv6 extension header exceeded      1           0
```

Table 15 Command output

Field	Description
AttackType	Type of the attack.
AttackTimes	Number of times that the attack occurred. This command output displays only attacks that are detected.
Dropped	Number of dropped packets.
ICMPv6 flood	ICMPv6 flood attack. This field is not displayed when no ICMPv6 flood attack is detected.
Large ICMPv6	Large ICMPv6 attack. This field is not displayed when no large ICMPv6 attack is detected.
ICMPv6 echo request	ICMPv6 echo request attack. This field is not displayed when no ICMPv6 echo request attack is detected.
ICMPv6 echo reply	ICMPv6 echo reply attack. This field is not displayed when no ICMPv6 echo reply attack is detected.
ICMPv6 group membership query	ICMPv6 group membership query attack. This field is not displayed when no ICMPv6 group membership query attack is detected.
ICMPv6 group membership report	ICMPv6 group membership report attack. This field is not displayed when no ICMPv6 group membership report attack is detected.
ICMPv6 group membership reduction	ICMPv6 group membership reduction attack. This field is not displayed when no ICMPv6 group membership reduction attack is detected.
ICMPv6 destination unreachable	ICMPv6 destination unreachable attack. This field is not displayed when no ICMPv6 destination unreachable attack is detected.
ICMPv6 time exceeded	ICMPv6 time exceeded attack. This field is not displayed when no ICMPv6 time exceeded attack is detected.
ICMPv6 parameter problem	ICMPv6 parameter problem attack. This field is not displayed when no ICMPv6 parameter problem attack is detected.
ICMPv6 packet too big	ICMPv6 packet too big attack. This field is not displayed when no ICMPv6 packet too big attack is detected.
IPv6 extension header abnormal	Abnormal IPv6 extension header attack. This field is not displayed when no abnormal IPv6 extension header attack is detected.
IPv6 extension header exceeded	IPv6 extension header exceeded attack. This field is not displayed when no IPv6 extension header exceeded attack is detected.

Related commands

`reset attack-defense statistics security-zone`

display attack-defense top-attack-statistics

Use **`display attack-defense top-attack-statistics`** to display top 10 attack statistics.

Syntax

display attack-defense top-attack-statistics { **last-1-hour** | **last-24-hours** | **last-30-days** } [**by-attacker** | **by-type** | **by-victim**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

last-1-hour: Specifies the most recent 1 hour.

last-24-hours: Specifies the most recent 24 hours.

last-30-days: Specifies the most recent 30 days.

by-attacker: Displays top 10 attack statistics by attacker.

by-type: Displays all attack statistics by attack type.

by-victim: Displays top 10 attack statistics by victim.

Usage guidelines

If you do not specify the **by-attacker**, **by-type**, or **by-victim** keyword, this command displays attack statistics by attacker, victim, attack type.

Examples

Display top 10 attack statistics in the most recent 1 hour.

```
<Sysname> display attack-defense top-attack-statistics last-1-hour
Top attackers:
No.     VPN instance   Attacker IP         Attacks
1                      200.200.200.55      21
2                      200.200.200.21      16
3                      200.200.200.133     12
4                      200.200.200.19      10
5                      200.200.200.4       8
6                      200.200.200.155     8
7                      200.200.200.93      5
8                      200.200.200.67      3
9                      200.200.200.70      1
10                     200.200.200.23      1

Top victims:
No.     VPN instance   Victim IP            Attacks
1       --             201.200.200.12       21
2       --             201.200.200.32       16
3       --             201.200.200.14       12
4       --             201.200.200.251      12
5       --             201.200.200.10       7
```

```
6       --              201.200.200.77       6
7       --              201.200.200.96       2
8       --              201.200.200.22       2
9       --              201.200.200.154      2
10      --              201.200.200.18       1

Top attack types:
Attack type       Attacks
Scan              155
Syn               155
```

Table 16 Command output

Field	Description
Top attackers	Top 10 attack statistics by attacker.
No.	Rank on the list.
VPN instance	VPN instance to which the attacker or victim belongs. If the attacker or victim belongs to the public network, this field does not display.
Attacks	Number of attacks.
Top victims	Top 10 attack statistics by victim.
Top attack types	Attack statistics by attack type.

Related commands

attack-defense top-attack-statistics enable

display blacklist destination-ip

Use **display blacklist destination-ip** to display destination IPv4 blacklist entries.

Syntax

display blacklist destination-ip [*destination-ip-address* [**vpn-instance** *vpn-instance-name*]] [**slot** *slot-number*] [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

destination-ip-address: Specifies a destination IPv4 address.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the destination IPv4 address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays destination IPv4 blacklist entries for all member devices.

count: Displays the number of matching destination IPv4 blacklist entries.

Usage guidelines

If you do not specify any parameters, this command displays all destination IPv4 blacklist entries.

Examples

Display all destination IPv4 blacklist entries.

```
<Sysname> display blacklist destination-ip
Slot 1:
IP address      VPN instance   Type    Aging (sec)  Dropped
192.168.11.5    --             Dynamic 10           353452
123.123.123.123 --             Dynamic 123          4294967295
201.55.7.45     --             Manual  Never        14478
Slot 2:
IP address      VPN instance   Type    Aging (sec)  Dropped
123.55.123.7    --             Dynamic 123       164698
201.55.7.33     --             Manual  Never     845969
```

Display the total number of destination IPv4 blacklist entries.

```
<Sysname> display blacklist destination-ip count
Slot 1:
Totally 3 blacklist entries.
Slot 2:
Totally 2 blacklist entries.
```

Table 17 Command output

Field	Description
IP address	IPv4 address in the destination blacklist entry.
VPN instance	MPLS L3VPN instance to which the blacklisted IPv4 address belongs. If the blacklisted IPv4 address is on the public network, this field does not display.
Type	Type of the destination IPv4 blacklist entry: • **Dynamic**—Dynamically generated. • **Manual**—Manually configured.
Aging (sec)	Remaining aging time of the destination IPv4 blacklist entry, in seconds. If no aging time is set for the entry, this field displays **Never**.
Dropped	Number of dropped packets that are destined for the IPv4 address.
Totally 3 blacklist entries.	Total number of destination IPv4 blacklist entries.

Related commands

blacklist destination-ip

display blacklist destination-ipv6

Use **display blacklist destination-ipv6** to display destination IPv6 blacklist entries.

Syntax

display blacklist destination-ipv6 [*destination-ipv6-address* [**vpn-instance** *vpn-instance-name*]] [**slot** *slot-number*] [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

destination-ipv6-address: Specifies a destination IPv6 address.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the destination IPv6 address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays destination IPv6 blacklist entries for all member devices.

count: Displays the number of matching destination IPv6 blacklist entries.

Usage guidelines

If you do not specify any parameters, this command displays all destination IPv6 blacklist entries.

Examples

Display all destination IPv6 blacklist entries.

```
<Sysname> display blacklist destination-ipv6
Slot 1:
IPv6 address         VPN instance      Type    Aging (sec)  Dropped
1::4                 --                Manual  Never        14478
1::5                 --                Dynamic 10           353452
2013:fe07:221a:4011: --                Dynamic 123          4294967295
2013:fe07:221a:4011
Slot 2:
IPv6 address         VPN instance      Type    Aging (sec)  Dropped
1::3                 --                Manual  Never        74679
20::33               --                Dynamic 10           1697898
```

Display the total number of destination IPv6 blacklist entries.

```
<Sysname> display blacklist destination-ipv6 count
Slot 1:
Totally 3 blacklist entries.
Slot 2:
Totally 2 blacklist entries.
```

Table 18 Command output

Field	Description
IPv6 address	IPv6 address in the destination blacklist entry.

Field	Description
VPN instance	MPLS L3VPN instance to which the blacklisted IPv6 address belongs. If the blacklisted IPv6 address is on the public network, this field does not display.
Type	Type of the destination IPv6 blacklist entry: • **Dynamic**—Dynamically generated. • **Manual**—Manually configured.
Aging (sec)	Remaining aging time of the destination IPv6 blacklist entry, in seconds. If no aging time is set for the entry, this field displays **Never**.
Dropped	Number of dropped packets that are destined for the IPv6 address.
Totally 3 blacklist entries.	Total number of destination IPv6 blacklist entries.

Related commands

blacklist destination-ipv6

display blacklist ip

Use **display blacklist ip** to display source IPv4 blacklist entries.

Syntax

display blacklist ip [*source-ip-address* [**vpn-instance** *vpn-instance-name*] [**ds-lite-peer** *ds-lite-peer-address*]] [**slot** *slot-number*] [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

source-ip-address: Specifies a source IPv4 address.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the IPv4 address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the IPv4 address is on the public network.

ds-lite-peer *ds-lite-peer-address*: Specifies the IPv6 address of the B4 element of the DS-Lite tunnel that transmits packets from the blacklisted IPv4 address.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays source IPv4 blacklist entries for all member devices.

count: Displays the number of matching source IPv4 blacklist entries.

Usage guidelines

If you do not specify any parameters, this command displays all source IPv4 blacklist entries.

Examples

Display all source IPv4 blacklist entries.

```
<Sysname> display blacklist ip
Slot 1:
IP address      VPN instance   DS-Lite tunnel peer  Type    TTL(sec) Dropped
192.168.11.5    --             --                   Dynamic 10       353452
123.123.123.123 --             2013::fe07:221a:4011 Dynamic 123      4294967295
201.55.7.45     --             2013::1              Manual  Never    14478
Slot 2:
IP address      VPN instance   DS-Lite tunnel peer  Type    TTL(sec) Dropped
123.55.123.7    --             --                   Dynamic 123      164698
201.55.7.33     --             --                   Manual  Never    845969
```

Display the total number of source IPv4 blacklist entries.

```
<Sysname> display blacklist ip count
Slot 1:
Totally 3 blacklist entries.
Slot 2:
Totally 2 blacklist entries.
```

Table 19 Command output

Field	Description
IP address	IPv4 address in the source blacklist entry.
VPN instance	MPLS L3VPN instance to which the blacklisted IPv4 address belongs. If the blacklisted IPv4 address is on the public network, this field does not display.
DS-Lite tunnel peer	IPv6 address of the DS-Lite tunnel peer. If the device is the AFTR of a DS-Lite tunnel, this field displays the IPv6 address of the B4 element from which the packet comes. In other situations, this field displays hyphens (**--**).
Type	Type of the source IPv4 blacklist entry: • **Dynamic**—Dynamically generated. • **Manual**—Manually configured.
TTL(sec)	Remaining aging time of the source IPv4 blacklist entry, in seconds. If no aging time is set for the entry, this field displays **Never**.
Totally 3 blacklist entries	Total number of source IPv4 blacklist entries.

Related commands

blacklist ip

display blacklist ipv6

Use **display blacklist ipv6** to display source IPv6 blacklist entries.

Syntax

display blacklist ipv6 [*source-ipv6-address* [**vpn-instance** *vpn-instance-name*]] [**slot** *slot-number*] [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

source-ipv6-address: Specifies a source IPv6 address.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the IPv6 address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the IPv6 address is on the public network.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays source IPv6 blacklist entries for all member devices.

count: Displays the number of matching source IPv6 blacklist entries.

Usage guidelines

If you do not specify any parameters, this command displays all source IPv6 blacklist entries.

Examples

Display all source IPv6 blacklist entries.

```
<Sysname> display blacklist ipv6
Slot 1:
IPv6 address         VPN instance      Type    TTL(sec) Dropped
1::4                 --                Manual  Never    14478
1::5                 --                Dynamic 10       353452
2013:fe07:221a:4011: --                Dynamic 123      4294967295
2013:fe07:221a:4011
Slot 2:
IPv6 address         VPN instance      Type    TTL(sec) Dropped
1::3                 --                Manual  Never    74679
20::33               --                Dynamic 10       1697898
```

Display the total number of source IPv6 blacklist entries.

```
<Sysname> display blacklist ipv6 slot 1 count
Slot 1:
Totally 3 blacklist entries.
Slot 2:
Totally 2 blacklist entries..
```

Table 20 Command output

Field	Description
IPv6 address	IPv6 address in the source blacklist entry.
VPN instance	MPLS L3VPN instance to which the blacklisted IPv6 address belongs. If the blacklisted IPv6 address is on the public network, this field does not display.
Type	Type of the source IPv6 blacklist entry: • **Dynamic**—Dynamically generated. • **Manual**—Manually configured.

Field	Description
TTL(sec)	Remaining aging time of the source IPv6 blacklist entry, in seconds. If no aging time is set for the entry, this field displays **Never**.
Totally 3 blacklist entries	Total number of source IPv6 blacklist entries.

Related commands

blacklist ipv6

display blacklist user

Use **display blacklist user** to display user blacklist entries.

Syntax

display blacklist user [*user-name*] [**domain** *domain-name*] [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

user-name: Specifies a user by the username, a case-sensitive string of 1 to 55 characters. If you do not specify a user, this command displays all user blacklist entries.

domain *domain-name*: Specifies a user identification domain by its name, a case-insensitive string of 1 to 255 characters. The user identification domain name cannot include question marks (?). If you do not specify a user identification domain, this command displays user blacklist entries that do not belong to any user identification domains.

count: Displays the number of matching user blacklist entries.

Examples

Display all user blacklist entries.

```
<Sysname> display blacklist user
User name    Domain name      Type       TTL(sec)  Dropped
Alex         domaina          Manual     10        353452
Bob                           Manual     123       4294967295
Cary                          Manual     Never     14478
```

Display the user blacklist entry for user **Alex** in user identification domain **domaina**.

```
<Sysname> display blacklist user Alex domain domaina
User name   Domain name      Type       TTL(sec)   Dropped
Alex        domaina          Manual     10         353452
```

Display the number of user blacklist entries.

```
<Sysname> display blacklist user count
Totally 3 blacklist entries.
```

Table 21 Command output

Field	Description
Username	Username in the user blacklist entry.
Domain name	User identification domain to which the user belongs.
Type	Type of the user blacklist entry. Only the manual mode is supported.
TTL(sec)	Remaining aging time of the user blacklist entry, in seconds. If no aging time is set for the entry, this field displays **Never**.
Dropped	Number of dropped packets sourced from the user.
Totally 3 blacklist entries	Total number of user blacklist entries.

Related commands

`blacklist global enable`

`blacklist user`

display client-verify protected ip

Use **`display client-verify protected ip`** to display protected IPv4 addresses for client verification.

Syntax

`display client-verify` { **`dns`** | **`dns-reply`** | **`http`** | **`sip`** | **`tcp`** } **`protected ip`** [*`ip-address`* [**`vpn`** *`vpn-instance-name`*]] [**`port`** *`port-number`*] [**`slot`** *`slot-number`*] [**`count`**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

`dns`: Specifies the DNS client verification feature.

`dns-reply`: Specifies the DNS response verification feature.

`http`: Specifies the HTTP client verification feature.

`sip`: Specifies the SIP client verification feature.

`tcp`: Specifies the TCP client verification feature.

`ip-address`: Specifies a protected IPv4 address. If you do not specify an IPv4 address, this command displays all protected IPv4 addresses.

`vpn-instance` *`vpn-instance-name`*: Specifies the MPLS L3VPN instance to which the protected IPv4 address belongs. The *`vpn-instance-name`* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the protected IPv4 address is on the public network.

port *port-number*: Specifies a protected port in the range of 1 to 65535. If you do not specify a port, this command displays protected IPv4 addresses with default ports. The default port for DNS client verification is port 53, the default port for HTTP client verification is port 80, and the default port for TCP client verification is all ports.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays protected IPv4 addresses for all member devices.

count: Displays the number of matching protected IPv4 addresses.

Examples

Display the protected IPv4 addresses for TCP client verification.

```
<Sysname> display client-verify tcp protected ip
Slot 1:
IP address           VPN instance     Port  Type    Requested   Trusted
192.168.11.5         --               23    Dynamic 353452      555
123.123.123.123      --               65535 Dynamic 4294967295  15151
201.55.7.45          --               10    Manual  15000       222
Slot 2:
IP address           VPN instance     Port  Type    Requested   Trusted
192.168.11.5         --               23    Dynamic 46790       78578
201.55.7.45          --               10    Dynamic 2368        7237
123.123.123.123      --               65535 Manual  24587       1385
```

Display the number of protected IPv4 addresses for TCP client verification.

```
<Sysname> display client-verify tcp protected ip count
Slot 1:
Totally 3 protected IP addresses.
Slot 2:
Totally 0 protected IP addresses.
```

Table 22 Command output

Field	Description
Totally 3 protected IP addresses	Total number of protected IPv4 addresses.
IP address	Protected IPv4 address.
VPN instance	MPLS L3VPN instance to which the protected IPv4 address belongs. If the protected IPv4 address is on the public network, this field does not display.
Port	Port protected by TCP client verification. If TCP client verification protects all ports, this field displays **any**.
Type	Type of the protected IPv4 address, **Manual** or **Dynamic**.
Requested	Number of packets destined for the protected IPv4 address.
Trusted	Number of packets that passed the client verification.

Related commands

client-verify protected ip

display client-verify protected ipv6

Use **display client-verify protected ipv6** to display protected IPv6 addresses for client verification.

Syntax

display client-verify { **dns** | **dns-reply** | **http** | **sip** | **tcp** } **protected ipv6** [*ipv6-address* [**vpn** *vpn-instance-name*]] [**port** *port-number*] [**slot** *slot-number*] [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

dns: Specifies the DNS client verification feature.

dns-reply: Specifies the DNS response verification feature.

http: Specifies the HTTP client verification feature.

sip: Specifies the SIP client verification feature.

tcp: Specifies the TCP client verification feature.

ipv6-address: Specifies a protected IPv6 address. If you do not specify an IPv6 address, this command displays all protected IPv6 addresses.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the protected IPv6 address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the protected IPv6 address is on the public network.

port *port-number*: Specifies a protected port in the range of 1 to 65535. If you do not specify a port, this command displays protected IPv6 addresses with default ports. The default port for DNS client verification is port 53, the default port for HTTP client verification is port 80, and the default port for TCP client verification is all ports.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays protected IPv6 addresses for all member devices.

count: Displays the number of matching protected IPv6 addresses.

Examples

Display the protected IPv6 addresses for TCP client verification.

```
<Sysname> display client-verify tcp protected ipv6
Slot 1:
IPv6 address         VPN instance     Port  Type    Requested   Trusted
1:2:3:4:5:6:7:8      --               100   Manual  14478       5501
1023::1123           --               65535 Dynamic 4294967295  15151
Slot 2:
IPv6 address         VPN instance     Port  Type    Requested   Trusted
1:2:3:4:5:6:7:8      --               100   Manual  4568        8798
```

```
1023::1123          --              65535 Dynamic 15969       4679
```

Display the number of protected IPv6 addresses for TCP client verification.

```
<Sysname> display client-verify tcp protected ip count
Slot 1:
Totally 3 protected IPv6 addresses.
Slot 2:
Totally 0 protected IPv6 addresses.
```

Table 23 Command output

Field	Description
Totally 3 protected IPv6 addresses	Total number of protected IPv6 addresses.
IPv6 address	Protected IPv6 address.
VPN instance	MPLS L3VPN instance to which the protected IPv6 address belongs. If the protected IPv6 address is on the public network, this field does not display.
Port	Port protected by TCP client verification. If TCP client verification protects all ports, this field displays **any**.
Type	Type of the protected IPv6 address, **Manual** or **Dynamic**.
Requested	Number of packets destined for the protected IPv6 address.
Trusted	Number of packets that passed the client verification.

Related commands

client-verify protected ipv6

display client-verify trusted ip

Use **display client-verify trusted ip** to display trusted IPv4 addresses for client verification.

Syntax

display client-verify { **dns** | **dns-reply** | **http** | **sip** | **tcp** } **trusted ip** [*ip-address* [**vpn** *vpn-instance-name*]] [**slot** *slot-number*] [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

dns: Specifies the DNS client verification feature.

dns-reply: Specifies the DNS response verification feature.

http: Specifies the HTTP client verification feature.

sip: Specifies the SIP client verification feature.

tcp: Specifies the TCP client verification feature.

ip-address: Specifies a trusted IPv4 address. If you do not specify an IPv4 address, this command displays all trusted IPv4 addresses.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the trusted IPv4 address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the trusted IPv4 address is on the public network.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays trusted IPv4 addresses for all member devices.

count: Displays the number of matching trusted IPv4 addresses.

Examples

Display the trusted IPv4 addresses for DNS client verification.

```
<Sysname> display client-verify dns trusted ip
Slot 1:
IP address      VPN instance        DS-Lite tunnel peer    TTL(sec)
11.1.1.2        --                  --                     3600
123.123.123.123 --                  --                     3550
Slot 2:
IP address      VPN instance        DS-Lite tunnel peer    TTL(sec)
11.1.1.3        --                  --                     1200
```

Display the number of trusted IPv4 addresses for DNS client verification.

```
<Sysname> display client-verify dns trusted ip count
Slot 1:
Totally 3 trusted IP addresses.
Slot 2:
Totally 0 trusted IP addresses.
```

Table 24 Command output

Field	Description
Totally 3 protected IP addresses	Total number of trusted IPv4 addresses.
IP address	Trusted IPv4 address.
VPN instance	MPLS L3VPN instance to which the trusted IPv4 address belongs. If the trusted IPv4 address is on the public network, this field does not display.
DS-Lite tunnel peer	IPv6 address of the DS-Lite tunnel peer. If the device is the AFTR of a DS-Lite tunnel, this field displays the IPv6 address of the B4 element from which the packet comes. In other situations, this field displays hyphens (--).
TTL(sec)	Remaining aging time of the trusted IPv4 address, in seconds.

display client-verify trusted ipv6

Use **display client-verify trusted ipv6** to display trusted IPv6 addresses for client verification.

Syntax

display client-verify { **dns** | **dns-reply** | **http** | **sip** | **tcp** } **trusted ipv6** [*ipv6-address* [**vpn** *vpn-instance-name*]] [**slot** *slot-number*]] [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

dns: Specifies the DNS client verification feature.

dns-reply: Specifies the DNS response verification feature.

http: Specifies the HTTP client verification feature.

sip: Specifies the SIP client verification feature.

tcp: Specifies the TCP client verification feature.

ipv6-address: Specifies a trusted IPv6 address. If you do not specify an IPv6 address, this command displays all trusted IPv6 addresses.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the trusted IPv6 address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the trusted IPv6 address is on the public network.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays trusted IPv6 addresses for all member devices.

count: Displays the number of matching trusted IPv6 addresses.

Examples

Display the trusted IPv6 addresses for DNS client verification.

```
<Sysname> display client-verify dns trusted ipv6
Slot 1:
IPv6 address                            VPN instance     TTL(sec)
1::3                                    --               1643
1234::1234                              --               1234
Slot 2:
IPv6 address                            VPN instance     TTL(sec)
1::3                                    --               1643
```

Display the number of trusted IPv6 list for DNS client verification.

```
<Sysname> display client-verify dns trusted ipv6 count
Slot 1:
Totally 3 trusted IPv6 addresses.
Slot 2:
Totally 0 trusted IPv6 addresses.
```

Table 25 Command output

Field	Description
Totally 3 protected IPv6 addresses	Number of trusted IPv6 addresses.
IPv6 address	Trusted IPv6 address.
VPN instance	MPLS L3VPN instance to which the trusted IPv6 address belongs. If the trusted IPv6 address is on the public network, this field does not display.
TTL(sec)	Remaining aging time of the trusted IPv6 address, in seconds.

display whitelist object-group

Use **display whitelist object-group** to display statistics about packets that match the address object groups on the whitelist.

Syntax

display whitelist object-group [*object-group-name*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

object-group-name: Specifies an address object group by its name, a case-insensitive string of 1 to 63 characters. If you do not specify an address object group, this command displays statistics about packets that match all address object groups on the whitelist.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays statistics for all member devices.

Usage guidelines

If you do not specify any parameters, this command displays statistics about packets that match all address object groups on the whitelist.

Examples

Display statistics about packets that match all address object groups on the whitelist.

```
<Sysname> display whitelist object-group
Slot 1:
Object group              Type          Matching Packets
objgrp-1                  IPv4          15696
objgrp-2                  IPv4          855864455
Slot 2:
Object group              Type          Matching Packets
objgrp-1                  IPv4          353452
```

Table 26 Command output

Field	Description
Object group	Name of the address object group.
Type	Type of the address object group.
Matching packets	Number of packets that match the address object group.

Related commands

`reset whitelist statistics`

`whitelist object-group`

dns-flood action

Use **`dns-flood action`** to specify global actions against DNS flood attacks.

Use **`undo dns-flood action`** to restore the default.

Syntax

`dns-flood action` { **`client-verify`** | **`drop`** | **`logging`** } *

`undo dns-flood action`

Default

No global action is specified for DNS flood attacks.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

`client-verify`: Adds the victim IP addresses to the protected IP list for DNS client verification. If DNS client verification is enabled, the device provides proxy services for protected servers. This keyword does not take effect on source-based flood attack prevention.

`drop`: Drops subsequent DNS packets destined for the victim IP addresses in destination-based flood attack prevention, or drops subsequent DNS packets originating from the attacker IP addresses in source-based flood attack prevention.

`logging`: Enables logging for DNS flood attack events. The log messages will be sent to the log system.

Usage guidelines

For the DNS flood attack detection to collaborate with the DNS client verification, make sure the **`client-verify`** keyword is specified and the DNS client verification is enabled. To enable DNS client verification, use the **`client-verify dns enable`** command.

The **`logging`** keyword enables the attack detection and prevention module to log DNS flood attack events and send log messages to the information center.

With the information center, you can set log message filtering and output rules, including output destinations.

The information center can output DNS flood attack logs to any destinations except the console and the monitor terminal. If you configure the console or monitor terminal as an output destination, the output destination setting will not take effect.

To view DNS flood attack logs stored on the device, use the **display logbuffer** command. Make sure you do not disable log output to the log buffer, which is enabled by default.

For more information about configuring the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Specify **drop** as the global action against DNS flood attacks in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] dns-flood action drop
```

Related commands

client-verify dns enable

dns-flood detect

dns-flood detect non-specific

dns-flood port

dns-flood source-threshold

dns-flood threshold

dns-flood detect

Use **dns-flood detect** to configure IP address-specific DNS flood attack detection.

Use **undo dns-flood detect** to remove the IP address-specific DNS flood attack detection configuration.

Syntax

dns-flood detect { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**port** *port-list*] [**threshold** *threshold-value*] [**action** { { **client-verify** | **drop** | **logging** } * | **none** }]

undo dns-flood detect { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]

Default

IP address-specific DNS flood attack detection is not configured.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

ip *ipv4-address*: Specifies the IPv4 address to be protected. The *ip-address* argument cannot be 255.255.255.255 or 0.0.0.0.

ipv6 *ipv6-address*: Specifies the IPv6 address to be protected. The IPv6 address cannot be a multicast address or ::.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the protected IP address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the protected IP address is on the public network.

port *port-list*: Specifies a space-separated list of up to 24 port number items. Each item specifies a port by its port number or a range of ports in the form of *start-port-number* to *end-port-number*. The *end-port-number* cannot be smaller than the *start-port-number*. If you do not specify this option, the global ports apply.

threshold *threshold-value*: Specifies the maximum receiving rate in pps for DNS packets that are destined for the protected IP address. The value range is 1 to 1000000.

action: Specifies the actions against a detected DNS flood attack. If no action is specified, the global actions set by the **dns-flood action** command apply.

client-verify: Adds the victim IP addresses to the protected IP list for DNS client verification. If DNS client verification is enabled, the device provides proxy services for protected servers.

drop: Drops subsequent DNS packets destined for the protected IP address.

logging: Enables logging for DNS flood attack events. The log messages will be sent to the log system.

none: Takes no action.

Usage guidelines

With DNS flood attack detection configured for an IP address, the device is in attack detection state. When the receiving rate of DNS packets destined for the IP address keeps reaching or exceeding the threshold, the device enters prevention state and takes the specified actions. When the rate drops below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

You can configure DNS flood attack detection for multiple IP addresses in one attack defense policy.

The **logging** keyword enables the attack detection and prevention module to log DNS flood attack events and send log messages to the information center.

With the information center, you can set log message filtering and output rules, including output destinations.

The information center can output DNS flood attack logs to any destinations except the console and the monitor terminal. If you configure the console or monitor terminal as an output destination, the output destination setting will not take effect.

To view DNS flood attack logs stored on the device, use the **display logbuffer** command. Make sure you do not disable log output to the log buffer, which is enabled by default.

For more information about configuring the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Configure DNS flood attack detection for 192.168.1.2 in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] dns-flood detect ip 192.168.1.2 port 53
threshold 2000
```

Related commands

dns-flood action

dns-flood detect non-specific

dns-flood port

dns-flood threshold

dns-flood detect non-specific

Use **dns-flood detect non-specific** to enable global DNS flood attack detection.

Use **undo dns-flood detect non-specific** to disable global DNS flood attack detection.

Syntax

dns-flood detect non-specific

undo dns-flood detect non-specific

Default

Global DNS flood attack detection is disabled.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Usage guidelines

The device supports the following DNS flood attack prevention types:

- **Source-based DNS flood attack prevention**—Monitors the receiving rate of DNS packets on a per-source IP basis.
- **Destination-based DNS flood attack prevention**—Monitors the receiving rate of DNS packets on a per-destination IP basis.

The global DNS flood attack detection applies to all IP addresses except for those specified by the **dns-flood detect** command. The global detection uses the global trigger threshold set by the **dns-flood threshold** or **dns-flood source-threshold** command and global actions specified by the **dns-flood action** command.

Examples

Enable global DNS flood attack detection in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] dns-flood detect non-specific
```

Related commands

dns-flood action

dns-flood detect

dns-flood port

dns-flood source-threshold

dns-flood threshold

dns-flood port

Use **dns-flood port** to specify the global ports to be protected against DNS flood attacks.

Use **undo dns-flood port** to restore the default.

Syntax

dns-flood port *port-list*

undo dns-flood port

Default

The global DNS flood attack prevention protects port 53.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

port-list: Specifies a space-separated list of up to 32 port number items. Each item specifies a port by its port number or a range of ports in the form of *start-port-number* to *end-port-number*. The *end-port-number* cannot be smaller than the *start-port-number*.

Usage guidelines

The device detects only DNS packets destined for the specified ports.

The global ports apply to global DNS flood attack detection and IP address-specific DNS flood attack detection with no port specified.

Examples

Specify the ports 53 and 61000 as the global ports to be protected against DNS flood attacks in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] dns-flood port 53 61000
```

Related commands

dns-flood action

dns-flood detect

dns-flood detect non-specific

dns-flood source-threshold

dns-flood threshold

dns-flood threshold

Use **dns-flood threshold** to set the global threshold for triggering destination-based DNS flood attack prevention.

Use **undo dns-flood threshold** to restore the default.

Syntax

dns-flood threshold *threshold-value*

undo dns-flood threshold

Default

The global threshold is 10000 for triggering destination-based DNS flood attack prevention.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

threshold-value: Specifies the maximum receiving rate in pps for DNS packets that are destined for an IP address. The value range is 0 to 1000000. If you set the threshold value to 0, the destination-based DNS flood attack prevention is disabled.

Usage guidelines

With global DNS flood attack detection configured, the device is in attack detection state. When the receiving rate of DNS packets destined for an IP address keeps reaching or exceeding the threshold, the device enters prevention state and takes the specified actions. When the rate drops below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

The global threshold applies to global DNS flood attack detection. Adjust the threshold according to the application scenarios.

- If the number of DNS packets sent to a protected DNS server is normally large, set a high threshold. A low threshold might affect the server services.
- For a network that is unstable or susceptible to attacks, set a low threshold.

Examples

Set the global threshold to 100 for triggering destination-based DNS flood attack prevention in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] dns-flood threshold 100
```

Related commands

dns-flood action

dns-flood detect

dns-flood detect non-specific

dns-flood port

dns-flood source-threshold

Use **dns-flood source-threshold** to set the global threshold for triggering source-based DNS flood attack prevention.

Use **undo dns-flood source-threshold** to restore the default.

Syntax

dns-flood source-threshold *threshold-value*

undo dns-flood source-threshold

Default

The global threshold is 10000 for triggering source-based DNS flood attack prevention.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

threshold-value: Specifies the maximum receiving rate in pps for DNS packets that originate from an IP address. The value range is 0 to 1000000. If you set the threshold value to 0, the source-based DNS flood attack prevention is disabled.

Usage guidelines

With global DNS flood attack detection configured, the device is in attack detection state. When the receiving rate of DNS packets originating from an IP address keeps reaching or exceeding the threshold, the device enters prevention state and takes the specified actions. When the rate drops below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

Examples

Set the global threshold to 100 for triggering source-based DNS flood attack prevention in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] dns-flood source-threshold 100
```

Related commands

dns-flood action

dns-flood detect ip

dns-flood detect non-specific

dns-flood port

dns-reply-flood action

Use **dns-reply-flood action** to specify global actions against DNS response flood attacks.

Use **undo dns-reply-flood action** to restore the default.

Syntax

dns-reply-flood action { **client-verify** | **drop** | **logging** } *

undo dns-reply-flood action

Default

No global action is specified for DNS response flood attacks.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

client-verify: Adds the victim IP addresses to the protected IP list for DNS response verification. If DNS response verification is enabled, the device provides proxy services for protected clients. This keyword does not take effect on source-based flood attack prevention.

drop: Drops subsequent DNS responses destined for the victim IP addresses in destination-based flood attack prevention, or drops subsequent DNS responses originating from the attacker IP addresses in source-based flood attack prevention.

logging: Enables logging for DNS response flood attack events. The log messages will be sent to the log system.

Usage guidelines

For the DNS response flood attack detection to collaborate with the DNS response verification, make sure the **client-verify** keyword is specified and the DNS response verification is enabled. To enable DNS response verification, use the **client-verify dns-reply enable** command.

The **logging** keyword enables the attack detection and prevention module to log DNS response flood attack events and send log messages to the information center.

With the information center, you can set log message filtering and output rules, including output destinations.

The information center can output DNS response flood attack logs to any destinations except the console and the monitor terminal. If you configure the console or monitor terminal as an output destination, the output destination setting will not take effect.

To view DNS response flood attack logs stored on the device, use the **display logbuffer** command. Make sure you do not disable log output to the log buffer, which is enabled by default.

For more information about configuring the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Specify **drop** as the global action against DNS response flood attacks in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] dns-reply-flood action drop
```

Related commands

client-verify dns-reply enable

dns-reply-flood detect

dns-reply-flood detect non-specific

dns-reply-flood source-threshold

dns-reply-flood threshold

dns-reply-flood detect

Use **dns-reply-flood detect** to configure IP address-specific DNS response flood attack detection.

Use **undo dns-reply-flood detect** to remove the IP address-specific DNS response flood attack detection configuration.

Syntax

dns-reply-flood detect { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**port** *port-list*] [**threshold** *threshold-value*] [**action** { { **client-verify** | **drop** | **logging** } * | **none** }]

undo dns-reply-flood detect { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]

Default

IP address-specific DNS response flood attack detection is not configured.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

ip *ipv4-address*: Specifies the IPv4 address to be protected. The *ip-address* argument cannot be 255.255.255.255 or 0.0.0.0.

ipv6 *ipv6-address*: Specifies the IPv6 address to be protected.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the protected IP address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the protected IP address is on the public network.

port *port-list*: Specifies a space-separated list of up to 24 port number items. Each item specifies a port by its port number or a range of ports in the form of *start-port-number* to *end-port-number*. The *end-port-number* cannot be smaller than the *start-port-number*. If you do not specify this option, the global ports apply.

threshold *threshold-value*: Specifies the maximum receiving rate in pps for DNS responses that are destined for the protected IP address. The value range is 1 to 1000000, and the default value is 1000.

action: Specifies the actions against a detected DNS response flood attack.

client-verify: Adds the victim IP addresses to the protected IP list for DNS response verification. If DNS response verification is enabled, the device provides proxy services for protected clients.

drop: Drops subsequent DNS responses destined for the protected IP address.

logging: Enables logging for DNS response flood attack events. The log messages will be sent to the log system.

none: Takes no action.

Usage guidelines

You can configure DNS response flood attack detection for multiple IP addresses in one attack defense policy.

With DNS response flood attack detection configured for an IP address, the device is in attack detection state. When the receiving rate of DNS responses destined for the IP address keeps reaching or exceeding the threshold, the device enters prevention state and takes the specified actions. When the rate drops below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

The **logging** keyword enables the attack detection and prevention module to log DNS response flood attack events and send log messages to the information center.

With the information center, you can set log message filtering and output rules, including output destinations.

The information center can output DNS response flood attack logs to any destinations except the console and the monitor terminal. If you configure the console or monitor terminal as an output destination, the output destination setting will not take effect.

To view DNS response flood attack logs stored on the device, use the **display logbuffer** command. Make sure you do not disable log output to the log buffer, which is enabled by default.

For more information about configuring the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Configure DNS response flood attack detection for 192.168.1.2 in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] dns-reply-flood detect ip 192.168.1.2 port 53 threshold 2000
```

Related commands

dns-reply-flood action

dns-reply-flood detect non-specific

dns-reply-flood port

dns-reply-flood threshold

dns-reply-flood detect non-specific

Use **dns-reply-flood detect non-specific** to enable global DNS response flood attack detection.

Use **undo dns-reply-flood detect non-specific** to disable global DNS response flood attack detection.

Syntax

dns-reply-flood detect non-specific

undo dns-reply-flood detect non-specific

Default

Global DNS response flood attack detection is disabled.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Usage guidelines

The device supports the following DNS response flood attack prevention types:

- **Source-based DNS response flood attack prevention**—Monitors the receiving rate of DNS responses on a per-source IP basis.
- **Destination-based DNS response flood attack prevention**—Monitors the receiving rate of DNS responses on a per-destination IP basis.

The global DNS response flood attack detection applies to all IP addresses except for those specified by the **dns-reply-flood detect** or **dns-reply-flood source-threshold** command. The global detection uses the global trigger threshold set by the **dns-reply-flood threshold** command and global actions specified by the **dns-flood action** command.

Examples

Enable global DNS response flood attack detection in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] dns-reply-flood detect non-specific
```

Related commands

dns-reply-flood action

dns-reply-flood detect

dns-reply-flood port

dns-reply-flood source-threshold

dns-reply-flood threshold

dns-reply-flood port

Use **dns-reply-flood port** to specify the global ports to be protected against DNS response flood attacks.

Use **undo dns-reply-flood port** to restore the default.

Syntax

dns-reply-flood port *port-list*

undo dns-reply-flood port

Default

The global DNS response flood attack prevention protects port 53.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

port-list: Specifies a space-separated list of up to 32 port number items. Each item specifies a port by its port number or a range of ports in the form of *start-port-number* to *end-port-number*. The *end-port-number* cannot be smaller than the *start-port-number*.

Usage guidelines

The device detects only DNS response packets destined for the specified ports.

The global ports apply to global DNS response flood attack detection and IP address-specific DNS response flood attack detection with no port specified.

Examples

Specify the ports 53 and 61000 as the global ports to be protected against DNS response flood attacks in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] dns-reply-flood port 53 61000
```

Related commands

dns-reply-flood action

dns-reply-flood detect

dns-reply-flood detect non-specific

dns-reply-flood source-threshold

dns-reply-flood threshold

dns-reply-flood threshold

Use **dns-reply-flood threshold** to set the global threshold for triggering destination-based DNS response flood attack prevention.

Use **undo dns-reply-flood threshold** to restore the default.

Syntax

dns-reply-flood threshold *threshold-value*

undo dns-reply-flood threshold

Default

The global threshold is 10000 for triggering destination-based DNS response flood attack prevention.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

threshold-value: Specifies the maximum receiving rate in pps for DNS responses that are destined for an IP address. The value range is 0 to 1000000. If you set the threshold value to 0, the destination-based DNS response flood attack prevention is disabled.

Usage guidelines

With global DNS response flood attack detection configured, the device is in attack detection state. When the receiving rate of DNS responses destined for an IP address keeps reaching or exceeding the threshold, the device enters prevention state and takes the specified actions. When the rate drops below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

The global threshold applies to global DNS response flood attack detection. Adjust the threshold according to the application scenarios.

- If the number of DNS responses sent to a protected DNS client is normally large, set a high threshold. A low threshold might affect the client services.
- For a network that is unstable or susceptible to attacks, set a low threshold.

Examples

Set the global threshold to 100 for triggering destination-based DNS response flood attack prevention in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] dns-reply-flood threshold 100
```

Related commands

dns-reply-flood action

dns-reply-flood detect ip

dns-reply-flood detect non-specific

dns-reply-flood port

dns-reply-flood source-threshold

Use **dns-reply-flood source-threshold** to set the global threshold for triggering source-based DNS response flood attack prevention.

Use **undo dns-reply-flood source-threshold** to restore the default.

Syntax

dns-reply-flood source-threshold *threshold-value*

undo dns-reply-flood source-threshold

Default

The global threshold is 10000 for triggering source-based DNS response flood attack prevention.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

threshold-value: Specifies the maximum receiving rate in pps for DNS responses that originate from an IP address. The value range is 0 to 1000000. If you set the threshold value to 0, the source-based DNS response flood attack prevention is disabled.

Usage guidelines

With global DNS response flood attack detection configured, the device is in attack detection state. When the receiving rate of DNS responses originating from an IP address keeps reaching or exceeding the threshold, the device enters prevention state and takes the specified actions. When the rate drops below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

Examples

Set the global threshold to 100 for triggering source-based DNS response flood attack prevention in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] dns-reply-flood source-threshold 100
```

Related commands

dns-reply-flood action

dns-reply-flood detect ip

dns-reply-flood detect non-specific

dns-reply-flood port

exempt acl

Use **exempt acl** to configure attack detection exemption.

Use **undo exempt acl** to restore the default.

Syntax

exempt acl [**ipv6**] { *acl-number* | **name** *acl-name* }

undo exempt acl [**ipv6**]

Default

Attack detection exemption is not configured.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

ipv6: Specifies an IPv6 ACL. To specify an IPv4 ACL, do not use this keyword.

acl-number: Specifies an ACL by its number:

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters. It must start with an English letter and to avoid confusion, it cannot be **all**.

Usage guidelines

The attack defense policy uses an ACL to identify exempted packets. The policy does not check the packets permitted by the ACL. You can configure the ACL to identify packets from trusted hosts. The exemption feature reduces the false alarm rate and improves packet processing efficiency.

If an ACL is used for attack detection exemption, only the following match criteria in the ACL permit rules take effect:

- Source IP address.
- Destination IP address.
- Source port.
- Destination port.
- Protocol.
- L3VPN instance.
- The **fragment** keyword for matching non-first fragments.

If the specified ACL does not exist or does not contain a rule, attack detection exemption does not take effect.

Examples

Configure an ACL to permit packets sourced from 1.1.1.1. Configure attack detection exemption for packets matching the ACL in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] acl basic 2001
```

```
[Sysname-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] attack-defense policy atk-policy-1
[attack-defense-policy-atk-policy-1] exempt acl 2001
```

Related commands

attack-defense policy

fin-flood action

Use **fin-flood action** to specify global actions against FIN flood attacks.

Use **undo fin-flood action** to restore the default.

Syntax

fin-flood action { **client-verify** | **drop** | **logging** } *

undo fin-flood action

Default

No global action is specified for FIN flood attacks.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

client-verify: Adds the victim IP addresses to the protected IP list for TCP client verification. If TCP client verification is enabled, the device provides proxy services for protected servers. This keyword does not take effect on source-based flood attack prevention.

drop: Drops subsequent FIN packets destined for the victim IP addresses in destination-based flood attack prevention, or drops subsequent FIN packets originating from the attacker IP addresses in source-based flood attack prevention.

logging: Enables logging for FIN flood attack events. The log messages will be sent to the log system.

Usage guidelines

For the FIN flood attack detection to collaborate with the TCP client verification, make sure the **client-verify** keyword is specified and the TCP client verification is enabled. To enable TCP client verification, use the **client-verify tcp enable** command.

The **logging** keyword enables the attack detection and prevention module to log FIN flood attack events and send log messages to the information center.

With the information center, you can set log message filtering and output rules, including output destinations.

The information center can output FIN flood attack logs to any destinations except the console and the monitor terminal. If you configure the console or monitor terminal as an output destination, the output destination setting will not take effect.

To view FIN flood attack logs stored on the device, use the **display logbuffer** command. Make sure you do not disable log output to the log buffer, which is enabled by default.

For more information about configuring the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Specify **drop** as the global action against FIN flood attacks in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] fin-flood action drop
```

Related commands

client-verify tcp enable

fin-flood detect

fin-flood detect non-specific

fin-flood source-threshold

fin-flood threshold

fin-flood detect

Use **fin-flood detect** to configure IP address-specific FIN flood attack detection.

Use **undo fin-flood detect** to remove the IP address-specific FIN flood attack detection configuration.

Syntax

fin-flood detect { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**threshold** *threshold-value*] [**action** { { **client-verify** | **drop** | **logging** } * | **none** }]

undo fin-flood detect { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]

Default

IP address-specific FIN flood attack detection is not configured.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

ip *ipv4-address*: Specifies the IPv4 address to be protected. The *ip-address* argument cannot be 255.255.255.255 or 0.0.0.0.

ipv6 *ipv6-address*: Specifies the IPv6 address to be protected. The IPv6 address cannot be a multicast address or ::.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the protected IP address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the protected IP address is on the public network.

threshold *threshold-value*: Specifies the maximum receiving rate in pps for FIN packets that are destined for the protected IP address. The value range is 1 to 1000000.

action: Specifies the actions against a detected FIN flood attack. If no action is specified, the global actions set by the **fin-flood action** command apply.

client-verify: Adds the victim IP addresses to the protected IP list for TCP client verification. If TCP client verification is enabled, the device provides proxy services for protected servers.

drop: Drops subsequent FIN packets destined for the protected IP address.

logging: Enables logging for FIN flood attack events. The log messages will be sent to the log system.

none: Takes no action.

Usage guidelines

With FIN flood attack detection configured for an IP address, the device is in attack detection state. When the receiving rate of FIN packets destined for the IP address keeps reaching or exceeding the threshold, the device enters prevention state and takes the specified actions. When the rate drops below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

You can configure FIN flood attack detection for multiple IP addresses in one attack defense policy.

The **logging** keyword enables the attack detection and prevention module to log FIN flood attack events and send log messages to the information center.

With the information center, you can set log message filtering and output rules, including output destinations.

The information center can output FIN flood attack logs to any destinations except the console and the monitor terminal. If you configure the console or monitor terminal as an output destination, the output destination setting will not take effect.

To view FIN flood attack logs stored on the device, use the **display logbuffer** command. Make sure you do not disable log output to the log buffer, which is enabled by default.

For more information about configuring the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Configure FIN flood attack detection for 192.168.1.2 in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] fin-flood detect ip 192.168.1.2 threshold 2000
```

Related commands

fin-flood action

fin-flood detect non-specific

fin-flood threshold

fin-flood detect non-specific

Use **fin-flood detect non-specific** to enable global FIN flood attack detection.

Use **undo fin-flood detect non-specific** to disable global FIN flood attack detection.

Syntax

fin-flood detect non-specific

undo fin-flood detect non-specific

Default

Global FIN flood attack detection is disabled.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Usage guidelines

The device supports the following FIN flood attack prevention types:

- **Source-based FIN flood attack prevention**—Monitors the receiving rate of FIN packets on a per-source IP basis.
- **Destination-based FIN flood attack prevention**—Monitors the receiving rate of FIN packets on a per-destination IP basis.

The global FIN flood attack detection applies to all IP addresses except for those specified by the **fin-flood detect** command. The global detection uses the global trigger threshold set by the **fin-flood threshold** or **fin-flood source-threshold** command and global actions specified by the **fin-flood action** command.

Examples

Enable global FIN flood attack detection in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] fin-flood detect non-specific
```

Related commands

fin-flood action

fin-flood detect

fin-flood source-threshold

fin-flood threshold

fin-flood threshold

Use **fin-flood threshold** to set the global threshold for triggering destination-based FIN flood attack prevention.

Use **undo fin-flood threshold** to restore the default.

Syntax

fin-flood threshold *threshold-value*

undo fin-flood threshold

Default

The global threshold is 10000 for triggering destination-based FIN flood attack prevention.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

threshold-value: Specifies the maximum receiving rate in pps for FIN packets that are destined for an IP address. The value range is 0 to 1000000. If you set the threshold value to 0, the destination-based FIN flood attack prevention is disabled.

Usage guidelines

With global FIN flood attack detection configured, the device is in attack detection state. When the receiving rate of FIN packets destined for an IP address keeps reaching or exceeding the threshold, the device enters prevention state and takes the specified actions. When the rate drops below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

The global threshold applies to global FIN flood attack detection. Adjust the threshold according to the application scenarios.

- If the number of FIN packets sent to a protected server, such as an HTTP or FTP server, is normally large, set a high threshold. A low threshold might affect the server services.
- For a network that is unstable or susceptible to attacks, set a low threshold.

Examples

Set the global threshold to 100 for triggering destination-based FIN flood attack prevention in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] fin-flood threshold 100
```

Related commands

fin-flood action

fin-flood detect

fin-flood detect non-specific

fin-flood source-threshold

Use **fin-flood source-threshold** to set the global threshold for triggering source-based FIN flood attack prevention.

Use **undo fin-flood source-threshold** to restore the default.

Syntax

fin-flood source-**threshold** *threshold-value*

undo fin-flood source-**threshold**

Default

The global threshold is 10000 for triggering source-based FIN flood attack prevention.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

threshold-value: Specifies the maximum receiving rate in pps for FIN packets that originate from an IP address. The value range is 0 to 1000000. If you set the threshold value to 0, the source-based FIN flood attack prevention is disabled.

Usage guidelines

With global FIN flood attack detection configured, the device is in attack detection state. When the receiving rate of FIN packets originating from an IP address keeps reaching or exceeding the threshold, the device enters prevention state and takes the specified actions. When the rate drops below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

Examples

Set the global threshold to 100 for triggering source-based FIN flood attack prevention in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] fin-flood source-threshold 100
```

Related commands

fin-flood action

fin-flood detect

fin-flood detect non-specific

http-flood action

Use **http-flood action** to specify global actions against HTTP flood attacks.

Use **undo http-flood action** to restore the default.

Syntax

http-flood action { **client-verify** | **drop** | **logging** } *

undo http-flood action

Default

No global action is specified for HTTP flood attacks.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

client-verify: Adds the victim IP addresses to the protected IP list for HTTP client verification. If HTTP client verification is enabled, the device provides proxy services for protected servers. This keyword does not take effect on source-based flood attack prevention.

drop: Drops subsequent HTTP packets destined for the victim IP addresses in destination-based flood attack prevention, or drops subsequent HTTP packets originating from the attacker IP addresses in source-based flood attack prevention.

logging: Enables logging for HTTP flood attack events. The log messages will be sent to the log system.

Usage guidelines

For the HTTP flood attack detection to collaborate with the HTTP client verification, make sure the **client-verify** keyword is specified and the HTTP client verification is enabled. To enable HTTP client verification, use the **client-verify http enable** command.

The **logging** keyword enables the attack detection and prevention module to log HTTP flood attack events and send log messages to the information center.

With the information center, you can set log message filtering and output rules, including output destinations.

The information center can output HTTP flood attack logs to any destinations except the console and the monitor terminal. If you configure the console or monitor terminal as an output destination, the output destination setting will not take effect.

To view HTTP flood attack logs stored on the device, use the **display logbuffer** command. Make sure you do not disable log output to the log buffer, which is enabled by default.

For more information about configuring the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Specify **drop** as the global action against HTTP flood attacks in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] http-flood action drop
```

Related commands

client-verify http enable

http-flood detect

http-flood detect non-specific

http-flood source-threshold

http-flood threshold

http-flood detect

Use **http-flood detect** to configure IP address-specific HTTP flood attack detection.

Use **undo http-flood detect** to remove the IP address-specific HTTP flood attack detection configuration.

Syntax

http-flood detect { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**port** *port-list*] [**threshold** *threshold-value*] [**action** { { **client-verify** | **drop** | **logging** } * | **none** }]

undo http-flood detect { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]

Default

IP address-specific HTTP flood attack detection is not configured.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

ip *ipv4-address*: Specifies the IPv4 address to be protected. The *ip-address* argument cannot be 255.255.255.255 or 0.0.0.0.

ipv6 *ipv6-address*: Specifies the IPv6 address to be protected. The IPv6 address cannot be a multicast address or ::.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the protected IP address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the protected IP address is on the public network.

port *port-list*: Specifies a space-separated list of up to 24 port number items. Each item specifies a port by its port number or a range of ports in the form of *start-port-number* to *end-port-number*. The *end-port-number* cannot be smaller than the *start-port-number*. If you do not specify this option, the global ports apply.

threshold *threshold-value*: Specifies the maximum receiving rate in pps for HTTP packets that are destined for the protected IP address. The value range is 1 to 1000000.

action: Specifies the actions against a detected HTTP flood attack. If no action is specified, the global actions set by the **http-flood action** command apply.

client-verify: Adds the victim IP addresses to the protected IP list for HTTP client verification. If HTTP client verification is enabled, the device provides proxy services for protected servers.

drop: Drops subsequent HTTP packets destined for the protected IP address.

logging: Enables logging for HTTP flood attack events. The log messages will be sent to the log system.

none: Takes no action.

Usage guidelines

With HTTP flood attack detection configured for an IP address, the device is in attack detection state. When the receiving rate of HTTP packets destined for the IP address keeps reaching or exceeding the threshold, the device enters prevention state and takes the specified actions. When the rate drops below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

You can configure HTTP flood attack detection for multiple IP addresses in one attack defense policy.

The **logging** keyword enables the attack detection and prevention module to log HTTP flood attack events and send log messages to the information center.

With the information center, you can set log message filtering and output rules, including output destinations.

The information center can output HTTP flood attack logs to any destinations except the console and the monitor terminal. If you configure the console or monitor terminal as an output destination, the output destination setting will not take effect.

To view HTTP flood attack logs stored on the device, use the **display logbuffer** command. Make sure you do not disable log output to the log buffer, which is enabled by default.

For more information about configuring the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Configure HTTP flood attack detection for 192.168.1.2 in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
```

```
[Sysname-attack-defense-policy-atk-policy-1] http-flood detect ip 192.168.1.2 port 80
8080 threshold 2000
```

Related commands

`http-flood action`

`http-flood detect non-specific`

`http-flood port`

`http-flood threshold`

http-flood detect non-specific

Use **`http-flood detect non-specific`** to enable global HTTP flood attack detection.

Use **`undo http-flood detect non-specific`** to disable global HTTP flood attack detection.

Syntax

`http-flood detect non-specific`

`undo http-flood detect non-specific`

Default

Global HTTP flood attack detection is disabled.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Usage guidelines

The device supports the following HTTP flood attack prevention types:

- **Source-based HTTP response flood attack prevention**—Monitors the receiving rate of HTTP packets on a per-source IP basis.
- **Destination-based HTTP response flood attack prevention**—Monitors the receiving rate of HTTP packets on a per-destination IP basis.

The global HTTP flood attack detection applies to all IP addresses except for those specified by the **`http-flood detect`** command. The global detection uses the global trigger threshold set by the **`http-flood threshold`** or **`http-flood source-threshold`** command and global actions specified by the **`http-flood action`** command.

Examples

Enable global HTTP flood attack detection in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] dns-flood detect non-specific
```

Related commands

`http-flood action`

`http-flood detect`

`http-flood source-threshold`

`http-flood threshold`

http-flood port

Use **http-flood port** to specify the global ports to be protected against HTTP flood attacks.

Use **undo http-flood port** to restore the default.

Syntax

http-flood port *port-list*

undo http-flood port

Default

The global HTTP flood attack prevention protects port 80.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

port-list: Specifies a space-separated list of up to 32 port number items. Each item specifies a port by its port number or a range of ports in the form of *start-port-number* to *end-port-number*. The *end-port-number* cannot be smaller than the *start-port-number*.

Usage guidelines

The device detects only HTTP packets destined for the specified ports.

The global ports apply to global HTTP flood attack detection and IP address-specific HTTP flood attack detection with no port specified.

Examples

Specify the ports 80 and 8080 as the global ports to be protected against HTTP flood attacks in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] http-flood port 80 8080
```

Related commands

http-flood action

http-flood detect

http-flood detect non-specific

http-flood source-threshold

http-flood threshold

http-flood threshold

Use **http-flood threshold** to set the global threshold for triggering destination-based HTTP flood attack prevention.

Use **undo http-flood threshold** to restore the default.

Syntax

http-flood threshold *threshold-value*

undo http-flood threshold

Default

The global threshold is 10000 for triggering destination-based HTTP flood attack prevention.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

threshold-value: Specifies the maximum receiving rate in pps for HTTP packets that are destined for an IP address. The value range is 0 to 1000000. If you set the threshold value to 0, the destination-based HTTP flood attack prevention is disabled.

Usage guidelines

With global HTTP flood attack detection configured, the device is in attack detection state. When the receiving rate of HTTP packets destined for an IP address keeps reaching or exceeding the threshold, the device enters prevention state and takes the specified actions. When the rate drops below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

The global threshold applies to global HTTP flood attack detection. Adjust the threshold according to the application scenarios.

- If the number of HTTP packets sent to a protected HTTP server is normally large, set a high threshold. A low threshold might affect the server services.
- For a network that is unstable or susceptible to attacks, set a low threshold.

Examples

Set the global threshold to 100 for triggering HTTP flood attack prevention in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] http-flood threshold 100
```

Related commands

http-flood action

http-flood detect

http-flood detect non-specific

http-flood port

http-flood source-threshold

Use **http-flood source-threshold** to set the global threshold for triggering source-based HTTP flood attack prevention.

Use **undo http-flood source-threshold** to restore the default.

Syntax

http-flood source-threshold *threshold-value*

undo http-flood source-threshold

Default

The global threshold is 10000 for triggering source-based HTTP flood attack prevention.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

threshold-value: Specifies the maximum receiving rate in pps for HTTP packets that originate from an IP address. The value range is 0 to 1000000. If you set the threshold value to 0, the source-based HTTP flood attack prevention is disabled.

Usage guidelines

With global HTTP flood attack detection configured, the device is in attack detection state. When the receiving rate of HTTP packets originating from an IP address keeps reaching or exceeding the threshold, the device enters prevention state and takes the specified actions. When the rate drops below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

Examples

Set the global threshold to 100 for triggering source-based HTTP flood attack prevention in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] http-flood source-threshold 100
```

Related commands

http-flood action

http-flood detect

http-flood detect non-specific

http-flood port

http-slow-attack action

Use **http-slow-attack action** to specify the global actions against HTTP slow attacks.

Use **undo http-slow-attack action** to restore the default.

Syntax

http-slow-attack action { **block-source** [**timeout** *minutes*] | **logging** } *

undo http-slow-attack action

Default

No global actions are specified for HTTP slow attacks.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

block-source: Drops subsequent packets from IP addresses that launch HTTP slow attacks. When the device detects an HTTP slow attack, it adds the IP address of the attack source as a dynamic IP blacklist entry. If the blacklist feature is enabled in the security zone to which the attack defense policy applies, the device drops packets originating from this IP address.

timeout *minutes*: Specifies the aging time in minutes for dynamically added blacklist entries. The value range is 1 to 10080, and the default is 10.

logging: Enables logging for HTTP slow attack events. The log messages will be sent to the log system.

Usage guidelines

For the dynamically added IP blacklist entries to take effect, make sure the blacklist feature is enabled in the security zone to which the attack defense policy applies.

Examples

In attack defense policy **atk-policy-1**, specify **block-source** and **logging** as the global actions against HTTP slow attacks, and set the aging time to 10 minutes for dynamic blacklist entries.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] http-slow-attack action logging
block-source timeout 10
```

Related commands

blacklist enable

blacklist global enable

http-slow-attack detect

http-slow-attack detect non-specific

http-slow-attack period

http-slow-attack port

http-slow-attack threshold

http-slow-attack detect

Use **http-slow-attack detect** to configure IP address-specific HTTP slow attack detection.

Use **undo http-slow-attack detect** to remove the IP address-specific HTTP slow attack detection configuration.

Syntax

http-slow-attack detect { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**port** { *start-port-number* [**to** *end-port-number*] } &<1-16>] [**threshold** { **alert-number** *alert-number* | **content-length** *content-length* | **payload-length** *payload-length* |

packet-number *packet-number* }*] [**period** *period*] [**action** { **block-source** [**timeout** *minutes*] | **logging** }*]

undo http-slow-attack detect { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]

Default

IP address-specific HTTP slow attack detection is not configured.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

ip *ipv4-address*: Specifies the IPv4 address to be protected. The *ip-address* argument cannot be 255.255.255.255 or 0.0.0.0.

ipv6 *ipv6-address*: Specifies the IPv6 address to be protected. The IPv6 address cannot be a multicast address or ::.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the protected IP address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the protected IP address is on the public network.

port *port-list*: Specifies a space-separated list of up to 16 port number items. Each item specifies a port by its port number or a range of ports in the form of *start-port-number* to *end-port-number*. The *end-port-number* cannot be smaller than the *start-port-number*. If you do not specify this option, the global ports apply.

threshold: Specifies the threshold for triggering HTTP slow attack prevention. If you do not specify this argument, the global threshold settings for triggering HTTP slow attack prevention apply.

alert-number *alert-number*: Specifies a threshold for HTTP concurrent connections. The value range is 1 to 1200000, and the default is 5000.

content-length *content-length*: Specifies a threshold for the **Content-Length** field value in an HTTP packet. The value range is 100 to 100000000, and the default is 10000.

payload-length *payload-length*: Specifies a threshold for the payload size in an HTTP packet. The value range is 1 to 1000, and the default is 50.

packet-number *packet-number*: Specifies a threshold for abnormal packets. The value range is 1 to 1000, and the default is 10.

period *period*: Specifies a detection period in the range of 1 to 1200 seconds. If you do not specify this option, the global detection period applies.

action: Specifies actions against HTTP slow attacks. If you do not specify an action, the global defensive actions apply.

block-source: Drops subsequent packets from IP addresses that launch HTTP slow attacks. When the device detects an HTTP slow attack, it adds the IP address of the attack source as a dynamic IP blacklist entry. If the blacklist feature is enabled in the security zone to which the attack defense policy applies, the device drops packets from this IP address.

timeout *minutes*: Specifies the aging time in minutes for dynamically added blacklist entries. The value range is 1 to 10080, and the default is 10. If you do not specify this option, the global setting applies.

logging: Enables logging for HTTP slow attack events. The log messages will be sent to the log system.

Usage guidelines

For the dynamically added IP blacklist entries to take effect, make sure the blacklist feature is enabled in the security zone to which the attack defense policy applies.

If you specify part of threshold parameters for IP address-specific HTTP slow attack detection, the default settings rather than the global settings apply to the unspecified threshold parameters.

Examples

Configure HTTP slow attack detection for 1.1.1.1 in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] http-slow-attack detect ip 1.1.1.1 port 80 8080 threshold alert-number 3000 content-length 10000 payload-length 20 packet-number 10 action block-source
```

Related commands

blacklist enable

blacklist global enable

http-slow-attack action

http-slow-attack detect non-specific

http-slow-attack period

http-slow-attack port

http-slow-attack threshold

http-slow-attack detect non-specific

Use **http-slow-attack detect non-specific** to enable global HTTP slow attack detection.

Use **undo http-slow-attack detect non-specific** to disable global HTTP slow attack detection.

Syntax

http-slow-attack detect non-specific

undo http-slow-attack detect non-specific

Default

Global HTTP slow attack detection is disabled.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Usage guidelines

After you enable global HTTP slow attack detection, the device uses the following global settings to protect IP addresses:

- Threshold settings set by using the **http-slow-attack threshold** command.
- Detection period set by using the **http-slow-attack period** command.
- Ports set by using the **http-slow-attack port** command.
- Defensive actions set by using the **http-slow-attack action** command.

Examples

Enable global HTTP slow attack detection in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] http-slow-attack detect non-specific
```

Related commands

http-slow-attack action

http-slow-attack detect

http-slow-attack period

http-slow-attack port

http-slow-attack threshold

http-slow-attack period

Use **http-slow-attack period** to set the global HTTP slow attack detection period.

Use **undo http-slow-attack period** to restore the default.

Syntax

http-slow-attack period *period*

undo http-slow-attack period

Default

The global HTTP slow attack detection period is 60 seconds.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

period *period*: Specifies the detection period in seconds. The value range is 1 to 1200, and the default is 60.

Examples

Set the HTTP slow attack detection period to 10 seconds in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] http-slow-attack period 10
```

Related commands

http-slow-attack action

http-slow-attack detect

http-slow-attack detect non-specific

http-slow-attack port

http-slow-attack threshold

http-slow-attack port

Use **http-slow-attack port** to specify global ports to be protected against HTTP slow attacks.

Use **undo http-slow-attack port** to restore the default.

Syntax

http-slow-attack port *port-list* &<1-32>

undo http-slow-attack port

Default

The global HTTP slow attack prevention protects port 80.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

port-list &<1-32>: Specifies a space-separated list of up to 32 port number items. Each item specifies a port by its port number or a range of ports in the form of *start-port-number* to *end-port-number*. The *end-port-number* cannot be smaller than the *start-port-number*.

Usage guidelines

The device detects only HTTP packets destined for the specified ports.

The global ports are used in global HTTP slow attack detection and IP address-specific HTTP slow attack detection with no protected ports specified.

As a best practice, specify port 80 as the global protected port against HTTP slow attacks. If you specify other ports, make sure these ports are used for HTTP communication. If the specified ports are not used for HTTP communication, the device resources will be wasted in inspecting non-HTTP slow attack packets.

Examples

Specify ports 80 and 8080 as the global ports to be protected against HTTP slow attacks in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] http-slow-attack port 80 8000
```

Related commands

http-slow-attack action

http-slow-attack detect

http-slow-attack detect non-specific

http-slow-attack period

http-slow-attack threshold

http-slow-attack threshold

Use **http-slow-attack threshold** to set global thresholds for triggering HTTP slow attack prevention.

Use **undo http-slow-attack threshold** to restore the default.

Syntax

http-slow-attack threshold [**alert-number** *alert-number* | **content-length** *content-length* | **payload-length** *payload-length* | **packet-number** *packet-number*]*

undo http-slow-attack threshold

Default

The device enters HTTP slow attack detection state when the number of HTTP concurrent connections exceeds 5000. An HTTP packet is a slow attack packet if its **Content-Length** field value is greater than 10000 and its payload is less than 50 bytes. When the device receives more than 10 slow attack packets within the detection period, it takes defensive actions.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

alert-number *alert-number*: Specifies a threshold for HTTP concurrent connections. The value range is 1 to 1200000, and the default is 5000.

content-length *content-length*: Specifies a threshold for the **Content-Length** field value in an HTTP packet. The value range is 100 to 100000000, and the default is 10000.

payload-length *payload-length*: Specifies a threshold for the payload size in an HTTP packet. The value range is 1 to 1000, and the default is 50.

packet-number *packet-number*: Specifies a threshold for HTTP slow attack packets. The value range is 1 to 1000, and the default is 10.

Usage guidelines

The device enters the HTTP slow attack detection state when the number of HTTP concurrent connections exceeds the threshold. An HTTP packet is a slow attack packet if its **Content-Length** field value is greater than the *content-length* value and its payload is less than the *payload-length* value. When the number of attack packets received within the detection period exceeds the threshold, the device takes defensive actions.

If you do not specify a threshold for a parameter, the default value for the parameter applies.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure global HTTP slow attack detection thresholds in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] http-slow-attack threshold alert-number
3000 content-length 10000 payload-length 20 packet-number 10
```

Related commands

http-slow-attack action

http-slow-attack detect

http-slow-attack detect non-specific

http-slow-attack period

http-slow-attack port

icmp-flood action

Use **icmp-flood action** to specify global actions against ICMP flood attacks.

Use **undo icmp-flood action** to restore the default.

Syntax

icmp-flood action { **drop** | **logging** } *

undo icmp-flood action

Default

No global action is specified for ICMP flood attacks.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

drop: Drops subsequent ICMP packets destined for the victim IP addresses in destination-based flood attack prevention, or drops subsequent ICMP packets originating from the attacker IP addresses in source-based flood attack prevention.

logging: Enables logging for ICMP flood attack events. The log messages will be sent to the log system.

Usage guidelines

The **logging** keyword enables the attack detection and prevention module to log ICMP flood attack events and send log messages to the information center.

With the information center, you can set log message filtering and output rules, including output destinations.

The information center can output ICMP flood attack logs to any destinations except the console and the monitor terminal. If you configure the console or monitor terminal as an output destination, the output destination setting will not take effect.

To view ICMP flood attack logs stored on the device, use the **display logbuffer** command. Make sure you do not disable log output to the log buffer, which is enabled by default.

For more information about configuring the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Specify **drop** as the global action against ICMP flood attacks in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
```

```
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] icmp-flood action drop
```

Related commands

icmp-flood detect non-specific

icmp-flood detect ip

icmp-flood source-threshold

icmp-flood threshold

icmp-flood detect ip

Use **icmp-flood detect ip** to configure IP address-specific ICMP flood attack detection.

Use **undo icmp-flood detect ip** to remove the IP address-specific ICMP flood attack detection configuration.

Syntax

icmp-flood detect ip *ip-address* [**vpn-instance** *vpn-instance-name*] [**threshold** *threshold-value*] [**action** { { **drop** | **logging** } * | **none** }]

undo icmp-flood detect ip *ip-address* [**vpn-instance** *vpn-instance-name*]

Default

IP address-specific ICMP flood attack detection is not configured.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the IPv4 address to be protected. The *ip-address* argument cannot be 255.255.255.255 or 0.0.0.0.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the protected IP address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the protected IP address is on the public network.

threshold *threshold-value*: Specifies the maximum receiving rate in pps for ICMP packets that are destined for the protected IP address. The value range is 1 to 1000000.

action: Specifies the actions against a detected ICMP flood attack. If no action is specified, the global actions set by the **icmp-flood action** command apply.

drop: Drops subsequent ICMP packets destined for the protected IP address.

logging: Enables logging for ICMP flood attack events. The log messages will be sent to the log system.

none: Takes no action.

Usage guidelines

With ICMP flood attack detection configured for an IP address, the device is in attack detection state. When the receiving rate of ICMP packets destined for the IP address keeps reaching or exceeding the threshold, the device enters prevention state and takes the specified actions. When the rate

drops below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

You can configure ICMP flood attack detection for multiple IP addresses in one attack defense policy.

The **logging** keyword enables the attack detection and prevention module to log ICMP flood attack events and send log messages to the information center.

With the information center, you can set log message filtering and output rules, including output destinations.

The information center can output ICMP flood attack logs to any destinations except the console and the monitor terminal. If you configure the console or monitor terminal as an output destination, the output destination setting will not take effect.

To view ICMP flood attack logs stored on the device, use the **display logbuffer** command. Make sure you do not disable log output to the log buffer, which is enabled by default.

For more information about configuring the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Configure ICMP flood attack detection for 192.168.1.2 in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] icmp-flood detect ip 192.168.1.2 threshold 2000
```

Related commands

icmp-flood action

icmp-flood detect non-specific

icmp-flood threshold

icmp-flood detect non-specific

Use **icmp-flood detect non-specific** to enable global ICMP flood attack detection.

Use **undo icmp-flood detect non-specific** to disable global ICMP flood attack detection.

Syntax

icmp-flood detect non-specific

undo icmp-flood detect non-specific

Default

Global ICMP flood attack detection is disabled.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Usage guidelines

The device supports the following ICMP flood attack prevention types:

- **Source-based ICMP flood attack prevention**—Monitors the receiving rate of ICMP packets on a per-source IP basis.
- **Destination-based ICMP flood attack prevention**—Monitors the receiving rate of ICMP packets on a per-destination IP basis.

The global ICMP flood attack detection applies to all IP addresses except for those specified by the **icmp-flood detect ip** command. The global detection uses the global trigger threshold set by the **icmp-flood threshold** or **icmp-flood source-threshold** command and global actions specified by the **icmp-flood action** command.

Examples

Enable global ICMP flood attack detection in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] icmp-flood detect non-specific
```

Related commands

icmp-flood action

icmp-flood detect ip

icmp-flood source-threshold

icmp-flood threshold

icmp-flood threshold

Use **icmp-flood threshold** to set the global threshold for triggering destination-based ICMP flood attack prevention.

Use **undo icmp-flood threshold** to restore the default.

Syntax

icmp-flood threshold *threshold-value*

undo icmp-flood threshold

Default

The global threshold is 10000 for triggering destination-based ICMP flood attack prevention.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

threshold-value: Specifies the maximum receiving rate in pps for ICMP packets that are destined for an IP address. The value range is 0 to 1000000. If you set the threshold value to 0, the destination-based ICMP flood attack prevention is disabled.

Usage guidelines

With global ICMP flood attack detection configured, the device is in attack detection state. When the receiving rate of ICMP packets destined for an IP address keeps reaching or exceeding the threshold, the device enters prevention state and takes the specified actions. When the rate drops below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

The global threshold applies to global ICMP flood attack detection. Adjust the threshold according to the application scenarios.

- If the number of ICMP packets sent to a protected server, such as an HTTP or FTP server, is normally large, set a high threshold. A low threshold might affect the server services.
- For a network that is unstable or susceptible to attacks, set a low threshold.

Examples

Set the global threshold to 100 for triggering destination-based ICMP flood attack prevention in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] icmp-flood threshold 100
```

Related commands

icmp-flood action

icmp-flood detect ip

icmp-flood detect non-specific

icmp-flood source-threshold

Use **icmp-flood source-threshold** to set the global threshold for triggering source-based ICMP flood attack prevention.

Use **undo icmp-flood source-threshold** to restore the default.

Syntax

icmp-flood source-threshold *threshold-value*

undo icmp-flood source-threshold

Default

The global threshold is 10000 for triggering source-based ICMP flood attack prevention.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

threshold-value: Specifies the maximum receiving rate in pps for ICMP packets that originate from an IP address. The value range is 0 to 1000000. If you set the threshold value to 0, the source-based ICMP flood attack prevention is disabled.

Usage guidelines

With global ICMP flood attack detection configured, the device is in attack detection state. When the receiving rate of ICMP packets originating from an IP address keeps reaching or exceeding the threshold, the device enters prevention state and takes the specified actions. When the rate drops below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

Examples

Set the global threshold to 100 for triggering source-based ICMP flood attack prevention in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] icmp-flood source-threshold 100
```

Related commands

icmp-flood action

icmp-flood detect

icmp-flood detect non-specific

icmpv6-flood action

Use **icmpv6-flood action** to specify global actions against ICMPv6 flood attacks.

Use **undo icmpv6-flood action** to restore the default.

Syntax

icmpv6-flood action { **drop** | **logging** } *

undo icmpv6-flood action

Default

No global action is specified for ICMPv6 flood attacks.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

drop: Drops subsequent ICMPv6 packets destined for the victim IP addresses in destination-based flood attack prevention, or drops subsequent ICMPv6 packets originating from the attacker IPv6 addresses in source-based flood attack prevention.

logging: Enables logging for ICMPv6 flood attack events. The log messages will be sent to the log system.

Usage guidelines

The **logging** keyword enables the attack detection and prevention module to log ICMPv6 flood attack events and send log messages to the information center.

With the information center, you can set log message filtering and output rules, including output destinations.

The information center can output ICMPv6 flood attack logs to any destinations except the console and the monitor terminal. If you configure the console or monitor terminal as an output destination, the output destination setting will not take effect.

To view ICMPv6 flood attack logs stored on the device, use the **display logbuffer** command. Make sure you do not disable log output to the log buffer, which is enabled by default.

For more information about configuring the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Specify **drop** as the global action against ICMPv6 flood attacks in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] icmpv6-flood action drop
```

Related commands

icmpv6-flood detect ipv6

icmpv6-flood detect non-specific

icmpv6-flood source-threshold

icmpv6-flood threshold

icmpv6-flood detect ipv6

Use **icmpv6-flood detect ipv6** to configure IPv6 address-specific ICMPv6 flood attack detection.

Use **undo icmpv6-flood detect ipv6** to remove the IPv6 address-specific ICMPv6 flood attack detection configuration.

Syntax

icmpv6-flood detect ipv6 *ipv6-address* [**vpn-instance** *vpn-instance-name*] [**threshold** *threshold-value*] [**action** { { **drop** | **logging** } * | **none** }]

undo icmpv6-flood detect ipv6 *ipv6-address* [**vpn-instance** *vpn-instance-name*]

Default

IPv6 address-specific ICMPv6 flood attack detection is not configured.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

Ipv6-address: Specifies the IPv6 address to be protected. The IPv6 address cannot be a multicast address or ::.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the protected IPv6 address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the protected IPv6 address is on the public network.

threshold *threshold-value*: Specifies the maximum receiving rate in pps for ICMPv6 packets that are destined for the protected IP address. The value range is 1 to 1000000.

action: Specifies the actions against a detected ICMPv6 flood attack. If no action is specified, the global actions set by the **icmpv6-flood action** command apply.

drop: Drops subsequent ICMPv6 packets destined for the protected IPv6 address.

logging: Enables logging for ICMPv6 flood attack events. The log messages will be sent to the log system.

none: Takes no action.

Usage guidelines

With ICMPv6 flood attack detection configured for an IPv6 address, the device is in attack detection state. When the receiving rate of ICMPv6 packets to the IPv6 address keeps reaching or exceeding the threshold, the device enters prevention state and takes the specified actions. When the rate drops below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

You can configure ICMPv6 flood attack detection for multiple IPv6 addresses in one attack defense policy.

The **logging** keyword enables the attack detection and prevention module to log ICMPv6 flood attack events and send log messages to the information center.

With the information center, you can set log message filtering and output rules, including output destinations.

The information center can output ICMPv6 flood attack logs to any destinations except the console and the monitor terminal. If you configure the console or monitor terminal as an output destination, the output destination setting will not take effect.

To view ICMPv6 flood attack logs stored on the device, use the **display logbuffer** command. Make sure you do not disable log output to the log buffer, which is enabled by default.

For more information about configuring the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Configure ICMPv6 flood attack detection for 2012::12 in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] icmpv6-flood detect ipv6 2012::12 threshold 2000
```

Related commands

icmpv6-flood action

icmpv6-flood detect non-specific

icmpv6-flood threshold

icmpv6-flood detect non-specific

Use **icmpv6-flood detect non-specific** to enable global ICMPv6 flood attack detection.

Use **undo icmpv6-flood detect non-specific** to disable global ICMPv6 flood attack detection.

Syntax

icmpv6-flood detect non-specific

undo icmpv6-flood detect non-specific

Default

Global ICMPv6 flood attack detection is disabled.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Usage guidelines

The device supports the following ICMPv6 flood attack prevention types:

- **Source-based ICMPv6 flood attack prevention**—Monitors the receiving rate of ICMPv6 messages on a per-source IP basis.
- **Destination-based ICMPv6 flood attack prevention**—Monitors the receiving rate of ICMPv6 messages on a per-destination IP basis.

The global ICMPv6 flood attack detection applies to all IPv6 addresses except for those specified by the **icmpv6-flood detect ipv6** command. The global detection uses the global trigger threshold set by the **icmpv6-flood threshold** or **icmpv6-flood source-threshold** command and global actions specified by the **icmpv6-flood action** command.

Examples

Enable global ICMPv6 flood attack detection in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] icmpv6-flood detect non-specific
```

Related commands

icmpv6-flood action

icmpv6-flood detect ipv6

icmpv6-flood source-threshold

icmpv6-flood threshold

icmpv6-flood threshold

Use **icmpv6-flood threshold** to set the global threshold for triggering destination-based ICMPv6 flood attack prevention.

Use **undo icmpv6-flood threshold** to restore the default.

Syntax

icmpv6-flood threshold *threshold-value*

undo icmpv6-flood threshold

Default

The global threshold is 10000 for triggering destination-based ICMPv6 flood attack prevention.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

threshold-value: Specifies the maximum receiving rate in pps for ICMPv6 packets that are destined for an IP address. The value range is 0 to 1000000. If you set the threshold value to 0, the destination-based ICMPv6 flood attack prevention is disabled.

Usage guidelines

With global ICMPv6 flood attack detection configured, the device is in attack detection state. When the receiving rate of ICMPv6 packets destined for an IPv6 address keeps reaching or exceeding the threshold, the device enters prevention state and takes the specified actions. When the rate drops below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

The global threshold applies to global ICMPv6 flood attack detection. Adjust the threshold according to the application scenarios.

- If the number of ICMPv6 packets sent to a protected server, such as an HTTP or FTP server, is normally large, set a high threshold. A low threshold might affect the server services.
- For a network that is unstable or susceptible to attacks, set a low threshold.

Examples

Set the global threshold to 100 for triggering destination-based ICMPv6 flood attack prevention in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] icmpv6-flood threshold 100
```

Related commands

icmpv6-flood action

icmpv6-flood detect ipv6

icmpv6-flood detect non-specific

icmpv6-flood source-threshold

Use **icmpv6-flood source-threshold** to set the global threshold for triggering source-based ICMPv6 flood attack prevention.

Use **undo icmpv6-flood source-source-threshold** to restore the default.

Syntax

icmpv6-flood source-threshold *threshold-value*

undo icmpv6-flood source-threshold

Default

The global threshold is 10000 for triggering source-based ICMPv6 flood attack prevention.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

threshold-value: Specifies the maximum receiving rate in pps for ICMPv6 packets that originate from an IPv6 address. The value range is 0 to 1000000. If you set the threshold value to 0, the source-based ICMPv6 flood attack prevention is disabled.

Usage guidelines

With global ICMPv6 flood attack detection configured, the device is in attack detection state. When the receiving rate of ICMPv6 packets originating from an IPv6 address keeps reaching or exceeding

the threshold, the device enters prevention state and takes the specified actions. When the rate drops below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

Examples

Set the global threshold to 100 for triggering source-based ICMPv6 flood attack prevention in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] icmpv6-flood source-threshold 100
```

Related commands

icmpv6-flood action

icmpv6-flood detect

icmpv6-flood detect non-specific

reset attack-defense malformed-packet statistics

Use **reset attack-defense malformed-packet statistics** to clear statistics about malformed packets.

Syntax

reset attack-defense malformed-packet statistics

Views

User view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command clears all statistics about malformed packets.

Examples

Clear statistics about malformed packets.

```
<Sysname> reset attack-defense malformed-packet statistics
```

Related commands

display attack-defense malformed-packet statistics

reset attack-defense policy flood

Use **reset attack-defense policy flood statistics** to clear flood attack detection and prevention statistics for protected IP addresses.

Syntax

reset attack-defense policy *policy-name* **flood protected** { **ip** | **ipv6** } **statistics**

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies an attack defense policy by its name. The policy name is a case-insensitive string of 1 to 31 characters. Valid characters include uppercase and lowercase letters, digits, underscores (_), and hyphens (-).

ip: Specifies protected IPv4 addresses.

ipv6: Specifies protected IPv6 addresses.

statistics: Clears flood attack detection and prevention statistics.

Examples

Clear flood attack detection and prevention statistics for protected IPv4 addresses in attack defense policy **abc**.

```
<Sysname> reset attack-defense policy abc flood protected ip statistics
```

Clear flood attack detection and prevention statistics for protected IPv6 addresses in attack defense policy **abc**.

```
<Sysname> reset attack-defense policy abc flood protected ipv6 statistics
```

Related commands

display attack-defense policy ip

display attack-defense policy ipv6

reset attack-defense statistics security-zone

Use **reset attack-defense statistics interface** to clear attack detection and prevention statistics for a security zone.

Syntax

reset attack-defense statistics security-zone *zone-name*

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

zone-name: Specifies a security zone by its name. The *zone-name* argument is a case-insensitive string of 1 to 31 characters. It cannot contain hyphens (-).

Examples

Clear attack detection and prevention statistics for security zone **DMZ**.

```
<Sysname> reset attack-defense statistics security-zone dmz
```

Related commands

display attack defense policy

reset attack-defense top-attack-statistics

Use **reset attack-defense top-attack-statistics** to clear top 10 attack statistics.

Syntax

reset attack-defense top-attack-statistics

Views

User view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Clear top 10 attack statistics.

```
<Sysname> reset attack-defense top-attack-statistics
```

Related commands

attack-defense top-attack-statistics enable

display attack-defense top-attack-statistics

reset blacklist destination-ip

Use **reset blacklist destination-ip** to delete dynamic destination IPv4 blacklist entries.

Syntax

reset blacklist destination-ip { *destination-ip-address* [**vpn-instance** *vpn-instance-name*] | **all** }

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

destination-ip-address: Specifies an IPv4 address.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the IPv4 address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the IPv4 address is on the public network.

all: Specifies all dynamic destination IPv4 blacklist entries.

Usage guidelines

This command deletes only dynamic destination IPv4 blacklist entries. To delete manual destination IPv4 blacklist entries, use the **undo blacklist destination-ip** command.

Examples

Delete all dynamic destination IPv4 blacklist entries.

```
<Sysname> reset blacklist destination-ip all
```

Related commands

display blacklist destination-ip

reset blacklist destination-ipv6

Use **reset blacklist destination-ipv6** to delete dynamic destination IPv6 blacklist entries.

Syntax

reset blacklist destination-ipv6 { *destination-ipv6-address* [**vpn-instance** *vpn-instance-name*] | **all** }

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

destination-ipv6-address : Specifies an IPv6 address.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the IPv6 address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the IPv6 address is on the public network.

all: Specifies all dynamic destination IPv4 blacklist entries.

Usage guidelines

This command deletes only dynamic destination IPv6 blacklist entries. To delete manual destination IPv6 blacklist entries, use the **undo blacklist destination-ipv6** command.

Examples

Delete all dynamic destination IPv6 blacklist entries.

```
<Sysname> reset blacklist destination-ipv6 all
```

Related commands

display blacklist ipv6

reset blacklist ip

Use **reset blacklist ip** to delete dynamic IPv4 blacklist entries.

Syntax

reset blacklist ip { *source-ip-address* [**vpn-instance** *vpn-instance-name*] [**ds-lite-peer** *ds-lite-peer-address*] | **all** }

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

source-ip-address: Specifies the IPv4 address for a blacklist entry.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the IPv4 address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the IPv4 address is on the public network.

ds-lite-peer *ds-lite-peer-address*: Specifies the IPv6 address of the B4 element of the DS-Lite tunnel that transmits packets from the blacklisted IPv4 address. Do not specify this option if the IPv4 address is on the public network.

all: Specifies all dynamic IPv4 blacklist entries.

Usage guidelines

This command deletes only dynamic IPv4 blacklist entries. To delete manual IPv4 blacklist entries, use the **undo blacklist ip** command.

Examples

Delete all dynamic IPv4 blacklist entries.

```
<Sysname> reset blacklist ip all
```

Related commands

display blacklist ip

reset blacklist ipv6

Use **reset blacklist ipv6** to delete dynamic IPv6 blacklist entries.

Syntax

reset blacklist ipv6 { *source-ipv6-address* [**vpn-instance** *vpn-instance-name*] | **all** }

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

source-ipv6-address: Specifies the IPv6 address for a blacklist entry.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the IPv6 address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the IPv6 address is on the public network.

all: Specifies all dynamic IPv6 blacklist entries.

Usage guidelines

This command deletes only dynamic IPv6 blacklist entries. To delete manual IPv6 blacklist entries, use the **undo blacklist ipv6** command.

Examples

Delete all dynamic IPv6 blacklist entries.

```
<Sysname> reset blacklist ipv6 all
```

Related commands

display blacklist ipv6

reset blacklist statistics

Use **reset blacklist statistics** to clear blacklist statistics.

Syntax

reset blacklist statistics

Views

User view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command resets the counter for dropped packets for all blacklist entries.

Examples

Clear blacklist statistics.

```
<Sysname> reset blacklist statistics
```

Related commands

display blacklist ip

display blacklist ipv6

reset client-verify protected statistics

Use **reset client-verify protected statistics** to clear protected IP statistics for client verification.

Syntax

reset client-verify { **dns** | **dns-reply** | **http** | **sip** | **tcp** } **protected** { **ip** | **ipv6** } **statistics**

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

dns: Specifies the DNS client verification feature.

dns-reply: Specifies the DNS response verification feature.

http: Specifies the HTTP client verification feature.

sip: Specifies the SIP client verification feature.

tcp: Specifies the TCP client verification feature.

ip: Specifies the protected IPv4 list.

ipv6: Specifies the protected IPv6 list.

Examples

Clear the protected IPv4 statistics for TCP client verification.

```
<Sysname> reset client-verify tcp protected ip statistics
```

Related commands

display client-verify protected ip

display client-verify protected ipv6

reset client-verify trusted

Use **reset client-verify trusted** to clear the trusted IP list for client verification.

Syntax

reset client-verify { **dns** | **dns-reply** | **http** | **sip** | **tcp** } **trusted** { **ip** | **ipv6** }

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

dns: Specifies the DNS client verification feature.

dns-reply: Specifies the DNS response verification feature.

http: Specifies the HTTP client verification feature.

sip: Specifies the SIP client verification feature.

tcp: Specifies the TCP client verification feature.

ip: Specifies the trusted IPv4 list.

ipv6: Specifies the trusted IPv6 list.

Examples

Clear the trusted IPv4 list for DNS client verification.

```
<Sysname> reset client-verify dns trusted ip
```

Related commands

display client-verify trusted ip

display client-verify trusted ipv6

reset whitelist statistics

Use **reset whitelist statistics** to clear statistics about packets that match the address object groups on the whitelist.

Syntax

reset whitelist statistics

Views

User view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command clears statistics about packets that match all address object groups on the whitelist.

Examples

Clear statistics about packets that match the address object groups on the whitelist.

```
<Sysname> reset whitelist statistics
```

Related commands

display whitelist object-group

rst-flood action

Use **rst-flood action** to specify global actions against RST flood attacks.

Use **undo rst-flood action** to restore the default.

Syntax

rst-flood action { **client-verify** | **drop** | **logging** } *

undo rst-flood action

Default

No global action is specified for RST flood attacks.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

client-verify: Adds the victim IP addresses to the protected IP list for TCP client verification. If TCP client verification is enabled, the device provides proxy services for protected servers. This keyword does not take effect on source-based flood attack prevention.

drop: Drops subsequent RST packets destined for the victim IP addresses in destination-based flood attack prevention, or drops subsequent RST packets originating from the attacker IP addresses in source-based flood attack prevention.

logging: Enables logging for RST flood attack events. The log messages will be sent to the log system.

Usage guidelines

For the RST flood attack detection to collaborate with the TCP client verification, make sure the **client-verify** keyword is specified and the TCP client verification is enabled. To enable TCP client verification, use the **client-verify tcp enable** command.

The **logging** keyword enables the attack detection and prevention module to log RST flood attack events and send log messages to the information center.

With the information center, you can set log message filtering and output rules, including output destinations.

The information center can output RST flood attack logs to any destinations except the console and the monitor terminal. If you configure the console or monitor terminal as an output destination, the output destination setting will not take effect.

To view RST flood attack logs stored on the device, use the **display logbuffer** command. Make sure you do not disable log output to the log buffer, which is enabled by default.

For more information about configuring the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Specify **drop** as the global action against RST flood attacks in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] rst-flood action drop
```

Related commands

client-verify tcp enable

rst-flood detect

rst-flood detect non-specific

rst-flood source-threshold

rst-flood threshold

rst-flood detect

Use **rst-flood detect** to configure IP address-specific RST flood attack detection.

Use **undo rst-flood detect** to remove the IP address-specific RST flood attack detection configuration.

Syntax

rst-flood detect { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**threshold** *threshold-value*] [**action** { { **client-verify** | **drop** | **logging** } * | **none** }]

undo rst-flood detect { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]

Default

IP address-specific RST flood attack detection is not configured.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

ip *ipv4-address*: Specifies the IPv4 address to be protected. The *ip-address* argument cannot be 255.255.255.255 or 0.0.0.0.

ipv6 *ipv6-address*: Specifies the IPv6 address to be protected. The IPv6 address cannot be a multicast address or ::.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the protected IP address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the protected IP address is on the public network.

threshold *threshold-value*: Specifies the maximum receiving rate in pps for RST packets that are destined for the protected IP address. The value range is 1 to 1000000.

action: Specifies the actions against a detected RST flood attack. If no action is specified, the global actions set by the **rst-flood action** command apply.

client-verify: Adds the victim IP addresses to the protected IP list for TCP client verification. If TCP client verification is enabled, the device provides proxy services for protected servers.

drop: Drops subsequent RST packets destined for the protected IP address.

logging: Enables logging for RST flood attack events. The log messages will be sent to the log system.

none: Takes no action.

Usage guidelines

With RST flood attack detection configured for an IP address, the device is in attack detection state. When the receiving rate of RST packets destined for the IP address keeps reaching or exceeding the threshold, the device enters prevention state and takes the specified actions. When the rate drops below the silence threshold (three-fourths of the threshold), the device considers returns to the attack detection state.

You can configure RST flood attack detection for multiple IP addresses in one attack defense policy.

The **logging** keyword enables the attack detection and prevention module to log RST flood attack events and send log messages to the information center.

With the information center, you can set log message filtering and output rules, including output destinations.

The information center can output RST flood attack logs to any destinations except the console and the monitor terminal. If you configure the console or monitor terminal as an output destination, the output destination setting will not take effect.

To view RST flood attack logs stored on the device, use the **display logbuffer** command. Make sure you do not disable log output to the log buffer, which is enabled by default.

For more information about configuring the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Configure RST flood attack detection for 192.168.1.2 in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] rst-flood detect ip 192.168.1.2 threshold
2000
```

Related commands

rst-flood action

rst-flood detect non-specific

rst-flood threshold

rst-flood detect non-specific

Use **rst-flood detect non-specific** to enable global RST flood attack detection.

Use **undo rst-flood detect non-specific** to disable global RST flood attack detection.

Syntax

rst-flood detect non-specific

undo rst-flood detect non-specific

Default

Global RST flood attack detection is disabled.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Usage guidelines

The device supports the following RST flood attack prevention types:

- **Source-based RST flood attack prevention**—Monitors the receiving rate of RST packets on a per-source IP basis.
- **Destination-based RST flood attack prevention**—Monitors the receiving rate of RST packets on a per-destination IP basis.

The global RST flood attack detection applies to all IP addresses except for those specified by the **rst-flood detect** command. The global detection uses the global trigger threshold set by the **rst-flood threshold** or **rst-flood source-threshold** command and global actions specified by the **rst-flood action** command.

Examples

Enable global RST flood attack detection in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] rst-flood detect non-specific
```

Related commands

rst-flood action

rst-flood detect

rst-flood source-threshold

rst-flood threshold

rst-flood threshold

Use **rst-flood threshold** to set the global threshold for triggering destination-based RST flood attack prevention.

Use **undo rst-flood threshold** to restore the default.

Syntax

rst-flood threshold *threshold-value*

undo rst-flood threshold

Default

The global threshold is 10000 for triggering destination-based RST flood attack prevention.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

threshold-value: Specifies the maximum receiving rate in pps for RST packets that are destined for an IP address. The value range is 0 to 1000000. If you set the threshold value to 0, the destination-based RST flood attack prevention is disabled.

Usage guidelines

With global RST flood attack detection configured, the device is in attack detection state. When the receiving rate of RST packets destined for an IP address keeps reaching or exceeding the threshold, the device enters prevention state and takes the specified actions. When the rate drops below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

The global threshold applies to global RST flood attack detection. Adjust the threshold according to the application scenarios.

- If the number of RST packets sent to a protected server, such as an HTTP or FTP server, is normally large, set a high threshold. A low threshold might affect the server services.
- For a network that is unstable or susceptible to attacks, set a low threshold.

Examples

Set the global threshold to 100 for triggering destination-based RST flood attack prevention in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] rst-flood threshold 100
```

Related commands

rst-flood action

rst-flood detect

rst-flood detect non-specific

rst-flood source-threshold

Use **rst-flood source-threshold** to set the global threshold for triggering source-based RST flood attack prevention.

Use **undo rst-flood source-threshold** to restore the default.

Syntax

rst-flood source-threshold *threshold-value*

undo rst-flood source-threshold

Default

The global threshold is 10000 for triggering source-based RST flood attack prevention.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

threshold-value: Specifies the maximum receiving rate in pps for RST packets that originate from an IP address. The value range is 0 to 1000000. If you set the threshold value to 0, the source-based RST flood attack prevention is disabled.

Usage guidelines

With global RST flood attack detection configured, the device is in attack detection state. When the receiving rate of RST packets originating from to an IP address keeps reaching or exceeding the threshold, the device enters prevention state and takes the specified actions. When the rate drops below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

Examples

Set the global threshold to 100 for triggering source-based RST flood attack prevention in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] rst-flood source-threshold 100
```

Related commands

rst-flood action

rst-flood detect

rst-flood detect non-specific

scan detect

Use **scan detect** to configure scanning attack detection.

Use **undo scan detect** to remove the scanning attack detection configuration.

Syntax

scan detect level { { **high** | **low** | **medium** } | **user-defined** { **port-scan-threshold** *threshold-value* | **ip-sweep-threshold** *threshold-value* } * [**period** *period-value*] } **action** { { **block-source** [**timeout** *minutes*] | **drop** } | **logging** } *

undo scan detect

Default

No scanning attack detection is configured.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

level: Specifies the level of the scanning attack detection.

high: Specifies the high level. This level can detect most of the scanning attacks, but has a high false alarm rate. Some packets from active hosts might be considered as attack packets. For high level detection, the detection cycle is 10 seconds. The threshold for triggering port scan attack prevention is 5000 packets in a detection cycle. The threshold for triggering IP sweep attack prevention is 5000 packets in a detection cycle.

low: Specifies the low level. This level provides basic scanning attack detection. It has a low false alarm rate but many scanning attacks cannot be detected. For low level detection, the detection cycle is 10 seconds. The threshold for triggering port scan attack prevention is 100000 packets in a detection cycle. The threshold for triggering IP sweep attack prevention is 100000 packets in a detection cycle.

medium: Specifies the medium level. Compared with the high and low levels, this level has medium false alarm rate and attack detection accuracy. For medium level detection, the detection cycle is 10 seconds. The threshold for triggering port scan attack prevention is 40000 packets. The threshold for triggering IP sweep attack prevention is 40000 packets.

user-defined: Specifies the user-defined level. This level allows you to set the thresholds and detection cycle for port scan and IP sweep attacks on demand.

port-scan-threshold *threshold-value*: Specifies the maximum number of packets sent from an IP address to different ports within a detection cycle. The value range is 1 to 1000000000.

ip-sweep-threshold *threshold-value*: Specifies the maximum number of packets sent from an IP address to different IP addresses within a detection cycle. The value range is 1 to 1000000000.

period *period-value*: Sets the scanning attack detection cycle in the range of 1 to 1000000000 seconds. The default value is 10.

action: Specifies the actions against scanning attacks.

block-source: Adds the attackers' IP addresses to the IP blacklist. If the blacklist feature is enabled on the receiving security zone, the device drops subsequent packets from the blacklisted IP addresses.

timeout *minutes*: Specifies the aging timer in minutes for the dynamically added blacklist entries, in the range of 1 to 10080. The default aging timer is 10 minutes.

drop: Drops subsequent packets from detected scanning attack sources. The log messages will be sent to the log system.

logging: Enables logging for scanning attack events.

Usage guidelines

To collaborate with the IP blacklist feature, make sure the blacklist feature is enabled in the security zone to which the attack defense policy is applied.

The aging timer set by the **timeout** *minutes* option must be longer than the statistics collection interval.

The **logging** keyword enables the attack detection and prevention module to log RST flood attack events and send log messages to the information center.

With the information center, you can set log message filtering and output rules, including output destinations.

The information center can output scanning attack logs to any destinations except the console and the monitor terminal. If you configure the console or monitor terminal as an output destination, the output destination setting will not take effect.

To view scanning attack logs stored on the device, use the **display logbuffer** command. Make sure you do not disable log output to the log buffer, which is enabled by default.

For more information about configuring the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Configure low level scanning attack detection and specify the prevention action as **drop** in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] scan detect level low action drop
```

Configure scanning attack detection in attack defense policy **atk-policy-1**. Specify the detection level as **low** and the prevention actions as **block-source** and **logging**. Set the aging time for the dynamically added IP blacklist entries to 10 minutes.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] scan detect level low action logging
block-source timeout 10
```

Configure scanning attack detection in the attack defense policy **atk-policy-1**. Specify the detection level as **user-defined** and detection cycle as 30 seconds. Set the port scan attack prevention threshold and IP sweep attack prevention threshold to 6000 packets and 80000 packets, respectively. Specify the prevention action as **block-source** and **logging**. Set the aging time for the dynamically added IP blacklist entries to 10 minutes.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] scan detect level user-defined
port-scan-threshold 6000 ip-sweep-threshold 80000 period 30 action logging block-source
timeout 10
```

Related commands

blacklist enable

blacklist global enable

signature { large-icmp | large-icmpv6 } max-length

Use **signature** { **large-icmp** | **large-icmpv6** } **max-length** to set the maximum length of safe ICMP or ICMPv6 packets. A large ICMP or ICMPv6 attack occurs if an ICMP or ICMPv6 packet larger than the specified length is detected.

Use **undo signature** { **large-icmp** | **large-icmpv6** } **max-length** to restore the default.

Syntax

signature { **large-icmp** | **large-icmpv6** } **max-length** *length*

undo signature { **large-icmp** | **large-icmpv6** } **max-length**

Default

The maximum length of safe ICMP or ICMPv6 packets is 4000 bytes.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

large-icmp: Specifies large ICMP packet attack signature.

large-icmpv6: Specifies large ICMPv6 packet attack signature.

length: Specifies the maximum length of safe ICMP or ICMPv6 packets, in bytes. The value range for ICMP packets is 28 to 65534. The value range for ICMPv6 packets is 48 to 65534.

Examples

Set the maximum length of safe ICMP packets for large ICMP attack to 50000 bytes in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] signature large-icmp max-length 50000
```

Related commands

signature detect

signature detect

Use **signature detect** to enable signature detection for single-packet attacks and specify the prevention actions.

Use **undo signature detect** to disable signature detection for single-packet attacks.

Syntax

signature detect { **fraggle** | **fragment** | **impossible** | **land** | **large-icmp** | **large-icmpv6** | **smurf** | **snork** | **tcp-all-flags** | **tcp-fin-only** | **tcp-invalid-flags** | **tcp-null-flag** | **tcp-syn-fin** | **tiny-fragment** | **traceroute** | **udp-bomb** | **winnuke** } [**action** { { **drop** | **logging** } * | **none** }]

undo signature detect { **fraggle** | **fragment** | **impossible** | **land** | **large-icmp** | **large-icmpv6** | **smurf** | **snork** | **tcp-all-flags** | **tcp-fin-only** | **tcp-invalid-flags** | **tcp-null-flag** | **tcp-syn-fin** | **tiny-fragment** | **traceroute** | **udp-bomb** | **winnuke** }

signature detect { **ip-option-abnormal** | **ping-of-death** | **teardrop** } **action** { **drop** | **logging** } *

undo signature detect { **ip-option-abnormal** | **ping-of-death** | **teardrop** }

signature detect icmp-type { *icmp-type-value* | **address-mask-reply** | **address-mask-request** | **destination-unreachable** | **echo-reply** | **echo-request** | **information-reply** | **information-request** | **parameter-problem** | **redirect** | **source-quench** | **time-exceeded** | **timestamp-reply** | **timestamp-request** } [**action** { { **drop** | **logging** } * | **none** }]

undo signature detect icmp-type { *icmp-type-value* | **address-mask-reply** | **address-mask-request** | **destination-unreachable** | **echo-reply** | **echo-request** | **information-reply** | **information-request** | **parameter-problem** | **redirect** | **source-quench** | **time-exceeded** | **timestamp-reply** | **timestamp-request** }

signature detect icmpv6-type { *icmpv6-type-value* | **destination-unreachable** | **echo-reply** | **echo-request** | **group-query** | **group-reduction** | **group-report** | **packet-too-big** | **parameter-problem** | **time-exceeded** } [**action** { { **drop** | **logging** } * | **none** }]

undo signature detect icmpv6-type { *icmpv6-type-value* | **destination-unreachable** | **echo-reply** | **echo-request** | **group-query** | **group-reduction** | **group-report** | **packet-too-big** | **parameter-problem** | **time-exceeded** }

signature detect ip-option { *option-code* | **internet-timestamp** | **loose-source-routing** | **record-route** | **route-alert** | **security** | **stream-id** | **strict-source-routing** } [**action** { { **drop** | **logging** } * | **none** }]

undo signature detect ip-option { *option-code* | **internet-timestamp** | **loose-source-routing** | **record-route** | **route-alert** | **security** | **stream-id** | **strict-source-routing** }

signature detect ipv6-ext-header *ext-header-value* [**action** { { **drop** | **logging** } * | **none** }]

undo signature detect ipv6-ext-header *next-header-value*

signature detect ipv6-ext-header-abnormal [**action** { { **drop** | **logging** } * | **none** }]

undo signature detect ipv6-ext-header-abnormal

signature detect ipv6-ext-header-exceed [**limit** *limit-value*] [**action** { { **drop** | **logging** } * | **none** }]

undo signature detect ipv6-ext-header-exceed

Default

Signature detection is disabled for all single-packet attacks.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

fraggle: Specifies the fraggle attack.

fragment: Specifies the IP fragment attack.

icmp-type: Specifies an ICMP packet attack by the packet type. You can specify the packet type by a number or a keyword:

- *icmp-type-value*: Specifies the ICMP packet type in the range of 0 to 255.
- **address-mask-reply**: Specifies the ICMP address mask reply type.
- **address-mask-request**: Specifies the ICMP address mask request type.
- **destination-unreachable**: Specifies the ICMP destination unreachable type.
- **echo-reply**: Specifies the ICMP echo reply type.
- **echo-request**: Specifies the ICMP echo request type.
- **information-reply**: Specifies the ICMP information reply type.
- **information-request**: Specifies the ICMP information request type.
- **parameter-problem**: Specifies the ICMP parameter problem type.
- **redirect**: Specifies the ICMP redirect type.
- **source-quench**: Specifies the ICMP source quench type.

- **time-exceeded**: Specifies the ICMP time exceeded type.
- **timestamp-reply**: Specifies the ICMP timestamp reply type.
- **timestamp-request**: Specifies the ICMP timestamp request type.

icmpv6-type: Specifies an ICMPv6 packet attack by the packet type. You can specify the packet type by a number or a keyword:

- *icmpv6-type-value*: Specifies the ICMPv6 packet type in the range of 0 to 255.
- **destination-unreachable**: Specifies the ICMPv6 destination unreachable type.
- **echo-reply**: Specifies the ICMPv6 echo reply type.
- **echo-request**: Specifies the ICMPv6 echo request type.
- **group-query**: Specifies the ICMPv6 group query type.
- **group-reduction**: Specifies the ICMPv6 group reduction type.
- **group-report**: Specifies the ICMPv6 group report type.
- **packet-too-big**: Specifies the ICMPv6 packet too big type.
- **parameter-problem**: Specifies the ICMPv6 parameter problem type.
- **time-exceeded**: Specifies the ICMPv6 time exceeded type.

impossible: Specifies the IP impossible packet attack.

ip-option: Specifies an IP option. You can specify the IP option by a number or a keyword:

- *option-code*: Specifies the IP option in the range of 1 to 255.
- **internet-timestamp**: Specifies the timestamp option.
- **loose-source-routing**: Specifies the loose source routing option.
- **record-route**: Specifies the record route option.
- **route-alert**: Specifies the route alert option.
- **security**: Specifies the security option.
- **stream-id**: Specifies the stream identifier option.
- **strict-source-routing**: Specifies the strict source route option.

ip-option-abnormal: Specifies the abnormal IP option attack.

ipv6-ext-header *ext-header-value*: Specifies an IPv6 extension header by its value in the range of 0 to 255.

ipv6-ext-header-abnormal: Specifies the abnormal IPv6 extension header attack.

ipv6-ext-header-exceed: Specifies the IPv6 extension header exceeded attack.

land: Specifies the Land attack.

large-icmp: Specifies the large ICMP packet attack.

large-icmpv6: Specifies the large ICMPv6 packet attack.

limit *limit-value*: Specifies the upper limit of IPv6 extension headers. The value range is 0 to 7, and the default is 0. An IPv6 packet is an IPv6 extension header exceeded attack packet if the number of its IPv6 extension headers exceeds the upper limit.

ping-of-death: Specifies the ping-of-death attack.

smurf: Specifies the smurf attack.

snork: Specifies the UDP snork attack.

tcp-all-flags: Specifies the attack where the TCP packet has all flags set.

tcp-fin-only: Specifies the attack where the TCP packet has only the FIN flag set.

tcp-invalid-flags: Specifies the attack that uses TCP packets with invalid flags.

tcp-null-flag: Specifies the attack where the TCP packet has no flags set.

tcp-syn-fin: Specifies the attack where the TCP packet has both SYN and FIN flags set.

teardrop: Specifies the teardrop attack.

tiny-fragment: Specifies the tiny fragment attack.

traceroute: Specifies the traceroute attack.

udp-bomb: Specifies the UDP bomb attack.

winnuke: Specifies the WinNuke attack.

action: Specifies the actions against the single-packet attack. If you do not specify this keyword, the default action of the attack level to which the single-packet attack belongs is used.

drop: Drops packets that match the specified signature.

logging: Enables logging for the specified single-packet attack.

none: Takes no action.

Usage guidelines

You can use this command multiple times to enable signature detection for multiple single-packet attack types.

When you specify a packet type by a number, if the packet type has a corresponding keyword, the keyword is displayed in command output. If the packet type does not have a corresponding keyword, the number is displayed.

In abnormal IPv6 extension header and IPv6 extension header exceeded attack detection, the device examines the ESP header and headers before it. Headers after the ESP header are not examined.

The **logging** keyword enables the attack detection and prevention module to log single-packet attack events and send log messages to the information center.

With the information center, you can set log message filtering and output rules, including output destinations.

The information center can output single-packet attack logs to any destinations except the console and the monitor terminal. If you configure the console or monitor terminal as an output destination, the output destination setting will not take effect.

To view single-packet attack logs stored on the device, use the **display logbuffer** command. Make sure you do not disable log output to the log buffer, which is enabled by default.

For more information about configuring the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Enable signature detection for the IP fragment attack and specify the prevention action as **drop** in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] signature detect fragment action drop
```

Related commands

signature level action

signature level action

Use **signature level action** to specify the actions against single-packet attacks on a specific level.

Use **undo signature level action** to restore the default.

Syntax

signature level { **high** | **info** | **low** | **medium** } **action** { { **drop** | **logging** } * | **none** }

undo signature level { **high** | **info** | **low** | **medium** } **action**

Default

For informational-level and low-level single-packet attacks, the action is **logging**.

For medium-level and high-level single-packet attacks, the actions are **logging** and **drop**.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

high: Specifies the high level. None of the currently supported single-packet attacks belongs to this level.

info: Specifies the informational level. For example, large ICMP packet attack is on this level.

low: Specifies the low level. For example, the traceroute attack is on this level.

medium: Specifies the medium level. For example, the WinNuke attack is on this level.

drop: Drops packets that match the specified level.

logging: Enable logging for single-packet attacks on the specified level.

none: Takes no action.

Usage guidelines

According to their severity, single-packet attacks are divided into four levels: **info**, **low**, **medium**, and **high**. Enabling signature detection for a specific level enables signature detection for all single-packet attacks on that level.

If you enable signature detection for a single-packet attack also by using the **signature detect** command, action parameters in the **signature detect** command take effect.

The **logging** keyword enables the attack detection and prevention module to log single-packet attack events and send log messages to the information center.

With the information center, you can set log message filtering and output rules, including output destinations.

The information center can output single-packet attack logs to any destinations except the console and the monitor terminal. If you configure the console or monitor terminal as an output destination, the output destination setting will not take effect.

To view single-packet attack logs stored on the device, use the **display logbuffer** command. Make sure you do not disable log output to the log buffer, which is enabled by default.

For more information about configuring the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Specify the action against informational-level single-packet attacks as **drop** in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy 1
[Sysname-attack-defense-policy-1] signature level info action drop
```

Related commands

signature detect

signature level detect

signature level detect

Use **signature level detect** to enable signature detection for single-packet attacks on a specific level.

Use **undo signature level detect** to disable signature detection for single-packet attacks on a specific level.

Syntax

signature level { **high** | **info** | **low** | **medium** } **detect**

undo signature level { **high** | **info** | **low** | **medium** } **detect**

Default

Signature detection is disabled for all levels of single-packet attacks.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

high: Specifies the high level. None of the currently supported single-packet attacks belongs to this level.

info: Specifies the informational level. For example, large ICMP packet attack is on this level.

low: Specifies the low level. For example, the traceroute attack is on this level.

medium: Specifies the medium level. For example, the WinNuke attack is on this level.

Usage guidelines

According to their severity, single-packet attacks are divided into four levels: **info**, **low**, **medium**, and **high**. Enabling signature detection for a specific level enables signature detection for all single-packet attacks on that level. Use the **signature level action** command to specify the actions against single-packet attacks on a specific level. If you enable signature detection for a single-packet attack also by using the **signature detect** command, action parameters in the **signature detect** command take effect.

To display the level to which a single-packet attack belongs, use the **display attack-defense policy** command.

Examples

Enable signature detection for informational-level single-packet attacks in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy 1
[Sysname-attack-defense-policy-1] signature level info detect
```

Related commands

display attack-defense policy

signature detect

signature level action

sip-flood action

Use **sip-flood action** to specify global actions against SIP flood attacks.

Use **undo sip-flood action** to restore the default.

Syntax

sip-flood action { **client-verify** | **drop** | **logging** } *

undo sip-flood action

Default

No global action is specified for SIP flood attacks.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

client-verify: Adds the victim IP addresses to the protected IP list for SIP client verification. If SIP client verification is enabled, the device provides proxy services for protected servers. This keyword does not take effect on source-based flood attack prevention.

drop: Drops subsequent SIP packets destined for the victim IP addresses in destination-based flood attack prevention, or drops subsequent SIP packets originating from the attacker IP addresses in source-based flood attack prevention.

logging: Enables logging for SIP flood attack events. The log messages will be sent to the log system.

Usage guidelines

For the SIP flood attack detection to collaborate with the SIP client verification, make sure the **client-verify** keyword is specified and the SIP client verification is enabled. To enable SIP client verification, use the **client-verify sip enable** command.

The **logging** keyword enables the attack detection and prevention module to log SIP flood attack events and send log messages to the information center.

With the information center, you can set log message filtering and output rules, including output destinations.

The information center can output SIP flood attack logs to any destinations except the console and the monitor terminal. If you configure the console or monitor terminal as an output destination, the output destination setting will not take effect.

To view SIP flood attack logs stored on the device, use the **display logbuffer** command. Make sure you do not disable log output to the log buffer, which is enabled by default.

For more information about configuring the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Specify **drop** as the global action against SIP flood attacks in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] sip-flood action drop
```

Related commands

client-verify sip enable

sip-flood detect

sip-flood detect non-specific

sip-flood port

sip-flood source-threshold

sip-flood threshold

sip-flood detect

Use **sip-flood detect** to configure IP address-specific SIP flood attack detection.

Use **undo sip-flood detect** to remove IP address-specific SIP flood attack detection configuration.

Syntax

sip-flood detect { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**port** *port-list*] [**threshold** *threshold-value*] [**action** { { **client-verify** | **drop** | **logging** } * | **none** }]

undo sip-flood detect { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]

Default

IP address-specific SIP flood attack detection is not configured.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

ip *ipv4-address*: Specifies the IPv4 address to be protected. The *ip-address* argument cannot be 255.255.255.255 or 0.0.0.0.

ipv6 *ipv6-address*: Specifies the IPv6 address to be protected. The IPv6 address cannot be a multicast address or ::.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the protected IP address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the protected IP address is on the public network.

port *port-list*: Specifies a space-separated list of up to 32 port number items. Each item specifies a port by its port number or a range of ports in the form of *start-port-number* to *end-port-number*. The *end-port-number* cannot be smaller than the *start-port-number*. If you do not specify this option, the global ports apply.

threshold *threshold-value*: Specifies the maximum receiving rate in pps for SIP packets that are destined for the protected IP address. The value range is 1 to 1000000, and the default value is 1000.

action: Specifies the actions against a detected SIP flood attack. If no action is specified, the global actions set by the **sip-flood action** command apply.

client-verify: Adds the victim IP addresses to the protected IP list for SIP client verification. If SIP client verification is enabled, the device provides proxy services for protected servers.

drop: Drops subsequent SIP packets destined for the protected IP address.

logging: Enables logging for SIP flood attack events. The log messages will be sent to the log system.

none: Takes no action.

Usage guidelines

With SIP flood attack detection configured for an IP address, the device is in attack detection state. When the receiving rate of SIP packets destined for the IP address keeps reaching or exceeding the threshold, the device enters prevention state and takes the specified actions. When the rate drops below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

You can configure SIP flood attack detection for multiple IP addresses in one attack defense policy.

The **logging** keyword enables the attack detection and prevention module to log SIP flood attack events and send log messages to the information center.

With the information center, you can set log message filtering and output rules, including output destinations.

The information center can output SIP flood attack logs to any destinations except the console and the monitor terminal. If you configure the console or monitor terminal as an output destination, the output destination setting will not take effect.

To view SIP flood attack logs stored on the device, use the **display logbuffer** command. Make sure you do not disable log output to the log buffer, which is enabled by default.

For more information about configuring the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Configure SIP flood attack detection for 192.168.1.2 in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] sip-flood detect ip 192.168.1.2 threshold
2000
```

Related commands

client-verify sip enable

sip-flood action

sip-flood detect non-specific

sip-flood port

sip-flood threshold

sip-flood detect non-specific

Use **sip-flood detect non-specific** to enable global SIP flood attack detection.

Use **undo sip-flood detect non-specific** to disable global SIP flood attack detection.

Syntax

sip-flood detect non-specific

undo sip-flood detect non-specific

Default

Global SIP flood attack detection is disabled.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Usage guidelines

The device supports the following SIP flood attack prevention types:

- **Source-based SIP flood attack prevention**—Monitors the receiving rate of SIP packets on a per-source IP basis.
- **Destination-based SIP flood attack prevention**—Monitors the receiving rate of SIP packets on a per-destination IP basis.

The global SIP flood attack detection applies to all IP addresses except those specified by the **sip-flood detect** command. The global detection is configured by using the following commands:

- Global ports set by using the **sip-flood port** command.
- Global trigger threshold set by using the **sip-flood threshold** or **sip-flood source-threshold** command.
- Global actions specified by using the **sip-flood action** command.

Examples

Enable global SIP flood attack detection in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] sip-flood detect non-specific
```

Related commands

sip-flood action

sip-flood detect

sip-flood port

sip-flood source-threshold

sip-flood threshold

sip-flood port

Use **sip-flood port** to specify the global ports to be protected against SIP flood attacks.

Use **undo sip-flood port** to restore the default.

Syntax

sip-flood port *port-list*

undo sip-flood port

Default

The global SIP flood attack prevention protects port 5060.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

port-list: Specifies a space-separated list of up to 32 port number items. Each item specifies a port by its port number or a range of ports in the form of *start-port-number* to *end-port-number*. The *end-port-number* cannot be smaller than the *start-port-number*.

Usage guidelines

The device detects only SIP packets destined for the specified ports.

The global ports apply to global SIP flood attack detection and IP address-specific SIP flood attack detection with no port specified.

Examples

Specify ports 5060 and 65530 as the global ports to be protected against SIP flood attacks in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] sip-flood port 5060 65530
```

Related commands

sip-flood action

sip-flood detect

sip-flood detect non-specific

sip-flood source-threshold

sip-flood threshold

sip-flood threshold

Use **sip-flood threshold** to set the global threshold for triggering destination-based SIP flood attack prevention.

Use **undo sip-flood threshold** to restore the default.

Syntax

sip-flood threshold *threshold-value*

undo sip-flood threshold

Default

The global threshold is 10000 for triggering destination-based SIP flood attack prevention.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

threshold-value: Specifies the maximum receiving rate in pps for SIP packets that are destined for an IP address. The value range is 0 to 1000000. If you set the threshold value to 0, the destination-based SIP flood attack prevention is disabled.

Usage guidelines

With global SIP flood attack detection configured, the device is in attack detection state. When the receiving rate of SIP packets destined for an IP address keeps reaching or exceeding the threshold, the device enters prevention state and takes the specified actions. When the rate drops below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

The global threshold applies to global SIP flood attack detection. Adjust the threshold according to the application scenarios.

- If the number of SIP packets sent to a protected SIP server is normally large, set a high threshold. A low threshold might affect the server services.
- For a network that is unstable or susceptible to attacks, set a low threshold.

Examples

Set the global threshold to 100 for triggering destination-based SIP flood attack prevention in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] sip-flood threshold 100
```

Related commands

sip-flood action

sip-flood detect

sip-flood detect non-specific

sip-flood source-threshold

Use **sip-flood source-threshold** to set the global threshold for triggering source-based SIP flood attack prevention.

Use **undo sip-flood source-threshold** to restore the default.

Syntax

sip-flood source-threshold *threshold-value*

undo sip-flood source-threshold

Default

The global threshold is 10000 for triggering source-based SIP flood attack prevention.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

threshold-value: Specifies the maximum receiving rate in pps for SIP packets that originate from an IP address. The value range is 0 to 1000000. If you set the threshold value to 0, the source-based SIP flood attack prevention is disabled.

Usage guidelines

With global SIP flood attack detection configured, the device is in attack detection state. When the receiving rate of SIP packets originating from an IP address keeps reaching or exceeding the threshold, the device enters prevention state and takes the specified actions. When the rate drops below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

Examples

Set the global threshold to 100 for triggering source-based SIP flood attack prevention in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] sip-flood source-threshold 100
```

Related commands

sip-flood action

sip-flood detect

sip-flood detect non-specific

sip-flood port

syn-ack-flood action

Use **syn-ack-flood action** to specify global actions against SYN-ACK flood attacks.

Use **undo syn-ack-flood action** to restore the default.

Syntax

syn-ack-flood action { **client-verify** | **drop** | **logging** }*

undo syn-ack-flood action

Default

No global action is specified for SYN-ACK flood attacks.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

client-verify: Adds the victim IP addresses to the protected IP list for TCP client verification. If TCP client verification is enabled, the device provides proxy services for protected servers. This keyword does not take effect on source-based flood attack prevention.

drop: Drops subsequent SYN-ACK packets destined for the victim IP addresses in destination-based flood attack prevention, or drops subsequent SYN-ACK packets originating from the attacker IP addresses in source-based flood attack prevention..

logging: Enables logging for SYN-ACK flood attack events. The log messages will be sent to the log system.

Usage guidelines

For the SYN-ACK flood attack detection to collaborate with the TCP client verification, make sure the **client-verify** keyword is specified and the TCP client verification is enabled. To enable TCP client verification, use the **client-verify tcp enable** command.

The **logging** keyword enables the attack detection and prevention module to log SYN-ACK flood attack events and send log messages to the information center.

With the information center, you can set log message filtering and output rules, including output destinations.

The information center can output SYN-ACK flood attack logs to any destinations except the console and the monitor terminal. If you configure the console or monitor terminal as an output destination, the output destination setting will not take effect.

To view SYN-ACK flood attack logs stored on the device, use the **display logbuffer** command. Make sure you do not disable log output to the log buffer, which is enabled by default.

For more information about configuring the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Specify **drop** as the global action against SYN-ACK flood attacks in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] syn-ack-flood action drop
```

Related commands

client-verify tcp enable

syn-ack-flood detect

syn-ack-flood detect non-specific

syn-ack-flood source-threshold

syn-ack-flood threshold

syn-ack-flood detect

Use **syn-ack-flood detect** to configure IP address-specific SYN-ACK flood attack detection.

Use **undo syn-ack-flood detect** to remove the IP address-specific SYN-ACK flood attack detection configuration.

Syntax

syn-ack-flood detect { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**threshold** *threshold-value*] [**action** { { **client-verify** | **drop** | **logging** } * | **none** }]

undo syn-ack-flood detect { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]

Default

IP address-specific SYN-ACK flood attack detection is not configured.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

ip *ipv4-address*: Specifies the IPv4 address to be protected. The *ip-address* argument cannot be 255.255.255.255 or 0.0.0.0.

ipv6 *ipv6-address*: Specifies the IPv6 address to be protected. The IPv6 address cannot be a multicast address or ::.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the protected IP address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the protected IP address is on the public network.

threshold *threshold-value*: Specifies the maximum receiving rate in pps for SYN-ACK packets that are destined for the protected IP address. The value range is 1 to 1000000.

action: Specifies the actions against a detected SYN-ACK flood attack. If no action is specified, the global actions set by the **syn-ack-flood action** command apply.

client-verify: Adds the victim IP addresses to the protected IP list for TCP client verification. If TCP client verification is enabled, the device provides proxy services for protected servers.

drop: Drops subsequent SYN-ACK packets destined for the protected IP address.

logging: Enables logging for SYN-ACK flood attack events. The log messages will be sent to the log system.

none: Takes no action.

Usage guidelines

With SYN-ACK flood attack detection configured for an IP address, the device is in attack detection state. When the receiving rate of SYN-ACK packets destined for the IP address keeps reaching or exceeding the threshold, the device enters prevention state and takes the specified actions. When the rate drops below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

You can configure SYN-ACK flood attack detection for multiple IP addresses in one attack defense policy.

The **logging** keyword enables the attack detection and prevention module to log SYN-ACK flood attack events and send log messages to the information center.

With the information center, you can set log message filtering and output rules, including output destinations.

The information center can output SYN-ACK flood attack logs to any destinations except the console and the monitor terminal. If you configure the console or monitor terminal as an output destination, the output destination setting will not take effect.

To view SYN-ACK flood attack logs stored on the device, use the **display logbuffer** command. Make sure you do not disable log output to the log buffer, which is enabled by default.

For more information about configuring the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Configure SYN-ACK flood attack detection for 192.168.1.2 in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] syn-ack-flood detect ip 192.168.1.2
threshold 2000
```

Related commands

syn-ack-flood action

syn-ack-flood detect non-specific

syn-ack-flood threshold

syn-ack-flood detect non-specific

Use **syn-ack-flood detect non-specific** to enable global SYN-ACK flood attack detection.

Use **undo syn-ack-flood detect non-specific** to disable global SYN-ACK flood attack detection.

Syntax

syn-ack-flood detect non-specific

undo syn-ack-flood detect non-specific

Default

Global SYN-ACK flood attack detection is disabled.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Usage guidelines

The device supports the following SYN-ACK flood attack prevention types:

- **Source-based SYN-ACK flood attack prevention**—Monitors the receiving rate of SYN-ACK packets on a per-source IP basis.
- **Destination-based SYN-ACK flood attack prevention**—Monitors the receiving rate of SYN-ACK packets on a per-destination IP basis.

The global SYN-ACK flood attack detection applies to all IP addresses except for those specified by the **syn-ack-flood detect** command. The global detection uses the global trigger threshold set by the **syn-ack-flood threshold** or **syn-ack-flood source-threshold** command and global actions specified by the **syn-ack-flood action** command.

Examples

Enable global SYN-ACK flood attack detection in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] syn-ack-flood detect non-specific
```

Related commands

syn-ack-flood action

syn-ack-flood detect

syn-ack-flood source-threshold

syn-ack-flood threshold

syn-ack-flood threshold

Use **syn-ack-flood threshold** to set the global threshold for triggering destination-based SYN-ACK flood attack prevention.

Use **undo syn-ack-flood threshold** to restore the default.

Syntax

syn-ack-flood threshold *threshold-value*

undo syn-ack-flood threshold

Default

The global threshold is 10000 for triggering destination-based SYN-ACK flood attack prevention.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

threshold-value: Specifies the maximum receiving rate in pps for SYN-ACK packets that are destined for an IP address. The value range is 0 to 1000000. If you set the threshold value to 0, the destination-based SYN-ACK flood attack prevention is disabled.

Usage guidelines

With global SYN-ACK flood attack detection configured, the device is in attack detection state. When the receiving rate of SYN-ACK packets destined for an IP address keeps reaching or exceeding the threshold, the device enters prevention state and takes the specified actions. When the rate drops below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

The global threshold applies to global SYN-ACK flood attack detection. Adjust the threshold according to the application scenarios.

- If the number of SYN-ACK packets sent to a protected server, such as an HTTP or FTP server, is normally large, set a high threshold. A low threshold might affect the server services.
- For a network that is unstable or susceptible to attacks, set a low threshold.

Examples

Set the global threshold to 100 for triggering destination-based SYN-ACK flood attack prevention in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] syn-ack-flood threshold 100
```

Related commands

syn-ack-flood action

syn-ack-flood detect

syn-ack-flood detect non-specific

syn-ack-flood source-threshold

Use **syn-ack-flood source-threshold** to set the global threshold for triggering source-based SYN-ACK flood attack prevention.

Use **undo syn-ack-flood source-threshold** to restore the default.

Syntax

syn-ack-flood source-threshold *threshold-value*

undo syn-ack-flood source-threshold

Default

The global threshold is 10000 for triggering source-based SYN-ACK flood attack prevention.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

threshold-value: Specifies the maximum receiving rate in pps for SYN-ACK packets that originate from an IP address. The value range is 0 to 1000000. If you set the threshold value to 0, the source-based SYN-ACK flood attack prevention is disabled.

Usage guidelines

With global SYN-ACK flood attack detection configured, the device is in attack detection state. When the receiving rate of SYN-ACK packets originating from an IP address keeps reaching or exceeding the threshold, the device enters prevention state and takes the specified actions. When the rate drops below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

Examples

Set the global threshold to 100 for triggering source-based SYN-ACK flood attack prevention in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] syn-ack-flood source-threshold 100
```

Related commands

syn-ack-flood action

syn-ack-flood detect

syn-ack-flood detect non-specific

syn-flood action

Use **syn-flood action** to specify global actions against SYN flood attacks.

Use **undo syn-flood action** to restore the default.

Syntax

syn-flood action { **client-verify** | **drop** | **logging** } *

undo syn-flood action

Default

No global action is specified for SYN flood attacks.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

client-verify: Adds the victim IP addresses to the protected IP list for TCP client verification. If TCP client verification is enabled, the device provides proxy services for protected servers. This keyword does not take effect on source-based flood attack prevention.

drop: Drops subsequent SYN packets destined for the victim IP addresses in destination-based flood attack prevention, or drops subsequent SYN packets originating from the attacker IP addresses in source-based flood attack prevention.

logging: Enables logging for SYN flood attack events. The log messages will be sent to the log system.

Usage guidelines

For the SYN flood attack detection to collaborate with the TCP client verification, make sure the **client-verify** keyword is specified and the TCP client verification is enabled. To enable TCP client verification, use the **client-verify tcp enable** command.

The **logging** keyword enables the attack detection and prevention module to log SYN flood attack events and send log messages to the information center.

With the information center, you can set log message filtering and output rules, including output destinations.

The information center can output SYN flood attack logs to any destinations except the console and the monitor terminal. If you configure the console or monitor terminal as an output destination, the output destination setting will not take effect.

To view SYN flood attack logs stored on the device, use the **display logbuffer** command. Make sure you do not disable log output to the log buffer, which is enabled by default.

For more information about configuring the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Specify **drop** as the global action against SYN flood attacks in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] syn-flood action drop
```

Related commands

syn-flood detect

syn-flood detect non-specific

syn-flood source-threshold

syn-flood threshold

syn-flood detect

Use **syn-flood detect** to configure IP address-specific SYN flood attack detection.

Use **undo syn-flood detect** to remove the IP address-specific SYN flood attack detection configuration.

Syntax

syn-flood detect { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**threshold** *threshold-value*] [**action** { { **client-verify** | **drop** | **logging** } * | **none** }]

undo syn-flood detect { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]

Default

IP address-specific SYN flood attack detection is not configured.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

ip *ipv4-address*: Specifies the IPv4 address to be protected. The *ip-address* argument cannot be 255.255.255.255 or 0.0.0.0.

ipv6 *ipv6-address*: Specifies the IPv6 address to be protected. The IPv6 address cannot be a multicast address or ::.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the protected IP address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the protected IP address is on the public network.

threshold *threshold-value*: Specifies the maximum receiving rate in pps for SYN packets that are destined for the protected IP address. The value range is 1 to 1000000.

action: Specifies the actions against a detected SYN flood attack. If no action is specified, the global actions set by the **syn-flood action** command apply.

client-verify: Adds the victim IP addresses to the protected IP list for TCP client verification. If TCP client verification is enabled, the device provides proxy services for protected servers.

drop: Drops subsequent SYN packets destined for the protected IP address.

logging: Enables logging for SYN flood attack events. The log messages will be sent to the log system.

none: Takes no action.

Usage guidelines

With SYN flood attack detection configured for an IP address, the device is in attack detection state. When the receiving rate of SYN packets destined for the IP address keeps reaching or exceeding the threshold, the device enters prevention state and takes the specified actions. When the rate drops below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

You can configure SYN flood attack detection for multiple IP addresses in one attack defense policy.

The **logging** keyword enables the attack detection and prevention module to log SYN flood attack events and send log messages to the information center.

With the information center, you can set log message filtering and output rules, including output destinations.

The information center can output SYN flood attack logs to any destinations except the console and the monitor terminal. If you configure the console or monitor terminal as an output destination, the output destination setting will not take effect.

To view SYN flood attack logs stored on the device, use the **display logbuffer** command. Make sure you do not disable log output to the log buffer, which is enabled by default.

For more information about configuring the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Configure SYN flood attack detection for 192.168.1.2 in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] syn-flood detect ip 192.168.1.2 threshold
2000
```

Related commands

syn-flood action

syn-flood detect non-specific

syn-flood threshold

syn-flood detect non-specific

Use **syn-flood detect non-specific** to enable global SYN flood attack detection.

Use **undo syn-flood detect non-specific** to disable global SYN flood attack detection.

Syntax

syn-flood detect non-specific

undo syn-flood detect non-specific

Default

Global SYN flood attack detection is disabled.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Usage guidelines

The device supports the following SYN flood attack prevention types:

- **Source-based SYN flood attack prevention**—Monitors the receiving rate of SYN packets on a per-source IP basis.
- **Destination-based SYN flood attack prevention**—Monitors the receiving rate of SYN packets on a per-destination IP basis.

The global SYN flood attack detection applies to all IP addresses except for those specified by the **syn-flood detect** command. The global detection uses the global trigger threshold set by the **syn-flood threshold** or **syn-flood source-threshold** command and global actions specified by the **syn-flood action** command.

Examples

Enable global SYN flood attack detection in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] syn-flood detect non-specific
```

Related commands

syn-flood action

syn-flood detect

syn-flood source-threshold

syn-flood threshold

syn-flood threshold

Use **syn-flood threshold** to set the global threshold for triggering destination-based SYN flood attack prevention.

Use **undo syn-flood threshold** to restore the default.

Syntax

syn-flood threshold *threshold-value*

undo syn-flood threshold

Default

The global threshold is 10000 for triggering destination-based SYN flood attack prevention.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

threshold-value: Specifies the maximum receiving rate in pps for SYN packets that are destined for an IP address. The value range is 0 to 1000000. If you set the threshold value to 0, the destination-based SYN flood attack prevention is disabled.

Usage guidelines

With global SYN flood attack detection configured, the device is in attack detection state. When the receiving rate of SYN packets destined for an IP address keeps reaching or exceeding the threshold, the device enters prevention state and takes the specified actions. When the rate drops below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

The global threshold applies to global SYN flood attack detection. Adjust the threshold according to the application scenarios.

- If the number of SYN packets sent to a protected server, such as an HTTP or FTP server, is normally large, set a high threshold. A low threshold might affect the server services.
- For a network that is unstable or susceptible to attacks, set a low threshold.

Examples

Set the global threshold to 100 for triggering destination-based SYN flood attack prevention in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] syn-flood threshold 100
```

Related commands

syn-flood action

syn-flood detect

syn-flood detect non-specific

syn-flood source-threshold

Use **syn-flood source-threshold** to set the global threshold for triggering source-based SYN flood attack prevention.

Use **undo syn-flood source-threshold** to restore the default.

Syntax

syn-flood source-threshold *threshold-value*

undo syn-flood source-threshold

Default

The global threshold is 10000 for triggering source-based SYN flood attack prevention.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

threshold-value: Specifies the maximum receiving rate in pps for SYN packets that originate from an IP address. The value range is 0 to 1000000. If you set the threshold value to 0, the source-based SYN flood attack prevention is disabled.

Usage guidelines

With global SYN flood attack detection configured, the device is in attack detection state. When the receiving rate of SYN packets originating from an IP address keeps reaching or exceeding the threshold, the device enters prevention state and takes the specified actions. When the rate drops below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

Examples

Set the global threshold to 100 for triggering source-based SYN flood attack prevention in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] syn-flood source-threshold 100
```

Related commands

syn-flood action

syn-flood detect

syn-flood detect non-specific

threshold-learn apply

Use **threshold-learn apply** to apply the most recent threshold that the device has learned.

Syntax

threshold-learn apply

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Usage guidelines

You can configure this command to apply the most recent threshold that the device has learned to a flood attack defense policy that meets the following requirements:

- The threshold learning feature is enabled for the policy.
- Auto applying the learned threshold is disabled for the policy.

The learned threshold is set as the global threshold for triggering flood attack prevention. The command does not take effect when auto application of the learned threshold is enabled for the policy. If you execute this command multiple times, the most recent configuration takes effect.

Before you apply the most recently learned threshold to a flood attack defense policy, make sure global attack detection is enabled for all existing flood types in this policy.

Examples

Apply the most recent threshold that the device has learned to attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] threshold-learn apply
```

Related commands

threshold-learn enable

threshold-learn auto-apply enable

Use **threshold-learn auto-apply enable** to enable auto application of the learned threshold.

Use **undo threshold-learn auto-apply enable** to disable auto application of the learned threshold.

Syntax

threshold-learn auto-apply enable

undo threshold-learn auto-apply enable

Default

Auto application of the learned threshold is disabled.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command applies to only flood attack defense policies that are enabled with the threshold learning feature (set with the **threshold-learn enable** command). Each time the device learns a threshold, it uses the learned value to update the global threshold for triggering flood attack prevention. The formula for calculating the new global threshold is learned threshold × (1 + tolerance value). The learned threshold equals the peak packet receiving rate that the device has learned within the learning duration.

To set a tolerance value, execute the **threshold-learn tolerance-value** command. Setting a tolerance value can prevent packet loss when the network experiences a traffic spike without being attacked.

Before you apply the most recently learned threshold to a flood attack defense policy, make sure global attack detection is enabled for all existing flood types in this policy.

Examples

Enable auto application of the learned threshold for attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] threshold-learn auto-apply enable
```

Related commands

threshold-learn enable

threshold-learn tolerance-value

threshold-learn duration

Use **threshold-learn duration** to set the threshold learning duration.

Use **undo threshold-learn duration** to restore the default.

Syntax

threshold-learn duration *duration*

undo threshold-learn duration

Default

The threshold learning duration is 1440 minutes.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

duration: Specifies the threshold learning duration in the range of 1 to 1200000 minutes.

Usage guidelines

The device starts threshold learning when you apply an attack defense policy enabled with the threshold learning feature. The learned threshold equals the peak packet receiving rate learned within the duration. To ensure that the device learns the peak rate in a whole day, set a learning duration longer than 1440 minutes (24 hours). If you change the learning duration during the learning process, the device will restart threshold learning.

Examples

Set the threshold learning duration to 2880 minutes (48 hours) for attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] threshold-learn duration 2880
```

Related commands

threshold-learn enable

threshold-learn loop

threshold-learn enable

Use **threshold-learn enable** to enable the threshold learning feature for flood attack prevention.

Use **undo threshold-learn enable** to disable the threshold learning feature for flood attack prevention.

Syntax

threshold-learn enable

undo threshold-learn enable

Default

The threshold learning feature for flood attack prevention is disabled.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Usage guidelines

An appropriate threshold can effectively prevent attacks. If the global threshold for triggering flood attack prevention is too low, false positives might occur, causing performance degradation or packet loss. If the global threshold is too high, false negatives might occur, making the network defenseless. Therefore, it is a good practice to enable the threshold learning feature. This feature allows the device to automatically learn the global threshold based on the traffic flows in the network.

Examples

Enable the threshold learning feature for attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] threshold-learn enable
```

Related commands

`threshold-learn auto-apply enable`

`threshold-learn duration`

threshold-learn interval

Use **`threshold-learn interval`** to set the threshold learning interval.

Use **`undo threshold-learn interval`** to restore the default.

Syntax

`threshold-learn interval` *`interval`*

`undo threshold-learn interval`

Default

The threshold learning interval is 1440 minutes.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

`interval`: Specifies a threshold learning interval in the range of 1 to 1200000 minutes.

Usage guidelines

The device performs periodic threshold learning when you apply an attack defense policy that meets the following requirements:

- The threshold learning feature is enabled for the policy by using the **`threshold-learn enable`** command.
- The periodic learning mode is set by using the **`threshold-learn mode periodic`** command.

Examples

Set the threshold learning interval to 120 minutes for attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] threshold-learn interval 120
```

Related commands

threshold-learn enable

threshold-learn mode

threshold-learn mode

Use **threshold-learn mode** to set the threshold learning mode.

Use **undo threshold-learn mode** to restore the default.

Syntax

threshold-learn mode { **once** | **periodic** }

undo threshold-learn mode

Default

The one-time learning mode is set.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

once: Specifies the one-time learning mode.

periodic: Specifies the periodic learning mode.

Usage guidelines

This command allows you to set the following threshold learning modes:

- **One-time learning**—The device performs threshold learning only once. This mode is applicable to stable networks.
- **Periodic learning**—The device performs threshold learning at intervals. The most recent learned threshold always takes effect. This mode is applicable to unstable networks. To set the threshold learning duration, use the **threshold-learn duration** command. To set the threshold learning interval, use the **threshold-learn interval** command.

Examples

Set the periodic learning mode for attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] threshold-learn mode periodic
```

Related commands

threshold-learn duration

threshold-learn enable

threshold-learn interval

threshold-learn tolerance-value

Use **threshold-learn tolerance-value** to set the threshold learning tolerance value.

Use **undo threshold-learn tolerance-value** to restore the default.

Syntax

threshold-learn tolerance-value *tolerance-value*

undo threshold-learn tolerance-value

Default

The threshold learning tolerance value is 50.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

tolerance-value: Specifies the threshold learning tolerance value in percentage, in the range of 0 to 4000.

Usage guidelines

When auto applying the learned threshold is enabled, the device uses the learned threshold and tolerance value to calculate the global threshold for triggering flood attack prevention. The formula for calculating the global threshold is learned threshold × (1 + tolerance value). Therefore, the calculated global threshold is larger than the learned threshold. This can prevent packet loss when the network experiences a traffic spike without being attacked.

The tolerance value takes effect only when auto applying the learned threshold is enabled.

Examples

Set the threshold learning tolerance value to 100 for attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] threshold-learn auto-apply enable
[Sysname-attack-defense-policy-atk-policy-1] threshold-learn tolerance-value 100
```

Related commands

threshold-learn auto-apply enable

threshold-learn enable

udp-flood action

Use **udp-flood action** to specify global actions against UDP flood attacks.

Use **undo udp-flood action** to restore the default.

Syntax

udp-flood action { **drop** | **logging** } *

undo udp-flood action

Default

No global action is specified for UDP flood attacks.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

drop: Drops subsequent UDP packets destined for the victim IP addresses in destination-based flood attack prevention, or drops subsequent UDP packets originating from the attacker IP addresses in source-based flood attack prevention.

logging: Enables logging for UDP flood attack events. The log messages will be sent to the log system.

Usage guidelines

The **logging** keyword enables the attack detection and prevention module to log UDP flood attack events and send log messages to the information center.

With the information center, you can set log message filtering and output rules, including output destinations.

The information center can output UDP flood attack logs to any destinations except the console and the monitor terminal. If you configure the console or monitor terminal as an output destination, the output destination setting will not take effect.

To view UDP flood attack logs stored on the device, use the **display logbuffer** command. Make sure you do not disable log output to the log buffer, which is enabled by default.

For more information about configuring the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Specify **drop** as the global action against UDP flood attacks in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] udp-flood action drop
```

Related commands

udp-flood detect

udp-flood detect non-specific

udp-flood source-threshold

udp-flood threshold

udp-flood detect

Use **udp-flood detect** to configure IP address-specific UDP flood attack detection.

Use **undo udp-flood detect** to remove the IP address-specific UDP flood attack detection configuration.

Syntax

udp-flood detect { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**threshold** *threshold-value*] [**action** { { **drop** | **logging** } * | **none** }]

undo udp-flood detect { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]

Default

IP address-specific UDP flood attack detection is not configured.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

ip *ipv4-address*: Specifies the IPv4 address to be protected. The *ip-address* argument cannot be 255.255.255.255 or 0.0.0.0.

ipv6 *ipv6-address*: Specifies the IPv6 address to be protected. The IPv6 address cannot be a multicast address or ::

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the protected IP address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Do not specify this option if the protected IP address is on the public network.

threshold *threshold-value*: Specifies the maximum receiving rate in pps for UDP packets that are destined for the protected IP address. The value range is 1 to 1000000.

action: Specifies the actions against a detected UDP flood attack. If no action is specified, the global actions set by the **udp-flood action** command apply.

drop: Drops subsequent UDP packets destined for the protected IP address.

logging: Enables logging for UDP flood attack events. The log messages will be sent to the log system.

none: Takes no action.

Usage guidelines

With UDP flood attack detection configured for an IP address, the device is in attack detection state. When the receiving rate of UDP packets destined for the IP address keeps reaching or exceeding the threshold, the device enters prevention state and takes the specified actions. When the rate drops below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

You can configure UDP flood attack detection for multiple IP addresses in one attack defense policy.

The **logging** keyword enables the attack detection and prevention module to log UDP flood attack events and send log messages to the information center.

With the information center, you can set log message filtering and output rules, including output destinations.

The information center can output UDP flood attack logs to any destinations except the console and the monitor terminal. If you configure the console or monitor terminal as an output destination, the output destination setting will not take effect.

To view UDP flood attack logs stored on the device, use the **display logbuffer** command. Make sure you do not disable log output to the log buffer, which is enabled by default.

For more information about configuring the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Configure UDP flood attack detection for 192.168.1.2 in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] udp-flood detect ip 192.168.1.2 threshold
2000
```

Related commands

udp-flood action

udp-flood detect non-specific

udp-flood threshold

udp-flood detect non-specific

Use **udp-flood detect non-specific** to enable global UDP flood attack detection.

Use **undo udp-flood detect non-specific** to disable global UDP flood attack detection.

Syntax

udp-flood detect non-specific

undo udp-flood detect non-specific

Default

Global UDP flood attack detection is disabled.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Usage guidelines

The device supports the following UDP flood attack prevention types:

- **Source-based UDP flood attack prevention**—Monitors the receiving rate of UDP packets on a per-source IP basis.
- **Destination-based UDP flood attack prevention**—Monitors the receiving rate of UDP packets on a per-destination IP basis.

The global UDP flood attack detection applies to all IP addresses except for those specified by the **udp-flood detect** command. The global detection uses the global trigger threshold set by the **udp-flood threshold** or **udp-flood source-threshold** command and global actions specified by the **udp-flood action** command.

Examples

Enable global UDP flood attack detection in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] udp-flood detect non-specific
```

Related commands

udp-flood action

udp-flood detect

udp-flood source-threshold

udp-flood threshold

udp-flood threshold

Use **udp-flood threshold** to set the global threshold for triggering destination-based UDP flood attack prevention.

Use **undo udp-flood threshold** to restore the default.

Syntax

udp-flood threshold *threshold-value*

undo udp-flood threshold

Default

The global threshold is 10000 for triggering destination-based UDP flood attack prevention.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

threshold-value: Specifies the maximum receiving rate in pps for UDP packets that are destined for an IP address. The value range is 0 to 1000000. If you set the threshold value to 0, the destination-based UDP flood attack prevention is disabled.

Usage guidelines

With global UDP flood attack detection configured, the device is in attack detection state. When the receiving rate of UDP packets destined for an IP address keeps reaching or exceeding the threshold, the device enters prevention state and takes the specified actions. When the rate drops below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

The global threshold applies to global UDP flood attack detection. Adjust the threshold according to the application scenarios.

- If the number of UDP packets sent to a protected server, such as an HTTP or FTP server, is normally large, set a high threshold. A low threshold might affect the server services.
- For a network that is unstable or susceptible to attacks, set a low threshold.

Examples

Set the global threshold to 100 for triggering destination-based UDP flood attack prevention in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] rst-flood threshold 100
```

Related commands

udp-flood action

udp-flood detect

udp-flood detect non-specific

udp-flood source-threshold

Use **udp-flood source-threshold** to set the global threshold for triggering source-based UDP flood attack prevention.

Use **undo udp-flood source-threshold** to restore the default.

Syntax

udp-flood source-threshold *threshold-value*

undo udp-flood source-threshold

Default

The global threshold is 10000 for triggering source-based UDP flood attack prevention.

Views

Attack defense policy view

Predefined user roles

network-admin

context-admin

Parameters

threshold-value: Specifies the maximum receiving rate in pps for UDP packets that originate from an IP address. The value range is 0 to 1000000. If you set the threshold value to 0, the source-based UDP flood attack prevention is disabled.

Usage guidelines

With global UDP flood attack detection configured, the device is in attack detection state. When the receiving rate of UDP packets originating from an IP address keeps reaching or exceeding the threshold, the device enters prevention state and takes the specified actions. When the rate drops below the silence threshold (three-fourths of the threshold), the device returns to the attack detection state.

Examples

Set the global threshold to 100 for triggering source-based UDP flood attack prevention in attack defense policy **atk-policy-1**.

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] udp-flood source-threshold 100
```

Related commands

udp-flood action

udp-flood detect

udp-flood detect non-specific

whitelist enable

Use **whitelist enable** to enable the whitelist feature on a security zone.

Use **undo whitelist enable** to disable the whitelist feature on a security zone.

Syntax

whitelist enable

undo whitelist enable

Default

The whitelist feature is disabled on a security zone.

Views

Security zone view

Predefined user roles

network-admin

context-admin

Usage guidelines

If the global whitelist feature is enabled, the whitelist feature is enabled on all security zones. If the global whitelist feature is disabled, you can use this command to enable the whitelist feature on individual security zones.

Examples

Enable the whitelist feature on security zone **Untrust**.

```
<Sysname> system-view
[Sysname] security-zone name untrust
[Sysname-security-zone-Untrust] whitelist enable
```

whitelist global enable

Use **whitelist global enable** to enable the global whitelist feature.

Use **undo whitelist global enable** to disable the global whitelist feature.

Syntax

whitelist global enable

undo whitelist global enable

Default

The global whitelist feature is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

If you enable the global whitelist feature, the whitelist feature is enabled on all security zones.

Examples

Enable the global whitelist feature.

```
<Sysname> system-view
[Sysname] whitelist global enable
```

whitelist object-group

Use **whitelist object-group** to add an address object group to the whitelist.

Use **undo whitelist object-group** to restore the default.

Syntax

whitelist object-group *object-group-name*

undo whitelist object-group

Default

No address object group is added to the whitelist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

object-group-name: Specifies an address object group by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

This command must be used together with the address object group feature. For more information about address object groups, see object group configuration in *Security Configuration Guide.*

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Add address object group **object-group1** to the whitelist.

```
<Sysname> system-view
[Sysname] whitelist object-group object-group1
```

Contents

Server connection detection commands

auto-learn enable

Use **auto-learn enable** to enable server connection learning for the specified learning period.

Use **undo auto-learn enable** to disable server connection learning.

Syntax

auto-learn enable period { **one-day** | **one-hour** | **seven-day** | **twelve-hour** }

undo auto-learn enable

Default

Server connection learning is disabled.

Views

Server connection learning configuration view

Predefined user roles

network-admin

context-admin

Parameters

period: Specifies the learning period.

one-day: Specifies one day.

one-hour: Specifies one hour.

seven-day: Specifies seven days.

twelve-hour: Specifies 12 hours.

Usage guidelines

This command enables the device to learn the connections initiated by the servers specified by using the **source-ip** command for the specified learning period.

This command is configurable only when both of the following conditions are met:

- Servers are specified for the learning process to learn connections.
- The server connection learning process is not running on the device.

To change the learning period of an ongoing server connection learning process, first execute the **undo auto-learn enable** command to stop the learning process, and then execute the **auto-learn enable** command.

Examples

Enable server connection learning for one day.

```
<Sysname> system-view
[Sysname] scd learning
[Sysname-scd-learning] auto-learn enable period one-day
```

Related commands

source-ip

display scd auto-learn config

Use **display scd auto-learn config** to display the server connection learning information.

Syntax

display scd auto-learn config

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display the server connection learning information.

```
<Sysname> display scd auto-learn config
Learning status              : Active
Learning time                : One-hour
Server address object groups : 146
Progress                     : 6%
Start time                   : 2018, 03, 27 10:50
End time                     : 2018, 03, 27 11:50
```

Table 1 Command output

Field	Description
Learning status	Server connection learning status. If server connection learning is in progress, this field displays **Active**. If server connection learning is not running, this field displays a hyphen (-)..
Learning time	Learning period, which can be **One-day**, **One-hour**, **Seven-day**, or **Twelve-hour**.
Server address object groups	Number of server IP address object groups specified for server connection learning.
Progress	Progress percentage of the server connection learning.
Start time	Start time of the server connection learning.
End time	End time of the server connection learning.

display scd learning record

Use **display scd auto-learn config** to display the server-initiated connections learned by server connection learning.

Syntax

display scd learning record [**protected-server** *ip-address*] [**destination-ip** *ip-address*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

protected-server *ip-address*: Specifies the IP address of the server.

destination-ip *ip-address*: Specifies the destination IP address of the server-initiated connections.

Usage guidelines

This command displays the server connection learning results, which provides the basis for you to create SCD policies to monitor and log illegal connections initiated by servers.

If you do not specify any parameters, this command displays the connections initiated by all servers specified for server connection learning.

Examples

Display the connections initiated by all servers specified for server connection learning.

```
<Sysname> display scd learning record
Id     Protected server    Destination IPv4 address   Protocol    Port
1      192.168.102.1       192.168.101.21             TCP         443
Total entries: 1
```

Display the connections initiated by server 192.168.102.1.

```
<Sysname> display scd learning record protected-server 192.168.102.1
Id     Protected server    Destination IPv4 address   Protocol    Port
1      192.168.102.1       192.168.101.21             TCP         443
Total entries: 1
```

Display the server-initiated connections destined for 192.168.101.21.

```
<Sysname> display scd learning record destination-ip 192.168.101.21
Id     Protected server    Destination IPv4 address   Protocol    Port
1      192.168.102.1       192.168.101.21             TCP         443
Total entries: 1
```

Table 2 Command output

Field	Description
ID	ID of the server connection learning record.
Protected server	IP address of the server initiated the connection.
Destination IPv4 address	IPv4 address the connection is destined for.
Protocol	Protocol used by the connection.
Port	Destination port number of the connection.
Total entries	Total number of the learned connections.

Related commands

reset scd learning record

display scd policy

Use **display scd policy** to display the server connection detection (SCD) policy information.

Syntax

display scd policy [**name** *policy-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

name *policy-name*: Displays detailed information about an SCD policy. The *policy-name*: argument specifies the policy name, a case-insensitive string of 1 to 63 characters. If you do not specify an SCD policy, this command displays brief information about all SCD policies.

Examples

Display brief information about all SCD policies.

```
<Sysname> display scd policy
Id     Name              Protected server  Rules       Logging     Policy status
1      policy1           1.1.1.1           0           Disabled    Disabled
Total entries: 1
```

Table 3 Command output

Field	Description
Id	Row ID of the SCD policy entry.
Name	Name of the SCD policy.
Protected server	IP address of the protected server. The SCD policy will monitor connections initiated by the server.
Rules	Number of SCD rules in the SCD policy. Each SCD rule defines a set of legal connections initiated by the server.
Logging	Enabling status of the logging for illegal connections (connections that do not match any SCD rules) initiated by the server.
Policy status	Enabling status of the SCD policy.
Total entries	Total number of the SCD policies.

Display detailed information about SCD policy **policy1**.

```
<Sysname> display scd policy name policy1
SCD policy name: policy1
 Protected server IPv4: 1.1.1.1
 Logging: Enabled
```

```
Policy status: Enabled
Rule ID: 1
 Permitted dest IPv4: 1.1.2.1
 Protocol: TCP port 1-4
 Protocol: UDP port 1,3,5,7,9,11,13,15,17,19,21,23
 Protocol: ICMP
```

Table 4 Command output

Field	Description
SCD policy name	Name of the SCD policy.
Protected server IPv4	IP address of the protected server. The SCD policy will monitor connections initiated by the server.
Rule ID	Number of an SCD rule in the SCD policy. Each SCD rule defines a set of legal connections initiated by the server.
Permitted dest IPv4	Destination IP address of the legal connections initiated by the server that match the SCD rule.
Protocol	Protocol used by the legal connections initiated by the server that match the SCD rule.
Logging	Enabling status of the logging for illegal connections (connections that do not match any SCD rules) initiated by the server.
Policy status	Enabling status of the SCD policy.

logging enable

Use **logging enable** to enable logging for illegal server-initiated connections detected by the SCD policy.

Use **undo logging enable** to disable logging for illegal server-initiated connections detected by the SCD policy.

Syntax

logging enable

undo logging enable

Default

Logging is disabled for illegal server-initiated connections detected by the SCD policy.

Views

SCD policy view

Predefined user roles

network-admin

context-admin

Usage guidelines

This feature enables the device to log server-initiated connections that do not match any rules in the SCD policy and send the logs to the device information center. With the information center, you can specify log output rules to output the logs to different destinations. For more information about the information center, see information center configuration in *Network Management and Monitoring Configuration Guide*.

Examples

Enable logging for illegal server-initiated connections that are detected by SCD policy **policy1**.

```
<Sysname> system-view
[Sysname] scd policy policy1
[Sysname-scd-policy-policy1] logging enable
```

Related commands

display scd policy

permit-dest-ip

Use **permit-dest-ip** to configure the destination IP address criterion for an SCD rule.

Use **undo permit-dest-ip** to remove the destination IP address criterion from an SCD rule.

Syntax

permit-dest-ip *ip-address*

undo permit-dest-ip

Default

The destination IP address criterion is not configured in an SCD rule.

Views

SCD policy rule view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies an IPv4 address, in dotted decimal notation.

Usage guidelines

Each SCD rule contains the following criteria to identify legal connections initiated by the protected server:

- A destination IP address criterion, which specifies the destination IP address for server-initiated connections.

  In one SCD policy, each SCD rule must use a unique destination IP address.
- One or more protocol criteria. Each protocol criterion specifies a protocol and optionally a set of destination port numbers.

A connection initiated by the protected server matches the SCD rule if the connection matches both the destination IP address criterion and a protocol criterion. Connections initiated by the server that do not match any SCD rules are considered illegal connections.

If you execute the command multiple times for an SCD rule, the most recent configuration takes effect.

As a best practice, use the following procedure to configure an SCD policy for a server:

1. Enable server connection learning on the device to learn the connections initiated by the server.
2. Configure SCD rules for legal connections according to the server connection learning results. To view the learned connections, use the **display scd learning record** command.

Examples

In SCD policy **policy1**, configure SCD rule 1 to match connections destined for 1.1.1.1.

```
<Sysname> system-view
[Sysname] scd policy policy1
[Sysname-scd-policy-policy1] rule 1
[Sysname-scd-policy-policy1-1] permit-dest-ip 1.1.1.1
```

Related commands

display scd policy

policy enable

Use **policy enable** to enable an SCD policy.

Use **undo policy enable** to disable an SCD policy.

Syntax

policy enable

undo policy enable

Default

An SCD policy is disabled.

Views

SCD policy view

Predefined user roles

network-admin

context-admin

Usage guidelines

An SCD policy takes effect only after it is enabled.

Examples

Enable SCD policy **policy1**.

```
<Sysname> system-view
[Sysname] scd policy policy1
[Sysname-scd-policy-policy1] policy enable
```

Related commands

display scd policy

protected-server

Use **protected-server** to specify the IP address of the protected server in an SCD policy.

Use **undo protected-server** to remove the protected server IP address from an SCD policy.

Syntax

protected-server *ip-address*

undo protected-server

Default

No protected server IP address is specified.

Views

SCD policy view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the IPv4 address of a protected server, in dotted decimal notation.

Usage guidelines

An SCD policy monitors only the connections initiated by the specified protected server.

The protected server IP address must be unique for each SCD policy.

If you execute this command for an SCD policy multiple times, the most recent configuration takes effect.

Examples

Configure SCD policy **policy1** to monitor connections initiated by server 192.168.1.10.

```
<Sysname> system-view
[Sysname] scd policy policy1
[Sysname-scd-policy-policy1] protected-server 192.168.1.10
```

Related commands

display scd policy

protocol

Use **protocol** to configure a protocol criterion for an SCD rule.

Use **undo protocol** to remove a protocol criterion from an SCD rule.

Syntax

protocol { **icmp** | **tcp port** *port-list* | **udp port** *port-list* }

undo protocol { **icmp** | **tcp** | **udp** }

Default

No protocol criterion is configured in an SCD rule.

Views

SCD rule view

Predefined user roles

network-admin

context-admin

Parameters

icmp: Specifies the ICMP protocol.

tcp port *port-list*: Specifies the TCP protocol and a list of up to 20 destination TCP port numbers in the range of 1 to 65535. The *port-list* argument specifies a space-separated list of port number items. Each item specifies a port by its number or specifies a range of port numbers in the form of *port-number1* **to** *port-number2*. The start port number must be identical to or lower than the end port number.

udp port *port-list*: Specifies the UDP protocol and a list of up to 20 destination UDP port numbers in the range of 1 to 65535. The *port-list* argument specifies a space-separated list of port number items. Each item specifies a port by its number or specifies a range of port numbers in the form of *port-number1* **to** *port- number2*. The start port number must be identical to or lower than the end port number.

Usage guidelines

Each SCD rule contains the following criteria to identify legal connections initiated by the protected server:

- A destination IP address criterion, which specifies the destination IP address for server-initiated connections.
- One or more protocol criteria. Each protocol criterion specifies a protocol and optionally a set of destination port numbers.

A connection initiated by the protected server matches the SCD rule if the connection matches both the destination IP address criterion and a protocol criterion. Connections initiated by the server that do not match any SCD rules are considered illegal connections.

You can use this command multiple times to specify different protocols in an SCD rule.

If you specify the TCP or UDP protocol with different port numbers in an SCD rule, the most recent configuration takes effect.

Examples

In SCD policy **policy1**, configure a protocol criterion in SCD rule 1 to match the TCP protocol with port numbers 80 and 1000 to 2000.

```
<Sysname> system-view
[Sysname] scd policy policy1
[Sysname-scd-policy-policy1] rule 1
[Sysname-scd-policy-policy1-1] protocol tcp port 80 1000 to 2000
```

Related commands

display scd policy

reset scd learning record

Use **reset scd learning record** to clear the server connection learning results.

Syntax

reset scd learning record

Views

User view

Predefined user roles

network-admin

context-admin

Examples

Clear the server connection learning results.

```
<Sysname> reset scd learning record
```

Related commands

display scd learning record

rule

Use **rule** to create an SCD rule and enter its view, or enter the view of an existing SCD rule.

Use **undo rule** to remove an SCD rule.

Syntax

rule *rule-id*

undo rule [*rule-id*]

Default

No SCD rules exist in an SCD policy.

Views

SCD policy view

Predefined user roles

network-admin

context-admin

Parameters

rule-id: Specifies a rule ID in the range of 1 to 65535.

Usage guidelines

Each SCD rule contains the following criteria to identify legal connections initiated by the protected server:

- A destination IP address criterion, which specifies the destination IP address for server-initiated connections.
- One or more protocol criteria. Each protocol criterion specifies a protocol and optionally a set of destination port numbers.

A connection initiated by the protected server matches the SCD rule if the connection matches both the destination IP address criterion and a protocol criterion. Connections initiated by the server that do not match any SCD rules are considered illegal connections.

If you do not specify a rule ID for the **undo rule** command, all SCD rules in the SCD policy will be deleted.

Examples

In SCD policy **policy1**, create SCD rule 1 and enter its view.

```
<Sysname> system-view
[Sysname] scd policy policy1
[Sysname-scd-policy-policy1] rule 1
[Sysname-scd-policy-policy1-1]
```

Related commands

display scd policy

scd learning

Use **scd learning** to enter server connection learning configuration view.

Use **undo scd learning** to remove all server connection learning configurations.

Syntax

scd learning

undo scd learning

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

Server connection learning allows the device to learn connections initiated by given servers. The learning results provide the basis for you to create SCD policies to monitor and log illegal connections initiated by the servers.

The **undo scd learning** command is not configurable when server connection learning is in progress.

Examples

```
<Sysname> system-view
[Sysname] scd learning
[Sysname-scd-learning]
```

scd policy

Use **scd policy** to create an SCD policy and enter its view, or enter the view of an existing SCD policy.

Use **undo scd policy** to remove an SCD policy.

Syntax

scd policy name *policy-name*

undo scd policy [**name** *policy-name*]

Default

No SCD policies exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

name *policy-name*: Specifies a unique name for the SCD policy. The SCD policy name is a case-insensitive string of 1 to 63 characters.

Usage guidelines

An SCD policy monitors the connections initiated by the specified protected server. You can configure the following settings in an SCD policy:

- Protected server IP address.
- SCD rules to identify legal connections initiated by the server.

- Logging for illegal connections initiated by the server.
- SCD policy enabling status.

If you do not specify an SCD policy for the **undo scd policy** command, all SCD policies will be deleted.

Examples

Create an SCD policy named **policy1** and enter its view.

```
<Sysname> system-view
[Sysname] scd policy name policy1
[Sysname-scd-policy-policy1]
```

Related commands

display scd policy

source-ip

Use **source-ip** to specify an IP address object group for server connection learning.

Use **undo source-ip** to remove an IP address object group specified for server connection learning.

Syntax

source-ip *object-group-name*

undo source-ip [*object-group-name*]

Default

No IP address object groups are specified for server connection learning.

Views

Server connection learning configuration view

Predefined user roles

network-admin

context-admin

Parameters

object-group-name: Specifies an IP address object group by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

Server connection learning will learn the connections initiated by the servers that use IP addresses in the specified IP address object groups.

You can repeat this command to specify a maximum of 1024 IP address object groups.

If you specify a nonexistent IP address object group, the system will creates an empty IP address object group with the specified name.

If you do not specify an IP address object group for the **undo source-ip** command, all IP address object groups specified for server connection learning will be removed.

The **source-ip** and **undo source-ip** commands are not configurable when sever connection learning is in progress.

For more information about address object groups, see object group configuration in *Security Configuration Guide*.

Examples

Specify IP address object group **abc** for SCD learning.

```
<Sysname> system-view
[Sysname] scd learning
[Sysname-scd-learning] source-ip abc
```

Related commands

object-group

Contents

ARP attack protection commands

Unresolvable IP attack protection commands

arp source-suppression enable

Use **arp source-suppression enable** to enable the ARP source suppression feature.

Use **undo arp source-suppression enable** to disable the ARP source suppression feature.

Syntax

arp source-suppression enable

undo arp source-suppression enable

Default

The ARP source suppression feature is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

Configure this feature on the gateways.

Examples

Enable the ARP source suppression feature.

```
<Sysname> system-view
[Sysname] arp source-suppression enable
```

Related commands

display arp source-suppression

arp source-suppression limit

Use **arp source-suppression limit** to set the maximum number of unresolvable packets that can be processed per source IP address within 5 seconds.

Use **undo arp source-suppression limit** to restore the default.

Syntax

arp source-suppression limit *limit-value*

undo arp source-suppression limit

Default

The device can process a maximum of 10 unresolvable packets per source IP address within 5 seconds.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

limit-value: Specifies the limit in the range of 2 to 1024.

Usage guidelines

If unresolvable packets received from an IP address within 5 seconds exceed the limit, the device stops processing the packets from that IP address until the 5 seconds elapse.

Examples

Configure the device to process a maximum of 100 unresolvable packets per source IP address within 5 seconds.

```
<Sysname> system-view
[Sysname] arp source-suppression limit 100
```

Related commands

display arp source-suppression

display arp source-suppression

Use **display arp source-suppression** to display information about the current ARP source suppression configuration.

Syntax

display arp source-suppression

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display information about the current ARP source suppression configuration.

```
<Sysname> display arp source-suppression
 ARP source suppression is enabled
 Current suppression limit: 100
```

Table 1 Command output

Field	Description
Current suppression limit	Maximum number of unresolvable packets that can be processed per source IP address within 5 seconds.

Source MAC-based ARP attack detection commands

arp source-mac

Use **arp source-mac** to enable the source MAC-based ARP attack detection feature and specify a handling method.

Use **undo arp source-mac** to disable the source MAC-based ARP attack detection feature.

Syntax

arp source-mac { **filter** | **monitor** }

undo arp source-mac [**filter** | **monitor**]

Default

The source MAC-based ARP attack detection feature is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

filter: Specifies the filter handling method.

monitor: Specifies the monitor handling method.

Usage guidelines

Configure this feature on the gateways.

This feature checks the number of ARP packets delivered to the CPU. If the number of packets from the same MAC address within 5 seconds exceeds a threshold, the device generates an ARP attack entry for the MAC address. Before the entry ages out, the device handles the attack by using either of the following methods:

- **Monitor**—Only generates log messages.
- **Filter**—Generates log messages and filters out subsequent ARP packets from the MAC address.

Make sure you have enabled the ARP logging feature before enabling the source MAC-based ARP attack detection feature. For information about the ARP logging feature, see ARP configuration in *Layer 3—IP Services Configuration Guide*.

If you do not specify any handling method in the **undo arp source-mac** command, the command disables this feature.

Examples

Enable the source MAC-based ARP attack detection feature and specify the filter handling method.

```
<Sysname> system-view
[Sysname] arp source-mac filter
```

arp source-mac aging-time

Use **arp source-mac aging-time** to set the aging time for ARP attack entries.

Use **undo arp source-mac aging-time** to restore the default.

Syntax

arp source-mac aging-time *time*

undo arp source-mac aging-time

Default

The aging time for ARP attack entries is 300 seconds.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

time: Sets the aging time for ARP attack entries, in the range of 60 to 6000 seconds.

Examples

Set the aging time for ARP attack entries to 60 seconds.

```
<Sysname> system-view
[Sysname] arp source-mac aging-time 60
```

arp source-mac exclude-mac

Use **arp source-mac exclude-mac** to exclude specific MAC addresses from source MAC-based ARP attack detection.

Use **undo arp source-mac exclude-mac** to remove the excluded MAC addresses from source MAC-based ARP attack detection.

Syntax

arp source-mac exclude-mac *mac-address*&<1-n>

undo arp source-mac exclude-mac [*mac-address*&<1-n>]

Default

No MAC addresses are excluded from source MAC-based ARP attack detection.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

mac-address&<1-n>: Specifies a MAC address list. The *mac-address* argument indicates an excluded MAC address in the format of H-H-H. &<1-n> indicates the number of excluded MAC addresses that you can configure. The value for n is 10.

Usage guidelines

If you do not specify a MAC address, the **undo arp source-mac exclude-mac** command removes all excluded MAC addresses.

Examples

Exclude a MAC address from source MAC-based ARP attack detection.

```
<Sysname> system-view
[Sysname] arp source-mac exclude-mac 001e-1200-0213
```

arp source-mac threshold

Use **arp source-mac threshold** to set the threshold for source MAC-based ARP attack detection. If the number of ARP packets sent from a MAC address within 5 seconds exceeds this threshold, the device recognizes this as an attack.

Use **undo arp source-mac threshold** to restore the default.

Syntax

arp source-mac threshold *threshold-value*

undo arp source-mac threshold

Default

The threshold for source MAC-based ARP attack detection is 30.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

threshold-value: Specifies the threshold for source MAC-based ARP attack detection. The value range for this argument is 1 to 5000.

Examples

Set the threshold for source MAC-based ARP attack detection to 30.

```
<Sysname> system-view
[Sysname] arp source-mac threshold 30
```

display arp source-mac

Use **display arp source-mac** to display ARP attack entries detected by source MAC-based ARP attack detection.

Syntax

display arp source-mac { **interface** *interface-type interface-number* | **slot** *slot-number* }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number.

slot *slot-number*: Specifies an IRF member device by its ID. If you do not specify a member device, this command displays ARP attack entries for the master device.

Examples

Display the ARP attack entries detected by source MAC-based ARP attack detection on GigabitEthernet 1/0/1.

```
<Sysname> display arp source-mac interface gigabitethernet 1/0/1
Source-MAC          VLAN ID  Interface               Aging-time
23f3-1122-3344      4094     GE1/0/1                 10
```

Table 2 Command output

Field	Description
Source-MAC	Source MAC address of the attack.
VLAN ID	ID of the VLAN in which the attack was detected.
Interface	Interface on which the attack was detected.
Aging-time	Aging time for the ARP attack entry, in seconds.

ARP packet source MAC consistency check commands

arp valid-check enable

Use **arp valid-check enable** to enable ARP packet source MAC address consistency check.

Use **undo arp valid-check enable** to disable ARP packet source MAC address consistency check.

Syntax

arp valid-check enable

undo arp valid-check enable

Default

ARP packet source MAC address consistency check is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

Configure this feature on gateways. The gateways can filter out ARP packets whose source MAC address in the Ethernet header is different from the sender MAC address in the message body.

Examples

Enable ARP packet source MAC address consistency check.

```
<Sysname> system-view
[Sysname] arp valid-check enable
```

ARP active acknowledgement commands

arp active-ack enable

Use **arp active-ack enable** to enable ARP active acknowledgement.

Use **undo arp active-ack enable** to disable ARP active acknowledgement.

Syntax

arp active-ack enable

undo arp active-ack enable

Default

ARP active acknowledgement is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

Configure this feature on gateways to prevent user spoofing.

Examples

Enable ARP active acknowledgement.

```
<Sysname> system-view
[Sysname] arp active-ack enable
```

Authorized ARP commands

arp authorized enable

Use **arp authorized enable** to enable authorized ARP on an interface.

Use **undo arp authorized enable** to disable authorized ARP on an interface.

Syntax

arp authorized enable

undo arp authorized enable

Default

Authorized ARP is disabled on the interface.

Views

Layer 3 Ethernet interface view

Layer 3 Ethernet subinterface view

Layer 3 aggregate interface view

Layer 3 aggregate subinterface view

VLAN interface view

Reth interface view

Reth subinterface view

Predefined user roles

network-admin

context-admin

Examples

Enable authorized ARP on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp authorized enable
```

ARP attack detection commands

arp detection enable

Use **arp detection enable** to enable ARP attack detection.

Use **undo arp detection enable** to disable ARP attack detection.

Syntax

arp detection enable

undo arp detection enable

Default

ARP attack detection is disabled.

Views

VLAN view

Predefined user roles

network-admin

context-admin

Examples

Enable ARP attack detection for VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] arp detection enable
```

Related commands

arp detection rule

arp detection rule

Use **arp detection rule** to configure a user validity check rule.

Use **undo arp detection rule** to delete a user validity check rule.

Syntax

arp detection rule *rule-id* { **deny** | **permit** } **ip** { *ip-address* [*mask*] | **any** } **mac** { *mac-address* [*mask*] | **any** } [**vlan** *vlan-id*]

undo arp detection rule [*rule-id*]

Default

No user validity check rule is configured.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

rule-id: Assigns an ID to the user validity check rule. The ID value range is 0 to 511. A smaller value represents a higher priority.

deny: Denies matching ARP packets.

permit: Permits matching ARP packets.

ip { *ip-address* [*mask*] | **any** }: Specifies the sender IP address as the match criterion.

- *ip-address*: Specifies an IP address in dotted decimal notation.
- *mask*: Specifies the address mask in dotted decimal notation. If you do not specify the mask, the *ip-address* argument specifies a host IP address.
- **any**: Matches any IP address.

mac { *mac-address* [*mask*] | **any** }: Specifies the sender MAC address as the match criterion.

- *mac-address*: Specifies a MAC address in the H-H-H format.
- *mask*: Specifies the MAC address mask in the H-H-H format. If you do not specify the mask, the argument specifies the host MAC address.
- **any**: Matches any MAC address.

vlan *vlan-id*: Specifies the ID of a VLAN in the specified rule. The value range for the *vlan-id* argument is 1 to 4094. If you do not specify a VLAN, the packets' VLAN information is not checked.

Usage guidelines

A user validity check rule takes effect only when ARP attack detection is enabled.

If you do not specify a rule ID, the **undo arp detection rule** command deletes all user validity check rules.

Examples

Configure a user validity check rule and enable ARP detection for VLAN 2.

```
<Sysname> system-view
[Sysname] arp detection rule 0 permit ip 10.1.1.1 255.255.0.0 mac 0001-0203-0405
ffff-ffff-0000
[Sysname] vlan 2
[Sysname-vlan2] arp detection enable
```

Related commands

arp detection enable

arp detection trust

Use **arp detection trust** to configure an interface as an ARP trusted interface.

Use **undo arp detection trust** to restore the default.

Syntax

arp detection trust

undo arp detection trust

Default

An interface is an ARP untrusted interface.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

context-admin

Examples

Configure GigabitEthernet 1/0/1 as an ARP trusted interface.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp detection trust
```

arp detection validate

Use **arp detection validate** to enable ARP packet validity check.

Use **undo arp detection validate** to disable ARP packet validity check.

Syntax

arp detection validate { **dst-mac** | **ip** | **src-mac** } *

undo arp detection validate [**dst-mac** | **ip** | **src-mac**] *

Default

ARP packet validity check is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

dst-mac: Checks the target MAC address of ARP responses. If the target MAC address is all-zero, all-one, or inconsistent with the destination MAC address in the Ethernet header, the packet is considered invalid and discarded.

ip: Checks the sender and target IP addresses of ARP replies, and the sender IP address of ARP requests. All-one or multicast IP addresses are considered invalid and the corresponding packets are discarded.

src-mac: Checks whether the sender MAC address in the message body is identical to the source MAC address in the Ethernet header. If they are identical, the packet is forwarded. Otherwise, the packet is discarded.

Usage guidelines

You can specify more than one object to be checked in one command line.

If no keyword is specified, the **undo arp detection validate** command disables ARP packet validity check for all objects.

Examples

Enable ARP packet validity check by checking the MAC addresses and IP addresses of ARP packets.

```
<Sysname> system-view
[Sysname] arp detection validate dst-mac ip src-mac
```

arp restricted-forwarding enable

Use **arp restricted-forwarding enable** to enable ARP restricted forwarding.

Use **undo arp restricted-forwarding enable** to disable ARP restricted forwarding.

Syntax

arp restricted-forwarding enable

undo arp restricted-forwarding enable

Default

ARP restricted forwarding is disabled.

Views

VLAN view

Predefined user roles

network-admin

context-admin

Examples

Enable ARP restricted forwarding in VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] arp restricted-forwarding enable
```

display arp detection

Use **display arp detection** to display the VLANs that are enabled with ARP attack detection.

Syntax

display arp detection

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

Examples

Display the VLANs that are enabled with ARP attack detection.

```
<Sysname> display arp detection
ARP detection is enabled in the following VLANs:
1-2, 4-5
```

Related commands

arp detection enable

display arp detection statistics

Use **display arp detection statistics** to display statistics for packets dropped by ARP attack detection.

Syntax

display arp detection statistics [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays dropped packet statistics for all interfaces.

Usage guidelines

This command displays numbers of packets discarded by user validity check and ARP packet validity check on interfaces.

Examples

Display statistics for packets dropped by ARP attack detection.

```
<Sysname> display arp detection statistics
State: U-Untrusted  T-Trusted
ARP packets dropped by ARP inspect checking:
Interface(State)            IP        Src-MAC   Dst-MAC   Inspect
GE1/0/1(U)                  40        0         0         78
GE1/0/2(U)                  0         0         0         0
GE1/0/3(T)                  0         0         0         0
GE1/0/4(U)                  0         0         30        0
```

Table 3 Command output

Field	Description
State	State of an interface: • **U**—ARP untrusted interface. • **T**—ARP trusted interface.
Interface(State)	Inbound interface of ARP packets. State specifies the port state, **trusted** or **untrusted**.
IP	Number of ARP packets discarded due to invalid sender and target IP addresses.
Src-MAC	Number of ARP packets discarded due to invalid source MAC address.
Dst-MAC	Number of ARP packets discarded due to invalid destination MAC address.
Inspect	Number of ARP packets that failed to pass user validity check.

Related commands

`reset arp detection statistics`

reset arp detection statistics

Use **`reset arp detection statistics`** to clear statistics for packets dropped by ARP attack detection.

Syntax

`reset arp detection statistics` [**`interface`** *`interface-type interface-number`*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

`interface` *`interface-type interface-number`*: Specifies an interface by its type and number. If you do not specify an interface, this command clears dropped packet statistics for all interfaces.

Examples

Clear statistics for packets dropped by ARP attack detection.

```
<Sysname> reset arp detection statistics
```

Related commands

display arp detection statistics

ARP scanning and fixed ARP commands

arp fixup

Use **arp fixup** to convert existing dynamic ARP entries to static ARP entries.

Syntax

arp fixup

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

The ARP conversion is a one-time operation. You can use this command again to convert the dynamic ARP entries learned later to static.

The static ARP entries converted from dynamic ARP entries have the same attributes as the manually configured static ARP entries. Due to the device's limit on the total number of static ARP entries, some dynamic ARP entries might fail the conversion.

The static ARP entries after conversion can include the following entries:

- Existing dynamic and static ARP entries before conversion.
- New dynamic ARP entries learned during the conversion.

Dynamic ARP entries that are aged out during the conversion are not converted to static ARP entries.

To delete a static ARP entry changed from a dynamic one, use the **undo arp** *ip-address* [*vpn-instance-name*] command. To delete all such static ARP entries, use the **reset arp all** or **reset arp static** command.

Examples

Convert existing dynamic ARP entries to static ARP entries.

```
<Sysname> system-view
[Sysname] arp fixup
```

arp scan

Use **arp scan** to trigger an ARP scanning in an address range.

Syntax

arp scan [*start-ip-address* **to** *end-ip-address*]

Views

Layer 3 Ethernet interface view

Layer 3 Ethernet subinterface view

Layer 3 aggregate interface view

Layer 3 aggregate subinterface view

VLAN interface view

Reth interface view

Reth subinterface view

Predefined user roles

network-admin

context-admin

Parameters

start-ip-address: Specifies the start IP address of the scanning range.

end-ip-address: Specifies the end IP address of the scanning range. The end IP address must be higher than or equal to the start IP address.

Usage guidelines

CAUTION:

ARP scanning will take some time and occupy a lot of device and network resources. To stop an ongoing scan, press **Ctrl** + **C**. Dynamic ARP entries are created based on ARP replies received before the scan is terminated.

ARP scanning automatically creates ARP entries for devices in the specified address range. IP addresses already in existing ARP entries are not scanned.

If the interface's primary and secondary IP addresses are in the address range, the sender IP address in the ARP request is the address on the smallest network segment.

If no address range is specified, the device learns ARP entries for devices on the subnet where the primary IP address of the interface resides. The sender IP address in the ARP requests is the primary IP address of the interface.

The start and end IP addresses must be on the same subnet as the primary IP address or secondary IP addresses of the interface.

Examples

Configure the device to scan neighbors on the network where the primary IP address of GigabitEthernet 1/0/1 resides.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp scan
```

Configure the device to scan neighbors in an address range.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp scan 1.1.1.1 to 1.1.1.20
```

ARP gateway protection commands

arp filter source

Use **arp filter source** to enable ARP gateway protection for a gateway.

Use **undo arp filter source** to disable ARP gateway protection for a gateway.

Syntax

arp filter source *ip-address*

undo arp filter source *ip-address*

Default

ARP gateway protection is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the IP address of a protected gateway.

Usage guidelines

You can enable ARP gateway protection for a maximum of eight gateways on an interface.

You cannot configure both the **arp filter source** and **arp filter binding** commands on the same interface.

Examples

Enable ARP gateway protection for the gateway with IP address 1.1.1.1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp filter source 1.1.1.1
```

ARP filtering commands

arp filter binding

Use **arp filter binding** to enable ARP filtering and configure an ARP permitted entry.

Use **undo arp filter binding** to remove an ARP permitted entry.

Syntax

arp filter binding *ip-address mac-address*

undo arp filter binding *ip-address*

Default

ARP filtering is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies a permitted sender IP address.

mac-address: Specifies a permitted sender MAC address.

Usage guidelines

If the sender IP and MAC addresses of an ARP packet match an ARP permitted entry, the ARP packet is permitted. If the sender IP and MAC addresses of an ARP packet do not match an ARP permitted entry, the ARP packet is discarded.

You can configure a maximum of eight ARP permitted entries on an interface.

You cannot configure both the **arp filter source** and **arp filter binding** commands on the same interface.

Examples

Enable ARP filtering and configure an ARP permitted entry.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp filter binding 1.1.1.1 0e10-0213-1023
```

Contents

ND attack defense commands

Source MAC-based ND attack detection commands

display ipv6 nd source-mac

Use **display ipv6 nd source-mac** to display source MAC-based ND attack detection entries.

Syntax

display ipv6 nd source-mac interface *interface-type interface-number* [**slot** *slot-number*] [**verbose**]

display ipv6 nd source-mac { **mac** *mac-address* | **vlan** *vlan-id* } **slot** *slot-number* [**verbose**]

display ipv6 nd source-mac slot *slot-number* [**count** | **verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number.

mac *mac-address*: Displays the ND attack detection entry for the specified MAC address. The MAC address format is H-H-H.

vlan *vlan-id*: Displays the source MAC-based ND attack detection entries for the specified VLAN. The VLAN ID is in the range of 1 to 4094.

slot *slot-number*: Displays the ND attack entries detected by the physical interfaces that reside on the specified member device and belong to the virtual interface. If you do not specify a member device, this command displays entries detected by the physical interfaces that reside on the master device and belong to the specified virtual interface.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays source MAC-based ND attack detection entries for the master device.

verbose: Displays detailed information about source MAC-based ND attack detection entries. If you do not specify this keyword, this command displays brief information about the source MAC-based ND attack detection entries.

count: Displays the number of source MAC-based ND attack detection entries. If you do not specify this keyword, the command displays source MAC-based ND attack detection entries.

Usage guidelines

The **slot** *slot-number* option is supported only when the **interface** *interface-type interface-number* option specifies a virtual interface.

This command is supported on the following virtual interfaces: Layer 2 aggregate interfaces, Layer 3 aggregate interfaces, Layer 3 aggregate subinterfaces, and VXLAN VSI interfaces.

If you do not specify any parameters, this command displays all source MAC-based ND attack detection entries.

Examples

Display source MAC-based ND attack detection entries on GigabitEthernet 1/0/1.

```
<Sysname> display ipv6 nd source-mac interface gigabitethernet 1/0/1
Source MAC    VLAN ID Interface             Aging time (sec) Packets dropped
23f3-1122-3344 4094   GE1/0/1               10               84467
```

Displays the number of source MAC-based ND attack detection entries.

```
<Sysname> display ipv6 nd source-mac count
Total source MAC-based ND attack detection entries: 1
```

Display detailed information about source MAC-based ND attack detection entries on GigabitEthernet 1/0/1.

```
<Sysname> display ipv6 nd source-mac interface gigabitethernet 1/0/1 verbose
Source MAC: 0001-0001-0001
VLAN ID: 4094
Hardware status: Succeeded
Aging time: 10 seconds
Interface: GigabitEthernet1/0/1
Attack time: 2019/06/04 15:53:34
Packets dropped: 84467
```

Table 1 Command output

Field	Description
Source MAC	MAC address from which an ND attack is launched.
VLAN ID	ID of the VLAN where the source MAC-based ND attack is detected.
Interface	Interface where the source MAC-based ND attack is detected.
Aging time	Remaining aging time of the source MAC-based ND attack detection entry, in seconds.
Packets dropped	Total number of dropped packets. For Layer 2 Ethernet interfaces, this field is not supported and the field value is **0**.
Total source MAC-based ND attack detection entries	Total number of source MAC-based ND attack detection entries.
Hardware status	Status of the source MAC-based ND attack entry setting to hardware: • Succeeded. • Failed. • Not supported. • Not enough resources.
Attack time	Time when the source MAC-based ND attack was detected. The time format is YYYY/MM/DD HH:MM:SS.

Related commands

reset ipv6 nd source-mac

display ipv6 nd source-mac configuration

Use **display ipv6 nd source-mac configuration** to display the configuration of source MAC-based ND attack detection.

Syntax

display ipv6 nd source-mac configuration

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

Examples

Display the configuration of source MAC-based ND attack detection.

```
<Sysname> display ipv6 nd source-mac configuration
IPv6 ND source-mac is enabled.
Mode: Filter       Threshold: 20
```

Table 2 Command output

Field	Description
IPv6 ND source-mac is enabled.	Source MAC-based ND attack detection is enabled.
IPv6 ND source-mac is disabled.	Source MAC-based ND attack detection is disabled.
Mode	Source MAC-based ND attack detection mode: • Filter. • Monitor.
Threshold	Threshold for source MAC-based ND attack detection.

Related commands

ipv6 nd source-mac

ipv6 nd source-mac threshold

ipv6 nd source-mac

Use **ipv6 nd source-mac** to enable source MAC-based ND attack detection and set the detection mode.

Use **undo ipv6 nd source-mac** to disable source MAC-based ND attack detection.

Syntax

ipv6 nd source-mac { **filter** | **monitor** }

undo ipv6 nd source-mac

Default

Source MAC-based ND attack detection is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

`filter`: Specifies the filter mode.

`monitor`: Specifies the monitor mode.

Usage guidelines

As a best practice, configure this command on gateway devices.

Source MAC-based ND attack detection checks the number of ND messages delivered to the CPU on a per source MAC basis. If the number of messages from the same MAC address within 5 seconds exceeds the threshold, the device generates an ND attack entry for the MAC address. The processing of the ND messages matching this entry depends on the detection mode. With ND logging enabled (by using the **`ipv6 nd check log enable`** command), source MAC-based ND attack detection processes the messages as follows:

- **Filter mode**—Filters out subsequent ND messages sent from the MAC address, and generates log messages.
- **Monitor mode**—Only generates log messages.

The device uses the entry aging time (fixed at 300 seconds) and the threshold to calculate a value:

The calculated value = (threshold/5) × 300

The device monitors the number of dropped packets for an entry. When the entry aging time is reached, it compares the number with the calculated value and takes actions accordingly:

- If the number of dropped packets is higher than or equal to the calculated value, the device resets the aging time for the entry.
- If the number of dropped packets is lower than the calculated value, the system deletes the entry and marks MAC address in the entry as a common MAC address.

When you change the detection mode from monitor to filter, the filter mode takes effect immediately. When you change the detection mode from filter to monitor, the device continues filtering ND messages that match existing attack entries.

Examples

Enable source MAC-based ND attack detection and set the detection mode to monitor.

```
<Sysname> system-view
[Sysname] ipv6 nd source-mac monitor
```

ipv6 nd source-mac threshold

Use **`ipv6 nd source-mac threshold`** to set the threshold for source MAC-based ND attack detection.

Use **`undo ipv6 nd source-mac threshold`** to restore the default.

Syntax

`ipv6 nd source-mac threshold` *`threshold-value`*

`undo ipv6 nd source-mac threshold`

Default

The threshold for source MAC-based ND attack detection is 30.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

threshold-value: Specifies the threshold for source MAC-based ND attack detection. The value range is 1 to 5000.

Usage guidelines

If the number of packets from the same MAC address within 5 seconds exceeds the threshold, the device generates an ND attack entry for the MAC address.

Examples

Set the threshold to 100 for source MAC-based ND attack detection

```
<Sysname> system-view
[Sysname] ipv6 nd source-mac threshold 100
```

reset ipv6 nd source-mac

Use **reset ipv6 nd source-mac** to delete source MAC-based ND attack detection entries.

Syntax

reset ipv6 nd source-mac [**interface** *interface-type interface-number* | **mac** *mac-address* | **vlan** *vlan-id*] [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

interface *interface-type interface-number*: Deletes the source MAC-based ND attack entries detected on the specified interface. The *interface-type interface-number* arguments specify an interface by its type and number.

mac *mac-address*: Deletes the source MAC-based ND attack entry for the specified MAC address. The MAC address format is H-H-H.

vlan *vlan-id*: Deletes the source MAC-based ND attack entries for the specified VLAN. The value range for the *vlan-id* argument is 1 to 4094.

slot *slot-number*: Specifies an IRF member device by its member ID.

Usage guidelines

If you do not specify any parameters, this command deletes all source MAC-based ND attack detection entries.

Examples

Delete all source MAC-based ND attack detection entries.

```
<Sysname> reset ipv6 nd source-mac
```

Related commands

display ipv6 nd source-mac

Interface-based ND attack suppression commands

display ipv6 nd attack-suppression configuration

Use **display ipv6 nd attack-suppression configuration** to display the configuration of interface-based ND attack suppression.

Syntax

display ipv6 nd attack-suppression configuration

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

Examples

Display the configuration of interface-based ND attack suppression.

```
<Sysname> display ipv6 nd attack-suppression configuration
IPv6 ND attack-suppression per-interface is enabled.
Threshold: 3000
```

Table 3 Command output

Field	Description
IPv6 ND attack-suppression per-interface is enabled.	The interface-based ND attack suppression is enabled.
IPv6 ND attack-suppression per-interface is disabled.	The interface-based ND attack suppression is disabled.
Threshold	Threshold for triggering interface-based ND attack suppression.

Related commands

ipv6 nd attack-suppression enable per-interface

display ipv6 nd attack-suppression per-interface

Use **display ipv6 nd attack-suppression per-interface** to display interface-based ND attack suppression entries.

Syntax

display ipv6 nd attack-suppression per-interface slot *slot-number* [**count** | **verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

Parameters

verbose: Displays detailed information about interface-based ND attack suppression entries. If you do not specify this keyword, the command displays brief information about ND attack suppression entries.

slot *slot-number*: Specifies an IRF member device by its member ID.

count: Specifies the number of interface-based ND attack suppression entries. If you do not specify this keyword, the command displays interface-based ND attack suppression entries.

Usage guidelines

If you do not specify any parameters, this command displays brief information about all interface-based ND attack suppression entries.

Examples

Display interface-based ND attack suppression entries on the specified slot.

```
<Sysname> display ipv6 nd attack-suppression per-interface slot 1
Interface             Suppression time (second) Packets dropped
GE1/0/1               200                       84467
GE1/0/2               140                       38293
```

Display the total number of interface-based ND attack suppression entries on the specified slot.

```
<Sysname> display ipv6 nd attack-suppression per-interface slot 1 count
Total ND attack suppression entries: 2
```

Display detailed information about the interface-based ND attack suppression entries on the specified slot.

```
<Sysname> display ipv6 nd attack-suppression per-interface slot 1 verbose
Interface: GigabitEthernet1/0/1
Suppression time: 200 seconds
Hardware status: Succeeded
Attack time: 2019/06/04 15:53:34
Packets dropped: 84467

Interface: GigabitEthernet1/0/2
Suppression time: 140 seconds
Hardware status: Succeeded
Attack time: 2019/06/04 14:53:34
Packets dropped: 38293
```

Figure 1 Command output

Field	Description
Interface	Interface in the ND attack suppression entry.
Suppression time (second)	Suppression time, in seconds.
Packets dropped	Total number of dropped packets.
Total ND attack suppression entries	Total number of ND attack suppression entries.
Hardware status	Status of the interface-based ND attack entry setting to hardware: • Succeeded. • Failed. • Not supported. • Not enough resources.
Suppression time	Remaining suppression time, in seconds.
Attack time	Time when the interface-based ND attack was detected. The time format is YYYY/MM/DD HH:MM:SS.

Related commands

reset ipv6 nd attack-suppression per-interface

reset ipv6 nd attack-suppression per-interface statistics

display ipv6 nd attack-suppression per-interface interface

Use **display ipv6 nd attack-suppression per-interface interface** to display interface-based ND attack suppression entries on an interface.

Syntax

display ipv6 nd attack-suppression per-interface interface *interface-type interface-number* [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

verbose: Displays detailed information about interface-based ND attack suppression entries. If you do not specify this keyword, the command displays brief information about ND attack suppression entries.

Examples

Display interface-based ND attack suppression entries on GigabitEthernet 1/0/1.

```
<Sysname> display ipv6 nd attack-suppression per-interface interface gigabitethernet 1/0/1
Interface             Suppression time (second) Packets dropped
GE1/0/1               200                       84467
```

Display detailed information about the interface-based ND attack suppression entries on GigabitEthernet 1/0/1.

```
<Sysname> display ipv6 nd attack-suppression per-interface interface gigabitethernet 1/0/1 verbose
Interface: GigabitEthernet1/0/1
Suppression time: 200 seconds
Hardware status: Succeeded
Attack time: 2019/06/04 15:53:34
Packets dropped: 84467
```

Figure 2 Command output

Field	Description
Interface	Interface in the ND attack suppression entry.
Suppression time (second)	Suppression time, in seconds.
Packets dropped	Total number of dropped packets.
Hardware status	Status of the interface-based ND attack entry setting to hardware: • Succeeded. • Failed. • Not supported. • Not enough resources.
Suppression time	Remaining suppression time, in seconds.
Attack time	Time when the interface-based ND attack was detected. The time format is YYYY/MM/DD HH:MM:SS.

Related commands

reset ipv6 nd attack-suppression per-interface

reset ipv6 nd attack-suppression per-interface statistics

ipv6 nd attack-suppression enable per-interface

Use **ipv6 nd attack-suppression enable per-interface** to enable interface-based ND attack suppression.

Use **undo ipv6 nd attack-suppression enable per-interface** to disable interface-based ND attack suppression.

Syntax

ipv6 nd attack-suppression enable per-interface

undo ipv6 nd attack-suppression enable per-interface

Default

Interface-based ND attack suppression is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

Use this feature to rate limit ND requests on each Layer 3 interface to prevent ND spoofing attacks. This feature monitors the number of ND requests that each Layer 3 interface received within 5 seconds. If the number on an interface exceeds the threshold, the device creates an ND attack suppression entry for the interface. During the suppression period (fixed at 300 seconds), the device drops ND messages received on this interface.

When the suppression time expires, the system examines the number of dropped ND messages on the interface within the suppression time:

- If the number is higher than or equal to a calculated value, the device resets the suppression time for the entry and continues the ND suppression on the interface.

  The calculated value = (threshold/5) × 300
- If the number is lower than the calculated value, the device deletes the suppression entry.

As a best practice, enable this feature on the gateway.

Examples

Enable interface-based ND attack suppression.

```
<Sysname> system-view
[Sysname] ipv6 nd attack-suppression enable per-interface
```

Related commands

display ipv6 nd attack-suppression per-interface

ipv6 nd attack-suppression threshold

ipv6 nd attack-suppression threshold

Use **ipv6 nd attack-suppression threshold** to set the threshold for triggering interface-based ND attack suppression.

Use **undo ipv6 nd attack-suppression threshold** to restore the default.

Syntax

ipv6 nd attack-suppression threshold *threshold-value*

undo ipv6 nd attack-suppression threshold

Default

The threshold for triggering interface-based ND attack suppression is 1000.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

threshold-value: Specifies the threshold for triggering interface-based ND attack suppression, in the range of 1 to 5000. The threshold defines the maximum number of ND requests that an interface can receive within 5 seconds.

Usage guidelines

When the number of ND requests that an interface received within 5 seconds exceeds the threshold, the device determines that the interface is being attacked.

Examples

Set the threshold to 500 for triggering interface-based ND attack suppression.

```
<Sysname> system-view
[Sysname] ipv6 nd attack-suppression threshold 500
```

Related commands

display ipv6 nd attack-suppression per-interface

ipv6 nd attack-suppression enable per-interface

reset ipv6 nd attack-suppression per-interface

Use **reset ipv6 nd attack-suppression per-interface** to delete interface-based ND attack suppression entries.

Syntax

reset ipv6 nd attack-suppression per-interface [**interface** *interface-type interface-number*] [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

interface *interface-type interface-number*: Deletes interface-based ND attack suppression entries for the specified interface. The *interface-type interface-number* arguments specify an interface by its type and number.

slot *slot-number*: Specifies an IRF member device by its member ID.

Usage guidelines

If you do not specify any parameters, this command deletes all interface-based ND attack suppression entries.

Examples

Delete all interface-based ND attack suppression entries.

```
<Sysname> reset ipv6 nd attack-interface per-interface
```

Related commands

display ipv6 nd attack-suppression per-interface

reset ipv6 nd attack-suppression per-interface statistics

Use **reset ipv6 nd attack-suppression per-interface statistics** to clear statistics for ND messages dropped by interface-based ND attack suppression.

Syntax

reset ipv6 nd attack-suppression per-interface statistics [**interface** *interface-type interface-number*] [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

interface *interface-type interface-number*: Clears statistics for ND messages dropped by interface-based ND attack suppression on the specified interface. The *interface-type interface-number* arguments specify an interface by its type and number.

slot *slot-number*: Specifies an IRF member device by its member ID.

Usage guidelines

After you execute this command, the value for the **Packets dropped** field from the output of the **display ipv6 nd attack-suppression per-interface** command will be cleared.

If you do not specify any parameters, this command clears all statistics for ND messages dropped by interface-based ND attack suppression.

Examples

Clear statistics for ND messages dropped by interface-based ND attack suppression.

```
<Sysname> reset ipv6 nd attack-interface per-interface statistics
```

Related commands

display ipv6 nd attack-suppression per-interface

Source MAC consistency check commands

ipv6 nd check log enable

Use **ipv6 nd check log enable** to enable the ND logging feature.

Use **undo ipv6 nd check log enable** to restore the default.

Syntax

ipv6 nd check log enable

undo ipv6 nd check log enable

Default

The ND logging feature is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

The ND logging feature logs source MAC inconsistency events, and sends the log messages to the information center. The information center can then output log messages from different source modules to different destinations. For more information about the information center, see *Network Management and Monitoring Configuration Guide*.

As a best practice, disable the ND logging feature to avoid excessive ND logs.

Examples

Enable the ND logging feature.

```
<Sysname> system-view
[Sysname] ipv6 nd check log enable
```

Related commands

ipv6 nd mac-check enable

ipv6 nd mac-check enable

Use **ipv6 nd mac-check enable** to enable source MAC consistency check for ND messages.

Use **undo ipv6 nd mac-check enable** to disable source MAC consistency check for ND messages.

Syntax

ipv6 nd mac-check enable

undo ipv6 nd mac-check enable

Default

Source MAC consistency check for ND messages is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

Use this command to enable source MAC consistency check on a gateway. The gateway checks the source MAC address and the source link-layer address for consistency for each ND message. If an inconsistency is found, the gateway drops the ND message.

Examples

Enable source MAC consistency check for ND messages.

```
<Sysname> system-view
[Sysname] ipv6 nd mac-check enable
```

Contents

IPv4 uRPF commands

display ip urpf

Use **display ip urpf** to display uRPF configuration.

Syntax

display ip urpf [**security-zone** *zone-name*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

security-zone *zone-name*: Specifies a security zone by its name, a case-insensitive string of 1 to 31 characters. The string cannot include hyphens (-).

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays uRPF configuration for all member devices.

Examples

Display uRPF configuration for the specified security zone.

```
<Sysname> display ip urpf security-zone Untrust
uRPF configuration information of security-zone Untrust(failed):
   Check type: strict
   Allow default route
   Link check
   Suppress drop ACL: 3000
```

Table 1 Command output

Field	Description
(failed)	The system failed to deliver the uRPF configuration to the forwarding chip because of insufficient chip resources. This field is not displayed if the delivery is successful.
Check type	uRPF check mode: loose or strict.
Allow default route	Using the default route is allowed.
Link check	Link layer check is enabled.
Suppress drop ACL	ACL used for drop suppression.

display ip urpf statistics security-zone

Use **display ip urpf statistics security-zone** to display uRPF statistics for a security zone.

Syntax

display ip urpf statistics security-zone *zone-name* [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

zone-name: Specifies a security zone by its name, a case-insensitive string of 1 to 31 characters. The string cannot include hyphens (-).

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all member devices.

Examples

Display uRPF statistics for security zone **Untrust**.

```
<Sysname> display ip urpf statistics security-zone Untrust slot 1
uRPF information:
  Drops           : 390712
  Suppressed drops: 0
```

Table 2 Command output

Field	Description
uRPF information	uRPF statistics.
Drops	Number of dropped packets.
Suppressed drops	Number of packets that are not dropped because they match the ACL for drop suppression.

Related commands

reset ip urpf statistics security-zone

ip urpf

Use **ip urpf** to enable uRPF.

Use **undo ip urpf** to disable uRPF.

Syntax

ip urpf { **loose** [**allow-default-route**] [**acl** *acl-number*] | **strict** [**allow-default-route**] [**acl** *acl-number*] [**link-check**] }

undo ip urpf

Default

uRPF is disabled.

Views

Security zone view

Predefined user roles

network-admin

context-admin

Parameters

loose: Enables loose uRPF check. To pass loose uRPF check, the source address of a packet must match the destination address of a FIB entry.

strict: Enables strict uRPF check. To pass strict uRPF check, the source address and receiving interface of a packet must match the destination address and output interface of a FIB entry. You can enable strict uRPF check only in VLAN interface view.

allow-default-route: Allows using the default route for uRPF check.

acl *acl-number*: Specifies an ACL by its number.

- For a basic ACL, the value range is 2000 to 2999.
- For an advanced ACL, the value range is 3000 to 3999.

link-check: Enables link layer check (Ethernet link).

Usage guidelines

uRPF can be deployed on a PE connected to a CE or an ISP, or on a CE.

Configure strict uRPF check for traffic that uses symmetric path and configure loose uRPF check for traffic that uses asymmetric path. A symmetric path exists for a session if the PE uses the same interface to receive upstream traffic and send downstream traffic. The path is asymmetric if the PE uses different interfaces to receive upstream traffic and send downstream traffic.

- Typically, symmetric path applies to traffic that goes through an ISP's PE interface connected to the CE. You can configure strict uRPF check for the security zone to which the PE interface belongs.
- Asymmetric path might exist for traffic that goes through a PE interface connected to another ISP. In this case, configure loose uRPF check for the security zone to which the PE interface belongs.

Typically, you do not need to configure the **allow-default-route** keyword on a PE device, because it has no default route pointing to a CE. If you enable uRPF on a security zone where the CE interface resides and the security zone has a default route pointing to the PE, specify the **allow-default-route** keyword.

You can use an ACL to match specific packets, so they are forwarded even if they fail to pass uRPF check.

If the specified ACL does not exist or does not contain rules, the ACL cannot match any packets.

If the **vpn-instance** keyword is specified in an ACL rule, the rule applies only to VPN packets. If the **vpn-instance** keyword is not specified in an ACL rule, the rule applies only to public network packets.

If a Layer 3 PE interface connects to a large number of PCs, configure the **link-check** keyword on the interface to enable link layer check. uRPF checks the validity of the source MAC address.

Examples

Configure strict uRPF check for security zone **Untrust**.

```
<Sysname> system-view
[Sysname] security-zone name Untrust
[Sysname-security-zone-Untrust] ip urpf strict
```

Related commands

display ip urpf

reset ip urpf statistics security-zone

Use **reset ip urpf statistics security-zone** to clear uRPF statistics for a security zone.

Syntax

reset ip urpf statistics security-zone *zone-name*

Views

User view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

zone-name: Specifies a security zone by its name, a case-insensitive string of 1 to 31 characters. The string cannot include hyphens (-).

Examples

Clear uRPF statistics for security zone **Untrust**.

```
<Sysname> reset ip urpf statistics security-zone Untrust
```

Related commands

display ip urpf statistics security-zone

IPv6 uRPF commands

display ipv6 urpf

Use **display ipv6 urpf security-zone** to display IPv6 uRPF configuration.

Syntax

display ipv6 urpf [**security-zone** *zone-name*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

security-zone *zone-name*: Specifies a security zone by its name, a case-insensitive string of 1 to 31 characters. The string cannot include hyphens (-).

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv6 uRPF configuration for all member devices.

Examples

Display IPv6 uRPF configuration for the specified security zone.

```
<Sysname> display ipv6 urpf security-zone Untrust
IPv6 uRPF configuration information of security-zone Untrust(failed):
   Check type: loose
   Allow default route
   Suppress drop ACL: 2000
```

Table 3 Command output

Field	Description
(failed)	The system failed to deliver the IPv6 uRPF configuration to the forwarding chip because of insufficient chip resources. This field is not displayed if the delivery is successful.
Check type	IPv6 uRPF check mode: loose or strict.
Allow default route	Using the default route is allowed.
Suppress drop ACL	IPv6 ACL used for drop suppression.

display ipv6 urpf statistics security-zone

Use **display ipv6 urpf statistics security-zone** to display IPv6 uRPF statistics for a security zone.

Syntax

display ipv6 urpf statistics security-zone *zone-name* [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

zone-name: Specifies a security zone by its name, a case-insensitive string of 1 to 31 characters. The string cannot include hyphens (-).

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all member devices.

Examples

Display IPv6 uRPF statistics for security zone **Untrust**.

```
<Sysname> display ipv6 urpf statistics security-zone Untrust slot 1
IPv6 uRPF information:
  Drops           : 390712
  Suppressed drops: 0
```

Table 4 Command output

Field	Description
IPv6 uRPF information	IPv6 uRPF statistics.
Drops	Number of dropped packets.
Suppressed drops	Number of packets that are not dropped because they match the ACL for drop suppression.

Related commands

reset ipv6 urpf statistics security-zone

ipv6 urpf

Use **ipv6 urpf** to enable IPv6 uRPF.

Use **undo ipv6 urpf** to disable IPv6 uRPF.

Syntax

ipv6 urpf { **loose** | **strict** } [**allow-default-route**] [**acl** *acl-number*]

undo ipv6 urpf

Default

IPv6 uRPF is disabled.

Views

Security zone view

Predefined user roles

network-admin

context-admin

Parameters

loose: Enables loose IPv6 uRPF check. To pass loose IPv6 uRPF check, the source address of a packet must match the destination address of an IPv6 FIB entry.

strict: Enables strict IPv6 uRPF check. To pass strict IPv6 uRPF check, the source address and receiving interface of a packet must match the destination address and output interface of an IPv6 FIB entry.

allow-default-route: Allows using the default route for IPv6 uRPF check.

acl *acl-number*: Specifies an IPv6 ACL by its number.

- For a basic IPv6 ACL, the value range is 2000 to 2999.
- For an advanced IPv6 ACL, the value range is 3000 to 3999.

Usage guidelines

IPv6 uRPF can be deployed on a CE or on a PE connected to either a CE or an ISP.

Configure strict IPv6 uRPF check for traffic that uses symmetric path and configure loose IPv6 uRPF check for traffic that uses asymmetric path. A symmetric path exists for a session if the PE uses the same interface to receive upstream traffic and send downstream traffic. The path is asymmetric if the PE uses different interfaces to receive upstream traffic and send downstream traffic.

- Typically, symmetric path applies to traffic that goes through an ISP's PE interface connected to the CE. You can configure strict IPv6 uRPF check for the security zone to which the PE interface belongs.
- Asymmetric path might exist for traffic that goes through a PE interface connected to another ISP. In this case, configure loose IPv6 uRPF check for the security zone to which the PE interface belongs.

You can use an ACL to match specific packets, so they are forwarded even if they fail to pass IPv6 uRPF check.

If the specified ACL does not exist or does not contain rules, the ACL cannot match any packets.

If the **vpn-instance** keyword is specified in an ACL rule, the rule applies only to VPN packets. If the **vpn-instance** keyword is not specified in an ACL rule, the rule applies only to public network packets.

Typically, you do not need to configure the **allow-default-route** keyword on a PE device, because it has no default route pointing to a CE. If you enable uRPF on a security zone where the CE interface resides and the security zone has a default route pointing to the PE, specify the **allow-default-route** keyword.

Examples

Configure loose IPv6 uRPF check for the security zone **Untrust**.

```
<Sysname> system-view
[Sysname] security-zone name Untrust
[Sysname-security-zone-Untrust] ipv6 urpf loose
```

Related commands

display ipv6 urpf

reset ipv6 urpf statistics security-zone

Use **reset ipv6 urpf statistics security-zone** to clear IPv6 uRPF statistics for a security zone.

Syntax

reset ipv6 urpf statistics security-zone *zone-name*

Views

User view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

zone-name: Specifies a security zone by its name, a case-insensitive string of 1 to 31 characters. The string cannot include hyphens (-).

Examples

Clear IPv6 uRPF statistics for security zone **Untrust**.

```
<Sysname> reset ipv6 urpf statistics security-zone Untrust
```

Related commands

display ipv6 urpf statistics security-zone

Contents

IP-MAC binding commands

display ip-mac binding ipv4

Use **display ip-mac binding ipv4** to display IPv4-MAC binding entries.

Syntax

display ip-mac binding ipv4 [*ipv4-address*] [**mac-address** *mac-address*] [**vlan** *vlan-id* | **vpn-instance** *vpn-instance-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ipv4-address: Specifies an IPv4 address. The IPv4 address cannot be an all 0s, a multicast address, or a loopback address. If you do not specify an IPv4 address, this command displays IPv4-MAC binding entries for all IPv4 addresses.

mac-address *mac-address*: Specifies a MAC address in the format of H-H-H. The MAC address cannot be all 0s, all Fs (a broadcast MAC address), or a multicast address. If you do not specify a MAC address, this command displays IPv4-MAC binding entries for all MAC addresses.

vlan *vlan-id*: Specifies a VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays IPv4-MAC binding entries for all VLANs.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. The specified VPN must already exist. If you do not specify a VPN instance, this command displays IPv4-MAC binding entries for the public network.

Examples

Display IPv4-MAC binding entries.

```
<Sysname> display ip-mac binding ipv4
Total entries: 1
IP address     MAC address          VPN instance     VLAN ID
1.1.1.1        0000-0000-0001       --               N/A
```

Table 1 Command output

Field	Description
Total entries	Total number of IPv4-MAC binding entries.
IP address	IPv4 address in the IPv4-MAC binding entry.
MAC address	MAC address in the IPv4-MAC binding entry.
VPN instance	Name of the VPN instance to which the IPv4-MAC binding entry belongs. If the binding entry belongs to the public network, this field displays hyphens (**--**).

Field	Description
VLAN ID	VLAN to which the IPv4-MAC binding entry belongs.

Related commands

ip-mac binding ipv4

display ip-mac binding ipv6

Use **display ip-mac binding ipv6** to display IPv6-MAC binding entries.

Syntax

display ip-mac binding ipv6 [*ipv6-address*] [**mac-address** *mac-address*] [**vlan** *vlan-id* | **vpn-instance** *vpn-instance-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ipv6-address: Specifies an IPv6 address. The IPv6 address cannot be all 0s, a multicast address, or a loopback address. If you do not specify an IPv6 address, this command displays IPv6-MAC binding entries for all IPv6 addresses.

mac-address *mac-address*: Specifies a MAC address in the format of H-H-H. The MAC address cannot be all 0s, all Fs (a broadcast MAC address), or a multicast address. If you do not specify a MAC address, this command displays IPv6-MAC binding entries for all MAC addresses.

vlan *vlan-id*: Specifies a VLAN by its ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays IPv6-MAC binding entries for all VLANs.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. The specified VPN must already exist. If you do not specify a VPN instance, this command displays IPv6-MAC binding entries for the public network.

Examples

Display IPv6-MAC binding entries.

```
<Sysname> display ip-mac binding ipv6
Total entries: 1
IP address     MAC address          VPN instance     VLAN ID
10::10         0000-0000-0001       --                N/A
```

Table 2 Command output

Field	Description
Total entries	Total number of IPv6-MAC binding entries.
IP address	IPv6 address in the IPv6-MAC binding entry.
MAC address	MAC address in the IPv6-MAC binding entry.

Field	Description
VPN instance	Name of the VPN instance to which the IPv6-MAC binding entry belongs. If the binding entry belongs to the public network, this field displays hyphens (**--**).
VLAN ID	VLAN to which the IPv6-MAC binding entry belongs.

Related commands

ip-mac binding ipv6

display ip-mac binding statistics

Use **display ip-mac binding statistics** to display statistics about packets dropped by the IP-MAC binding feature.

Syntax

display ip-mac binding statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays statistics about packets dropped by the IP-MAC binding feature for all member devices.

Usage guidelines

When the deny action is set for packets that do not match any IP-MAC binding entries, this command displays statistics about the following packets:

- Packets that do not exactly match any IP-MAC binding entries.
- Packets that do not match any IP-MAC binding entries.

Examples

Display statistics about packets dropped by the IP-MAC binding feature on the specified slot.

```
<Sysname> display ip-mac binding statistics slot 1
Slot 1:
Statistics about dropped packets:
IPv4 drop statistics:
  IPv4 ip-mac binding dropped packets because partial match ip: 3
  IPv4 ip-mac binding dropped packets because partial match mac: 0
  IPv4 ip-mac binding dropped packets because no match entry: 12
IPv6 drop statistics:
  IPv6 ip-mac binding dropped packets because partial match ip: 0
  IPv6 ip-mac binding dropped packets because partial match mac: 0
  IPv6 ip-mac binding dropped packets because no match entry: 0
```

Table 3 Command output

Field	Description
IPv4 drop statistics	Number of IPv4 packets dropped by the IP-MAC binding feature.
IPv4 ip-mac binding dropped packets because partial match ip	Number of IPv4 packets that were dropped because no matching IPv4-MAC binding entries were found for the source MAC address.
IPv4 ip-mac binding dropped packets because partial match mac	Number of IPv4 packets that were dropped because no matching IPv4-MAC binding entry was found for the source IP address.
IPv4 ip-mac binding dropped packets because no match entry	Number of IPv4 packets that were dropped because no matching IPv4-MAC binding entry was found for the source IP address and source MAC address.
IPv6 drop statistics	Number of IPv6 packets dropped by the IP-MAC binding feature.
IPv6 ip-mac binding dropped packets because partial match ip	Number of IPv6 packets that were dropped because no matching IPv6-MAC binding entries were found for the source MAC address.
IPv6 ip-mac binding dropped packets because partial match mac	Number of IPv6 packets that were dropped because no matching IPv6-MAC binding entry was found for the source IP address.
IPv6 ip-mac binding dropped packets because no match entry	Number of IPv6 packets that were dropped because no matching IPv6-MAC binding entry was found for the source IP address and source MAC address.

Related commands

`reset ip-mac binding statistics`

display ip-mac binding status

Use **`display ip-mac binding status`** to display the status of the IP-MAC binding feature.

Syntax

`display ip-mac binding status`

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Usage guidelines

This command displays the status of the IP-MAC binding feature and the default action for packets that do not match any IP-MAC binding entries.

Examples

Display the status of the IP-MAC binding feature.

```
<Sysname> display ip-mac binding status
```

```
ip-mac binding: Disabled
ip-mac binding no-match action: Deny
```

Table 4 Command output

Field	Description
ip-mac binding	Status of the IP-MAC binding feature, **Enabled** or **Disabled**.
ip-mac binding no-match action	The default action for packets that do not match any IP-MAC binding entries: • **Permit**—Forwards packets. • **Deny**—Drops packets.

ip-mac binding enable

Use **ip-mac binding enable** to enable the IP-MAC binding feature.

Use **undo ip-mac binding enable** to disable the IP-MAC binding feature.

Syntax

ip-mac binding enable

undo ip-mac binding enable

Default

The IP-MAC binding feature is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

The IP-MAC binding feature uses IP-MAC binding entries to match the source IP address and source MAC address in incoming packets:

- If both the source IP address and source MAC address match the same binding entry, the feature permits the packet.
- If only the source IP address or source MAC address matches a binding entry, the feature denies the packet.
- If the source IP address and the source MAC address match no binding entries, the feature processes the packet based on the specified action.

The IP-MAC binding entries are static. Therefore, this feature is applicable to only scenario that all users are statically assigned IP addresses. Using this feature in a network where users' IP addresses are dynamically assigned through DHCP might cause communication failure.

Examples

Enable the IP-MAC binding feature.

```
<Sysname> system-view
[Sysname] ip-mac binding enable
```

ip-mac binding interface

Use **ip-mac binding interface** to generate IP-MAC binding entries based on existing ARP and ND entries on an interface.

Syntax

ip-mac binding interface *interface-type interface-number*

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interface-type interface-number: Specifies an interface by its name and type. The interface must be a Layer 3 Ethernet interface or subinterface, Layer 3 aggregate interface or subinterface, Reth interface or subinterface, or VLAN interface.

Usage guidelines

Use this command to generate IP-MAC binding entries based on existing ARP entries and ND entries on an interface. If the newly generated IP-MAC binding entries conflict with the existing IP-MAC binding entries, the device retains the existing entries.

To generate IP-MAC binding entries based on ARP entries and ND entries newly added after the command execution, re-execute this command.

To delete IPv4-MAC binding entries generated by using this command, use the **undo ip-mac binding ipv4** command. To delete IPv6-MAC binding entries generated by using this command, use the **undo ip-mac binding ipv6** command.

IP-MAC binding entries are static. Therefore, the binding entries generated by using this command are not updated when the relevant ARP or ND entries change.

Examples

Generate IP-MAC binding entries based on existing ARP and ND entries on GigabitEthernet 0/0/1.

```
<Sysname> system-view
[Sysname] ip-mac binding interface gigabitethernet 1/0/1
```

ip-mac binding ipv4

Use **ip-mac binding ipv4** to create an IPv4-MAC binding entry.

Use **undo ip-mac binding ipv4** to delete IPv4-MAC binding entries.

Syntax

ip-mac binding ipv4 *ipv4-address* **mac-address** *mac-address* [**vlan** *vlan-id* | **vpn-instance** *vpn-instance-name*]

undo ip-mac binding ipv4 { **all** | *ipv4-address* **mac-address** *mac-address* [**vlan** *vlan-id* | **vpn-instance** *vpn-instance-name*] }

Default

No IPv4-MAC binding entries are configured.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-address: Specifies an IPv4 address. The IPv4 address cannot be all 0s, a multicast address, or a loopback address.

mac-address *mac-address*: Specifies a MAC address in the format of H-H-H. The MAC address cannot be all 0s, all Fs (a broadcast MAC address), or a multicast address.

vlan *vlan-id*: Specifies a VLAN ID in the range of 1 to 4094.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. The specified VPN must already exist. If you do not specify a VPN instance, the IPv4-MAC binding entry belongs to the public network.

all: Specifies all IPv4-MAC binding entries.

Usage guidelines

A MAC address can be bound to multiple IPv4 addresses. However, an IPv4 address can be bound to only one MAC address. To bind an IPv4 address in a binding entry to another MAC address, you must delete the existing binding entry, and then create the new binding entry.

IPv4-MAC binding entries created by using this command are globally effective.

The device supports a maximum of 1024 IPv4-MAC binding entries.

Examples

Create an IPv4-MAC binding entry to permit packets with source IPv4 address 192.168.0.1 and source MAC address 0001-0001-0001.

```
<Sysname> system-view
[Sysname] ip-mac binding ipv4 192.168.0.1 mac-address 0001-0001-0001
```

Related commands

display ip-mac binding ipv4

ip-mac binding ipv6

Use **ip-mac binding ipv6** to create an IPv6-MAC binding entry.

Use **undo ip-mac binding ipv6** to delete IPv6-MAC binding entries.

Syntax

ip-mac binding ipv6 *ipv6-address* **mac-address** *mac-address* [**vlan** *vlan-id* | **vpn-instance** *vpn-instance-name*]

undo ip-mac binding ipv6 { **all** | *ipv6-address* **mac-address** *mac-address* [**vlan** *vlan-id* | **vpn-instance** *vpn-instance-name*] }

Default

No IPv6-MAC binding entries are configured.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address: Specifies an IPv6 address. The IPv6 address cannot be all 0s, a multicast address, or a loopback address.

mac-address *mac-address*: Specifies a MAC address in the format of H-H-H. The MAC address cannot be all 0s, all Fs (a broadcast MAC address), or a multicast address.

vlan *vlan-id*: Specifies a VLAN by its ID in the range of 1 to 4094.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. The specified VPN must already exist. If you do not specify a VPN instance, the IPv6-MAC binding entry belongs to the public network.

all: Specifies all IPv6-MAC binding entries.

Usage guidelines

A MAC address can be bound to multiple IPv6 addresses. However, an IPv6 address can be bound to only one MAC address. To bind an IPv6 address in a binding entry to another MAC address, you must delete the existing binding entry and then create the new binding entry.

IPv6-MAC binding entries created by using this command are globally effective.

The device supports a maximum of 1024 IPv6-MAC binding entries.

Examples

Create an IPv6-MAC binding entry to permit packets with source IPv6 address 2012::12:25 and source MAC address 0001-0001-0001.

```
<Sysname> system-view
[Sysname] ip-mac binding ipv6 2012::12:25 mac-address 0001-0001-0001
```

Related commands

display ip-mac binding ipv6

ip-mac binding no-match action deny

Use **ip-mac binding no-match action deny** to set the default action to deny for packets that do not match any IP-MAC binding entries.

Use **undo ip-mac binding no-match action deny** to restore the default.

Syntax

ip-mac binding no-match action deny

undo ip-mac binding no-match action deny

Default

The default action for packets that do not match any IP-MAC binding entries is permit.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

Use this command to permit only packets with both source IP address and source MAC address matching the same binding entry.

Examples

Set the default action to deny for packets that do not match any IP-MAC binding entries.

```
<Sysname> system-view
[Sysname] ip-mac binding no-match action deny
```

reset ip-mac binding statistics

Use **reset ip-mac binding statistics** to clear statistics about packets dropped by the IP-MAC binding feature.

Syntax

reset ip-mac binding statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears statistics about packets dropped by the IP-MAC binding feature on all member devices.

Examples

Clear statistics about packets dropped by the IP-MAC binding feature on the specified slot.

```
<Sysname> reset ip-mac binding statistics slot 1
```

Related commands

display ip-mac binding statistics

Contents

APR commands

app-group

Use **app-group** to create an application group and enter its view, or enter the view of an existing application group.

Use **undo app-group** to delete the specified application group.

Syntax

app-group *group-name*

undo app-group *group-name*

Default

No application groups exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies the application group name, a case-insensitive string of 1 to 63 characters. The names **invalid** and **other** are not allowed.

Usage guidelines

You can create a maximum of 1000 application groups on the device.

Examples

Create an application group named **aaa** and enter its view.

```
<Sysname> system-view
[Sysname] app-group aaa
[Sysname-app-group-aaa]
```

Related commands

copy app-group

description

include application

application statistics enable

Use **application statistics enable** to enable the application statistics feature on the specified direction of an interface.

Use **undo application statistics enable** to disable the application statistics feature on the specified direction of an interface.

Syntax

application statistics enable [**inbound** | **outbound**]

undo application statistics enable [**inbound** | **outbound**]

Default

The application statistics feature is disabled on both directions of an interface.

Views

Layer 2 interface view/Layer 3 interface view

Predefined user roles

network-admin

context-admin

Parameters

inbound: Specifies the inbound direction of the interface.

outbound: Specifies the outbound direction of the interface.

Usage guidelines

IMPORTANT:

The application statistics feature consumes a large amount of system memory. When the system generates a low-memory alarm, disable the application statistics feature on interfaces.

If no direction is specified, application statistics is enabled in both the inbound and outbound directions.

When this feature is enabled, the device separately counts the number of packets or bytes that the interface has received or sent for each application protocol. It also calculates the transmission rates of the interface for these protocols.

To display application statistics, use the **display application statistics** command.

Examples

Enable application statistics in the inbound direction of GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] application statistics enable inbound
```

Enable application statistics in the outbound direction of GigabitEthernet 1/0/2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] application statistics enable outbound
```

Enable application statistics in the inbound and outbound directions of GigabitEthernet 1/0/3.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/3
[Sysname-GigabitEthernet1/0/3] application statistics enable
```

Enable application statistics in the inbound direction of Vlan-interface 2.

```
<Sysname> system-view
[Sysname] interface Vlan-interface 2
[Sysname-Vlan-interface2] application statistics enable inbound
```

Related commands

display application statistics

apr protocol detection-threshold application-other

Use **apr protocol detection-threshold application-other** to configure detection thresholds for categorizing an application as type **other**.

Use **undo apr protocol detection-threshold application-other** to restore the default.

Syntax

apr protocol *protocol-name* **detection-threshold** { **packet-count** *count* | **payload-length** *length* } **application-other**

undo apr protocol *protocol-name* **detection-threshold** { **packet-count** | **payload-length** } **application-other**

Default

The device uses predefined detection thresholds in the signature library for categorizing an application as type **other**.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

protocol-name: Specifies a protocol by its name, a case-insensitive string of 1 to 63 characters.

packet-count *count*: Specifies the maximum number of packets to be detected, in the range of 1 to 128.

payload-length *length*: Specify the maximum payload length to be detected, in the range of 64 to 65536 bytes.

Usage guidelines

If the device cannot identify the application to which the packets of a protocol belongs after detection thresholds are reached, it categorizes the packets as belonging to type **other**.

You can configure both the packet count threshold and the payload length threshold for the same protocol.

To display the detection threshold settings, use the **display apr protocol detection-threshold-other** command.

Examples

Configure the payload length threshold as 2500 bytes for HTTP and use the predefined packet count threshold.

```
<Sysname> system-view
[Sysname] apr protocol http detection-threshold payload-length 2500 application-other
```

Related commands

display apr protocol detection-threshold-other

apr set detectlen

Use **apr set detectlen** to set the maximum detected length for an NBAR rule.

Use **undo apr set detectlen** to restore the default.

Syntax

apr set detectlen *bytes*

undo apr set detectlen

Default

The maximum detected length is not set for an NBAR rule.

Views

NBAR rule view

Predefined user roles

network-admin

context-admin

Parameters

bytes: Specifies the maximum detected length in bytes for an NBAR rule. The value range is 0 to 4294967295.

Usage guidelines

The maximum detected length determines whether to inspect subsequent packets after the device recognizes an application:

- If the inspected byte count already reaches the maximum number, the device will not inspect subsequent packets.
- If the inspected byte count does not reach the maximum number, the device will inspect subsequent packets until the maximum number is reached.

If no maximum detected length is configured, the device continues to inspect subsequent packets for application recognition after recognizing an application. Inspection of subsequent packets affects device performance.

When you set the maximum detected length, make sure you fully understand its impact on system performance.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the maximum detected length to 100000 bytes for NBAR rule **abcd**.

```
<Sysname> system-view
[Sysname] nbar application abcd protocol http
[Sysname-nbar-application-abcd] apr set detectlen 100000
```

Related commands

nbar application

apr signature auto-update

Use **apr signature auto-update** to enable automatic update for the APR signature library and enter auto-update configuration view.

Use **undo apr signature auto-update** to disable automatic update for the APR signature library.

Syntax

apr signature auto-update

undo apr signature auto-update

Default

Automatic update is disabled for the APR signature library.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

Use this command to update the APR signature library if the device can access the signature library services at the NSFOCUS website.

Examples

Enable automatic update for the APR signature library and enter auto-update configuration view.

```
<Sysname> system-view
[Sysname] apr signature auto-update
[Sysname-apr-autoupdate]
```

Related commands

override-current

update schedule

apr signature auto-update-now

Use **apr signature auto-update-now** to manually trigger an automatic update for the APR signature library.

Syntax

apr signature auto-update-now

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command starts the automatic APR signature library update process and backs up the current APR signature file. This command is independent of the **apr signature auto-update** command.

Use this command to update the APR signature library if you find a new version of APR signature library at the NSFOCUS website.

Examples

Manually trigger an automatic update for the APR signature library.

```
<Sysname> system-view
[Sysname] apr signature auto-update-now
```

apr signature rollback

Use **apr signature rollback** to roll back the APR signature library.

Syntax

apr signature rollback { **factory** | **last** }

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

factory: Rolls back the APR signature library to the factory version.

last: Rolls back the APR signature library to the last version.

Usage guidelines

You can use this command if you find that high error rate or abnormality occurs when the device uses the current APR signature library for application recognition.

Each time a rollback operation is performed, the device backs up the current version of the APR signature library. If you repeat the **apr signature rollback last** command multiple times, the APR signature library will repeatedly switch between the current version and the last version.

To ensure that the APR signature library can be successfully rolled back to the last version, back up the current APR signature library each time you update the library.

Examples

Roll back the APR signature library to the last version.

```
<Sysname> system-view
[Sysname] apr signature rollback last
```

apr signature update

Use **apr signature update** to manually update the APR signature library.

Syntax

apr signature update [**override-current**] *file-path*

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

override-current: Overwrites the old APR signature file. If you do not specify this keyword, the old APR signature file will be saved as a backup signature file on the device after the update.

file-path: Specifies the path of the new APR signature file, a case-insensitive string of 1 to 255 characters.

Usage guidelines

Use this command to update APR signature library if the device cannot access the signature library services at the NSFOCUS website.

You can use either of the following methods to manually update the APR signature library:

- **Local update**—By using the locally stored APR signature file.

  The APR signature file must be stored on the mater device for a successful update.

  The following table describes the formats of the *file-path* argument for different update scenarios:

Update scenario	Format of *file-path*	Remarks
The update file is stored in the current working directory.	*filename*	To display the current working directory, use the **pwd** command (see file system management in *Fundamentals Command Reference)*.
The update file is stored in a different directory on the same storage medium.	*filename*	Before updating the signature library, you must use the **cd** command to open the directory where the update file is stored. For information about the **cd** command, see file system management in *Fundamentals Command Reference.*
The update file is stored on a different storage medium.	*path/filename*	Before updating the signature library, you must first use the **cd** command to open the root directory of the storage medium where the file is stored. For information about the **cd** command, see file system management in *Fundamentals Command Reference.*

- **FTP/TFTP update**—By using the APR signature file stored on an FTP or TFTP server.

  The following table describes the formats of the *file-path* argument for different update scenarios:

Update scenario	Format of *file-path*	Remarks
The update file is stored on an FTP server.	*ftp://username:password@ server address/filename*	The *username* argument represents the FTP login username. The *password* argument represents the FTP login password. The *server address* argument represents the IP address or host name of the FTP server. If an FTP login username or password includes colons (:), at signs (@), or slashes (/), you must replace these special characters with the corresponding escape characters. • The escape character for the colon (:) character is %3A or %3a. • The escape character for the at sign (@) character is %40. • The escape character for the slash (/)

Update scenario	Format of *file-path*	Remarks
		character is %2F or %2f.
The update file is stored on a TFTP server.	*tftp://server address/filename*	The *server address* argument represents the IP address or host name of the TFTP server.

If you specify the host name, make sure the following requirements are met:

- The device can resolve the IP address of the FTP or TFTP server through static or dynamic domain name resolution.
- The device and server can reach each other.
  - For information about DNS, see *Layer 3—IP Services Configuration Guide*.

Examples

Manually update the APR signature library by using an APR signature file stored on a TFTP server.

```
<Sysname> system-view
[Sysname] apr signature update tftp://192.168.0.1/apr-1.0.2-en.dat
```

Manually update the APR signature library by using an APR signature file stored on an FTP server.

```
<Sysname> system-view
[Sysname] apr signature update
ftp://user%3A123:user%40abc%2F123@192.168.0.10/apr-1.0.2-en.dat
```

Manually update the APR signature library by using an APR signature file stored on the device, The file is stored in directory **cfa0:/apr-1.0.23-en.dat**. In this example, the working directory is **cfa0:**.

```
<Sysname> system-view
[Sysname] apr signature update apr-1.0.23-en.dat
```

Manually update the APR signature library by using an APR signature file stored on the device, The file is stored in directory **cfa0:/dpi/apr-1.0.23-en.dat**. In this example, the working directory is **cfa0:**.

```
<Sysname> cd dpi
<Sysname> system-view
[Sysname] apr signature update apr-1.0.23-en.dat
```

Manually update the APR signature library by using an APR signature file stored on the device, The file is stored in directory **cfb0:/dpi/apr-1.0.23-en.dat**. In this example, the working directory is **cfa0:**.

```
<Sysname> cd cfb0:/
<Sysname> system-view
[Sysname] apr signature update dpi/apr-1.0.23-en.dat
```

copy app-group

Use **copy app-group** to copy all application protocols in an application group to another group.

Syntax

copy app-group *group-name*

Views

Application group view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies the name of the source application group, a case-insensitive string of 1 to 63 characters. The names **invalid** and **other** are not allowed.

Usage guidelines

Execute this command multiple times to copy application protocols in different groups to the current group.

Examples

Copy application protocols in group **bcd** to group **abc**.

```
<Sysname> system-view
[Sysname] app-group abc
[Sysname-app-group-abc] copy app-group bcd
```

Related commands

app-group

include application

description (application group view)

Use **description** to configure the description of an application group.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

An application group is described as **"User-defined application group"**.

Views

Application group view

Predefined user roles

network-admin

context-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 127 characters. If the string includes spaces, use a pair of quotation marks ("") to enclose all characters.

Usage guidelines

Configure descriptions for different application groups for identification and management purposes.

Examples

Configure a description for application group **aaa**.

```
<Sysname> system-view
[Sysname] app-group aaa
```

```
[Sysname-app-group-aaa] description "User defined aaa group"
```

Related commands

app-group

description (NBAR rule view)

Use **description** to configure the description of a user-defined NBAR rule.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

A user-defined NBAR rule is described as **"User defined application"**.

Views

NBAR rule view

Predefined user roles

network-admin

context-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 127 characters.

Usage guidelines

Configure descriptions for different user-defined NBAR rules for identification and management purposes.

Examples

Configure a description for user-defined NBAR rule **abcd**.

```
<Sysname> system-view
[Sysname] nbar application abcd protocol http
[Sysname-nbar-application-abcd] description "A user-defined application based on HTTP"
```

Related commands

nbar application

destination

Use **destination** to specify a destination IP address or subnet as a match criterion in a user-defined NBAR rule.

Use **undo destination** to restore the default.

Syntax

destination ip *ipv4-address* [*mask-length*]

undo destination

Default

A user-defined NBAR rule matches packets destined for all IP addresses.

Views

NBAR rule view

Predefined user roles

network-admin

context-admin

Parameters

ip *ipv4-address*: Specifies a destination IPv4 address or IPv4 subnet, in dotted decimal notation.

mask-length: Specifies the mask length for IPv4 addresses, in the range of 0 to 32. If you do not specify this argument, the default mask length is 32.

Usage guidelines

If you execute this command multiple times for the same NBAR rule, the most recent configuration takes effect.

Examples

Configure user-defined NBAR rule **abcd** to match packets destined for IPv4 subnet 192.168.1.0/24.

```
<Sysname> system-view
[Sysname] nbar application abcd protocol http
[Sysname-nbar-application-abcd] destination ip 192.168.1.0 24
```

Related commands

nbar application

detection

Use **detection** to configure a detection item for a signature.

Use **undo detection** to delete detection items for a signature.

Syntax

detection *detection-id* **field** *field-name* **match-type** { **exclude** | **include** } { **hex** *hex-vector* | **regex** *regex-pattern* | **text** *text-string* } [**offset** *offset-value* [**depth** *depth-value*] | **relative-offset** *relative-offset-value* [**relative-depth** *relative-depth-value*]]

undo detection { **all** | *detection-id* }

Default

No detection items are configured for a signature.

Views

NBAR rule signature view

Predefined user roles

network-admin

context-admin

Parameters

detection-id: Specifies a detection item ID in the range of 1 to 255.

field *field-name*: Specifies a protocol field by its name, a case-sensitive string of 1 to 31 characters. The detection item is matched in the scope of the specified protocol field. You can enter a question mark to obtain a list of supported protocol fields.

match-type { **exclude** | **include** }: Specifies the match type as **exclude** or **include**.

hex *hex-vector*: Specifies a hexadecimal vector as the match pattern. The *hex-vector* argument is a string of 8 to 256 characters. The argument must start and end with a vertical bar (|).

regex *regex-pattern*: Specifies a regular expression as the match pattern. The *regex-pattern* argument is a case-sensitive string of 3 to 253 characters.

text *text-string*: Specifies a string as the match pattern. The *string* argument is a case-sensitive string of 3 to 256 characters.

offset *offset-value*: Specifies the offset from the beginning of the specified protocol field, in the range of 0 to 65535 bytes. A packet matches the signature after the offset. If you do not specify this option, a packet matches the signature from the beginning of the specified protocol field.

depth *depth-value*: Specifies the depth of the detection item, in the range of 3 to 65535 bytes.

relative-offset *relative-offset-value*: Specifies the offset from the end of the previous detection item, in the range of -32767 to 32767 bytes. A packet matches the signature after the offset. If the offset value is minus, the detection item is before the previous detection item.

relative-depth *relative-depth-value*: Specifies the relative depth of the detection item, in the range of 3 to 65535 bytes.

all: Specifies all detection items.

Usage guidelines

You can configure multiple detection items for an NBAR rule signature. The relationship among detection items is logic AND, and the match order is the configuration order. A packet matches a signature only if all detection items are matched.

As a best practice to ensure correct detection results, configure the protocol fields in the order they appear in HTTP packets.

Examples

Configure a detection item in user-defined NBAR rule **app_http**.

```
<Sysname> system-view
[Sysname] nbar application app_http protocol http
[Sysname-nbar-application-app_http] signature 1 field uri string abcdefg
[Sysname-nbar-application-signature-app_http-1] detection 1 field uri match-type include
text abc offset 10 depth 50
```

direction

Use **direction** to specify a direction as a match criterion in a user-defined NBAR rule.

Use **undo direction** to restore the default.

Syntax

direction { **to-client** | **to-server** }

undo direction

Default

A user-defined NBAR rule matches packets in both directions.

Views

NBAR rule view

Predefined user roles

network-admin

context-admin

Parameters

to-client: Specifies the direction from server to client.

to-server: Specifies the direction from client to server.

Usage guidelines

If you execute this command multiple times for the same NBAR rule, the most recent configuration takes effect.

Examples

Configure user-defined NBAR rule **abcd** to match packets from client to server.

```
<Sysname> system-view
[Sysname] nbar application abcd protocol http
[Sysname-nbar-application-abcd] direction to-server
```

Related commands

nbar application

disable

Use **disable** to disable a user-defined NBAR rule.

Use **undo disable** to restore the default.

Syntax

disable

undo disable

Default

A user-defined NBAR rule is enabled.

Views

NBAR rule view

Predefined user roles

network-admin

context-admin

Usage guidelines

Use this command to disable a user-defined NBAR rule if the following conditions exist:

- The NBAR rule will not be used in the foreseeable future.
- You do not want to delete the NBAR rule.

Examples

Disable user-defined NBAR rule **abcd**.

```
<Sysname> system-view
[Sysname] nbar application abcd protocol http
```

```
[Sysname-nbar-application-abcd] disable
```

Related commands

nbar application

display app-group

Use **display app-group** to display information about the specified application groups.

Syntax

display app-group [**name** *group-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

name *group-name*: Specifies an application group by its name. The *group-name* argument is a case-insensitive string of 1 to 63 characters. The names **invalid** and **other** are not allowed. If you do not specify an application group, this command displays information about all application groups.

Examples

Display information about all application groups.

```
<Sysname> display app-group
User-defined count:3
Group Name                     Type         Group ID
 6767                          User-defined   0x00800002
 er                            User-defined   0x00800001
 hbc                           User-defined   0x00800003
```

Display information about application group **er**.

```
<Sysname> display app-group name er
 Group English name: er
 Group Chinese name: er
 Group ID:         0x00800001
 Type:            User-defined

Application count:  2
 Include application list:
 Application name               Type         App ID
 114Travel                     Pre-defined    0x0000542c
 banc                          User-defined   0x00800001

pre-defined app-group count:0
 Include pre-defined app-group list:
 App-group name                 Type         App-group ID
```

Table 1 Command output

Field	Description
User-defined count	Number of application groups.
Group Name	Name of the application group.
Group English name	English name of the application group.
Type	Application protocol attribute: • **Pre-defined**. • **User-defined**. This filed always displays **User-defined** for application groups.
Application count	Number of application protocols in the application group.
Include application list	Application protocol list.
Application name	Application protocol name.
App ID	Application protocol ID.
pre-defined app-group count	Number of predefined application groups in the application group. This field is not supported in the current software version.
Include pre-defined app-group list	List of predefined application groups. This field is not supported in the current software version.
App-group name	Name of a predefined application group. This field is not supported in the current software version.
App-group ID	ID of a predefined application group. This field is not supported in the current software version.

Related commands

app-group

include

display application

Use **display application** to display information about the specified application protocols.

Syntax

display application [**name** *application-name* | **pre-defined** | **user-defined**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

name *application-name*: Specifies an application protocol by its name. The *application-name* argument is a case-insensitive string of 1 to 63 characters. The names **invalid** and **other** are not allowed.

pre-defined: Specifies the predefined application protocols.

user-defined: Specifies the user-defined application protocols.

Usage guidelines

If you do not specify any parameters, this command displays information about all application protocols.

Examples

Display information about all predefined application protocols.

```
<Sysname> display application pre-defined
 Pre-defined count: 817

 Application name        Type        App ID     Tunnel  Encrypted  DetectLen
 12530WAP_Application_We  Pre-defined  0x000003ac  No     No        0
 b_HTTP
 12580_Application_HTTP   Pre-defined  0x00000312  No     No        0
 126_Web_Email_Download_  Pre-defined  0x000002b7  No     No        0
 HTTP
 126_Web_Email_Login_HTT  Pre-defined  0x000002b3  No     No        0
 P
 126_Web_Email_Read_Emai  Pre-defined  0x000002b4  No     No        0
 l_HTTP
 126_Web_Email_Receive_E  Pre-defined  0x000002b6  No     No        0
 mail_HTTP
 126_Web_Email_Send_Emai  Pre-defined  0x000002b5  No     No        0
 l_HTTP
 126_Web_Email_Upload_HT  Pre-defined  0x000002b8  No     No        0
 TP
 139_mobile_weibo_commen  Pre-defined  0x000001da  No     No        0
 t_HTTP
 139_mobile_weibo_login_  Pre-defined  0x000001d9  No     No        0
 HTTP
 139_mobile_weibo_login_  Pre-defined  0x00000444  No     No        0
---- More ----
```

Display information about all user-defined application protocols.

```
<Sysname> display application user-defined
 User-defined count: 4

 Application name        Type        App ID     Tunnel  Encrypted  DetectLen
 def                  User-defined  0x00800002  No     No        0
 dfer                 User-defined  0x00800003  No     No        0
 efer                 User-defined  0x00800004  No     No        0
```

```
 fdfad                 User-defined  0x00800001  No     No        0
```

Display information about all application protocols.

```
<Sysname> display application
 Total count:       821
 Pre-defined count:  817
 User-defined count: 4

 Application name        Type        App ID     Tunnel  Encrypted  DetectLen
 12530WAP_Application_We  Pre-defined  0x000003ac  No     No        0
 b_HTTP
 12580_Application_HTTP   Pre-defined  0x00000312  No     No        0
 126_Web_Email_Download_  Pre-defined  0x000002b7  No     No        0
 HTTP
 126_Web_Email_Login_HTT  Pre-defined  0x000002b3  No     No        0
 P
 126_Web_Email_Read_Emai  Pre-defined  0x000002b4  No     No        0
 l_HTTP
 126_Web_Email_Receive_E  Pre-defined  0x000002b6  No     No        0
 mail_HTTP
 126_Web_Email_Send_Emai  Pre-defined  0x000002b5  No     No        0
 l_HTTP
 126_Web_Email_Upload_HT  Pre-defined  0x000002b8  No     No        0
 TP
 139_mobile_weibo_commen  Pre-defined  0x000001da  No     No        0
 t_HTTP
 139_mobile_weibo_login_  Pre-defined  0x000001d9  No     No        0
 HTTP
 139_mobile_weibo_login_  Pre-defined  0x00000444  No     No        0
 HTTPS
 139Mail_Login_HTTP      Pre-defined  0x000001cb  No     No        0
 139Mail_Login_HTTPS     Pre-defined  0x0000038c  No     No        0
 139Mail_Login_TCP       Pre-defined  0x0000044b  No     No        0
 163TV_HTTP             Pre-defined  0x000004c3  No     No        0
 17173_Application_HTTP   Pre-defined  0x00000350  No     No        0
 178Game_Application_HTT  Pre-defined  0x00000222  No     No        0
 P
 17K_fiction_Application  Pre-defined  0x00000330  No     No        0
 _HTTP
 19lou_Login_http_stream  Pre-defined  0x000002c0  No     No        0

 19lou_Publish_Or_Reply_  Pre-defined  0x000002c2  No     No        0
 http_stream1
 19lou_Publish_Or_Reply_  Pre-defined  0x000002c3  No     No        0
 http_stream2
 19lou_View_http_stream   Pre-defined  0x000002c1  No     No        0
 1ting_Music_Application  Pre-defined  0x000001bc  No     No        0
 _Mobile_HTTP
 21CN_Email_Read_HTTP    Pre-defined  0x000003fb  No     No        0
```

```
 21CN_Email_Send_HTTP    Pre-defined  0x000003fc  No     No       0
---- More ----
```

Display information about application protocol **Telnet**.

```
<Sysname> display application name telnet
 Application English Name: telnet
 Application Chinese Name: telnet
 Application ID:   0x0000000e
 Tunnel:         No
 Encrypted:       No
```

Table 2 Command output

Field	Description
Total count	Total number of application protocols.
Pre-defined count	Number of predefined application protocols.
User-defined count	Number of user-defined application protocols.
Application name	Name of the application protocol.
Type	Application protocol type: • **Pre-defined**. • **User-defined**.
App ID/Application ID	ID of the application protocol.
Tunnel	Whether or not the protocol is a tunnel protocol, such as L2TP: • **Yes**. • **No**.
Encrypted	Whether or not the protocol is a cryptographic protocol: • **Yes**. • **No**.
DetectLen	Length of data to be inspected for application recognition. The length can be predefined or user defined. The measurement unit is byte.

Related commands

app-group

include

display application statistics

Use **display application statistics** to display statistics for the specified application protocols.

Syntax

display application statistics [**direction** { **inbound** | **outbound** } | **interface** *interface-type interface-number* [**slot** *slot-number*] | **name** *application-name*] *

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

direction: Specifies the direction of the interface.

inbound: Specifies the inbound direction.

outbound: Specifies the outbound direction.

interface *interface-type interface-number*: Specifies an interface by its type and number.

slot *slot-number*: Specifies an IRF member by its member ID. This option is available only for global interfaces, such as VLAN interfaces and tunnel interfaces.

name *application-name*: Specifies an application protocol by its name, a case-insensitive string of 1 to 63 characters. The names **invalid** and **other** are not allowed.

Usage guidelines

If you do not specify any options or keywords, this command displays statistics for application protocols on all interfaces in both inbound and outbound directions.

This command displays statistics for application protocols only after the application statistics feature is enabled on the specified interfaces. Disabling the application statistics feature on the specified interfaces deletes the corresponding application statistics.

You can display statistics for application protocols based on certain criteria, including application protocol names, interface directions, interface names, or a combination of the criteria.

Examples

Display application statistics for GigabitEthernet 1/0/1.

```
<Sysname> display application statistics interface gigabitethernet 1/0/1
Interface : GigabitEthernet1/0/1
Application   In/Out  Packets          Bytes             PPS     BPS
Slot 1 :
http          IN     275             78631             0        275
              OUT    357             255251            0       101
https         IN     403             39267             0       44
              OUT    681             623501            0       32
netbios-dgm    IN     3              729               0       32
              OUT    0               0                 0       0
netbios-ns    IN     248             22816             2       1423
              OUT    0               0                 0       0
telnet         IN     801            43374             10     4509
              OUT    1519            65388             20     6774
```

Table 3 Command output

Field	Description
Interface	Interface name.
Application	Name of the application protocol.
In/Out	Interface direction: • **In**—Inbound. • **Out**—Outbound.
Packets	Number of packets received or sent by the interface.
Bytes	Number of bytes received or sent by the interface.
PPS	Packets received or sent per second.
BPS	Bytes received or sent per second.

Related commands

app-group

application statistics enable

display application statistics top

Use **display application statistics top** to display statistics for application protocols on an interface in descending order, based on the specified criteria.

Syntax

display application statistics top *number* { **bps** | **bytes** | **packets** | **pps** } **interface** *interface-type interface-number* [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

number: Specifies the number of application statistics entries to be displayed. The value range is 0 to 4294967295.

bytes: Sorts application protocols by traffic size in bytes.

bps: Sorts application protocols by traffic rate in bps.

packets: Sorts application protocols by traffic size in packet count.

pps: Sorts application protocols by traffic rate in pps.

interface *interface-type interface-number*: Specifies an interface by its type and number.

slot *slot-number*: Specifies an IRF member by its member ID. This option is available only for global interfaces, such as VLAN interfaces and tunnel interfaces.

Usage guidelines

This command displays application statistics only after the application statistics feature is enabled on the specified interface. Disabling the application statistics feature on the interface deletes the existing statistics.

The system uses the sum of inbound and outbound statistics to rank the application protocols. If the sum statistics for multiple application protocols is the same, the system displays these protocols in alphabetical order.

Examples

Display the top three application protocols that have received and sent the most packets on GigabitEthernet 1/0/1.

```
<Sysname> display application statistics top 3 packets interface gigabitethernet 1/0/1
Interface : GigabitEthernet1/0/1
Application   In/Out Packets          Bytes             PPS     BPS
Slot 1 :
telnet         IN    1389            75219             0       44
               OUT   2626            112745            0       54
https          IN    468             42830             0       123
               OUT   746             626101            0       91
netbios-ns     IN    965             88780             2       1411
               OUT   0               0                 0       0
```

Table 4 Command output

Field	Description
Interface	Interface name.
Application	Name of the application protocol.
In/Out	Interface direction: • **In**—Inbound. • **Out**—Outbound.
Packets	Number of packets received or sent by the interface.
Bytes	Number of bytes received or sent by the interface.
PPS	Packets received or sent per second.
BPS	Bytes received or sent per second.

Related commands

app-group

application statistics enable

display apr protocol detection-threshold-other

Use **display apr protocol detection-threshold-other** to display detection threshold settings for applications categorized as type **other**.

Syntax

display protocol [*protocol-name*] **detection-threshold-other**

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

protocol-name: Specifies a protocol by its name, a case-insensitive string of 1 to 63 characters. If you do not specify a protocol, this command displays the detection threshold settings for all protocols.

Examples

Display the detection threshold settings for all protocols.

```
<Sysname> display apr protocol detection-threshold-other
Detection threshold information:
Protocol: general_udp
  Packet count: 45
  Payload length: 3200 bytes

Protocol: general_tcp
  Packet count: 40
  Payload length: 3000 bytes

 Protocol: http
  Packet count: 10
  Payload length: 2500 bytes

 Protocol: https
  Packet count: 20
  Payload length: 2800 bytes
```

display apr signature library

Use **display apr signature library** to display APR signature library information.

Syntax

display apr signature library

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display APR signature library information.

```
<Sysname> display apr signature library
```

```
APR signature library information:
Type      SigVersion       ReleaseTime               Size
Current    1.0.49          Tue Sep 13 06:54:01 2016   659744
Last       1.0.52          Wed Nov 02 07:14:03 2016   702640
Factory    1.0.0           Fri Dec 31 16:00:00  1999   77040
```

Table 5 Command output

Field	Description
Type	Version type of the APR signature library: • **Current**. • **Last**. • **Factory**.
SigVersion	Version of the APR signature library.
ReleaseTime	Release time of the APR signature library.
Size	Size of the APR signature library, in bytes.

display port-mapping pre-defined

Use **display port-mapping pre-defined** to display information about the predefined port-mappings.

Syntax

display port-mapping pre-defined

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display information about all predefined port mappings.

```
<Sysname> display port-mapping pre-defined
Application                 Protocol Port
afs3-kaserver               TCP      7004
                            UDP      7004
aol                         TCP      5190, 5191, 5192, 5193
                            UDP      5190, 5191, 5192, 5193
appleqtc                    TCP      458
                            UDP      458
bgp                         TCP      179
                            UDP      179
```

Table 6 Command output

Field	Description
Application	Application protocol using the port mapping.
Protocol	Transport layer protocol.
Port	Port number of the application protocol.

Related commands

display port-mapping

port-mapping

display port-mapping user-defined

Use **display port-mapping user-defined** to display information about the user-defined port mappings.

Syntax

display port-mapping user-defined [**application** *application-name* | **port** *port-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

application *application-name*: Specifies an application protocol by its name, a case-insensitive string of 1 to 63 characters. The names **invalid** and **other** are not allowed.

port *port-number*: Specifies a port by its number, in the range of 0 to 65535.

Usage guidelines

If you do not specify an application protocol or a port number, this command displays all user-defined port mappings on the device.

Examples

Display all user-defined port mappings on the device.

```
<Sysname> display port-mapping user-defined
 Application      Port  Protocol    Match Type  Match Condition
-------------------------------------------------------------
 FTP              21    TCP         ---          ---
 FTP              21    UDP         IPv4 host   10.10.10.1(vpn1)
 FTP              2121   UDP         IPv4 host   [11.10.10.1, 11.10.10.10](vpn2)
 FTP              21    UDP         IPv4 subnet 10.10.10.1/24
 FTP              21    SCTP        IPv6 host   2000:fdb8::1:00ab:853c:39ab
 HTTP             899    TCP         IPv4 ACL    2002
```

```
HTTP            999    SCTP       IPv6 ACL    2002
```

Table 7 Command output

Field	Description
Application	Application protocol using port mapping.
Port	Port number to which the application protocol is mapped.
Protocol	Transport layer protocol.
Match Type	Match types: • **---**—No match types or match conditions are specified, and all packets that have the specified port are recognized as the packets of the specified application protocol. • **IPv4 host**—A match based on the destination IPv4 addresses of the packet. • **IPv6 host**—A match based on the destination IPv6 addresses of the packet. • **IPv4 subnet**—A match based on the destination IPv4 subnet of the packet. • **IPv6 subnet**—A match based on the destination IPv6 subnet of the packet. • **IPv4 ACL**—A match based on the IPv4 ACL. • **IPv6 ACL**—A match based on the IPv6 ACL.
Match Condition	Match conditions: • For the match type of IPv4 host or IPv6 host, the destination IP addresses of the packets are displayed. • For the match type of IPv4 subnet or IPv6 subnet, the destination subnet addresses of the packets are displayed. • For the match type of IPv4 ACL or IPv6 ACL, the correct ACL number is displayed. For IP address-based and subnet-based host-port mappings, the MPLS L3VPN instance names are also displayed if you have configured them.

include application

Use **include application** to add application protocols to an application group.

Use **undo include application** to remove application protocols from an application group.

Syntax

include application *application-name*

undo include application *application-name*

Default

No application protocols exist in an application group.

Views

Application group view

Predefined user roles

network-admin

context-admin

Parameters

application-name: Specifies an application protocol by its name, a case-insensitive string of 1 to 63 characters. The names **invalid** and **other** are not allowed.

Usage guidelines

Execute this command multiple times to add multiple predefined or user-defined application protocols to an application group. The number of application protocols in an application group is not limited.

If you add a nonexistent application protocol to the application group, the system first creates the protocol before adding it to the application group. Whether the device can recognize the packets of this protocol depends on your configuration.

Examples

Add HTTP and FTP to group **abc**.

```
<Sysname> system-view
[Sysname] app-group abc
[Sysname-app-group-abc] include application http
[Sysname-app-group-abc] include application ftp
```

Related commands

app-group

copy app-group

nbar application

Use **nbar application** to create a user-defined NBAR rule and enter its view, or enter the view of an existing NBAR rule.

Use **undo nbar application** to delete a user-defined NBAR rule.

Syntax

nbar application *application-name* **protocol** { **http** | **tcp** | **udp** }

undo nbar application *application-name*

Default

No user-defined NBAR rules exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

application-name: Specifies an application protocol by its name, a case-insensitive string of 1 to 63 characters. The following names are not allowed:

- **invalid**.
- **other**.
- Names of predefined application protocols.

http: Specifies HTTP packets to which the NBAR rule is applied.

tcp: Specifies TCP packets to which the NBAR rule is applied.

udp: Specifies UDP packets to which the NBAR rule is applied.

Usage guidelines

By default, predefined NBAR rules exist, and these NBAR rules cannot be deleted or modified. If the predefined NBAR rules cannot meet the user needs, use this command to create user-defined NBAR rules.

Examples

Create a user-defined NBAR rule named **abcd** and apply the rule to HTTP packets.

```
<Sysname> system-view
[Sysname] nbar application abcd protocol http
[Sysname-nbar-application-abcd]
```

override-current

Use **override-current** to overwrite the current signature file for an update operation if the APR signature library is automatically updated at a regular basis.

Use **undo override-current** to restore the default.

Syntax

override-current

undo override-current

Default

If the APR signature library is automatically updated at a regular basis, the current APR signature file is not overwritten for an update operation. Instead, the device will back up the current APR signature file.

Views

Auto-update configuration view

Predefined user roles

network-admin

context-admin

Usage guidelines

Use this command only if the device memory is insufficient.

This command disables the APR signature library from being rolled back to the last version. Do not use this command if the device memory is sufficient.

Examples

Overwrite the current APR signature file for a regular online auto-update operation.

```
<Sysname> system-view
[Sysname] apr signature auto-update
[Sysname-apr-autoupdate] override-current
```

Related commands

apr signatures auto-update

port-mapping

Use **port-mapping** to configure a general port mapping.

Use **undo port-mapping** to remove a general port mapping.

Syntax

port-mapping application *application-name* **port** *port-number* [**protocol** *protocol-name*]

undo port-mapping application *application-name* **port** *port-number* [**protocol** *protocol-name*]

Default

An application protocol is mapped to a common port.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

application *application-name*: Specifies an application protocol by its name, a case-insensitive string of 1 to 63 characters. The names **invalid** and **other** are not allowed.

port *port-number*: Specifies a port by its number, in the range of 0 to 65535.

protocol *protocol-name*: Specifies a transport layer protocol by its name, including:

- **dccp**: Specifies DCCP.
- **sctp**: Specifies SCTP.
- **tcp**: Specifies TCP.
- **udp**: Specifies UDP.
- **udp-lite**: Specifies UDP-Lite.

Usage guidelines

If no transport layer protocol is specified, packets that meet the following conditions are recognized as the specified application protocol's packets:

- Packets are encapsulated by any transport layer protocol.
- Packets have the specified port.

If the destination port of a packet matches a general port mapping, APR recognizes the packet as the specified application protocol's packet.

A mapping with the transport layer protocol specified has a higher priority than one without it.

If two port mappings are configured with the same port number and transport layer protocol, but with different application protocols, the most recent configuration takes effect.

To change the port number mapped to an application protocol, perform the following tasks:

1. Use the **undo port-mapping application** command to remove the existing general port mapping.
2. Use the **port-mapping application** command to specify a different port number for the application protocol.

Examples

Create a general port mapping of port 3456 to FTP.

```
<Sysname> system-view
[Sysname] port-mapping application ftp port 3456
```

Related commands

display port-mapping user-defined

port-mapping acl

Use **port-mapping acl** to configure an ACL-based host-port mapping.

Use **undo port-mapping acl** to remove an ACL-based host-port mapping.

Syntax

port-mapping application *application-name* **port** *port-number* [**protocol** *protocol-name*] **acl** [**ipv6**] *acl-number*

undo port-mapping application *application-name* **port** *port-number* [**protocol** *protocol-name*] **acl** [**ipv6**] *acl-number*

Default

An application protocol is mapped to a common port.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

application *application-name*: Specifies an application protocol by its name, a case-insensitive string of 1 to 63 characters. The names **invalid** and **other** are not allowed.

port *port-number*: Specifies a port by its number in the range of 0 to 65535.

protocol *protocol-name*: Specifies a transport layer protocol by its name, including:

- **dccp**: Specifies DCCP.
- **sctp**: Specifies SCTP.
- **tcp**: Specifies TCP.
- **udp**: Specifies UDP.
- **udp-lite**: Specifies UDP-Lite.

acl [**ipv6**] *acl-number*: Specifies the number of an ACL, in the range of 2000 to 2999. To specify an IPv6 ACL, include the **ipv6** keyword. To specify an IPv4 ACL, do not include the **ipv6** keyword. The ACL will not count traffic that matches this ACL-based host-port mapping even if match counting is enabled for the ACL.

Usage guidelines

APR uses ACL-based host-port mappings to recognize packets. A packet is recognized as an application protocol packet when it matches all the following conditions in a mapping:

- The packet's destination IP address matches the specified source IP address defined in the ACL.

- The packet's destination port matches the specified port in the mapping.
- The transport layer protocol that encapsulates the packet matches the specified transport layer protocol if you specify a transport layer protocol in the mapping.

If two port mappings are configured with the same port number, transport layer protocol, and ACL, but with different application protocols, the most recent configuration takes effect.

A mapping with the transport layer protocol specified has a higher priority than one without it.

Examples

Create a port mapping of port 3456 to FTP for the packets matching ACL 2000.

```
<Sysname> system-view
[Sysname] port-mapping application ftp port 3456 acl 2000
```

Related commands

display port-mapping user-defined

port-mapping host

Use **port-mapping host** to configure an IP address-based host-port mapping.

Use **undo port-mapping host** to remove an IP address-based host-port mapping.

Syntax

port-mapping application *application-name* **port** *port-number* [**protocol** *protocol-name*] **host** { **ip** | **ipv6** } *start-ip-address* [*end-ip-address*] [**vpn-instance** *vpn-instance-name*]

undo port-mapping application *application-name* **port** *port-number* [**protocol** *protocol-name*] **host** { **ip** | **ipv6** } *start-ip-address* [*end-ip-address*] [**vpn-instance** *vpn-instance-name*]

Default

An application protocol is mapped to a common port.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

application *application-name*: Specifies an application protocol by its name, a case-insensitive string of 1 to 63 characters. The names **invalid** and **other** are not allowed.

port *port-number*: Specifies a port by its number, in the range of 0 to 65535.

protocol *protocol-name*: Specifies a transport layer protocol by its name, including:

- **dccp**: Specifies DCCP.
- **sctp**: Specifies SCTP.
- **tcp**: Specifies TCP.
- **udp**: Specifies UDP.
- **udp-lite**: Specifies UDP-Lite.

ip: Specifies IPv4 addresses.

ipv6: Specifies IPv6 addresses.

start-ip-address [*end-ip-address*]: Specifies a range of IPv4 or IPv6 addresses. The *start-ip-address* argument represents the start IP address, and the *end-ip-address* argument represents the end IP address. To specify only one IP address, provide only the start IP address. To specify a range of IP addresses, provide both the start and end IP addresses, and make sure the end IP address is higher than the start IP address.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you configure a mapping for the public network, do not specify this option.

Usage guidelines

APR uses IP address-based host-port mappings to recognize packets. A packet is recognized as an application protocol packet when it matches all the following conditions in a mapping:

- The packet is destined for the specified IP address or IP subnet in the mapping.
- The packet's destination port matches the specified port in the mapping.
- The transport layer protocol that encapsulates the packet matches the specified transport layer protocol if you specify a transport layer protocol in the mapping.

No overlapping of IP addresses is tolerable for the host-port mappings configured with the same application protocol, port number, and transport layer protocol.

If two port mappings are configured with the same port number, transport layer protocol, and IP address or IP address ranges, but with different application protocols, the most recent configuration takes effect.

A mapping with the transport layer protocol specified has a higher priority than one without it.

Examples

Create a mapping of port 3456 to FTP for the IPv4 packets sent to the host at 1.1.1.1 to 1.1.1.10.

```
<Sysname> system-view
[Sysname] port-mapping application ftp port 3456 host ip 1.1.1.1 1.1.1.10
```

Create a mapping of port 3456 to FTP for the IPv6 packets sent to 1::1.

```
<Sysname> system-view
[Sysname] port-mapping application ftp port 3456 host ipv6 1::1
```

Related commands

display port-mapping user-defined

port-mapping subnet

Use **port-mapping subnet** to configure a subnet-based host-port mapping.

Use **undo port-mapping subnet** to remove a subnet-based host-port mapping.

Syntax

port-mapping application *application-name* **port** *port-number* [**protocol** *protocol-name*] **subnet** { **ip** *ipv4-address* { *mask-length* | *mask* } | **ipv6** *ipv6-address* *prefix-length* } [**vpn-instance** *vpn-instance-name*]

undo port-mapping application *application-name* **port** *port-number* [**protocol** *protocol-name*] **subnet** { **ip** *ipv4-address* { *mask-length* | *mask* } | **ipv6** *ipv6-address* *prefix-length* } [**vpn-instance** *vpn-instance-name*]

Default

An application protocol is mapped to a common port.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

application *application-name*: Specifies an application protocol by its name, a case-insensitive string of 1 to 63 characters. The names **invalid** and **other** are not allowed.

port *port-number*: Specifies a port by its number, in the range of 0 to 65535.

protocol *protocol-name*: Specifies a transport layer protocol by its name, including:

- **dccp**: Specifies DCCP.
- **sctp**: Specifies SCTP.
- **tcp**: Specifies TCP.
- **udp**: Specifies UDP.
- **udp-lite**: Specifies UDP-Lite.

ip *ipv4-address* { *mask-length* | *mask* }: Specifies an IPv4 subnet.

- The *ipv4-address* argument specifies the IPv4 network address.
- The *mask-length* argument specifies the mask length of the IPv4 subnet, in the range of 1 to 32.
- The *mask* argument specifies the subnet mask in dotted decimal notation.

ipv6 *ipv6-address prefix-length*: Specifies an IPv6 subnet. The *ipv6-address* argument specifies the IPv6 network address, and the *prefix-length* argument specifies the length of the IPv6 prefix, in the range of 1 to 128.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you configure a mapping for the public network, do not specify this option.

Usage guidelines

APR uses subnet-based host-port mappings to recognize packets. A packet is recognized as an application protocol packet when it matches all the following conditions in a mapping:

- The packet is destined for the specified IP subnet in the mapping.
- The packet's destination port matches the specified port in the mapping.
- The transport layer protocol that encapsulates the packet matches the specified transport layer protocol if you specify a transport layer protocol in the mapping.

If multiple subnet-based mappings are applied to packets and these subnets overlap, APR matches the packets destined for the overlapped segment with the port mapping of the subnet that has the smallest range.

If two port mappings are configured with the same port number, transport layer protocol, and subnet, but with different application protocols, the most recent configuration takes effect.

A mapping with the transport layer protocol specified has a higher priority than one without it.

Examples

Create a mapping of port 3456 to FTP for the packets sent to the IPv4 hosts on subnet 1.1.1.0/24.

```
<Sysname> system-view
[Sysname] port-mapping application ftp port 3456 subnet ip 1.1.1.0 24
```

Create a mapping of port 3456 to FTP for the packets sent to the IPv6 hosts on subnet 1:: /120.

```
<Sysname> system-view
[Sysname] port-mapping application ftp port 3456 subnet ipv6 1:: 120
```

Related commands

display port-mapping user-defined

reset application statistics

Use **reset application statistics** to clear application statistics for interfaces.

Syntax

reset application statistics [**interface** *interface-type interface-number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command clears application statistics for all interfaces.

Examples

Clear application statistics for GigabitEthernet 1/0/1.

```
<Sysname> reset application statistics interface gigabitethernet 1/0/1
```

Clear application statistics for all interfaces.

```
<Sysname> reset application statistics
```

Related commands

application statistics enable

display application statistics

risk type

Use **risk type** to configure a risk type for a user-defined application.

Use **undo risk type** to remove a risk type of a user-defined application.

Syntax

risk type *risk-type*

undo risk type [*risk-type*]

Default

A user-defined application does not have any risk type.

Views

User-defined application view

Predefined user roles

network-admin

context-admin

Parameters

risk-type: Specifies a risk type by its name, a case-insensitive string of 1 to 63 characters. You can enter a question mark (?) to obtain a list of supported risk types.

Usage guidelines

You can configure this command multiple times to specify multiple risk types for a user-defined application. The more risk types a user-defined application has, the higher risk level the application has. You can configure security policies according to the risk level.

If you do not specify a risk type when executing the **undo risk type** command, all risk types of the user-defined application are removed.

Examples

Configure risk types **Tunneling** and **Misoperation** for user-defined application **app1**.

```
<Sysname> system-view
[Sysname] user-defined-application app1
[Sysname-user-defined-app-app1] risk type Tunneling
[Sysname-user-defined-app-app1] risk type Misoperation
```

service-port

Use **service-port** to specify a port number or a port range as a match criterion in a user-defined NBAR rule.

Use **undo service-port** to restore the default.

Syntax

service-port { *port-num* | **range** *start-port end-port* }

undo service-port

Default

A user-defined NBAR rule matches packets of all port numbers.

Views

NBAR rule view

Predefined user roles

network-admin

context-admin

Parameters

port-num: Specifies the port number in the range of 0 to 65535.

range: Specifies a port range.

start-port: Specifies the start port number for the port range, in the range of 0 to 65535.

end-port: Specifies the end port number for the port range, in the range of 0 to 65535. The end port number cannot be smaller than the start port number.

Usage guidelines

The specified port number or port range is used to match the packets' destination ports first. If no match is found for a packet, the device continues to match its source port. A packet is determined as a matching packet as long as one of the ports is matched.

If you execute this command multiple times for the same NBAR rule, the most recent configuration takes effect.

Examples

Configure user-defined NBAR rule **abcd** to match packets with port numbers 2001 through 2004.

```
<Sysname> system-view
[Sysname] nbar application abcd protocol http
[Sysname-nbar-application-abcd] service-port range 2001 2004
```

Related commands

direction

signature

Use **signature** to create an NBAR rule signature and enter its view, or enter the view of an existing NBAR rule signature.

Use **undo signature** to cancel the signature configuration.

Syntax

signature [*signature-id*] [**field** *field-name*] [**offset** *offset-value*] { **hex** *hex-vector* | **regex** *regex-pattern* | **string** *string* }

undo signature *signature-id*

Default

No signatures are configured for a user-defined NBAR rule.

Views

NBAR rule view

Predefined user roles

network-admin

context-admin

Parameters

signature-id: Specifies the signature ID in the range of 1 to 65535. If you do not specify this argument when creating a signature, the system automatically assigns the signature a signature ID and records the signature ID. The increment of automatically assigned signature IDs is 5. A new signature ID is the nearest unassigned multiple of the increment to the latest automatically assigned signature ID. For example, if the system automatically assigns ID 5 to a signature, the next signature ID to be assigned automatically will be 10. If signature ID 10 has been assigned manually to a signature, the next signature ID to be assigned automatically will be 15.

field *field-name*: Specifies a protocol field by its name. The specified protocol field must be predefined. This option is available for configuration only if the NBAR rule is applied to HTTP packets. If you do not specify this option, the configured signature takes effect on all fields in HTTP packets.

offset *offset-value*: Specifies the offset from the beginning of the data field, in bytes. The value range for the *offset-value* argument is 0 to 65535. A packet matches the signature after

the offset. If you do not specify this option, a packet matches the signature from the beginning. If you also specify the **field** *field-name* option, the offset begins from the protocol field.

hex *hex-vector*: Specifies a hexadecimal vector as the match pattern. The *hex-vector* argument is a string of 6 to 254 characters. The argument must start and end with a vertical bar (|) and must contain an even number of characters.

regex *regex-pattern*: Specifies a regular expression as the match pattern. The *regex-pattern* argument is a case-sensitive string of 3 to 253 characters, and it must meet the following requirements:

- Contains a maximum of four branches. For example, **abc(c|d|e|\x3D)** is valid, and **abc(c|onreset|onselect|onchange|style\x3D)** is invalid.
- Nested braces are not allowed. For example, **ab((abcs*?))** is invalid.
- A branch cannot be specified after another branch. For example, **ab(a|b)(c|d)^\\r\\n]+?** is invalid.
- A minimum of four non-wildcard characters must exist before an asterisk (*) or question mark (?). For example, **abc*** is invalid and **abcd*DoS\x2d\d{5}\x20\x2bxi\\r\\nJOIN** is valid.

string *string*: Specifies a string as the match pattern. The *string* argument is a case-sensitive string of 3 to 256 characters.

Usage guidelines

You can repeat this command to configure multiple signatures of different match patterns in a user-defined NBAR rule. If the signatures have different signature IDs, all signatures take effect. The logical relation of these signatures is OR, which indicates that a packet that matches any signature matches the NBAR rule. If the signatures have the same signature ID, the most recent configuration takes effect.

Examples

Create user-defined NBAR rule **abcd**, and then add signature 1 in the NBAR rule to define packet match string **abcdefg** and enter the signature view.

```
<Sysname> system-view
[Sysname] nbar application abcd protocol http
[Sysname-nbar-application-abcd] signature 1 string abcdefg
[Sysname-nbar-application-abcd-signature-1]
```

Configure user-defined NBAR rule **ddd** to match packets with signature 2 which defines hexadecimal vector **123456**, and enter the view of the NBAR rule signature.

```
<Sysname> system-view
[Sysname] nbar application ddd protocol http
[Sysname-nbar-application-ddd] signature 2 hex |123456|
[Sysname-nbar-application-ddd-signature-2]
```

Related commands

detection

source

Use **source** to specify a source IP address or subnet as a match criterion in a user-defined NBAR rule.

Use **undo source** to restore the default.

Syntax

source ip *ipv4-address* [*mask-length*]

undo source

Default

A user-defined NBAR rule matches packets sourced from all IP addresses.

Views

NBAR rule view

Predefined user roles

network-admin

context-admin

Parameters

ip *ipv4-address*: Specifies a source IPv4 address or IPv4 subnet, in dotted decimal notation.

mask-length: Specifies the mask length for IPv4 addresses, in the range of 0 to 32.

Usage guidelines

If you execute this command multiple times for the same NBAR rule, the most recent configuration takes effect.

Examples

Configure user-defined NBAR rule **abcd** to match packets sourced from IPv4 subnet 192.168.2.0/24.

```
<Sysname> system-view
[Sysname] nbar application abcd protocol http
[Sysname-nbar-application-abcd] source ip 192.168.2.0 24
```

Related commands

nbar application

update schedule

Use **update schedule** to set the update schedule for automatic update, including the update interval and update time.

Use **undo update schedule** to restore the default.

Syntax

update schedule { **daily** | **weekly** { **fri** | **mon** | **sat** | **sun** | **thu** | **tue** | **wed** } } **start-time** *time* **tingle** *minutes*

undo update schedule

Default

The device automatically updates the APR signature library between 02:01:00 to 04:01:00 every day.

Views

Auto-update configuration view

Predefined user roles

network-admin

context-admin

Parameters

daily: Specifies the daily update interval.

weekly: Specifies the weekly update interval. You can specify one day in a week for the update:

- **fri**: Specifies Friday.
- **mon**: Specifies Monday.
- **sat**: Specifies Saturday.
- **sun**: Specifies Sunday.
- **thu**: Specifies Thursday.
- **tue**: Specifies Tuesday.
- **wed**: Specifies Wednesday.

start-time *time*: Specifies the start time for the update, in the format of hh:mm:ss. The value range for the *time* argument is 00:00:00 to 23:59:59.

tingle *minutes*: Specifies the tolerance time in minutes. The value range for the *minutes* argument is 0 to 120 minutes. An automatic update will occur at a time point between the following time points:

- Start time minus half of the tolerance time.
- Start time plus half of the tolerance time.

For example, if the specified start time is 01:00:00 and the tolerance time is 60 minutes, the update starts during the period from 00:30:00 to 01:30:00.

Examples

Configure the device to automatically update the APR signature library at 23:10:00 every Monday with a tolerance time of 10 minutes.

```
<Sysname> system-view
[Sysname] apr signature auto-update
[Sysname-apr-autoupdate] update schedule weekly mon start-time 23:10:00 tingle 10
```

Related commands

apr signature auto-update

user-defined-application

Use **user-defined-application** to enter the view of a user-defined application.

Use **undo user-defined-application** to delete a user-defined application.

Syntax

user-defined-application *application-name*

undo user-defined-application *application-name*

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

application-name: Specifies an application by its name, a case-insensitive string of 1 to 63 characters. The names of predefined applications and names **invalid** and **other** are not allowed.

Usage guidelines

You can configure a risk type for an NBAR or PBAR user-defined application after entering the view of the user-defined application. The user-defined application must already exist.

Examples

Enter the view of user-defined application **app1**.

```
<Sysname> system-view
[Sysname] user-defined-application app1
[Sysname-user-defined-app-app1]
```

Related commands

nbar application

port-mapping

port-mapping acl

port-mapping host

port-mapping subnet

Contents

Keychain commands

accept-lifetime

Use **accept-lifetime** to set the receiving lifetime for a key of a keychain.

Use **undo accept-lifetime** to restore the default.

Syntax

accept-lifetime daily *start-day-time* **to** *end-day-time*

accept-lifetime date { *month-day*&<1-31> | *start-month-day* **to** *end-month-day* }

accept-lifetime day { *week-day* | *start-week-day* **to** *end-week-day* }

accept-lifetime month { *month* | *start-month* **to** *end-month* }

accept-lifetime utc *start-time start-date* { **duration** { *duration-value* | **infinite** } | **to** *end-time end-date* }

undo accept-lifetime

Default

The receiving lifetime is not configured for a key of a keychain.

Views

Key view

Predefined user roles

network-admin

context-admin

Parameters

daily: Specifies the key to be effective in the specified time range of each day.

start-day-time **to** *end-day-time*: Specifies the time range of each day. Both the start time and the end time are in the HH:MM:SS format. The value range for the *start-day-time* argument and the *end-day-time* argument is 0:0:0 to 23:59:59. You can omit the SS parameter to set a whole number of minutes, or omit both the SS and MM parameters to set a whole number of hours.

date: Specifies the key to be effective on the specified dates of each month.

month-day&<1-31>: Specifies a space-separated list of up to 31 dates of a month. The value range for the *month-day* argument is 1 to 31.

start-month-day **to** *end-month-day*: Specifies the date range of each month. The end date must be greater than the start date.

day: Specifies the key to be effective on the specified days of each week.

week-day: Specifies a day in a week. Values include **mon**, **tue**, **wed**, **thu**, **fri**, **sat**, and **sun**. You can specify this argument multiple times with different values.

start-week-day **to** *end-week-day*: Specifies the day range of each week. The end day must be greater than the start day.

month: Specifies the key to be effective in the specified months of each year.

month: Specifies a month in a year. Values include **jan**, **feb**, **mar**, **apr**, **may**, **jun**, **jul**, **aug**, **sep**, **oct**, **nov**, and **dec**. You can specify this argument multiple times with different values.

start-month **to** *end-month*: Specifies the month range of each year. The end month must be greater than the start month.

utc: Specifies the receiving lifetime in absolute time mode. The key takes effect in the specified time range, for example, from 08:00 2015/9/1 to 18:00 2015/9/3.

start-time: Specifies the start time in the HH:MM:SS format. The value range for this argument is 0:0:0 to 23:59:59. You can omit the SS parameter to set a whole number of minutes, or omit both the SS and MM parameters to set a whole number of hours.

start-date: Specifies the start date in the MM/DD/YYYY or YYYY/MM/DD format. The value range for YYYY is 2000 to 2035.

duration *duration-value*: Specifies the lifetime of the key, in the range of 1 to 2147483646 seconds.

duration infinite: Specifies that the key never expires after it becomes valid.

to: Specifies the end time and date.

end-time: Specifies the end time in the HH:MM:SS format. The value range for this argument is 0:0:0 to 23:59:59.

end-date: Specifies the end date in the MM/DD/YYYY or YYYY/MM/DD format. The value range for YYYY is 2000 to 2035.

Usage guidelines

A key becomes a valid accept key when the following requirements are met:

- A key string has been configured.
- An authentication algorithm has been specified.
- The system time is within the specified receiving lifetime.

If an application receives a packet that carries a key ID, and the key is valid, the application uses the key to authenticate the packet. If the key is not valid, packet authentication fails.

If the received packet does not carry a key ID, the application uses all valid keys in the keychain to authenticate the packet. If the packet does not pass any authentication, packet authentication fails.

An application can use multiple valid keys to authenticate packets received from a peer.

Examples

Set the receiving lifetime for key 1 of keychain **abc** in absolute time mode.

```
<Sysname> system-view
[Sysname] keychain abc mode absolute
[Sysname-keychain-abc] key 1
[Sysname-keychain-abc-key-1] accept-lifetime utc 12:30 2015/1/21 to 18:30 2015/1/21
```

Set the receiving lifetime for key 1 of keychain **123** in weekly periodic time mode.

```
<Sysname> system-view
[Sysname] keychain 123 mode periodic weekly
[Sysname-keychain-123] key 1
[Sysname-keychain-123-key-1] accept-lifetime day fri
```

Related commands

display keychain

accept-tolerance

Use **accept-tolerance** to set a tolerance time for accept keys in a keychain.

Use **undo accept-tolerance** to restore the default.

Syntax

accept-tolerance { *value* | **infinite** }

undo accept-tolerance

Default

No tolerance time is configured for accept keys in a keychain.

Views

Keychain view

Predefined user roles

network-admin

context-admin

Parameters

value: Specifies a tolerance time in the range of 1 to 8640000 seconds.

infinite: Specifies that the accept keys never expire.

Usage guidelines

After a tolerance time is configured, the start time and the end time configured in the **accept-lifetime utc** command are extended for the period of the tolerance time.

If authentication information is changed, information mismatch occurs on the local and peer devices, and the service might be interrupted. Use this command to ensure continuous packet authentication.

Examples

Set the tolerance time to 100 seconds for accept keys in keychain **abc**.

```
<Sysname> system-view
[Sysname] keychain abc mode absolute
[Sysname-keychain-abc] accept-tolerance 100
```

Configure the accept keys in keychain **abc** to never expire.

```
<Sysname> system-view
[Sysname] keychain abc mode absolute
[Sysname-keychain-abc] accept-tolerance infinite
```

Related commands

display keychain

authentication-algorithm

Use **authentication-algorithm** to specify an authentication algorithm for a key.

Use **undo authentication-algorithm** to restore the default.

Syntax

authentication-algorithm { **hmac-md5** | **hmac-sha-1** | **hmac-sha-256 | hmac-sm3** | **md5** | **sm3** }

undo authentication-algorithm

Default

No authentication algorithm is specified for a key.

Views

Key view

Predefined user roles

network-admin

context-admin

Parameters

hmac-md5: Specifies the HMAC-MD5 authentication algorithm.

hmac-sha-1: Specifies the HMAC-SHA-1 authentication algorithm.

hmac-sha-256: Specifies the HMAC-SHA-256 authentication algorithm.

hmac-sm3: Specifies the HMAC-SM3 authentication algorithm.

md5: Specifies the MD5 authentication algorithm.

sm3: Specifies the SM3 authentication algorithm.

Usage guidelines

If an application does not support the authentication algorithm specified for a key, the application cannot use the key for packet authentication.

Examples

Specify the MD5 authentication algorithm for key 1 of keychain **abc** in absolute time mode.

```
<Sysname> system-view
[Sysname] keychain abc mode absolute
[Sysname-keychain-abc] key 1
[Sysname-keychain-abc-key-1] authentication-algorithm md5
```

Related commands

display keychain

default-send-key

Use **default-send-key** to specify a key in a keychain as the default send key.

Use **undo default-send-key** to restore the default.

Syntax

default-send-key

undo default-send-key

Default

No key in a keychain is specified as the default send key.

Views

Key view

Predefined user roles

network-admin

context-admin

Usage guidelines

When send keys in a keychain are inactive, the default send key can be used for packet authentication.

A keychain can have only one default send key. The default send key must be configured with an authentication algorithm and a key string.

Examples

Specify key **1** in keychain **abc** as the default send key.

```
<Sysname> system-view
[Sysname] keychain abc mode absolute
[Sysname-keychain-abc] key 1
[Sysname-keychain-abc-key-1] default-send-key
```

Related commands

display keychain

display keychain

Use **display keychain** to display keychain information.

Syntax

display keychain [**name** *keychain-name* [**key** *key-id*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

name *keychain-name*: Specifies a keychain by its name, a case-sensitive string of 1 to 63 characters. If you do not specify a keychain, this command displays information about all keychains.

key *key-id*: Specifies a key by its ID in the range of 0 to 281474976710655. If you do not specify a key, this command displays information about all keys in a keychain.

Examples

Display information about all keychains.

```
<Sysname> display keychain

 Keychain name          : abc
   Mode                 : absolute
   Accept tolerance     : 0
   TCP kind value       : 254
   TCP algorithm value
     HMAC-MD5           : 5
     HMAC-SHA-256       : 7
```

```
  MD5                : 3
  HMAC-SM3           : 52
  SM3                : 51
Default send key ID  : None
Active send key ID   : 1
Active accept key IDs: 1 2

Key ID               : 1
  Key string         : $c$3$vuJpEX3Lah7xcSR2uqmrTK2IZQJZguJh3g==
  Algorithm          : md5
  Send lifetime      : 01:00:00 2015/01/22 to 01:00:00 2015/01/25
  Send status        : Active
  Accept lifetime    : 01:00:00 2015/01/22 to 01:00:00 2015/01/27
  Accept status      : Active

Key ID               : 2
  Key string         : $c$3$vuJpEX3Lah7xcSR2uqmrTK2IZQJZguJh3g==
  Algorithm          : md5
  Send lifetime      : 01:00:01 2015/01/25 to 01:00:00 2015/01/27
  Send status        : Inactive
  Accept lifetime    : 01:00:00 2015/01/22 to 01:00:00 2015/01/27
  Accept status      : Active
```

Table 1 Command output

Field	Description
Mode	Time mode for the keychain: • Absolute. • Periodic daily. • Periodic weekly. • Periodic monthly. • Periodic yearly.
Accept tolerance	Tolerance time (in seconds) for accept keys of the keychain.
TCP kind value	Value for the TCP kind field. The default value is 254.
TCP algorithm value	ID of the TCP authentication algorithm. The default algorithm ID is 5 for HMAC-MD5, 7 for HMAC-SHA-256, 3 for MD5, 52 for HMAC-SM3, and 51 for SM3.
Default send key ID	ID of the default send key. The status for the key is displayed in parentheses.
Key string	Key string in encrypted form.
Algorithm	Authentication algorithm for the key: • **hmac-md5** • **hmac-sha-1** • **hmac-sha-256** • **hmac-sm3** • **md5** • **sm3**
Send lifetime	Sending lifetime for the key.

Field	Description
Send status	Status of the send key: **Active** or **Inactive**.
Accept lifetime	Receiving lifetime for the key.
Accept status	Status of the accept key: **Active** or **Inactive**.

key

Use **key** to create a key for a keychain and enter its view, or enter the view of an existing key.

Use **undo key** to delete a key and all its configurations for a keychain.

Syntax

key *key-id*

undo key *key-id*

Default

No keys exist.

Views

Keychain view

Predefined user roles

network-admin

context-admin

Parameters

key-id: Specifies a key ID in the range of 0 to 281474976710655.

Usage guidelines

The keys in a keychain must have different key IDs.

Examples

Create key 1 and enter its view.

```
<Sysname> system-view
[Sysname] keychain abc mode absolute
[Sysname-keychain-abc] key 1
[Sysname-keychain-abc-key-1]
```

Related commands

display keychain

keychain

Use **keychain** to create a keychain and enter its view, or enter the view of an existing keychain.

Use **undo keychain** to delete a keychain and all its configurations.

Syntax

keychain *keychain-name* [**mode** { **absolute** | **periodic** { **daily** | **monthly** | **weekly** | **yearly** } }]

undo keychain *keychain-name*

Default

No keychains exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

keychain-name: Specifies a keychain name, a case-sensitive string of 1 to 63 characters.

mode: Specifies a time mode.

absolute: Specifies the absolute time mode. In this mode, each time point during a key's lifetime is the UTC time and is not affected by the system's time zone or daylight saving time.

periodic: Specifies the periodic time mode. In this mode, a key's lifetime is calculated based on the local time and is affected by the system's time zone and daylight saving time.

daily: Specifies the daily periodic time mode.

monthly: Specifies the monthly periodic time mode.

weekly: Specifies the weekly periodic time mode.

yearly: Specifies the yearly periodic time mode.

Usage guidelines

You must specify the time mode when you create a keychain. You cannot change the time mode for an existing keychain.

The time mode is not required when you enter the view of an existing keychain.

Examples

Create keychain **abc**, specify the absolute time mode for it, and enter keychain view.

```
<Sysname> system-view
[Sysname] keychain abc mode absolute
[Sysname-keychain-abc]
```

Related commands

display keychain

key-string

Use **key-string** to configure a key string for a key.

Use **undo key-string** to restore the default.

Syntax

key-string { **cipher** | **plain** } *string*

undo key-string

Default

No key string is configured for a key.

Views

Key view

Predefined user roles

network-admin

context-admin

Parameters

cipher: Specifies a key in encrypted form.

plain: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. Its plaintext form is a case-sensitive string of 1 to 255 characters. Its encrypted form is a case-sensitive string of 33 o 373 characters.

Usage guidelines

If the length of a plaintext key exceeds the length limit supported by an application, the application uses the supported length of the key to authenticate packets.

Examples

Set the key string to **123456** in plaintext form for key 1.

```
<Sysname> system-view
[Sysname] keychain abc mode absolute
[Sysname-keychain-abc] key 1
[Sysname-keychain-abc-key-1] key-string plain 123456
```

Related commands

display keychain

send-lifetime

Use **send-lifetime** to set the sending lifetime for a key of a keychain.

Use **undo send-lifetime** to restore the default.

Syntax

send-lifetime daily *start-day-time* **to** *end-day-time*

send-lifetime date { *month-day*&<1-31> | *start-month-day* **to** *end-month-day* }

send-lifetime day { *week-day* | *start-week-day* **to** *end-week-day* }

send-lifetime month { *month* | *start-month* **to** *end-month* }

send-lifetime utc *start-time start-date* { **duration** { *duration-value* | **infinite** } | **to** *end-time end-date* }

undo send-lifetime

Default

The sending lifetime is not configured for a key of a keychain.

Views

Key view

Predefined user roles

network-admin

context-admin

Parameters

daily: Specifies the key to be effective in the specified time range of each day.

start-day-time **to** *end-day-time*: Specifies the time range of each day. Both the start time and the end time are in the HH:MM:SS format. The value range for the *start-day-time* argument and the *end-day-time* argument is 0:0:0 to 23:59:59. You can omit the SS parameter to set a whole number of minutes, or omit both the SS and MM parameters to set a whole number of hours.

date: Specifies the key to be effective on the specified dates of each month.

month-day&<1-31>: Specifies a space-separated list of up to 31 dates of a month. The value range for the *month-day* argument is 1 to 31.

start-month-day **to** *end-month-day*: Specifies the date range of each month. The end date must be greater than the start date.

day: Specifies the key to be effective on the specified days of each week.

week-day: Specifies a day in a week. Values include **mon**, **tue**, **wed**, **thu**, **fri**, **sat**, and **sun**. You can specify this argument multiple times with different values.

start-week-day **to** *end-week-day*: Specifies the day range of each week. The end day must be greater than the start day.

month: Specifies the key to be effective in the specified months of each year.

month: Specifies a month in a year. Values include **jan**, **feb**, **mar**, **apr**, **may**, **jun**, **jul**, **aug**, **sep**, **oct**, **nov**, and **dec**. You can specify this argument multiple times with different values.

start-month **to** *end-month*: Specifies the month range of each year. The end month must be greater than the start month.

utc: Specifies the sending lifetime in absolute time mode. The key takes effect in the specified time range, for example, from 08:00 2015/9/1 to 18:00 2015/9/3.

start-time: Specifies the start time in the HH:MM:SS format. The value range for this argument is 0:0:0 to 23:59:59. You can omit the SS parameter to set a whole number of minutes, or omit both the SS and MM parameters to set a whole number of hours.

start-date: Specifies the start date in the MM/DD/YYYY or YYYY/MM/DD format. The value range for YYYY is 2000 to 2035.

duration *duration-value*: Specifies the lifetime of the key, in the range of 1 to 2147483646 seconds.

duration infinite: Specifies that the key never expires after it becomes valid.

to: Specifies the end time and date.

end-time: Specifies the end time in the HH:MM:SS format. The value range for this argument is 0:0:0 to 23:59:59.

end-date: Specifies the end date in the MM/DD/YYYY or YYYY/MM/DD format. The value range for YYYY is 2000 to 2035.

Usage guidelines

A key becomes a valid send key when the following requirements are met:

- A key string has been configured.

- An authentication algorithm has been specified.
- The system time is within the specified sending lifetime.

To make sure only one key in a keychain is used at a time to authenticate packets to a peer, set non-overlapping sending lifetimes for the keys in the keychain.

Examples

Set the sending lifetime for key 1 of keychain **abc** in absolute time mode.

```
<Sysname> system-view
[Sysname] keychain abc mode absolute
[Sysname-keychain-abc] key 1
[Sysname-keychain-abc-key-1] send-lifetime utc 12:30 2015/1/21 to 18:30 2015/1/21
```

Set the sending lifetime for key 1 of keychain **123** in weekly periodic time mode.

```
<Sysname> system-view
[Sysname] keychain 123 mode periodic weekly
[Sysname-keychain-123] key 1
[Sysname-keychain-123-key-1] send-lifetime day fri
```

Related commands

display keychain

tcp-algorithm-id

Use **tcp-algorithm-id** to set an algorithm ID for a TCP authentication algorithm.

Use **undo tcp-algorithm-id** to restore the default.

Syntax

tcp-algorithm-id { **hmac-md5** | **hmac-sha-256** | **hmac-sm3** | **md5** | **sm3** } *algorithm-id*

undo tcp-algorithm-id { **hmac-md5** | **hmac-sha-256** | **hmac-sm3** | **md5** | **sm3** }

Default

The algorithm ID is 3 for the MD5 authentication algorithm, 5 for the HMAC-MD5 authentication algorithm, 7 for the HMAC-SHA-256 authentication algorithm, 51 for the SM3 authentication algorithm, and 52 for the HMAC-SM3 authentication algorithm.

Views

Keychain view

Predefined user roles

network-admin

context-admin

Parameters

hmac-md5: Specifies the HMAC-MD5 authentication algorithm, which provides a key length of 16 bytes.

hmac-sha-256: Specifies the HMAC-SHA-256 authentication algorithm, which provides a key length of 16 bytes.

hmac-sm3: Specifies the HMAC-SM3 authentication algorithm, which provides a key length of 32 bytes.

md5: Specifies the MD5 authentication algorithm, which provides a key length of 16 bytes.

sm3: Specifies the SM3 authentication algorithm, which provides a key length of 32 bytes.

algorithm-id: Specifies an algorithm ID in the range of 1 to 63.

Usage guidelines

If an application uses keychain authentication during TCP connection establishment, the incoming and outgoing TCP packets will carry the TCP Enhanced Authentication Option. The *algorithm-id* field in the option represents the authentication algorithm ID. The algorithm IDs are not assigned by IANA. They are vendor-specific.

To communicate with a peer device from another vendor, the local device must have the same algorithm ID as the peer device. For example, if the algorithm ID is 3 for the HMAC-MD5 algorithm on the peer device, you must execute the **tcp-algorithm-id hmac-md5** 3 command on the local device.

Examples

Create keychain **abc** and set the algorithm ID to 1 for the HMAC-MD5 authentication algorithm.

```
<Sysname> system-view
[Sysname] keychain abc mode absolute
[Sysname-keychain-abc] tcp-algorithm-id hmac-md5 1
```

Related commands

display keychain

tcp-kind

Use **tcp-kind** to set the kind value in the TCP Enhanced Authentication Option.

Use **undo tcp-kind** to restore the default.

Syntax

tcp-kind *kind-value*

undo tcp-kind

Default

The kind value is 254 in the TCP Enhanced Authentication Option.

Views

Keychain view

Predefined user roles

network-admin

context-admin

Parameters

kind-value: Specifies the kind value in the range of 28 to 255.

Usage guidelines

If an application uses keychain authentication during TCP connection establishment, the incoming and outgoing TCP packets will carry the TCP Enhanced Authentication Option. For a successful packet authentication, the local device and the peer device must have the same kind value setting in the TCP Enhanced Authentication Option.

Examples

Set the kind value to 252 for keys in keychain **abc** in absolute time mode.

```
<Sysname> system-view
```

```
[Sysname] keychain abc mode absolute
[Sysname-keychain-abc] tcp-kind 252
```

Related commands

display keychain

Contents

Crypto engine commands

display crypto-engine

Use **display crypto-engine** to display crypto engine information.

Syntax

display crypto-engine

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Usage guidelines

If the device does not have hardware crypto engines, this command displays information only about software crypto engines.

Examples

Display crypto engine information.

```
<Sysname> display crypto-engine
  Crypto engine name: Software crypto engine
  Crypto engine state: Enabled
  Crypto engine type: Software
  Slot ID: 1
  CPU ID: 0
  Crypto engine ID: 0
  Crypto device name: Software
  Crypto device serial number:
  Symmetric algorithms:  des-cbc des-ecb 3des-cbc aes-cbc aes-ecb aes-ctr camellia_cbc
md5 sha1 sha2-256 sha2-384 sha2-512 md5-hmac sha1-hmac sha2-256-hmac sha2-384-hmac
sha2-512-hmac aes-xcbc aes-xcbc-hmac sm3 sm3-hmac sm4-cbc
  Asymmetric algorithms:
  Random number generation function: Supported

  Crypto engine name: Cavium crypto driver
  Crypto engine state: Enabled
  Crypto engine type: Hardware
  Slot ID: 1
  CPU ID: 0
  Crypto engine ID: 1
  Crypto device name: Cavium crypto
  Crypto device serial number:
```

```
  Symmetric algorithms: des-cbc des-ecb 3des-cbc 3des-ecb aes-cbc aes-ecb aes-ctr md5 sha1
sha2-256 sha2-384 sha2-512 md5-hmac sha1-hmac sha2-256-hmac sha2-384-hmac sha2-512-hmac
aes-xcbc-hmac sm4-cbc
  Asymmetric algorithms: dh-group1 dh-group2 dh-group5 dh-group14
  Random number generation function: Supported
```

Table 1 Command output

Field	Description
Crypto engine state	Hardware crypto engine state: • Enabled. • Disabled. This field always displays **Enabled** for software crypto engines.
Crypto engine type	Crypto engine type: • Hardware. • Software.
Crypto device name	Name of the crypto device. This field displays **Software** for software crypto engines. For hardware crypto engines, the value of this field varies by device model.
Crypto device serial number	Serial number of the crypto device. This field is always empty for software crypto engines. For hardware crypto engines, the value of this field varies by device model.
Symmetric algorithms	Supported symmetric algorithms.
Asymmetric algorithms	Supported asymmetric algorithms.
Random number generation function	Whether random number generation function is supported: • Supported. • Not supported.

display crypto-engine statistics

Use **display crypto-engine statistics** to display crypto engine statistics.

Syntax

display crypto-engine statistics [**engine-id** *engine-id* **slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

engine-id *engine-id*: Specifies a crypto engine by its ID. The value range for the *engine-id* argument is 0 to 4294967295.

slot *slot-number*: Specifies an IRF member device by its member ID.

Usage guidelines

If hardware crypto engines are not enabled or the device does not have hardware crypto engines, this command displays statistics only for software crypto engines.

If you do not specify any parameters, this command displays crypto engine statistics for all member devices.

Examples

Display all crypto engine statistics.

```
<Sysname> display crypto-engine statistics
  Slot ID: 1
  CPU ID: 0
  Crypto engine ID: 0
  Submitted sessions: 0
  Failed sessions: 0
  Symmetric operations: 0
  Symmetric errors: 0
  Asymmetric operations: 0
  Asymmetric errors: 0
  Get-random operations: 0
  Get-random errors: 0
```

Display statistics for crypto engine 1 on the specified slot.

```
<Sysname> display crypto-engine statistics engine-id 1 slot 1
  Submitted sessions: 0
  Failed sessions: 0
  Symmetric operations: 0
  Symmetric errors: 0
  Asymmetric operations: 0
  Asymmetric errors: 0
  Get-random operations: 0
  Get-random errors: 0
```

Table 2 Command output

Field	Description
Submitted sessions	Number of established sessions.
Failed sessions	Number of failed sessions.
Symmetric operations	Number of operations using symmetric algorithms.
Symmetric errors	Number of failed operations using symmetric algorithms.
Asymmetric operations	Number of operations using asymmetric algorithms.
Asymmetric errors	Number of failed operations using asymmetric algorithms.
Get-random operations	Number of operations for obtaining random numbers.
Get-random errors	Number of failed operations for obtaining random numbers.

Related commands

reset crypto-engine statistics

reset crypto-engine statistics

Use **reset crypto-engine statistics** to clear crypto engine statistics.

Syntax

reset crypto-engine statistics [**engine-id** *engine-id* **slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

engine-id *engine-id*: Specifies a crypto engine by its ID. The value range for the *engine-id* argument is 0 to 4294967295.

slot *slot-number*: Specifies an IRF member device by its member ID.

Usage guidelines

If you do not specify any parameters, this command clears crypto engine statistics for all member devices.

Examples

Clear statistics for all crypto engines.

```
<Sysname> reset crypto-engine statistics
```

Clear statistics for crypto engine 1 on the specified slot.

```
<Sysname> reset crypto-engine statistics engine-id 1 slot 1
```

Related commands

display crypto-engine statistics

Contents

MAC learning through a Layer 3 device commands

display snmp-server arp-sync table

Use **display snmp-server arp-sync table** to display ARP entries synchronized through SNMP.

Syntax

display snmp-server arp-sync table

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display ARP entries synchronized through SNMP.

```
<Sysname> display snmp-server arp-sync table
IP Address       MAC Address        Aging(M)
1.1.1.1          00e0-0000-0001     1
Total:1
```

Table 1 Command output

Field	Description
Aging(M)	Aging time in minutes.

Related commands

reset snmp-server arp-sync table

reset snmp-server arp-sync table

Use **reset snmp-server arp-sync table** to clear ARP entries synchronized through SNMP.

Syntax

reset snmp-server arp-sync table

Views

User view

Predefined user roles

network-admin

context-admin

Examples

Clear ARP entries synchronized through SNMP.

```
<Sysname> reset snmp-server arp-sync table
```

Related commands

display snmp-server arp-sync table

snmp-server arp-sync { interval | timeout } *

Use **snmp-server arp-sync** { **interval** | **timeout** } * to set parameters for synchronizing APR entries through SNMP.

Use **undo snmp-server arp-sync** { **interval** | **timeout** } to restore the default.

Syntax

snmp-server arp-sync { **interval** *interval* | **timeout** *time* } *

undo snmp-server arp-sync { **interval** | **timeout** }

Default

The interval for sending SNMP requests is 5 seconds and the timeout for SNMP responses is 3 seconds.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interval *interval*: Specifies the interval for sending SNMP requests in the range of 5 to 30 seconds.

timeout *time*: Specifies the timeout for SNMP responses in the range of 1 to 5 seconds.

Usage guidelines

With this feature configured, the device sends SNMP requests for ARP entry synchronization to the target Layer 3 device at the specified intervals. If the device does not receive an SNMP response before the timeout expires within the specified interval, the device re-sends SNMP requests.

Examples

Set the interval for sending SNMP requests and the timeout for SNMP responses to 10 and 2 seconds, respectively.

```
<Sysname> system-view
[Sysname] snmp-server arp-sync interval 10 timeout 2
```

snmp-server arp-sync enable

Use **snmp-server arp-sync enable** to enable ARP entry synchronization through SNMP.

Use **undo snmp-server arp-sync enable** to disable ARP entry synchronization through SNMP.

Syntax

snmp-server arp-sync enable

undo snmp-server arp-sync enable

Default

ARP entry synchronization through SNMP is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

With this feature enabled, the device acts as an NMS to learn all ARP entries on a Layer 3 device (agent) to obtain the MAC address of the Layer 3 device.

Examples

Enable ARP entry synchronization through SNMP.

```
<Sysname> system-view
[Sysname] snmp-server arp-sync enable
```

snmp-server arp-sync target-host

Use **snmp-server arp-sync target-host** to configure the target Layer 3 device for ARP synchronization through SNMP.

Use **undo snmp-server arp-sync target-host** to remove the configuration of the target Layer 3 device for ARP synchronization through SNMP.

Syntax

SNMPv2c:

snmp-server arp-sync target-host address *ip-address* **community** { **simple** | **cipher** } *community-name* **v2c**

undo snmp-server arp-sync target-host address *ip-address* **community** { **simple** | **cipher** } *community-name*

SNMPv3:

snmp-server arp-sync target-host address *ip-address* **usm-user v3** *user-name* [{ **simple** | **cipher** } **authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode** { **aes128** | **des56** } *pri-password*]]

undo snmp-server arp-sync target-host address *ip-address* **usm-user v3** *user-name*

Default

No target Layer 3 device is configured for ARP synchronization through SNMP.

Views

System view

Predefined user roles

network-admin

contex-admin

Parameters

address *ip-address*: Specifies an IPv4 address of the target Layer 3 device.

simple: Specifies a community name in plaintext form. For security purposes, the community name specified in plaintext form will be stored in encrypted form.

cipher: Specifies a community name in encrypted form.

community-name: Specifies the community name. The plaintext form is a case-sensitive string of 1 to 32 characters. The encrypted form is a case-sensitive string of 33 to 73 characters. Input a string as escape characters after a backslash (\).

v2c: Specifies SNMPv2c.

user-name: Specifies a username, a case-sensitive string of 1 to 32 characters.

v3: Specifies SNMPv3.

simple: Specifies an authentication key and an encryption key in plaintext from. The keys will be converted to a digest in encrypted form and stored in the device.

cipher: Specifies an authentication key and an encryption key in encrypted form. The keys will be converted to a digest in encrypted form and stored in the device.

authentication-mode: Specifies an authentication algorithm. If you do not specify the keyword, the system does not perform authentication.

- **md5**: Specifies the HMAC-MD5 authentication algorithm. For information about the HMAC-MD5 algorithm, see IPsec configuration in *VPN Instance Configuration Guide*.
- **sha**: Specifies the HMAC-SHA1 authentication algorithm. For information about the HMAC-SHA1 algorithm, see IPsec configuration in *VPN Instance Configuration Guide*.

auth-password: Specifies a case-sensitive authentication key in plaintext form or encrypted form. The value is a string of 8 to 64 characters.

privacy-mode: Specifies an encryption algorithm. If you do not specify this keyword, the system does not perform encryption.

- **aes128**: Specifies the Advanced Encryption Standard (AES) algorithm that uses a 128-bit key.
- **des56**: Specifies the Data Encryption Standard (DES) algorithm that uses a 56-bit key.

priv-password: Specifies a case-sensitive encryption key in plaintext form or encrypted form. The value is a string of 8 to 64 characters.

Usage guidelines

You can configure this command multiple times to specify multiple Layer 3 devices for ARP entry synchronization.

Examples

Configure the device to use the plaintext-form community name **testCommunity** to synchronize ARP entries from Layer 3 device 10.1.1.1 through SNMPv2c.

```
<Sysname> system-view
[Sysname] snmp-server arp-sync target-host address 10.1.1.1 community simple
testCommunity v2c
```

Configure the device to use username **testUser** to synchronize ARP entries from Layer 3 device 10.1.1.1 through SNMPv3 by using authentication algorithm **HMAC-SHA1**, plaintext-form authentication key **123456TESTauth&!**, encryption algorithm **DES**, and plaintext-form encryption key **123456TESTencr&!**.

```
<Sysname> system-view
[Sysname] snmp-server arp-sync target-host address 10.1.1.1 usm-user v3 testUser simple
authentication-mode sha 123456TESTauth&! privacy-mode des56 123456TESTencr&!
```

Contents

SMS commands

app id

Use **app-id** to specify the app ID for the third-party SMS platform.

Use **undo app-id** to restore the default.

Syntax

app-id *app-id*

undo app-id

Default

No app ID is specified for the third-party SMS platform.

Views

SMS gateway view

Predefined user roles

network-admin

context-admin

Parameters

app-id: Specifies the app ID of the third-party SMS platform, a case-sensitive string of 1 to 31 characters.

Usage guidelines

The app ID is encapsulated in the header field of HTTP requests and sent to the third-party SMS platform for the identity authentication of the SMS gateway. The platform determines the secret key for decryption according to the received app ID and grants the corresponding services to the SMS gateway.

The app ID is provided by the third-party SMS platform.

Examples

Specify **abc** as the app ID of the third-party SMS platform for SMS gateway **gw1**.

```
<Sysname> system-view
[Sysname] sms-gateway gw1
[Sysname-sms-gateway-gw1] app-id abc
```

Related commands

secret-key

display sms-gateway

Use **display sms-gateway** to display SMS gateway information.

Syntax

display sms-gateway [**brief** | **name** *gateway-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

brief: Displays brief information about all SMS gateways. If you do not specify this keyword, the command displays detailed SMS gateway information.

name *gateway-name*: Specifies an SMS gateway by its name. An SMS gateway name is a case-insensitive string of 1 to 31 characters, and can contain only letters, digits, and underscores (_). If you do not specify an SMS gateway, this command displays information about all SMS gateways.

Usage guidelines

The configured secret key for SMS data encryption will be displayed in cipher text.

Examples

Display detailed information about all SMS gateways.

```
<Sysname> display sms-gateway

Total Number of SMS gateways: 2
SMS gateway name: gw1
  SMS platform: emay
  App ID: abc
  Secret key: $c$3$zvzJI1AMQ4OVHCkSnXXoAOUyd2STdtIFtQDlJETCg=
  VPN instance: vpn1

SMS gateway name: gw2
  SMS platform: emay
  App ID: 123
  Secret key: $c$3$AS4tqlnOVODYEQ5IMHJNyNTTAyBPotXgw==
  VPN instance: vpn1
```

Table 1 Command output

Field	Description
SMS platform	SMS platform used by the SMS gateway to send SMS messages.
App ID	App ID for the third-party SMS platform.
Secret key	Secret key (in cipher text) for SMS data encryption.
VPN instance	VPN instance associated with the SMS gateway.

Display brief information about all SMS gateways.

```
<Sysname> display sms-gateway brief
SMS gateway name               SMS platform     VPN instance
gw1                            emay             vpn1
gw2                            emay             vpn1
```

Table 2 Command output

Field	Description
SMS platform	SMS platform used by the SMS gateway to send SMS messages.
VPN instance	VPN instance associated with the SMS gateway.

secret-key

Use **secret-key** to specify the secret key for SMS data encryption.

Use **undo secret-key** to restore the default.

Syntax

secret-key { **cipher** | **simple** } *string*

undo secret-key

Default

No secret key is specified for SMS data encryption.

Views

SMS gateway view

Predefined user roles

network-admin

context-admin

Parameters

cipher: Specifies a ciphertext secret key.

simple: Specifies a plaintext secret key. A plaintext secret key is stored in cipher text.

string: Specifies a case-sensitive secret-key string. A plaintext secret key is a string of 1 to 63 characters, and a ciphertext secret key is a string of 1 to 117 characters.

Usage guidelines

The secret key is provided by the third-party SMS platform.

The secret key uniquely corresponds to the app ID configured by the **app-id** command for the third-party SMS platform.

The service module sends SMS data to the SMS gateway, and then the SMS gateway performs the following operations:

1. Parses and converts the SMS data into data that can be recognized by the third-party SMS platform.
2. Uses the secret key and algorithms to encrypt the SMS data.
3. Sends the encrypted data to the third-party SMS platform.

The third-party SMS platform performs the following operations after receiving the encrypted data:

1. Obtains the app ID in the header field of the HTTP request.
2. Uses the secret key that corresponds to the app ID to decrypt the data to plaintext data.
3. Sends the data in an SMS message to the user mobile number.

Examples

Specify the plaintext secret key as **TESTplat&!** for SMS data encryption.

```
<Sysname> system-view
[Sysname] sms-gateway gw1
[Sysname-sms-gateway-gw1] secret-key simple TESTplat&!
```

Related commands

app-id

sms-gateway

Use **sms-gateway** to create an SMS gateway and enter its view, or enter the view of an existing SMS gateway.

Use **undo sms-gateway** to remove an SMS gateway.

Syntax

sms-gateway *gateway-name*

undo sms-gateway *gateway-name*

Default

No SMS gateways exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

gateway-name: Specifies an SMS gateway by its name, a case-insensitive string of 1 to 31 characters. Valid characters are letters, digits, and underscores (_).

Usage guidelines

The device implements SMS sending through an SMS gateway as follows:

1. A service module sends SMS data to the SMS gateway.
2. The SMS gateway converts the SMS data to the data that can be recognized by the third-party SMS platform.
3. The SMS gateway sends the SMS data to the third-party SMS platform through HTTP.
4. The third-party SMS platform sends the SMS message to the user mobile number.

SMS settings are configured in SMS gateway view, including the SMS platform, app ID for logging in to the third-party SMS platform, and secret key for SMS data encryption.

An SMS gateway can be associated with multiple service modules that require SMS services.

Examples

Create an SMS gateway named **gw1** and enter its view.

```
<Sysname> system-view
[Sysname] sms-gateway gw1
[Sysname-sms-gateway-gw1]
```

Related commands

display sms-gateway

sms-platform

Use **sms-platform** to specify the SMS platform that sends messages.

Use **undo sms-platform** to restore the default.

Syntax

sms-platform emay

undo sms-platform

Default

No SMS platform is specified for sending messages.

Views

SMS gateway view

Predefined user roles

network-admin

context-admin

Parameters

emay: Specifies the Emay SMS platform.

Usage guidelines

To use the third-party SMS platform specified by this command, you must also configure **app-id** and **secret-key** for the platform on the SMS gateway.

Examples

Specify the SMS platform as **emay** for SMS gateway **gw1**.

```
<Sysname> system-view
[Sysname] sms-gateway gw1
[Sysname-sms-gateway-gw1] sms-platform emay
```

Related commands

app-id

secret-key

sms-send test-mobile

Use **sms-send test-mobile** to send a test SMS message to the specified mobile number.

Syntax

sms-send test-mobile *number*

Views

SMS gateway view

Predefined user roles

network-admin

context-admin

Parameters

number: Specifies the mobile number for receiving test messages, which is a string of 1 to 31 digits.

Usage guidelines

Use this command to test whether the configured SMS gateway can operate correctly. The SMS gateway is considered to be normal if the mobile number receives an **App ID XXX verification passed** message.

Examples

Send a test message to mobile number 111111 for SMS gateway **gw1**.

```
<Sysname> system-view
[Sysname] sms-gateway gw1
[Sysname-sms-gateway-gw1] sms-send test-mobile 111111
```

Related commands

app-id

secret-key

sms-platform

vpn-instance

Use **vpn-instance** to specify the VPN instance for an SMS gateway.

Use **undo vpn-instance** to restore the default.

Syntax

vpn-instance *vpn-instance-name*

undo vpn-instance

Default

An SMS gateway belongs to the public network.

Views

SMS gateway view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance-name: Specifies the name of an MPLS L3VPN instance, a case-sensitive string of 1 to 31 characters.

Usage guidelines

After you execute this command, the resources contained by an SMS gateway will belong to the associated VPN instance.

You can specify only one VPN instance for an SMS gateway.

Examples

Specify VPN instance **vpn1** for SSL VPN gateway **gw1**.

```
<Sysname> system-view
[Sysname] sms-gateway gw1
[Sysname-sms-gateway-gw1] vpn-instance vpn1
```

NSFOCUS Firewall Series

NF DPI Command Reference

NSFOCUS Technologies, Inc.

Document version: 6W600-20230221

Preface

This command reference describes the commands for configuring DPI features, including DPI engine, IPS, URL filtering, data filtering, file filtering, anti-virus, data analysis center, proxy policy.

This preface includes the following topics about the documentation:

- Audience.
- Conventions.

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators.

Conventions

The following information describes the conventions used in the documentation.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select a minimum of one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
CAUTION:	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Contents

DPI engine commands

app-profile

Use **app-profile** to create a deep packet inspection (DPI) application profile and enter its view, or enter the view of an existing DPI application profile.

Use **undo app-profile** to delete a DPI application profile.

Syntax

app-profile *profile-name*

undo app-profile *profile-name*

Default

No DPI application profiles exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

profile-name: Specifies a DPI application profile name. The profile name is a case-insensitive string of 1 to 63 characters. Valid characters are letters, digits, and underscores (_).

Usage guidelines

The DPI application profile is a security service template that can include DPI service policies such as URL filtering policy.

A DPI application profile takes effect after a security policy rule uses it as the action. The DPI engine inspects the packets matching the rule and submits the packets to the associated DPI service module for processing.

Examples

Create a DPI application profile named **abc** and enter its view.

```
<Sysname> system-view
[Sysname] app-profile abc
[Sysname-app-profile-abc]
```

authentication enable

Use **authentication enable** to enable email client authentication.

Use **undo authentication enable** to disable email client authentication.

Syntax

authentication enable

undo authentication enable

Default

Email client authentication is enabled.

Views

Email parameter profile view

Predefined user roles

network-admin

context-admin

Usage guidelines

Use this command when the email server specified by the **email-server** command requires client authentication.

Examples

Disable email client authentication.

```
<Sysname> system-view
[Sysname] inspect email parameter-profile c1
[Sysname-inspect-email-c1] undo authentication enable
```

block-period

Use **block-period** to set the block period during which a source IP address is blocked.

Use **undo block-period** to restore the default.

Syntax

block-period *period*

undo block-period

Default

A source IP address is blocked for 1800 seconds.

Views

Block source parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

period: Specifies the block period in the range of 1 to 86400 seconds.

Usage guidelines

For the block period to take effect, make sure the blacklist feature is enabled.

The device drops the packet that matches an inspection rule and adds the packet's source IP address to the IP blacklist.

- If the blacklist feature is enabled, the device directly drops subsequent packets from the source IP address during the block period.
- If the blacklist feature is disabled, the block period does not take effect. The device inspects all packets and drops the matching ones.

For more information about the blacklist feature, see attack detection and prevention in the *Security Configuration Guide*.

Examples

Set the block period to 3600 seconds in block source parameter profile **b1**.

```
<Sysname> system-view
[Sysname] inspect block-source parameter-profile b1
[Sysname-inspect-block-source-b1] block-period 3600
```

Related commands

blacklist enable (security zone view) (*Security Command Reference*)

blacklist global enable (*Security Command Reference*)

inspect block-source parameter-profile

capture-limit

Use **capture-limit** to set the maximum volume of captured packets that can be cached.

Use **undo capture-limit** to restore the default.

Syntax

capture-limit *kilobytes*

undo capture-limit

Default

The device can cache a maximum of 512 Kilobytes of captured packets.

Views

Capture parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

kilobytes: Specifies the maximum volume in the range of 0 to 1024 Kilobytes.

Usage guidelines

The device caches captured packets locally. It exports the cached captured packets to a URL when the volume of cached captured packets reaches the maximum, and clears the cache. After the export, the device starts to capture packets again.

If you set the maximum volume of cached captured packets to 0 Kilobytes, the device immediately exports a packet to the URL after the packet is captured.

Examples

Set the maximum volume of cached captured packets to 1024 Kilobytes in the capture parameter profile **c1**.

```
<Sysname> system-view
[Sysname] inspect capture parameter-profile c1
[Sysname-inspect-capture-c1] capture-limit 1024
```

Related commands

export repeating-at

export url

inspect capture parameter-profile

display inspect md5-verify configuration

Use **display inspect md5-verify configuration** to display information about the MD5 hash-based virus inspection for all files feature.

Syntax

display inspect md5-verify configuration

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display information about the MD5 hash-based virus inspection for all files feature.

```
<Sysname> system-view
[Sysname] display inspect md5-verify configuration
MD5 file verification for all files: Enabled
```

Table 1 Command output

Field	Description
MD5 file verification for all files	Status of the MD5 hash-based virus inspection for all files feature: **Enabled** or **Disabled**.

Related commands

inspect md5-verify all-files

display inspect status

Use **display inspect status** to display the status of the DPI engine.

Syntax

display inspect status

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display the status of the DPI engine.

```
<Sysname> display inspect status
```

```
Chassis 0 Slot 1:
 Running status: Normal
```

Table 2 Command output

Field	Description
Running status	Status of the DPI engine: • **DPI administratively disabled**. • **DPI auto-bypass for protocol xxx**. • **DPI disabled due to high CPU usage**. • **Normal**—The DPI engine is running correctly.
Usage threshold has already been reached for the following CPU cores: xxx	This sentence appears when one or more CPU cores reach the CPU core usage alarm threshold. DPI will not use these CPU cores to process services.

Related commands

monitor cpu-usage threshold core (*Fundamentals Command Reference*)

email-limit

Use **email-limit** to configure output limit for log entries sent to the email server.

Use **undo email-limit** to restore the default.

Syntax

email-limit interval *interval* **max-number** *value*

undo email-limit

Default

The device allows sending a maximum of 10 log entries within five minutes.

Views

Email parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

interval *interval*: Specifies email sending interval in the range of 1 to 10 minutes.

max-number *max-number*: Specifies the maximum number of emails per interval, in the range of 1 to 100.

Usage guidelines

This command prevents the device from frequently sending too many log entries to the email server.

The device caches the log entries and sends them when the specified interval is reached.

If the number of cached log entries has reached the upper limit, the device compares the severity level of a new log entry with the severity levels of the cached log entries. If the severity level of the new log entry is higher than that of a cached log entry, the new log entry will overwrite the most recently cached log entry with the lowest severity level. The severity level of a new log entry is the severity level of the matching IPS signatures.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Allow the device to send a maximum of 20 log entries within five minutes to the email server.

```
<Sysname> system-view
[Sysname] inspect email parameter-profile test
[Sysname-inspect-email-test] email-limit interval 5 max-number 20
```

email-server

Use **email-server** to specify the email server.

Use **undo email-server** to restore the default.

Syntax

email-server *address-string*

undo email-server

Default

No email server is specified.

Views

Email parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

address-string: Specifies the email server address, a case-sensitive string of 3 to 63 characters.

Usage guidelines

The email server address can be an IP address or a host name.

If you specify the email server by host name, make sure the device can resolve the host name into its IP address through static or dynamic DNS. Make sure the device and the email server can reach each other. For more information about DNS, see *Layer 3—IP Services Configuration Guide*.

If you execute this command multiple times for the same email parameter profile, the most recent configuration takes effect.

Examples

Specify the email server **rndcas.123.com**.

```
<Sysname> system-view
[Sysname] inspect email parameter-profile c1
[Sysname-inspect-email-c1] email-server rndcas.123.com
```

Specify the email server at 192.168.1.1.

```
<Sysname> system-view
[Sysname] inspect email parameter-profile c1
[Sysname-inspect-email-c1] email-server 192.168.1.1
```

export repeating-at

Use **export repeating-at** to set the daily export time for cached captured packets.

Use **export repeating-at** to restore the default.

Syntax

export repeating-at *time*

undo export repeating-at

Default

The system exports cached captured packets at 1:00 a.m. every day.

Views

Capture parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

time: Specifies the daily export time in the format of hh:mm:ss in the range of 00:00:00 to 23:59:59.

Usage guidelines

The device exports cached captured packets to a URL and clears the cache at the daily export time, whether or not the volume of cached captured packets reaches the maximum.

Examples

Configure the device to export cached captured packets at 2:00 a.m. every day in the capture parameter profile **c1**.

```
<Sysname> system-view
[Sysname] inspect capture parameter-profile c1
[Sysname-inspect-capture-c1] export repeating-at 02:00:00
```

Related commands

capture-limit

export url

inspect capture parameter-profile

export url

Use **export url** to specify the URL to which the cached captured packets are exported.

Use **export url** to restore the default.

Syntax

export url *url-string*

undo export url

Default

No URL is specified for exporting the cached captured packets.

Views

Capture parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

url-string: Specifies the URL, a string of 1 to 255 characters.

Usage guidelines

The device exports the cached captured packets to the specified URL at the daily export time or when the volume of cached captured packets reaches the maximum. After the captured packets are exported, the system clears the cache.

If you do not specify a URL, the device still exports the cached captured packets but the export fails.

Examples

Configure the device to export cached captured packets to URL tftp://192.168.100.100/upload in the capture parameter profile **c1**.

```
<Sysname> system-view
[Sysname] inspect capture parameter-profile c1
[Sysname-inspect-capture-c1] export url tftp://192.168.100.100/upload
```

Related commands

capture-limit

export repeating-at

inspect capture parameter-profile

import block warning-file

Use **import block warning-file** to import a user-defined alarm message from a warning file.

Syntax

import block warning-file *file-path*

Default

The device uses the default alarm message "**The site you are accessing has a security risk and thereby is blocked**."

Views

Warning parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

file-path: Specifies the warning file path, a string of 1 to 200 characters.

Usage guidelines

After you execute the **inspect warning parameter-profile** command, the system automatically generates a warning file named **av-httpDeclare-xxx** in the **dpi/av/warning** directory. The **xxx** represents the name of the warning parameter profile.

A default alarm message is predefined in the warning file. If an end-point user visits a virus-infected website, the device will block the website access and displays the alarm message on the browser of the end-point user.

You can execute the **import block warning-file** command to specify a user-defined alarm message from a file. Only HTML and TXT files are supported.

The device supports the following import methods:

- **Local import**—Imports the message from the warning file that is stored locally.

  Store the warning file on the master device for successful import.

  The format of the *file-path* argument varies by the location of the warning file to be imported.

The warning file is stored…	Format of *file-path*	Remarks
In the current working directory	*filename*	To display the current working directory, use the **pwd** command. For information about the **pwd** command, see file system management in *Fundamentals Command Reference*.
In a directory different from the working directory on the same storage medium	*filename*	Before importing the warning file, you must first use the **cd** command to open the directory where the file is stored. For information about the **cd** command, see file system management in *Fundamentals Command Reference*.
On a storage medium different from the working directory	*path/filename*	Before importing the warning file, you must first use the **cd** command to open the root directory of the storage medium where the file is stored. For information about the **cd** command, see file system management in *Fundamentals Command Reference.*

- **FTP/TFTP import**—Imports the message from the warning file that is stored on an FTP or TFTP server.

  The format of the *file-path* argument varies by the location of the warning file to be imported.

The warning file is stored on	Format of *file-path*	Remarks
An FTP server	ftp://*username*:*password*@*server*/*filename*	The *username* and *password* arguments represent the FTP login username and password, respectively. The *server* argument represents the IP address or host name of the FTP server. If a colon (:), at sign (@), or forward slash (/) exists in the username or password, you must convert it into its escape characters. The escape characters are **%3A** or **%3a** for a colon, **%40** for an at sign, and **%2F** or **%2f** for a forward slash.

A TFTP server.	tftp://*server*/*filename*	The *server* argument represents the IP address or host name of the TFTP server.

NOTE:

To specify a warning file on an FTP or TFTP server, make sure the device and the server can reach each other. If you specify the server by its host name, you must also make sure the device can resolve the host name into an IP address through static or dynamic DNS. For more information about DNS, see *Layer 3—IP Services Configuration Guide*.

Examples

Import a user-defined alarm message from the warning file on a TFTP server.

```
<Sysname> system-view
[Sysname] inspect warning parameter-profile warn
[Sysname-inspect-warning-warn] import block warning-file tftp://192.168.0.1/warning.txt
```

Import a user-defined alarm message from the warning file on an FTP server. The FTP login username and password are **user** and **password**, respectively.

```
<Sysname> system-view
[Sysname] inspect warning parameter-profile warn
[Sysname-inspect-warning-warn] import block warning-file
ftp://user:password@192.168.0.1/warning.txt
```

Import a user-defined alarm message from the warning file stored locally. The file is stored in directory **cfa0:/warning.txt**, and the current working directory is **cfa0**.

```
<Sysname> system-view
[Sysname] inspect warning parameter-profile warn
[Sysname-inspect-warning-warn] import block warning-file warning.txt
```

inspect activate

Use **inspect activate** to activate the policy and rule configurations for DPI service modules.

Syntax

inspect activate

Default

The creation, modification, and deletion of DPI service policies and rules will be activated automatically.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

CAUTION:

This command causes transient DPI service interruption. DPI-based services might also be interrupted. For example, security policies cannot control access to applications.

By default, the system will detect whether another configuration change (such as creation, modification, or deletion) occurs within a 20-second interval after a configuration change for DPI service modules such as URL filtering:

- If no configuration change occurs within the interval, the system performs an activation operation at the end of the next interval to make the configuration take effect.
- If a configuration change occurs within the interval, the system continues to periodically check whether a configuration change occurs within the interval.

To activate the policy and rule configurations for DPI service modules immediately, you can execute the **inspect activate** command.

Examples

Activate the policy and rule configurations for DPI service modules.

```
<Sysname> system-view
[Sysname] inspect activate
```

inspect auto-bypass

Use **inspect auto-bypass enable** to enable automatic bypass of the DPI engine.

Use **undo inspect auto-bypass enable** to disable automatic bypass of the DPI engine.

Syntax

inspect auto-bypass enable

undo inspect auto-bypass enable

Default

Automatic bypass of the DPI engine is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

With this feature enabled, the DPI engine automatically disables inspection on packets of the specified protocol after a device reboot caused by packet inspection errors.

Examples

Enable automatic bypass of the DPI engine.

```
<Sysname> system-view
[Sysname] inspect auto-bypass enable
This feature might cause some functions of the DPI engine to be unavailable. Continue?
[Y/N]:y
```

inspect block-source parameter-profile

Use **inspect block-source parameter-profile** to create a block source parameter profile and enter its view, or enter the view of an existing block source parameter profile.

Use **undo inspect block-source parameter-profile** to delete a block source parameter profile.

Syntax

inspect block-source parameter-profile *parameter-name*

undo inspect block-source parameter-profile *parameter-name*

Default

No block source parameter profiles exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

parameter-name: Specifies a block source parameter profile name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

In block source parameter profile view, you can set parameters for the block source action, such as the block period.

Examples

Create a block source parameter profile named **b1** and enter its view.

```
<Sysname> system-view
[Sysname] inspect block-source parameter-profile b1
[Sysname-inspect-block-source-b1]
```

Related commands

block-period

inspect bypass

Use **inspect bypass** to disable the DPI engine.

Use **undo inspect bypass** to enable the DPI engine.

Syntax

inspect bypass

undo inspect bypass

Default

The DPI engine is enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

CAUTION:

This command causes packets of any protocols not to be processed by DPI. DPI-based services might also be interrupted. For example, security policies cannot control access to applications.

Packet inspection in the DPI engine is a complex and resource-consuming process. When the CPU usage is high, you can disable the DPI engine to guarantee the device performance.

Examples

Disable the DPI engine.

```
<Sysname> system-view
[Sysname] inspect bypass
```

Related commands

display inspect status

inspect bypass protocol

Use **inspect bypass protocol** to specify the protocols to bypass the DPI engine.

Use **undo inspect bypass protocol** to disable DPI engine bypass for protocols.

Syntax

inspect bypass protocol { **dns** | **ftp** | **ftp-data** | **http** | **https** | **imap** | **nfs** | **pop3** | **rtmp** | **sip** | **smb** | **smtp** | **telnet** | **tftp** } *

undo inspect bypass protocol [**dns** | **ftp** | **ftp-data** | **http** | **https** | **imap** | **nfs** | **pop3** | **rtmp** | **sip** | **smb** | **smtp** | **telnet** | **tftp**] *

Default

The DPI engine inspects all supported protocols.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

dns: Specifies the DNS protocol.

ftp: Specifies the FTP protocol.

ftp-data: Specifies the FTP data protocol.

http: Specifies the HTTP protocol.

https: Specifies the HTTPS protocol.

imap: Specifies the IMAP protocol.

nfs: Specifies the NFS protocol.

pop3: Specifies the POP3 protocol.

rtmp: Specifies the RTMP protocol.

sip: Specifies the SIP protocol.

smb: Specifies the SMB protocol.

smtp: Specifies the SMTP protocol.

telnet: Specifies the Telnet protocol.

tftp: Specifies the TFTP protocol.

Usage guidelines

If you do not specify any keyword when executing the **undo inspect bypass protocol** command, the DPI engine inspects all supported protocols.

As a best practice, you can specify the protocols to bypass the DPI engine when either of the following conditions is met:

- Inspection on packets of the specified protocols is not required. You can disable the DPI engine for the specified protocols to reduce the occupation of device resources and improve the device performance.
- Inspection on packets of the specified protocols causes device reboot. You can specify the protocols to bypass the DPI engine to avoid device reboot caused by inspection error and ensure the inspection on packets of other protocols.

Examples

Specify the HTTP protocol to bypass the DPI engine.

```
<Sysname> system-view
[Sysname] inspect bypass protocol http
This feature might cause the DPI engine to be unavailable for the specified protocol.
Continue? [Y/N]:y
```

Related commands

display inspect status

inspect cache-option maximum

Use **inspect cache-option maximum** to set the maximum number of options to be cached per TCP or UDP data flow for further inspection.

Use **undo inspect cache-option** to restore the default.

Syntax

inspect cache-option maximum *max-number*

undo inspect cache-option

Default

The DPI engine can cache a maximum of 32 options per TCP or UDP data flow.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

max-number: Specifies the maximum number of options to be cached per TCP or UDP data flow. The value range is 1 to 254.

Usage guidelines

An inspection rule can contain multiple AC patterns, and each AC pattern can be associated with multiple options. A TCP or UDP data flow matches an inspection rule if the packets of the flow match all the AC patterns and options in the rule.

If a packet of a TCP or UDP data flow matches one AC pattern in an inspection rule, the DPI engine cannot determine whether the flow matches the rule. The DPI engine continues to match packets of the flow against the remaining options and AC patterns in the rule. For any options that cannot be matched, the DPI engine caches them to match subsequent packets. The DPI engines determines that the flow matches the rule when all options and AC patterns in the rule are matched.

The more options DPI engine caches, the more likely that DPI engine identifies the application information and the more accurate the DPI engine inspection. However, caching more options requires more memory. If the device has a high memory usage, configure the DPI engine to cache less options to improve the device performance.

Typically, the default setting is sufficient for most scenarios.

Examples

Configure the DPI engine to cache a maximum of four options per TCP or UDP data flow for further inspection.

```
<Sysname> system-view
[Sysname] inspect cache-option maximum 4
```

inspect capture parameter-profile

Use **inspect capture parameter-profile** to create a capture parameter profile and enter its view, or enter the view of an existing capture parameter profile.

Use **undo inspect capture parameter-profile** to delete a capture parameter profile.

Syntax

inspect capture parameter-profile *parameter-name*

undo inspect capture parameter-profile *parameter-name*

Default

No capture parameter profiles exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

profile-name: Specifies a capture parameter profile name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

In capture parameter profile view, you can set parameters for the packet capture action, such as the maximum volume of cached captured packets.

Only the IPS module supports the packet capture action.

Examples

Create a capture parameter profile named **c1** and enter its view.

```
<Sysname> system-view
[Sysname] inspect capture parameter-profile c1
[Sysname-inspect-capture-c1]
```

Related commands

capture-limit

export repeating-at

export url

inspect cloud-server

Use **inspect cloud-server** to specify the server used by DPI services for cloud query.

Use **undo inspect cloud-server** to remove the cloud query server specified for DPI services.

Syntax

inspect cloud-server *host-name*

undo inspect cloud-server

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

host-name: Specifies the cloud query server by its host name, a case-insensitive string of 1 to 255 characters. Valid characters include letters, digits, underscores (_), hyphens (-), and dots (.)

Usage guidelines

The cloud query server supports URL filtering cloud query and anti-virus MD5 value cloud query.

For successful cloud query, make sure the device can resolve the host name of the cloud query server into an IP address through DNS. For more information about DNS, see DNS configuration in *Layer 3—IP Services Configuration Guide.*

This command is supported only on the default context. For more information about contexts, see context configuration in *Virtual Technologies Configuration Guide.*

Examples

Specify the server with host name **service.nsfocus.com.cn** for cloud query.

```
<Sysname> system-view
[Sysname] inspect cloud-server service.nsfocus.com.cn
```

Related commands

cloud-query enable (anti-virus policy view)

cloud-query enable (URL filtering policy view)

inspect coverage

Use **inspect coverage** to configure a DPI engine inspection mode.

Use **undo inspect coverage** to restore the default.

Syntax

inspect coverage { **balanced** | **large-coverage** | **high-performance** | **user-defined** }

undo inspect coverage

Default

The DPI engine uses the balanced mode.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

balanced: Specifies the balanced mode. This mode makes a tradeoff between the device performance and inspection coverage.

large-coverage: Specifies the large coverage mode. This mode appropriately reduces device performance to achieve the best inspection coverage.

high-performance: Specifies the high performance mode. This mode appropriately reduces the inspection coverage to ensure the best device performance.

user-defined: Specifies the user-defined mode. This mode allows you to adjust the inspection length of the DPI engine as required.

Usage guidelines

Select an inspection mode as required:

- **Balanced mode**—Applicable to most scenarios. This mode makes a tradeoff between the device performance and inspection coverage. The maximum length is 32 Kilobytes for FTP, HTTP, SMB, NFS, and email streams, and the maximum file length for MD5 inspection is 2048 Kilobytes.
- **Large coverage mode**—Applicable to the scenarios that require large inspection coverage. This mode improves the inspection coverage at the cost of device performance. The maximum length is 128 Kilobytes for FTP, HTTP, SMB, NFS, and email streams, and the maximum file length for MD5 inspection is 5120 Kilobytes.
- **High performance mode**—Applicable to the scenarios that requires high device performance. This mode improves the device performance while ensuring a certain inspection coverage. The maximum length is 32 Kilobytes for FTP, HTTP, SMB, NFS, and email streams, and the maximum file length for MD5 inspection is 32 Kilobytes.
- **User-defined mode**—Applicable to the scenarios that have specific requirements for inspection coverage and device performance. In this mode, you can execute the **inspect stream-fixed-length and inspect md5-fixed-length commands to** set the maximum stream length for inspection and maximum file length for MD5 value calculation, respectively.

Examples

Configure the user-defined mode as the DPI engine inspection mode.

```
<Sysname> system-view
[Sysname] inspect coverage user-defined
```

Related commands

inspect file-fixed-length enable

inspect stream-fixed-length enable

inspect cpu-threshold disable

Use **inspect cpu-threshold disable** to disable inspection suspension upon excessive CPU usage.

Use **undo inspect cpu-threshold disable** to enable inspection suspension upon excessive CPU usage.

Syntax

inspect cpu-threshold disable

undo inspect cpu-threshold disable

Default

Inspection suspension upon excessive CPU usage is enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

Packet inspection in the DPI engine is a complex and resource-consuming process.

Inspection suspension upon excessive CPU usage works as follows:

- When the device's CPU usage rises to or above the CPU usage threshold, the DPI engine suspends packet inspection to guarantee the device performance.
- When the device's CPU usage drops to or below the CPU usage recovery threshold, the DPI engine resumes packet inspection.

Do not disable inspection suspension upon excessive CPU usage if the device's CPU usage is high.

Examples

Disable inspection suspension upon excessive CPU usage.

```
<Sysname> system-view
[Sysname] inspect cpu-threshold disable
```

Related commands

display inspect status

inspect bypass

inspect stream-fixed-length disable

inspect dual-active enable

Use **inspect dual-active enable** to enable support for HA dual-active mode.

Use **undo inspect dual-active enable** to disable support for HA dual-active mode.

Syntax

inspect dual-active enable

undo inspect dual-active enable

Default

Support for HA dual-active mode is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

The feature ensures the device in dual-active mode can correctly process DPI services in a network with asymmetric forwarding of flows.

This feature takes effect only when the device operates in HA dual-active mode.

For more information about HA dual-active mode, see RBM-based hot backup configuration in *High Availability Configuration Guide*.

Examples

Enable support for HA dual-active mode.

```
<Sysname> system-view
[Sysname] inspect dual-active enable
```

Related commands

backup-mode dual-active (*High Availability Command Reference*)

inspect email parameter-profile

Use **inspect email parameter-profile** to create an email parameter profile and enter its view, or enter the view of an existing email parameter profile.

Use **undo inspect email parameter-profile** to delete an email parameter profile.

Syntax

inspect email parameter-profile *parameter-name*

undo inspect email parameter-profile *parameter-name*

Default

No email parameter profiles exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

parameter-name: Specifies an email parameter profile name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

In email parameter profile view, you can set parameters for the email action. Email parameters include the email server, the email sender and receiver, and the username and password for logging in to the email server.

Examples

Create an email parameter profile named **c1** and enter its view.

```
<Sysname> system-view
[Sysname] inspect email parameter-profile c1
[Sysname-inspect-email-c1]
```

inspect file-fixed-length

Use **inspect file-fixed-length** to set the fixed length for file inspection.

Use **undo inspect file-fixed-length** to restore the default.

Syntax

inspect file-fixed-length { **email** | **ftp** | **http** | **nfs** | **smb** } * *length-value*

undo inspect file-fixed-length

Default

The fixed length is 32 Kilobytes for FTP, HTTP, NFS, SMB, and email files.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

email: Specifies email protocols, including SMTP, POP3 and IMAP.

ftp: Specifies the FTP protocol.

http: Specifies the HTTP protocol.

nfs: Specifies the NFS protocol.

smb: Specifies the SMB protocol.

length-value: Specifies the fixed length in the range of 1 to 2048 Kilobytes.

Usage guidelines

This command can be executed only if the DPI engine inspection mode is user-defined mode.

Typically, virus signatures are embedded in the first half of a file. Narrowing the inspection scope of each file improves the file inspection efficiency.

If a data stream contains multiple files, this feature inspects only the fixed length data of each file.

Because files are transmitted in a data stream, the fixed length of files must not be longer than that of the data stream configured by the **inspect stream-fixed-length** command.

Examples

Set the fixed length to 128 Kilobytes for inspecting each HTTP file.

```
<Sysname> system-view
[Sysname] inspect file-fixed-length http 128
```

Related commands

inspect coverage user-defined

inspect file-fixed-length enable

inspect stream-fixed-length

inspect file-fixed-length enable

Use **inspect file-fixed-length enable** to enable file fixed length inspection.

Use **undo inspect file-fixed-length enable** to disable file fixed length inspection.

Syntax

inspect file-fixed-length enable

undo inspect file-fixed-length enable

Default

The file fixed length inspection is disabled and the file inspection length is not limited.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command can be executed only if the DPI engine inspection mode is user-defined mode.

The file fixed length inspection feature enables the DPI engine to inspect only a fixed length of file data instead of the entire file in each data stream.

With this feature configured, the DPI engine cannot identify the remaining file data that exceeds the defined fixed length, affecting the data filtering service.

Examples

Enable file fixed length inspection.

```
<Sysname> system-view
[Sysname] inspect file-fixed-length enable
```

Related commands

inspect coverage user-defined

inspect file-fixed-length

inspect file-uncompr-len

Use **inspect file-uncompr-len** to set the maximum data size that can be decompressed in a file.

Use **undo inspect file-uncompr-len** to restore the default.

Syntax

inspect file-uncompr-len *max-size*

undo inspect file-uncompr-len

Default

A maximum of 100 MB data can be decompressed in a file.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

max-size: Specifies the maximum data size in the range of 1 to 200 MB.

Usage guidelines

The device can decompress .zip files for file data inspection. This command specifies the maximum data size that can be decompressed in a file. The remaining file data will be ignored.

Set an appropriate maximum data size for file decompression. A large data size might make the device get stuck in decompressing large files and the device forwarding performance might be affected. A small data size will affect the accuracy of the file inspection results for DPI services (such as anti-virus and data filtering).

Examples

Set the maximum data size that can be decompressed in a file to 150 MB.

```
<Sysname> system-view
[Sysname] inspect file-uncompr-len 150
```

inspect logging parameter-profile

Use **inspect logging parameter-profile** to create a logging parameter profile and enter its view, or enter the view of an existing logging parameter profile.

Use **undo inspect logging parameter-profile** to delete a logging parameter profile.

Syntax

inspect logging parameter-profile *parameter-name*

undo inspect logging parameter-profile *parameter-name*

Default

No logging parameter profiles exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

profile-name: Specifies a logging parameter profile name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

In logging parameter profile view, you can set parameters for the logging action, such as the log output method.

Examples

Create a logging parameter profile named **log1** and enter its view.

```
<Sysname> system-view
[Sysname] inspect logging parameter-profile log1
[Sysname-inspect-logging-log1]
```

Related commands

log

inspect md5-fixed-length

Use **inspect md5-fixed-length** to set the fixed file length for MD5 inspection.

Use **undo inspect md5-fixed-length** to restore the default.

Syntax

inspect md5-fixed-length { **email** | **ftp** | **http** | **nfs** | **smb** } * *length*

undo inspect md5-fixed-length

Default

The fixed length of FTP, HTTP, SMB, NFS, and email files for MD5 inspection is 2048 Kilobytes.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

email: Specifies email protocols, including SMTP, POP3, and IMAP.

ftp: Specifies the FTP protocol.

http: Specifies the HTTP protocol.

nfs: Specifies the NFS protocol.

smb: Specifies the SMB protocol.

length: Specifies the fixed file length for MD5 inspection, in the range of 1 to 5120 Kilobytes. Make sure the fixed file length for MD5 inspection is longer than the fixed length for stream inspection.

Usage guidelines

This command can be executed only if the DPI engine inspection mode is user-defined mode.

For some DPI services, such as anti-virus services, the DPI engine inspects the packet signatures and MD5 values at the same time. After reaching the fixed length for stream inspection, the DPI engine will stop the packet signature inspection but will not stop the MD5 inspection until the fixed MD5 inspection length is reached.

The increase of the file length for MD5 inspection will reduce the device performance but improve the success rate of the MD5 inspection. The decrease of the file length for MD5 inspection will improve the device performance but reduce the success rate of the MD5 inspection.

Examples

Set the fixed lengths of FTP and HTTP files for MD5 inspection to 1024 Kilobytes and 512 Kilobytes, respectively.

```
<Sysname> system-view
[Sysname] inspect md5-fixed-length ftp 1024 http 512
```

Related commands

inspect coverage user-defined

inspect md5-fixed-length enable

inspect md5-fixed-length enable

Use **inspect md5-fixed-length enable** to enable MD5 fixed-length file inspection.

Use **undo inspect md5-fixed-length enable** to disable MD5 fixed-length file inspection.

Syntax

inspect md5-fixed-length enable

undo inspect md5-fixed-length enable

Default

MD5 fixed-length file inspection is enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command can be executed only if the DPI engine inspection mode is user-defined mode.

The MD5 fixed-length file inspection feature enables the DPI engine to calculate the MD5 values of files of fixed lengths. When a file length reaches the defined file length for MD5 inspection, the DPI engine stops calculating the MD5 value for the file.

Examples

Disable MD5 fixed-length file inspection.

```
<Sysname> system-view
[Sysname] undo inspect md5-fixed-length enable
```

Related commands

inspect coverage user-defined

inspect md5-fixed-length

inspect md5-verify all-files

Use **inspect md5-verify all-files** to enable MD5 hash-based virus inspection for all files.

Use **undo inspect md5-verify all-files** to restore the default.

Syntax

inspect md5-verify all-files

undo inspect md5-verify all-files

Default

The DPI engine performs MD5 hash-based virus inspection only for executable files, office files, and compressed files.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This feature enables the DPI engine to generate MD5 hashes for all files and to compare the generated MD5 hashes with the MD5 rules in the signature library. If the MD5 hash generated for a file matches an MD5 rule in the signature library, the file is considered to contain viruses.

This feature might degrade the processing performance of other services. Enable it only when necessary.

Examples

Enable MD5 hash-based virus inspection for all files.

```
<Sysname> system-view
[Sysname] inspect md5-verify all-files
```

Related commands

display inspect md5-verify configuration

inspect optimization disable

Use **inspect optimization disable** to disable a DPI engine optimization feature.

Use **undo inspect optimization disable** to enable a DPI engine optimization feature.

Syntax

inspect optimization [**chunk** | **no-acsignature** | **raw** | **uncompress** | **url-normalization**] **disable**

undo inspect optimization [**chunk** | **no-acsignature** | **raw** | **uncompress** | **url-normalization**] **disable**

Default

All DPI engine optimization features are enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

chunk: Specifies the chunked packet decoding feature.

no-acsignature: Specifies the inspection rules that do not contain AC patterns.

raw: Specifies the application layer payload decoding feature.

uncompress: Specifies the HTTP body decompression feature.

url-normalization: Specifies the HTTP URL normalization feature.

Usage guidelines

If you do not specify any parameter, this command applies to all DPI engine optimization features.

DPI engine supports the following optimization features:

- **Chunked packet decoding**—Chunk is a packet transfer mechanism of the HTTP body. DPI engine must decode a chunked HTTP body before it inspects the HTTP body. When the device throughput is too low to ensure basic communication, you can disable DPI engine from decoding chunked packets to improve the device performance. However, when chunked packet decoding is disabled, the DPI engine cannot identify some attacks that exploit security vulnerabilities.
- **Inspection rules that do not contain AC patterns**—Inspection rules that do not contain AC patterns contain only options. These rules match packets by fields such as port numbers and error codes rather than by character strings. These rules by default are enabled to improve the inspection accuracy. However, when the device throughput is too low to ensure basic communication, you can disable these rules to improve the device performance.
- **Application layer payload decoding**—For application layer protocols featuring encoding and decoding, such as HTTP, SMTP, POP3, and IMAP4, DPI engine must decode the payload before inspection. When the device throughput is too low to ensure basic communication, you can disable DPI engine from decoding application layer payloads to improve the device performance. However, disabling application layer payload decoding affects the inspection accuracy of the DPI engine. For example, the DPI engine might fail to applications that need to be decoded, such as DingTalk. Additionally, the auditing function based on these applications cannot take effect.
- **HTTP body decompression**—If the HTTP body field is compressed, DPI engine must decompress the body before inspection. When the device throughput is too low to ensure basic communication, you can disable DPI engine from decompressing the HTTP body field to improve the device performance. However, when HTTP body decompression is disabled, the DPI engine cannot identify some attacks that exploit security vulnerabilities.
- **HTTP URL normalization**—HTTP URL normalization is the process by which the absolute path in a URL is normalized and special URLs are standardized and checked. For example, the absolute path **test/dpi/../index.html** is normalized as **test/index.html**. When the device throughput is too low to ensure basic communication, you can disable DPI engine from normalizing HTTP URLs to improve the device performance. However, when HTTP URL normalization is disabled, the DPI engine cannot identify some attacks that exploit security vulnerabilities.

Examples

Disable all DPI engine optimization features.

```
<Sysname> system-view
[Sysname] inspect all disable
```

inspect packet maximum

Use **inspect packet maximum** to set the maximum number of payload-carrying packets to be inspected per data flow.

Use **undo inspect packet** to restore the default.

Syntax

inspect packet maximum *max-number*

undo inspect packet

Default

The DPI engine can inspect a maximum of 32 payload-carrying packets per data flow.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

max-number: Specifies the maximum number of payload-carrying packets to be inspected per data flow, in the range of 1 to 254.

Usage guidelines

If DPI engine finds that the first payload-carrying packet of a data flow does not match any inspection rule, it continues to inspect the next payload-carrying packet, and so on. If DPI engine has inspected the maximum number of payload-carrying packets but finds no matching inspection rule, it determines the flow does not match any rule and allows the flow to pass.

The more payload-carrying packets DPI engine inspects, the more likely that DPI engine identifies the application information and the more accurate the DPI engine inspection.

Typically, the default setting is sufficient for most scenarios. You can adjust the setting according to your network condition.

- If the device throughput is high, increase the maximum number value.
- If the device throughput is low, decrease the maximum number value.

Examples

Allow the DPI engine to inspect a maximum of 16 payload-carrying packets per data flow for application identification.

```
<Sysname> system-view
[Sysname] inspect packet maximum 16
```

inspect real-ip detect-field priority

Use **inspect real-ip detect-field priority** to set the priority of an inspected field for real source IP inspection.

Use **undo inspect real-ip detect-field priority** to cancel the priority of an inspected field for real source IP inspection.

Syntax

inspect real-ip detect-field { **cdn-src-ip** | **tcp-option** | **x-real-ip** | **xff** } **priority** *priority-value*

undo inspect real-ip detect-field { **cdn-src-ip** | **tcp-option** | **x-real-ip** | **xff** } **priority**

Default

No priority is specified for any inspected field in the real source IP inspection, and all inspected fields use priority value 0. The device inspects the fields in the order of the **xff**, **cdn-src-ip**, **x-real-ip**, and **tcp-option** fields.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

cdn-src-ip: Specifies the Cdn-Src-Ip field in the HTTP header.

tcp-option: Specifies the TCP Options field.

xff: Specifies the X-Forwarded-For field in the HTTP header.

x-real-ip: Specifies the X-Real-IP field in the HTTP header.

priority *priority-value*: Specifies a priority for an inspected field, in the range of 1 to 100. The larger the priority value, the higher the priority. Each inspected filed must have a unique priority value.

Usage guidelines

With real source IP inspection enabled, the device obtains the real source IP address of the client by inspecting multiple fields in the packets by default.

When multiple IP addresses are detected, the devices uses the IP address obtained from the field with the highest priority as the final real source IP address.

Examples

Set the priority to 10 for the X-Forwarded-For field.

```
<Sysname> system-view
[Sysname] inspect real-ip detect-field xff priority 10
```

inspect real-ip detect-field tcp-option

Use **inspect real-ip detect-field tcp-option** to configure real source IP inspection for the TCP Options field.

Use **undo inspect real-ip detect-field tcp-option** to restore the default.

Syntax

inspect real-ip detect-field tcp-option hex *hex-vector* [**offset** *offset-value*] [**depth** *depth-value*] [**ip-offset** *ip-offset-value*]

undo inspect real-ip detect-field tcp-option

Default

Real source IP inspection is not configured for the TCP Options field, and the device does not obtain the real source IP address from the TCP Options field.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

hex *hex-vector*: Specifies a case-sensitive hexadecimal string of 6 to 66 characters. Specify an even number of characters, and enclose the string with two vertical bars (|), for example |1234f5b6|.

offset *offset-value*: Specifies an offset in bytes after which the hexadecimal string lookup starts, in the range of 0 to 32. If you do not specify this option, the lookup starts from the beginning of the TCP Options field.

depth *depth-value*: Specifies the number of bytes to locate the hexadecimal string, in the range of 2 to 40. If you do not specify this option, the device searches the whole TCP Options field for the hexadecimal string.

ip-offset *ip-offset-value*: Specifies an offset in bytes after which the real source IP address is, in the range of 0 to 32. If you do not specify this option, the data after the hexadecimal string is the real source IP address.

Usage guidelines

To enable the device to locate the real source IP address in the TCP Option field, you must first define a hexadecimal string. If no hexadecimal string is found, the device will stop searching the TCP Options field for the real IP address.

Examples

Configure the device to search bytes 3 to 12 for the hexadecimal string **|0102|** in the TCP Options field, and define that the real source IP address is 2 bytes away from the hexadecimal string.

```
<Sysname> system-view
[Sysname] inspect real-ip detect-field tcp-option hex |0102| offset 2 depth 10 ip-offset
2
```

inspect real-ip detect-field xff

Use **inspect real-ip detect-field xff** to configure real source IP address inspection for the X-Forwarded-For field.

Use **undo inspect real-ip detect-field xff** to restore the default.

Syntax

inspect real-ip detect-field xff { **head** | **tail** }

undo inspect real-ip detect-field xff

Default

The rightmost IP address in the X-Forwarded-For field is the real source IP address.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

head: Specifies the first IP address in the X-Forwarded-For field as the real source IP address.

tail: Specifies the last IP address in the X-Forwarded-For field as the real source IP address.

Usage guidelines

When a client connects to a Web server through an HTTP proxy, the HTTP header might contain the X-Forwarded-For field that carries multiple IP addresses. The standard syntax of the X-Forwarded-For field is <client>, <proxy1>, <proxy2>,…<proxyn>. If a request goes through multiple proxies, the IP addresses of each successive proxy are listed. The rightmost IP address is the IP address of the most recent proxy and the leftmost IP address is the IP address of the originating client.

Examples

Specify the leftmost IP address in the X-Forwarded-For field as the real source IP address.

```
<Sysname> system-view
[Sysname] inspect real-ip detect-field xff head
```

Related commands

inspect real-ip enable

inspect real-ip enable

Use **inspect real-ip enable** to enable real source IP inspection.

Use **undo inspect real-ip enable** to disable real source IP inspection.

Syntax

inspect real-ip enable

undo inspect real-ip enable

Default

Real source IP inspection is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

When a client connects to a Web server through HTTP proxies, the source IP address of the request packet will change. To identify the source IP attacks accurately, you can enable this feature to obtain the real source IP address from the corresponding fields in the request.

Examples

Enable real source IP inspection.

```
<Sysname> system-view
[Sysname] inspect real-ip enable
```

inspect real-ip record-filename nfs maximum

Use **inspect record-filename nfs maximum** to set the maximum number of NFS file names recorded.

Use **undo inspect record-filename nfs maximum** to restore the default.

Syntax

inspect record-filename nfs maximum *max-number*

undo inspect record-filename nfs maximum

Default

The maximum number of NFS file names recorded is calculated according to the actual memory size of the device.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

max-number: Specifies the maximum number of NFS file names recorded, in the range of 0 to 4294967295. The value 0 indicates that the number of NFS file names recorded is not limited.

Usage guidelines

The DPI engine records file names during file detection for users to obtain file information in logs. The record process occupies memory resources. The more files detected, the more memory resources occupied. In an environment using NFS to transfer a large number of files, Execute this command to limit the memory resources consumed by recording file names.

In scenarios requiring high performance, you can set a small limit to reduce memory consumption. In scenarios not requiring high performance, you can set a great limit to enable users to obtain more file information.

Examples

Set the maximum number of NFS file names recorded to 110000.

```
<Sysname> system-view
[Sysname] inspect record-filename nfs maximum 110000
```

inspect redirect parameter-profile

Use **inspect redirect parameter-profile** to create a redirect parameter profile and enter its view, or enter the view of an existing redirect parameter profile.

Use **undo inspect redirect parameter-profile** to delete a redirect parameter profile.

Syntax

inspect redirect parameter-profile *parameter-name*

undo inspect redirect parameter-profile *parameter-name*

Default

No redirect parameter profiles exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

parameter-name: Specifies a redirect parameter profile name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

In redirect parameter profile view, you can set parameters for the redirect action, such as the URL to which packets are redirected.

Examples

Create a redirect parameter profile named **r1** and enter its view.

```
<Sysname> system-view
```

```
[Sysname] inspect redirect parameter-profile r1
[Sysname-inspect-redirect-r1]
```

inspect signature auto-update proxy

Use **inspect signature auto-update proxy** to specify the proxy server used by DPI services for online signature update.

Use **undo inspect signature auto-update proxy** to restore the default.

Syntax

inspect signature auto-update proxy { **domain** *domain-name* | **ip** *ip-address* } [**port** *port-number*] [**user** *user-name* **password** { **cipher** | **simple** } *string*]

undo inspect signature auto-update proxy

Default

The proxy server used by DPI services for online signature update is not specified.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

domain *domain-name*: Specifies a proxy server by its domain name, a case-insensitive string of 3 to 63 characters.

ip *ip-address*: Specifies a proxy server by its IPv4 address.

port *port-number*: Specifies the port number used by the proxy server. The value range is 1 to 65535, and the default is 80.

user *user-name*: Specifies the username used to log in to the proxy server. The username is a case-insensitive string of 1 to 31 characters.

password: Specifies the password used to log in to the proxy server.

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password in plaintext form will be stored in encrypted form.

string: Specifies the password string. Its plaintext form is a case-sensitive string of 1 to 31 characters. Its encrypted form is a case-sensitive string of 1 to 73 characters.

Usage guidelines

The device must access the company's website for online signature update of DPI services such as URL filtering. If direct connectivity is not available, the device can access the company's website through the specified proxy server. For more information about online signature update, see *DPI Configuration Guide*.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify server **http://www.abc.com/** on port 8888 as the proxy server and set the login username and password to **admin**.

```
<Sysname> system-view
[Sysname] inspect signature auto-update proxy domain www.abc.com port 8888 user admin
password simple admin
```

inspect source-port-identify enable

Use **inspect source-port-identify enable** to enable source port-based application identification.

Use **undo inspect source-port-identify enable** to disable source port-based application identification.

Syntax

inspect source-port-identify enable

undo inspect source-port-identify enable

Default

Source port-based application identification is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

You can use this feature to identify traffic of applications that use fixed source ports when the following conditions are true:

- The types of traffic transmitted over networks are relatively unvaried and use fixed source ports.
- Destination port-based application identification or signature-based traffic content identification is not supported.

The application identification results produced by this feature might not be accurate. Configure this feature according to your live network as a best practice.

Examples

Enable source port-based application identification.

```
<sysname> system-view
[sysname] inspect source-port-identify enable
```

inspect stream-fixed-length

Use **inspect stream-fixed-length** to set the fixed length for stream inspection.

Use **undo inspect stream-fixed-length** to restore the default.

Syntax

inspect stream-fixed-length { **email** | **ftp** | **http** | **nfs** | **smb** } * *length*

undo inspect stream-fixed-length

Default

The fixed length is 32 Kilobytes for FTP, HTTP, NFS, SMB, and email streams.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

email: Specifies email protocols, including SMTP, POP3 and IMAP.

ftp: Specifies the FTP protocol.

http: Specifies the HTTP protocol.

nfs: Specifies the NFS protocol.

smb: Specifies the SMB protocol.

length: Specifies the fixed length in the range of 1 to 2048 Kilobytes.

Usage guidelines

This command can be executed only if the DPI engine inspection mode is user-defined mode.

The larger the inspection length value, the lower the device throughput, and the higher the packet inspection accuracy.

Examples

Set the fixed length to 35 Kilobytes for inspecting each FTP stream and 40 Kilobytes for inspecting each HTTP stream.

```
<Sysname> system-view
[Sysname] inspect stream-fixed-length ftp 35 http 40
```

Related commands

inspect coverage user-defined

inspect cpu-threshold disable

inspect stream-fixed-length disable

inspect stream-fixed-length disable

Use **inspect stream-fixed-length disable** to disable stream fixed length inspection.

Use **undo inspect stream-fixed-length disable** to enable stream fixed length inspection.

Syntax

inspect stream-fixed-length disable

undo inspect stream-fixed-length disable

Default

The stream fixed length inspection feature is enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command can be executed only if the DPI engine inspection mode is user-defined mode.

The stream fixed length inspection feature enables the DPI engine to inspect only a fixed length of data for a stream instead of the whole packet data in a stream.

Examples

Disable stream fixed length inspection.

```
<Sysname> system-view
[Sysname] inspect stream-fixed-length disable
```

Related commands

`inspect coverage user-defined`

`inspect cpu-threshold disable`

`inspect stream-fixed-length`

inspect tcp-reassemble enable

Use **`inspect tcp-reassemble enable`** to enable the TCP segment reassembly feature.

Use **`undo inspect tcp-reassemble enable`** to disable the TCP segment reassembly feature.

Syntax

`inspect tcp-reassemble enable`

`undo inspect tcp-reassemble enable`

Default

The TCP segment reassembly feature is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

DPI engine inspection might fail if TCP segments arrive at the engine out of order. For example, the DPI engine searches for the keywords **this is a secret**. If the TCP segment containing **`a secret`** arrives before the one containing **`this is`**, the inspection fails.

The TCP segment reassembly feature enables the device to cache out-of-order TCP segments of the same TCP flow and reassembles the segments before submitting them to the DPI engine for inspection. This helps improve the DPI engine inspection accuracy.

The segment reassembly fails due to missing segments when the number of cached TCP segments of a flow reaches the limit. In this case, the device submits the cached segments without reassembling them and all subsequent segments of the flow to the DPI engine. This helps reduces degradation of the device performance.

Examples

Enable the TCP segment reassembly feature.

```
<Sysname> system-view
[Sysname] inspect tcp-reassemble enable
```

Related commands

inspect tcp-reassemble max-segment

inspect tcp-reassemble max-segment

Use **inspect tcp-reassemble max-segment** to set the maximum number of TCP segments that can be cached per TCP flow.

Use **undo inspect tcp-reassemble max-segment** to restore the default.

Syntax

inspect tcp-reassemble max-segment *max-number*

undo inspect tcp-reassemble max-segment

Default

A maximum of 10 TCP segments can be cached for reassembly per TCP flow.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

max-number: Specifies the maximum number in the range of 10 to 50.

Usage guidelines

Set the limit for the number of TCP segments that can be cached per flow according to your network requirements. The higher the limit, the higher the inspection accuracy, and the lower the device performance.

This command takes effect only when the TCP segment reassembly feature is enabled.

Examples

Allow the device to cache a maximum of 20 TCP segments for each TCP flow.

```
<Sysname> system-view
[Sysname] inspect tcp-reassemble max-segment 20
```

Related commands

inspect tcp-reassemble enable

inspect uncompress maximum

Use **inspect uncompress maximum** to set the maximum number of file decompression operations.

Use **undo inspect uncompress maximum** to restore the default.

Syntax

inspect uncompress maximum *max-number*

undo inspect uncompress maximum

Default

The maximum number of file decompression operations is calculated according to the actual memory size of the device.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

max-number: Specifies the maximum number of file decompression operations, in the range of 0 to 4294967295. The value 0 indicates that the number of file decompression operations is not limited.

Usage guidelines

The DPI engine consumes memory resources each time it performs a file decompression operation. A large number of file decompression operations might consume a large number of memory resources. Execute this command to limit the memory resources consumed by file decompression operations.

This command is supported only on the default context. For more information about contexts, see *Virtual Technologies Configuration Guide*.

Examples

Set the maximum number of file decompression operations to 120000.

```
<Sysname> system-view
[Sysname] inspect uncompress maximum 120000
```

inspect warning parameter-profile

Use **inspect warning parameter-profile** to create a warning parameter profile and enter its view, or enter the view of an existing warning parameter profile.

Use **undo inspect warning parameter-profile** to delete a warning parameter profile.

Syntax

inspect warning parameter-profile *profile-name*

undo inspect warning parameter-profile *profile-name*

Default

No warning parameter profiles exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

profile-name: Specifies a warning parameter profile name, a case-insensitive string of 1 to 63 characters. Valid characters are letters, digits, underscores (_).

Usage guidelines

After you create a warning parameter profile, you can import a user-defined alarm message from a file.

Examples

Create a warning parameter profile named **w1** and enter its view.

```
<Sysname> system-view
[Sysname] inspect warning parameter-profile w1
[Sysname-inspect-warning-w1]
```

Related commands

`import block warning-file`

`reset block warning-file`

`warning parameter-profile`

log

Use **`log`** to specify the log storage method.

Use **`undo log`** to cancel the specified log storage method.

Syntax

`log` { **`email`** | **`syslog`** }

`undo log` { **`email`** | **`syslog`** }

Default

Logs are exported to the information center.

Views

Logging parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

`email`: Emails the logs to a receiver.

`syslog`: Exports the logs to the information center.

Examples

Configure the device to export logs to the information center in logging parameter profile **log1**.

```
<Sysname> system-view
[Sysname] inspect logging parameter-profile log1
[Sysname-inspect-logging-log1] log syslog
```

Related commands

`inspect logging parameter-profile`

log language

Use **`log language`** to set the language for IPS log output to Chinese.

Use **undo log language** to restore the default.

Syntax

log language chinese

undo log language chinese

Default

IPS logs are output in English.

Views

Logging parameter profile view

Predefined user roles

network-admin

context-admin

Usage guidelines

After you execute this command, only the attack name field of the IPS logs supports displaying in Chinese. For more information about IPS logs, see "IPS commands."

Examples

Set the language for IPS log output to Chinese.

```
<Sysname> system-view
[Sysname] inspect logging parameter-profile log1
[Sysname-inspect-log-para-log1] log language chinese
```

Related commands

inspect logging parameter-profile

password

Use **password** to specify the password for logging in to the email server.

Use **undo password** to restore the default.

Syntax

password { **cipher** | **simple** } *string*

undo password

Default

No password is specified for logging in to the email server.

Views

Email parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

pwd-string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 63 characters. Its encrypted form is a case-sensitive string of 1 to 117 characters.

Usage guidelines

If you execute this command multiple times for the same email parameter profile, the most recent configuration takes effect.

Examples

Specify **abc123** as the plaintext password for logging in to the email server.

```
<Sysname> system-view
[Sysname] inspect email parameter-profile c1
[Sysname-inspect-email-c1] password simple abc123
```

Related commands

authentication enable

receiver

Use **receiver** to specify the email receiver address.

Use **undo receiver** to restore the default.

Syntax

receiver *address-string*

undo receiver

Default

No email receiver address is specified.

Views

Email parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

address-string: Specifies the address of the email receiver, a case-sensitive string of 3 to 502 characters.

Usage guidelines

You can specify multiple semicolon-separated email receiver addresses in one command.

Examples

Specify the email receiver addresses **123@abc.com** and **nnn@abc.com**.

```
<Sysname> system-view
[Sysname] inspect email parameter-profile c1
[Sysname-inspect-email-c1] receiver 123@abc.com;nnn@abc.com
```

redirect-url

Use **redirect-url** to specify the URL to which packets are redirected.

Use **undo redirect-url** to restore the default.

Syntax

redirect-url *url-string*

undo redirect-url

Default

No URL is specified for packet redirecting.

Views

Redirect parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

url-string: Specifies the URL, a case-sensitive string of 9 to 63 characters. The URL must start with **http://** or **https://**, for example, **http://www.example.com**.

Usage guidelines

After you specify a URL, matching packets will be redirected to the webpage that the URL identifies.

Examples

Specify **http://www.abc.com/upload** as the URL for packet redirecting.

```
<Sysname> system-view
[Sysname] inspect redirect parameter-profile r1
[Sysname-inspect-redirect-r1] redirect-url http://www.abc.com/upload
```

Related commands

inspect redirect parameter-profile

reset block warning-file

Use **reset block warning-file** to restore the default alarm message.

Syntax

reset block warning-file

Views

Warning parameter profile view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command allows you to clear the user-defined alarm message and restore the default message.

Examples

Restore the default alarm message in the warning parameter profile **w1**.

```
<Sysname> system-view
[Sysname] inspect warning parameter-profile w1
[Sysname-inspect-warning-w1] reset block warning-file
```

Related commands

import warning-file

secure-authentication enable

Use **secure-authentication enable** to enable the secure password transmission feature.

Use **undo secure-authentication enable** to disable the secure password transmission feature.

Syntax

secure-authentication enable

undo secure-authentication enable

Default

The secure password transmission feature is disabled.

Views

Email parameter profile view

Predefined user roles

network-admin

context-admin

Usage guidelines

After the secure password transmission feature is enabled, a security channel is established between the device and the email server to transmit the password for email server login.

Examples

Enable the secure password transmission feature.

```
<Sysname> system-view
[Sysname] inspect email parameter-profile c1
[Sysname-inspect-email-c1] secure-authentication enable
```

Related commands

authentication enable

sender

Use **sender** to specify the email sender address.

Use **undo sender** to restore the default.

Syntax

sender *address-string*

undo sender

Default

No email sender address is specified.

Views

Email parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

address-string: Specifies the address of the email sender, a case-sensitive string of 3 to 63 characters.

Usage guidelines

The email sender address is the source address that the device uses to send emails to destinations.

Examples

Specify the email sender address **abc@123.com**.

```
<Sysname> system-view
[Sysname] inspect email parameter-profile c1
[Sysname-inspect-email-c1] sender abc@123.com
```

username

Use **username** to specify the username for logging in to the email server.

Use **undo username** to restore the default.

Syntax

username *name-string*

undo username

Default

No username is specified for logging in to the email server.

Views

Email parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

name-string: Specifies the username, a case-sensitive string of 1 to 63 characters.

Usage guidelines

If you execute this command multiple times for the same email parameter profile, the most recent configuration takes effect.

Examples

Specify **han** as the username for logging in to the email server.

```
<Sysname> system-view
[Sysname] inspect email parameter-profile c1
[Sysname-inspect-email-c1] username han
```

Related commands

authentication enable

Contents

IPS commands

action (IPS policy view)

Use **action** to configure the action criterion for IPS signature filtering in an IPS policy.

Use **undo action** to restore the default.

Syntax

action { **block-source** | **drop** | **permit** | **reset** } *

undo action

Default

The action attribute is not used for IPS signature filtering.

Views

IPS policy view

Predefined user roles

network-admin

context-admin

Parameters

block-source: Specifies the block source action.

drop: Specifies the drop action.

permit: Specifies the permit action.

reset: Specifies the reset action.

Usage guidelines

This command filters the IPS signatures that an IPS policy uses based on the actions associated with the signatures.

You can specify multiple actions in an action criterion. The IPS policy uses an IPS signature if the signature is associated with any of the specified actions.

If you execute this command in an IPS policy multiple times, the most recent configuration takes effect.

Examples

Configure IPS policy **test** to use IPS signatures associated with the drop or reset action.

```
<Sysname> system-view
[Sysname] ips policy test
[Sysname-ips-policy-test] action drop reset
```

action (IPS signature view)

Use **action** to configure the actions for a user-defined IPS signature.

Use **undo action** to restore the default.

Syntax

action { **block-source** | **drop** | **permit** | **reset** } [**capture** | **logging**] *

undo action

Default

The action for the user-defined IPS signature is **permit**.

Views

User-defined IPS signature view

Predefined user roles

network-admin

context-admin

Parameters

block-source: Specifies the block source action.

drop: Specifies the drop action.

permit: Specifies the permit action.

reset: Specifies the reset action.

logging: Specifies the logging action.

capture: Specifies the capture action.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the drop action for user-defined IPS signature **mysignature**.

```
<Sysname> system-view
[Sysname] ips signature user-defined name mysignature
[Sysname-ips-signature-mysignature] action drop
```

attack-category

Use **attack-category** to specify an attack category criterion to filter IPS signatures in an IPS policy.

Use **undo attack-category** to delete an attack category criterion.

Syntax

attack-category { *category* [*subcategory*] | **all** }

undo attack-category { *category* [*subcategory* | **all**] }

Default

The attack category attribute is not used for IPS signature filtering.

Views

IPS policy view

Predefined user roles

network-admin

context-admin

Parameters

category-name: Specifies an attack category.

subcategory: Specifies a subcategory of the attack category. If you do not specify a subcategory, this command matches any IPS signature with a subcategory of the specified attack category.

all: Specifies all attack categories.

Usage guidelines

This command filters the IPS signatures that an IPS policy uses based on the attack category attribute of the signatures.

You can execute this command multiple times to specify multiple attack category criteria in an IPS policy. The IPS policy uses an IPS signature if the signature matches any of the configured attack category criteria.

Examples

Configure IPS policy **test** to use IPS signatures with the **SQLInjection** attack subcategory of the **Vulnerability** attack category.

```
<Sysname> system-view
[Sysname] ips policy test
[Sysname-ips-policy-test] attack-category Vulnerability SQLInjection
```

description (IPS whitelist entry view)

Use **description** to configure the description for an IPS whitelist entry.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

An IPS whitelist entry does not have any description.

Views

IPS whitelist entry view

Predefined user roles

network-admin

context-admin

Parameters

text: Specifies a description, a case-insensitive string of 1 to 255 characters. The description can contain spaces.

Usage guidelines

A description allows easy identification of an IPS whitelist entry.

Examples

Specify the description as **News information** for IPS whitelist entry 1.

```
<Sysname> system-view
[Sysname] ips whitelist 1
[Sysname-ips-whitelist-1] description News information
```

description (user-defined IPS signature view)

Use **description** to configure the description for a user-defined IPS signature.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

A user-defined IPS signature does not have any description.

Views

User-defined IPS signature view

Predefined user roles

network-admin

context-admin

Parameters

text: Specifies a description, a case-insensitive string of 1 to 127 characters.

Usage guidelines

A description allows easy identification of a user-defined IPS signature.

Examples

Specify the description as **mydescription** for user-defined IPS signature **mysignature**.

```
<Sysname> system-view
[Sysname] ips signature user-defined name mysignature
[Sysname-ips-signature-mysignature] description mydescription
```

destination-address

Use **destination-address** to specify a destination IP address filtering criterion in a user-defined signature rule.

Use **undo destination-address** to remove a destination IP address filtering criterion from a user-defined signature rule.

Syntax

destination-address ip *ip-address*

undo destination-address

Default

No destination IP address is specified as the filtering criterion in a user-defined signature rule.

Views

User-defined IPS signature rule view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies an IPv4 address. It is used to match the packet destination IPv4 address.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

In rule 1 of user-defined IPS signature **mysignature**, specify the keyword type as the match pattern type and specify destination IP address 10.1.1.1 as a filtering criterion.

```
<Sysname> system-view
[Sysname] ips signature user-defined name mysignature
[Sysname-ips-signature-mysignature] rule 1 l4-protocol tcp l5-protocol http pattern-type keyword
[Sysname-ips-signature-mysignature-rule-1] destination-address ip 10.1.1.1
```

destination-port

Use **destination-port** to specify a destination port filtering criterion in a user-defined signature rule.

Use **undo destination-port** to restore the default.

Syntax

destination-port *start-port* [**to** *end-port*]

undo destination-port

Default

No destination ports are specified as the filtering criteria in a user-defined signature rule.

Views

User-defined IPS signature rule view

Predefined user roles

network-admin

context-admin

Parameters

start-port: Specifies the start port number of a destination port range, in the range of 1 to 65535.

to *end-port*: Specifies the end port number of a destination port range, in the range of 1 to 65535. If you do not specify this option, only the start port number is specified.

Usage guidelines

The port numbers are used to match the destination port numbers of the specified transport layer protocol.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

In rule 1 of user-defined IPS signature **mysignature**, specify the keyword type as the match pattern type and specify the destination port range as 1 to 3550.

```
<Sysname> system-view
[Sysname] ips signature user-defined name mysignature
[Sysname-ips-signature-mysignature] rule 1 l4-protocol tcp l5-protocol http pattern-type keyword
```

```
[Sysname-ips-signature-mysignature-rule-1] destination-port 1 to 3550
```

detection-integer

Use **detection-integer** to configure an integer detection item in a user-defined signature rule.

Use **undo detection-integer** to remove an integer detection item from a user-defined signature rule.

Syntax

detection-integer field *field-name* **match-type** { **eq** | **gt** | **gt-eq** | **lt** | **lt-eq** | **nequ** } *number*

undo detection-integer

Default

No integer detection items are configured in a user-defined signature rule.

Views

User-defined IPS signature rule view

Predefined user roles

network-admin

context-admin

Parameters

field-name: Specifies a protocol field by its name, a case-insensitive string. To view the names of supported protocol fields, enter a question mark (?) after the **field** keyword.

match-type { **eq** | **gt** | **gt-eq** | **lt** | **lt-eq** | **nequ** } *number*: Specifies a match operator in the detection item:

- **eq**: Matches numbers that are equal to the specified number.
- **gt**: Matches numbers that are greater than the specified number.
- **gt-eq**: Matches numbers that are greater than or equal to the specified number.
- **lt**: Matches numbers that are less than the specified number.
- **lt-eq**: Matches numbers that are less than or equal to the specified number.
- **nequ**: Matches numbers that are not equal to the specified number.

number: Specifies a number in the range of 1 to 4294967295.

Usage guidelines

A user-defined IPS signature rule can contain multiple detection items. A packet matches a rule only when the packet matches all detection items in the rule. The match order of the detection items is their configuration order. To avoid detection errors, configure the detection items based on the sequence of the protocol fields in the protocol.

Examples

In user-defined IPS signature **mysignature**, create rule 1 for UDP and SIP protocols and specify the integer match pattern type. Create a detection item in the rule to match packets whose **SIP.Content-Length** field value is 50.

```
<Sysname> system-view
[Sysname] ips signature user-defined name mysignature
[Sysname-ips-signature-mysignature] rule 1 l4-protocol UDP l5-protocol SIP pattern-type
integer
```

```
[Sysname-ips-signature-mysignature-rule-1] detection-integer field SIP.Content-Length
match-type eq 50
```

detection-keyword

Use **detection-keyword** to configure a keyword detection item in a user-defined signature rule.

Use **undo detection-keyword** to remove a keyword detection item from a user-defined signature rule.

Syntax

detection-keyword *detection-id* **field** *field-name* **match-type** { **exclude** | **include** } { **hex** *hex-string* | **regex** *regex-pattern* | **text** *text-string* } [**offset** *offset-value* [**depth** *depth-value*] | **relative-offset** *relative-offset-value* [**relative-depth** *relative-depth-value*]]

undo detection-keyword *detection-id*

Default

No keyword detection items are configured in a user-defined signature rule.

Views

User-defined IPS signature rule view

Predefined user roles

network-admin

context-admin

Parameters

detection-id: Specifies a detection item ID, in the range of 1 to 10.

field *field-name*: Specifies a protocol field by its name, in a case-insensitive string. To view the names of supported protocol fields, enter a question mark (?) after the **field** keyword.

match-type { **exclude** | **include** }: Specifies a match operator in the detection item:

- **include**: Matches contents that include the specified string.
- **exclude**: Matches contents that do not include the specified string.

hex *hex-string*: Specifies a case-sensitive hexadecimal string of 8 to 254 characters. Valid characters contain integers, and letters of A to F and a to f. An even number of characters are required, and enclose the characters with two vertical bars (|), for example |1234f5b6|.

regex *regex-pattern*: Specifies a case-sensitive regular expression string of 3 to 255 characters. The string can only start with letters, digits, and underscores (_), and must contain 3 consecutive non-wildcard characters.

text *text-string*: Specifies a case-insensitive text string of 3 to 255 characters.

offset *offset-value*: Specifies an offset in bytes after which the match operation starts, in the range of 1 to 65535. The offset starts from the beginning of the protocol field. If you do not specify the *offset-value* argument, the match operation starts from the beginning of the protocol field.

depth *depth-value*: Specifies the number of bytes to match, in the range of 3 to 65535. If you do not specify *depth-value* argument, the detection item detects the whole protocol field.

relative-offset *relative-offset-value*: Specifies an offset in bytes after which the match operation starts, in the range of –32767 to –1 and 1 to 32767. The offset starts from the end of the previous detection item. If the offset value is positive, it offsets backward. If the offset value is negative, it offsets forward.

relative-depth *relative-depth-value*: Specifies the number of bytes to be matched, in the range of 3 to 65535.

Usage guidelines

This command is available only after the detection trigger condition is configured.

A user-defined IPS signature rule can contain multiple detection items. A packet matches a rule only when the packet matches all detection items in the rule. The match order of detection items is their configuration order.

The detection item only inspects the specified protocol field range. To define the start and end positions for the match operation, use either the offset and depth, or the relative offset and relative depth.

To avoid detection errors, configure detection items based on the sequence of protocol fields in the HTTP protocol.

Examples

In user-defined IPS signature **mysignature**, create rule 1 for TCP and HTTP protocols and specify the keyword match pattern type. Create a detection item in the rule to match packets whose **http.host** field inlcudes **abc**. Specify the offset and depth as 10 bytes and 50 bytes, respectively.

```
<Sysname> system-view
[Sysname] ips signature user-defined name mysignature
[Sysname-ips-signature-mysignature] rule 1 l4-protocol tcp l5-protocol http pattern-type keyword
[Sysname-ips-signature-mysignature-rule-1] detection-keyword 1 field http.host match-type include text abc offset 10 depth 50
```

Related commands

trigger

direction

Use **direction** to specify the direction attribute in a user-defined signature.

Use **undo direction** to restore the default.

Syntax

direction { **any** | **to-client** | **to-server** }

undo direction

Default

The direction attribute of a user-defined IPS signature is **any**.

Views

User-defined IPS signature view

Predefined user roles

network-admin

context-admin

Parameters

any: Specifies both directions.

to-server: Specifies the client-to-server direction.

to-client: Specifies the server-to-client direction.

Usage guidelines

You cannot execute this command multiple times to change the direction attribute. To change the direction attribute, first execute **undo direction**. Use the **undo** command with caution because the **undo** command also deletes all rules in the signature.

Examples

In user-defined IPS signature **mysignature**, specify the server-to-client direction.

```
<Sysname> system-view
[Sysname] ips signature user-defined name mysignature
[Sysname-ips-signature-mysignature] direction to-client
```

display ips policy

Use **display ips policy** to display IPS policy information.

Syntax

display ips policy *policy-name*

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

policy-name: Specifies an IPS policy by its name, a case-insensitive string of 1 to 63 characters.

Examples

Display information about IPS policy **aa**.

```
<Sysname> display ips policy aa
Total signatures        :10929     failed:0
 Pre-defined  signatures:10925     failed:0
 Snort  signatures      :0         failed:0
 User-config  signatures:0         failed:0


Flag:
  B: Block-Source  D: Drop  P: Permit  Rs: Reset  Rd: Redirect  C: Capture  L: L
ogging
  Pre: predefined   Snort: Snort  User: user-config
Type RuleID    Target          SubTarget       Severity Direction Category
  SubCategory     Status  Action
Pre  1         OperationSystem LinuxUnix       High     Server    Vulnerability
  RemoteCodeExecu Enable  RsL
Pre  2         OperationSystem LinuxUnix       High     Server    Vulnerability
  MemoryCorruptio Enable  RsL
Pre  4         OfficeSoftware  MicrosoftOffice High     Any       Vulnerability
```

```
  Overflow        Enable  RsL
Pre  5         OfficeSoftware  MicrosoftOffice High     Any       Vulnerability
  MemoryCorruptio Enable  RsL
Pre  6         Browser         InternetExplore High     Any       Vulnerability
  MemoryCorruptio Enable  RsL
Pre  7         Browser         InternetExplore High     Any       Vulnerability
  MemoryCorruptio Enable  RsL
Pre  8         ApplicationSoft MediaPlayer     High     Any       Vulnerability
  RemoteCodeExecu Enable  RsL
Pre  9         ApplicationSoft Security        High     Server    Vulnerability
  Overflow        Enable  DL
Pre  10        Browser         InternetExplore High     Server    Vulnerability
  InsecureLibrary Enable  RsL
Pre  11        Browser         InternetExplore High     Any       InformationDis
c SensitiveInfo   Enable  RsL
Pre  12        OfficeSoftware  MicrosoftOffice Critical Any       Vulnerability
  RemoteCodeExecu Enable  RsL
Pre  13        OfficeSoftware  MicrosoftOffice High     Any       Vulnerability
  MemoryCorruptio Enable  RsL
Pre  14        ApplicationSoft IM              High     Server    Vulnerability
  InsecureLibrary Enable  RsL
Pre  15        Browser         InternetExplore High     Any       Vulnerability
  RemoteCodeExecu Enable  RsL
---- More ----
```

Table 1 Command output

Field	Description
Total signatures	Total number of IPS signatures.
Pre-defined signatures	Total number of predefined IPS signatures.
User-config signatures	Total number of user-configured signatures.
Snort signatures	Total number of Snort signatures.
Type	Type of the IPS signature: • **Pre**—Predefined IPS signatures. • **User**—User-defined signatures that are manually configured. • **Snort**—Snort signatures that are imported from a Snort file.
RuleID	Signature ID.
Target	Attacked target.
SubTarget	Attacked subtarget.
Severity	Attack severity level of the signature, **Low**, **Medium**, **High**, or **Critical**.
Direction	Traffic direction to which the IPS signature applies: • **Any**—Both server to client and client to server directions. • **Client**—Server to client direction. • **Server**— Client to server direction.
Category	Attack category of the signature.
Subcategory	Attack subcategory of the signature.

Field	Description
Status	Status of the IPS signature, **Enabled** or **Disabled**.
Action	Actions for matching packets: • **Block-source**—Drops matching packets and adds the sources of the packets to the IP blacklist. • **Drop**—Drops matching packets. • **Permit**—Permits matching packets to pass. • **Reset**—Closes the TCP or UDP connections for matching packets by sending TCP reset messages or ICMP port unreachable messages. • **Redirect**—Redirects matching packets to a webpage. • **Capture**—Captures matching packets. • **Logging**—Logs matching packets.

Related commands

ips policy

display ips signature

Use **display ips signature** to display brief IPS signature information.

Syntax

display ips signature [**pre-defined** | **user-defined** { **snort** | **user-config** }] [**direction** { **any** | **to-client** | **to-server** }] [**category** *category-name* | **fidelity** { **high** | **low** | **medium** } | **protocol** { **icmp** | **ip** | **tcp** | **udp** } | **severity** { **critical** | **high** | **low** | **medium** }] *

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

pre-defined: Specifies predefined IPS signatures.

user-defined: Specifies user-defined IPS signatures.

snort: Specifies Snort signatures that are imported from a Snort file. These imported signatures are also user-defined signatures.

user-config: Specifies user-defined signatures that are manually configured.

direction { **any** | **to-client** | **to-server** }: Specifies a direction attribute. If you do not specify a direction attribute, this command displays IPS signatures with any direction attribute.

- **to-server**: Specifies the client to server direction of a session.
- **to-client**: Specifies the server to client direction of a session.
- **any**: Specifies both directions of a session.

category *category-name*: Specifies an attack category. To view the names of supported attack categories, enter a question mark (?) after the **category** keyword. If you do not specify an attack category, this command displays IPS signatures for all attack categories.

fidelity { **high** | **low** | **medium** }: Specifies a fidelity level. If you do not specify a fidelity level, this command displays IPS signatures of all fidelity levels. The fidelity level indicates the attack detection accuracy.

- **low**: Specifies the low fidelity.
- **medium**: Specifies the medium fidelity.
- **high**: Specifies the high fidelity.

protocol { **icmp** | **ip** | **tcp** | **udp** }: Specifies a protocol. If you do not specify a protocol, this command displays IPS signatures for all protocols.

severity { **critical** | **high** | **low** | **medium** }: Specifies an attack severity level. If you do not specify a severity level, this command displays IPS signatures for all severity levels of attacks.

- **low**: Specifies the low severity level.
- **medium**: Specifies the medium severity level.
- **high**: Specifies the high severity level.
- **critical**: Specifies the critical severity level.

Usage guidelines

If you do not specify any options, this command displays all IPS signatures.

Examples

Display predefined IPS signatures of the medium fidelity level for TCP.

```
<Sysname> display ips signature pre-defined protocol tcp fidelity medium
Pre-defined  signatures:465       failed:0

Flag:
  Pre: predefined   User: user-config   Snort: Snort

Type Sig-ID    Direction Severity Fidelity Category      Protocol   Sig-Name
Pre  1         To-server High     Medium   Vulnerability TCP        -
Pre  2         To-server High     Medium   Vulnerability TCP        -
Pre  3         To-client High     Medium   Vulnerability TCP        -
Pre  4         To-client High     Medium   Vulnerability TCP        -
Pre  5         To-client High     Medium   Vulnerability TCP        -
Pre  6         To-client High     Medium   Vulnerability TCP        -
Pre  7         To-client High     Medium   Vulnerability TCP        -
Pre  8         To-client High     Medium   Vulnerability TCP        -
Pre  10        To-server High     Medium   Vulnerability TCP        -
Pre  11        To-client High     Medium   Vulnerability TCP        -
Pre  12        To-client Critical Medium   Vulnerability TCP        -
Pre  13        To-client High     Medium   Vulnerability TCP        -
Pre  14        To-server High     Medium   Vulnerability TCP        -
Pre  15        To-client High     Medium   Vulnerability TCP        -
Pre  16        To-client Critical Medium   Vulnerability TCP        -
Pre  17        To-client High     Medium   Vulnerability TCP        -
Pre  18        To-client High     Medium   Vulnerability TCP        -
---- More ----
```

Display IPS signatures of the high attack severity level for UDP.

```
<Sysname> display ips signature severity high protocol udp
Total signatures        :7         failed:0
 Pre-defined  signatures total:7         failed:0
 User-config  signatures total:0         failed:0
 snort signatures total:1         failed:1

Flag:
  Pre: predefined   User: user-defined   Snort: Snort

Type Sig-ID    Direction Severity Fidelity Category      Protocol   Sig-Name
Pre  9         To-server High     Medium   Vulnerability UDP        -
Pre  45        To-server High     Medium   Vulnerability UDP        -
Pre  187       Any       High     Medium   Vulnerability UDP        -
Pre  196       Any       High     Medium   Vulnerability UDP        -
Pre  223       To-server High     Medium   Vulnerability UDP        -
Pre  234       To-client High     Medium   Vulnerability UDP        -
Pre  338       To-client High     Medium   Vulnerability UDP        -
---- More ----
```

Table 2 Command output

Field	Description
Total signatures	Total number of IPS signatures.
failed	Total number of IPS signatures that failed to be imported and loaded during signature update.
Pre-defined signatures total	Total number of predefined IPS signatures.
User-config signatures total	Total number of user-configured signatures.
Snort signatures total	Total number of Snort signatures.
Type	Type of the IPS signature: • **Pre**—Predefined IPS signatures. • **User**—User-defined signatures that are manually configured. • **Snort**—Snort signatures that are imported from a Snort file.
Sig-ID	Signature ID.
Direction	Direction attribute of the signature: • **Any**—Specifies both directions of a session. • **To-server**—Specifies the client to server direction of a session. • **To-client**—Specifies the server to client direction of a session.
Severity	Attack severity level of the signature, **Low**, **Medium**, **High**, or **Critical**.
Fidelity	Fidelity level of the signature, **Low**, **Medium**, or **High**.
Category	Attack category of the signature.
Protocol	Protocol attribute of the signature.
Sig-Name	Name of the IPS signature.

display ips signature pre-defined

Use **display ips signature pre-defined** to display detailed information about a predefined IPS signature.

Syntax

display ips signature pre-defined *signature-id*

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

signature-id: Specifies the signature ID. The value range is 1 to 536870911.

Examples

Display detailed information about predefined IPS signature 1.

```
<Sysname> display ips signature pre-defined 1
 Type         : Pre-defined
 Signature ID: 1
 Status       : Enabled
 Action       : Reset & Logging
 Name         : GNU_Bash_CVE-2014-6271_Remote_Code_Execution_Vulnerability
 Protocol     : TCP
 Severity     : High
 Fidelity     : Medium
 Direction    : To-server
 Category     : Vulnerability
 Reference    : CVE-2014-6271;
 Description : GNU Bash through 4.3 processes trailing strings after function definitions
in the values of environment variables, which allows remote attackers to execute arbitrary
code via a crafted environment, as demonstrated by vectors involving the ForceCommand
feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts
executed by unspecified DHCP clients, and other situations in which setting the environment
occurs across a privilege boundary from Bash execution, aka \"ShellShock.\" NOTE: the
original fix for this issue was incorrect; CVE-2014-7169 has been assigned to cover the
vulnerability that is still present after the incorrect fix.
```

Table 3 Command output

Field	Description
Type	Type of the IPS signature: • **Pre**—Predefined IPS signatures. • **User**—User-defined signatures.
Signature ID	Signature ID.
Status	Status of the IPS signature, **Enabled** or **Disabled**.

Field	Description
Action	Actions for matching packets: • **Block-source**—Drops matching packets and adds the sources of the packets to the IP blacklist. • **Drop**—Drops matching packets. • **Permit**—Permits matching packets to pass. • **Reset**—Closes the TCP or UDP connections for matching packets by sending TCP reset messages or ICMP port unreachable messages. • **Capture**—Captures matching packets. • **Logging**—Logs matching packets.
Name	Name of the IPS signature.
Protocol	Protocol attribute of the signature.
Severity	Attack severity, **Low**, **Medium**, **High**, or **Critical**.
Fidelity	Fidelity level of the signature, **Low**, **Medium**, or **High**.
Direction	Direction attribute of the signature: • **Any**—Specifies both directions of a session. • **To-server**—Specifies the client to server direction of a session. • **To-client**—Specifies the server to client direction of a session.
Category	Attack category of the signature.
Reference	Reference for the signature.
Description	Description for the signature.

display ips signature library

Use **`display ips signature library`** to display IPS signature library information.

Syntax

`display ips signature library`

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display IPS signature library information.

```
<Sysname> display ips signature library
IPS signature library information:
Type     SigVersion         ReleaseTime               Size
Current  1.02               Fri Sep 13 09:05:35 2014  71594
Last     -                  -                         -
Factory  1.00               Fri Sep 11 09:05:35 2014  71394
```

Table 4 Command output

Field	Description
Type	Version type of the IPS signature library: • **Current**—Current version. • **Last**—Previous version. • **Factory**—Factory default version.
SigVersion	Version number of the IPS signature library.
ReleaseTime	Release time of the IPS signature library.
Size	Size of the IPS signature file in bytes.

display ips signature user-defined

Use **display ips signature user-defined** to display detailed information about a user-defined IPS signature.

Syntax

display ips signature user-defined { **snort** | **user-config** } *signature-id*

Views

Any view

Predefined user roles

network-admin

context-admin

Parameters

snort: Specifies the Snort signatures.

user-config: Specifies the user-configured signatures.

signature-id: Specifies the signature ID. The value range for Snort signatures is 536870913 to 1073741823. The value range for user-configured signatures is 1073741840 to 1342177264.

Examples

Display detailed information about Snort signature 536870914.

```
<Sysname> display ips signature user-defined snort 536870914
 Type        : Snort
 Signature ID: 536870914
 Status      : Enabled
 Action      : drop
 Name        : Snort name
 Protocol    : TCP
 Severity    : High
 Fidelity    : Medium
 Direction   : To-server
 Category    : Vulnerability
 Reference   : CVE-2014-6271;
 Description : Some description.
```

Table 5 Command output

Field	Description
Type	Type of the user-defined IPS signature. **Snort** indicates that the signature is imported from a Snort file.
Signature ID	Signature ID.
Status	Status of the IPS signature, **Enabled** or **Disabled**.
Action	Actions for matching packets: • **Block-source**—Drops matching packets and adds the sources of the packets to the IP blacklist. • **Drop**—Drops matching packets. • **Permit**—Permits matching packets to pass. • **Reset**—Closes the TCP or UDP connections for matching packets by sending TCP reset messages or ICMP port unreachable messages. • **Capture**—Captures matching packets. • **Logging**—Logs matching packets.
Name	Name of the IPS signature.
Protocol	Protocol attribute of the signature.
Severity	Attack severity, **Low**, **Medium**, **High**, or **Critical**.
Fidelity	Fidelity level of the signature, **Low**, **Medium**, or **High**.
Direction	Direction attribute of the signature: • **Any**—Specifies both directions of a session. • **To-server**—Specifies the client to server direction of a session. • **To-client**—Specifies the server to client direction of a session.
Category	Attack category of the signature.
Reference	Reference for the signature.
Description	Description for the signature.

Display detailed information about user-configured IPS signature 1073741840.

```
<Sysname> display ips signature user-defined user-config 1073741840
 Type: User-config
 Signature ID: 1073741840
 Signature name: lkx
 Status:       Enable
 Action:       Permit
 Severity:     Low
 Fidelity:     High
 Direction:    Any
 Rulelogic:    And
 Total rule:   1

  Rule ID:     1
   L4-protocol: TCP
   L5-protocol: HTTP
   Match-type: keyword
   Destination-address: 1.1.1.1
```

```
   Destination-port: 50-60
   Trigger entry:
    Field: HTTP.Accept
    Value: 12ljlj
   Detection entry list:
    Entry ID   Field                          Match-type Content-type Content

    1          HTTP.Accept                    exclude    text         ljljl

---- More --
```

Table 6 Command output

Field	Description
Type	Type of the user-defined IPS signature. **User-config** indicates that the signature is configured manually.
Signature ID	Signature ID.
Signature name	Name of the IPS signature.
Status	Status of the IPS signature, **Enabled** or **Disabled**.
Action	Actions for matching packets: • **Block-source**—Drops matching packets and adds the sources of the packets to the IP blacklist. • **Drop**—Drops matching packets. • **Permit**—Permits matching packets to pass. • **Reset**—Closes the TCP or UDP connections for matching packets by sending TCP reset messages or ICMP port unreachable messages. • **Capture**—Captures matching packets. • **Logging**—Logs matching packets.
Severity	Attack severity, **Low**, **Medium**, **High**, or **Critical**.
Fidelity	Fidelity level of the signature, **Low**, **Medium**, or **High**.
Direction	Direction attribute of the signature: • **Any**—Specifies both directions. • **To-server**—Specifies the client-to-server direction. • **To-client**—Specifies the server-to-client direction.
Rulelogic	Logical operator between rules in the IPS signature.
Description	Description for the signature.
Total rule	Total number of rules.
Rule ID	Rule ID.
L4-protocol	Transport layer protocol as a filtering criterion in the rule.
L5-protocol	Application layer protocol as a filtering criterion in the rule.
Match type	Signature match pattern type, **Keyword** or **Integer**.
Source address	Source address as a filtering criterion.
Source port	Source port as a filtering criterion.
Destination address	Destination address as a filtering criterion.
Destination port	Destination port as a filtering criterion.

Field	Description
Trigger entry	Detection trigger condition in the rule.
Field	Protocol field to inspect in the detection trigger condition.
Value	Contents to inspect in the detection trigger condition.
Offset	Offset after which the inspection starts.
Depth	Number of bytes to be inspected.
Detection entry list	Detection item list.
Entry ID	Detection item ID.
Field	Protocol field to inspect in the detection item.
Match type	Match operation in the detection item.
Content-type	Type of the match pattern: • **hex**—Specifies a hexadecimal string. • **regex**—Specifies a regular expression string. • **text**—Specifies a text string.
Content	Contents to inspect in the detection item.

display ips signature user-defined parse-failed

Use **display ips signature user-defined parse-failed** to display information about the user-defined IPS signatures that failed to be parsed during signature import.

Syntax

display ips signature user-defined parse-failed

Views

Any view

Predefined user roles

network-admin

context-admin

Examples

Display information about the user-defined IPS signatures that failed to be imported

```
<Sysname> display ips signature user-defined parse-failed
LineNo  SID         Information
1       None        Error: Invalid actions.
                    Tip: Only actions {alert|drop|pass|reject|sdrop|log} are supported
2       1010082     Error: Invalid signature ID.
                    Tip: The signature ID must be in the range of 1 to 536870912
3       1010083     Error: Invalid protocol.
                    Tip: Only protocols {tcp|udp|icmp|ip} are supported
4       1010084     Error: Invalid direction.
                    Tip: Only directions {'<>'|'->'} are supported
```

Table 7 Command output

Field	Description
LineNo	Line number where the signature is located in the Snort file.
SID	Signature ID.
Information	Signature information: • **Error**—Reason for the parse failure. • **Tip**—Tip for editing the signature rule in the file.

Related commands

`ips signature import snort`

email parameter-profile

Use **`email parameter-profile`** to specify a parameter profile for the email action.

Use **`undo email parameter-profile`** to remove the parameter profile from the email action.

Syntax

`email parameter-profile` *`parameter-profile-name`*

`undo email parameter-profile`

Default

No parameter profile is specified for the email action.

Views

IPS policy view

Predefined user roles

network-admin

context-admin

Parameters

`parameter-profile-name`: Specifies a parameter profile by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

This command takes effect only after the global parameter profile is disabled by the **`undo global-parameter enable`** command.

This command is required after you use the **`log email`** command to specify the log output method as email. For information about configuring an email parameter profile, see "DPI engine commands."

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the parameter profile **email1** for the **email** action in IPS policy **policy1**.

```
<Sysname> system-view
[Sysname] ips policy policy1
[Sysname-ips-policy-policy1] email parameter-profile email1
```

Related commands

`log`

global-parameter enable

email severity-level

Use **email severity-level** to specify the lowest severity level of the matching IPS signatures for log output via email.

Use **undo email severity-level** to restore the default.

Syntax

email severity-level { **critical** | **high** | **low** | **medium** }

undo email severity-level

Default

The lowest severity level of the matching IPS signatures for log output via email is **low**.

Views

IPS policy view

Predefined user roles

network-admin

context-admin

Parameters

critical: Specifies the critical severity level.

high: Specifies the high severity level.

low: Specifies the low severity level.

medium: Specifies the medium severity level.

Usage guidelines

This command filters logs by the severity level of an IPS signature for log output via email. The system sends emails for IPS logs only when the severity levels of the matching IPS signatures are not lower than specified severity level.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the lowest severity level of the matching IPS signatures for log output via email as **high** in IPS policy **test**.

```
<Sysname> system-view
[Sysname] ips policy test
[Sysname-ips-policy-test] email severity-level high
```

global-parameter enable

Use **global-parameter enable** to enable the global parameter profiles.

Use **undo global-parameter enable** to disable the global parameter profiles.

Syntax

global-parameter enable

undo global-parameter enable

Default

The global parameter profiles are enabled.

Views

IPS policy view

Predefined user roles

network-admin

context-admin

Usage guidelines

The **block source**, **capture**, and **logging** actions take effect only after a parameter profile is specified. You can specify a parameter profile for an IPS action as follows:

- Specify a global parameter profile in system view. The setting takes effect in all IPS policies.
- Specify a parameter profile in IPS policy view, which is a policy-specific setting. Only the email action supports a parameter profile in IPS policy view.

The global parameter profile for an IPS action takes precedence over a policy-specific parameter profile for the action.

To have a parameter profile for an IPS action in an IPS policy take effect, make sure the global parameter profile is disabled.

As a best practice, enable the global parameter profile after the global parameter profile configuration is completed.

Examples

Enable the global parameter profiles in IPS policy **policy1**.

```
<Sysname> system-view
[Sysname] ips policy policy1
[Sysname-ips-policy-policy1] global-parameter enable
```

Related commands

email parameter-profile

ips parameter-profile

log

http-method

Use **http-method** to specify a request method filtering criterion in a user-defined signature rule.

Use **undo http-method** delete a request method filtering criterion from a user-defined signature rule.

Syntax

http-method *method-name*

undo http-method

Default

No request method filtering criterion is specified in a user-defined signature rule.

Views

User-defined IPS signature rule view

Predefined user roles

network-admin

context-admin

Parameters

method-name: Specifies the name of an HTTP request method, a case-insensitive string, such as GET and POST. To view the supported request methods, enter a question mark (?) after the **http-method** keyword.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

In rule 1 of user-defined IPS signature **mysignature**, specify the keyword type as the match pattern type and specify the GET request method as a filtering criterion.

```
<Sysname> system-view
[Sysname] ips signature user-defined name mysignature
[Sysname-ips-signature-mysignature] rule 1 l4-protocol tcp l5-protocol http pattern-type keyword
[Sysname-ips-signature-mysignature-rule-1] http-method get
```

ips apply policy

Use **ips apply policy** to apply an IPS policy to a DPI application profile.

Use **undo ips apply policy** to remove the application.

Syntax

ips apply policy *policy-name* **mode** { **alert** | **protect** }

undo ips apply policy

Default

No IPS policy is applied to a DPI application profile.

Views

DPI application profile view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies an IPS policy by its name, a case-insensitive string of 1 to 63 characters.

mode: Specifies an IPS policy mode.

alert: Only captures or logs matching packets.

protect: Takes all actions specified for signatures to process matching packets

Usage guidelines

An IPS policy takes effect only after it is applied to a DPI application profile.

You can apply only one IPS policy to a DPI application profile. If you execute this command multiple times, the most recent configuration takes effect.

Examples

Apply IPS policy **ips1** to DPI application profile **sec**. Set the IPS policy mode to **protect**.

```
<Sysname> system-view
[Sysname] app-profile sec
[Sysname-app-profile-sec] ips apply policy ips1 mode protect
```

Related commands

app-profile

ips policy

ips capture-cache

Use **ips capture-cache** to specify the number of the captured packets to be cached for threat analysis.

Use **undo ips capture-cache** to restore the default.

Syntax

ips capture-cache *number*

undo ips capture-cache

Default

The number of the captured packets to be cached is not specified, and the device does not cache any captured packets.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

number: Specifies the number of the captured packets to be cached, in the range of 1 to 10. If the value is set to 1, the device caches only the hit packet.

Usage guidelines

This command enables the device to cache the IPS captured packets.

The device caches the specified number of packets captured before and after the hit packet matching the IPS policy, including the hit packet. When the specified number of packets are cached, the device writes all cached packets into the capture file. The number of the cached packets will be less than the specified number in one of the following situations:

- The action, such as block or redirect on the hit packet causes the packets after the hit packet to be dropped.
- The device has no capacity to cache the specified number of packets.

Examples

Allow the device to cache a maximum of five IPS captured packets.

```
<Sysname> system-view
[Sysname] ips capture-cache 5
```

Related commands

inspect capture parameter-profile

signature override

signature override

ips parameter-profile

Use **ips parameter-profile** to specify a parameter profile for an IPS action.

Use **undo ips parameter-profile** to remove the parameter profile from an IPS action.

Syntax

ips { **block-source** | **capture** | **email** | **logging** | **redirect** } **parameter-profile** *parameter-name*

undo ips { **block-source** | **capture** | **email** | **logging** | **redirect** } **parameter-profile**

Default

No parameter profile is specified for an IPS action.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

block-source: Specifies a parameter profile for the **block-source** action.

capture: Specifies a parameter profile for the **capture** action.

email: Specifies a parameter profile for the **email** action.

logging: Specifies a parameter profile for the **logging** action.

redirect: Specifies a parameter profile for the **redirect** action.

parameter-profile *parameter-name*: Specifies a parameter profile by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

Use this command to specify the parameter profile used by an IPS action. A parameter profile is a set of parameters that determine how the action is executed. If you do not specify a parameter profile for an action, or if the specified profile does not exist, the default action parameter settings are used.

For information about configuring parameter profiles, see *DPI Configuration Guide*.

Examples

Create parameter profile **ips1**. Set the source IP address blocking period to 1111 seconds.

```
<Sysname> system-view
[Sysname] inspect block-source parameter-profile ips1
[Sysname-inspect-block-source-ips1] block-period 1111
[Sysname-inspect-block-source-ips1] quit
```

Specify the parameter profile **ips1** for the **block-source** action.

```
[Sysname] ips block-source parameter-profile ips1
```

Related commands

inspect block-source parameter-profile

inspect capture parameter-profile

inspect logging parameter-profile

inspect email parameter-profile

inspect redirect parameter-profile

ips policy

Use **ips policy** to create an IPS policy and enter its view, or enter the view of an existing IPS policy.

Use **undo ips policy** to delete an IPS policy.

Syntax

ips policy *policy-name*

undo ips policy *policy-name*

Default

An IPS policy named **default** exists.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies the IPS policy name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

An IPS policy includes all signatures on the device, whether or not the signatures are added to the device before the policy is created.

You cannot modify the signatures in the default IPS policy. In a user-defined policy, you can enable or disable a signature, or edit the actions for a signature.

Examples

Create IPS policy **ips1** and enter its view.

```
<Sysname> system-view
[Sysname] ips policy ips1
[Sysname-ips-policy-ips1]
```

ips signature auto-update

Use **ips signature auto-update** to enable automatic IPS signature library update and enter automatic IPS signature library update configuration view.

Use **undo ips signature auto-update** to disable automatic IPS signature library update.

Syntax

ips signature auto-update

undo ips signature auto-update

Default

Automatic IPS signature library update is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

After you enable automatic IPS signature library update, the device periodically accesses the NSFOCUS website to download the latest IPS signatures.

Examples

Enable automatic IPS signature library update and enter automatic IPS signature library update configuration view.

```
<Sysname> system-view
[Sysname] ips signature auto-update
[Sysname-ips-autoupdate]
```

Related commands

update schedule

ips signature auto-update-now

Use **ips signature auto-update-now** to trigger an automatic signature library update manually.

Syntax

ips signature auto-update-now

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

After you execute this command, the device immediately starts the automatic signature library update process no matter whether or not automatic signature library update is enabled. The device automatically backs up the current signature library before overwriting it.

You can execute this command anytime you find a new version of signature library on the NSFOCUS website.

Examples

Trigger an automatic signature library update manually.

```
<Sysname> system-view
[Sysname] ips signature auto-update-now
```

ips signature import snort

Use **ips signature import snort** to import Snort signatures.

Syntax

ips signature import snort *file-path*

Default

No Snort signatures exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

file-path: Specifies the path of the file where the Snort signatures to be imported are stored. The value for this argument is a string of 1 to 255 characters.

Usage guidelines

To add your own IPS signatures, create an IPS signature file in the Snort format and use this command to import the signatures.

Make sure the IPS signature file contains all user-defined signatures that you want to use. All existing user-defined signatures on the device will be overwritten by the imported signatures.

To view the imported IPS signatures, use the **display ips signature user-defined** command.

The following methods are available for Snort signature import:

- **Local method**—Imports Snort signatures from a local IPS signature file.

  The following describes the format of the *file-path* parameter for different import scenarios.

Import scenario	Format of *file-path*	Remarks
The import file is stored in the current working directory.	*filename*	To display the current working directory, use the **pwd** command. For information about the **pwd** command, see file system management in *Fundamentals Command Reference*.
The import file is stored in a different directory on the same storage medium.	*filename*	Before configuring the **ips signature import snort** command, use the **cd** command to open the directory where the file is stored. For information about the **cd** command, see file system management in *Fundamentals Command Reference.*
The import file is stored on a different storage medium.	*path/filename*	Before configuring the **ips signature import snort** command, use the **cd** command to open the root directory of the storage medium where the file is stored. For information about the **cd**

Import scenario	Format of *file-path*	Remarks
		command, see file system management in *Fundamentals Command Reference.*

- **FTP/TFTP method**—Imports Snort signatures from an IPS signature file stored on an FTP or TFTP server.

  The following describes the format of the *file-path* parameter for different import scenarios.

Import scenario	Format of *file-path*	Remarks
The import file is stored on an FTP server.	*ftp://username:password@server address/filename*	The *username* parameter represents the FTP login username. The *password* parameter represents the FTP login password. The *server address* parameter represents the IP address or host name of the FTP server. Replace the following special characters in the FTP login username and password with their respective escape characters: • **Colon (:)**—%3A or %3a. • **At sign (@)**—%40. • **Forward slash (/)**—%2F or %2f.
The import file is stored on a TFTP server.	*tftp://server address/filename*	The *server address* parameter represents the IP address or host name of the TFTP server.

When you configure a Snort rule in the IPS signature file, follow these restrictions and guidelines:

- Use the correct syntax for the rule.
- Specify an SID in the range of 1 to 536870911 for the rule. Rules with larger IDs are invalid.
- The SID of the rule must be different from the SIDs of any existing Snort rules on the device.
- Be sure to configure the **msg** field for the rule. If the **msg** field is not configured, the attack name of the rule will not be displayed in the IPS syslog message.
- Make sure the application specified in the rule is identifiable. Otherwise, no packets can match the rule.

Examples

Import Snort signatures from an IPS signature file that is stored on a TFTP server.

```
<Sysname> system-view
[Sysname] ips signature import snort tftp://192.168.0.1/snort.rules
```

Related commands

display ips signature user-defined

ips signature remove snort

ips signature remove snort

Use **ips signature remove snort** to delete all imported Snort IPS signatures.

Syntax

ips signature remove snort

Views

System view

Predefined user roles

network-admin

context-admin

Examples

Delete all imported Snort IPS signatures.

```
<Sysname> system-view
[Sysname] ips signature remove snort
```

Related commands

ips signature import snort

ips signature rollback

Use **ips signature rollback** to roll back the IPS signature library.

Syntax

ips signature rollback { **factory** | **last** }

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

factory: Rolls back the IPS signature library to the factory default version.

last: Rolls back the IPS signature library to the previous version.

Usage guidelines

If an IPS signature library update causes exceptions or a high false alarm rate, you can roll back the IPS signature library.

Before performing an IPS signature library rollback, the device backs up the current IPS signature library as the previous version. For example, the previous library version is V1 and the current library version is V2. If you perform a rollback to the previous version, library version V1 becomes the current version and library version V2 becomes the previous version. If you perform a rollback to the previous version again, the library rolls back to library version V2.

Examples

Roll back the IPS signature library to the previous version.

```
<Sysname> system-view
[Sysname] ips signature rollback last
```

ips signature update

Use **ips signature update** to manually update the IPS signature library.

Syntax

ips signature update [**override-current**] *file-path* [**vpn-instance** *vpn-instance-name*]

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

override-current: Overwrites the current IPS signature library without backing up the library. For the device to back up the current IPS signature library before overwriting the library, do not specify this keyword.

file-path: Specifies the IPS signature file path, a string of 1 to 255 characters.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance to which the TFTP or FTP server belongs by the instance's name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the TFTP or FTP server belongs to the public network.

Usage guidelines

If the device cannot access the NSFOCUS website, use one of the following methods to manually update the IPS signature library:

- **Local update**—Updates the IPS signature library by using a locally stored update IPS signature file.

  Store the update file on the master device for successful signature library update.

  The following describes the format of the *file-path* parameter for different update scenarios.

Update scenario	Format of *file-path*	Remarks
The update file is stored in the current working directory.	*filename*	To display the current working directory, use the **pwd** command. For information about the **pwd** command, see file system management in *Fundamentals Command Reference.*
The update file is stored in a different directory on the same storage medium.	*filename*	Before configuring the **ips signature update** command, use the **cd** command to open the directory where the file is stored. For information about the **cd** command, see file system management in *Fundamentals Command Reference.*
The update file is stored on a different storage medium.	*path/filename*	Before configuring the **ips signature update** command, use the **cd** command to open the root directory of the storage medium where the file is stored. For information about the **cd** command, see file system management in *Fundamentals Command Reference.*

- **FTP/TFTP update**—Updates the IPS signature library by using the file stored on an FTP or TFTP server.

  The following describes the format of the *file-path* parameter for different update scenarios.

Update scenario	Format of *file-path*	Remarks
The update file is stored on an FTP server.	*ftp://username:password@server address/filename*	The *username* parameter represents the FTP login username. The *password* parameter represents the FTP login password. The *server address* parameter represents the IP address or host name of the FTP server. Replace the following special characters in the FTP login username and password with their respective escape characters: • **Colon (:)**—%3A or %3a. • **At sign (@)**—%40. • **Forward slash (/)**—%2F or %2f.
The update file is stored on a TFTP server.	*tftp://server address/filename*	The *server address* parameter represents the IP address or host name of the TFTP server.

NOTE:

To update the signature library successfully, make sure the device and the FTP or TFTP server can reach each other. If you specify the FTP or TFTP server by its host name, you must also make sure the device can resolve the host name into an IP address through static or dynamic DNS. For more information about DNS, see *Layer 3—IP Services Configuration Guide*.

Examples

Manually update the IPS signature library by using an IPS signature file stored on a TFTP server.

```
<Sysname> system-view
[Sysname] ips signature update tftp://192.168.0.10/ips-1.0.2-en.dat
```

Manually update the IPS signature library by using an IPS signature file stored on an FTP server. The FTP login username and password are **user:123** and **user@abc/123**, respectively.

```
<Sysname> system-view
[Sysname] ips signature update
ftp://user%3A123:user%40abc%2F123@192.168.0.10/ips-1.0.2-en.dat
```

Manually update the IPS signature library by using an IPS signature file stored on the device. The file is stored in directory **cfa0:/ips-1.0.23-en.dat**, and the current working directory is **cfa0:**.

```
<Sysname> system-view
[Sysname] ips signature update ips-1.0.23-en.dat
```

Manually update the IPS signature library by using an IPS signature file stored on the device. The file is stored in directory **cfa0:/dpi/ips-1.0.23-en.dat**, and the current working directory is **cfa0:**.

```
<Sysname> cd dpi
<Sysname> system-view
[Sysname] ips signature update ips-1.0.23-en.dat
```

Manually update the IPS signature library by using an IPS signature file stored on the device. The file is stored in directory **cfb0:/dpi/ips-1.0.23-en.dat**, and the current working directory is the **cfa0:**.

```
<Sysname> cd cfb0:/
<Sysname> system-view
[Sysname] ips signature update dpi/ips-1.0.23-en.dat
```

ips signature update-log

Use **ips signature update-log send-time** to enable logging for IPS signature library update and rollback events and daily output of the logs at the specified time.

Use **undo ips signature update-log send-time** to disable logging for IPS signature library update and rollback events.

Syntax

ips signature update-log send-time *time*

undo ips signature update-log send-time

Default

Logging for IPS signature library update and rollback events is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

time: Specifies the daily log output time, in the format of hh:mm. The value range is 00:00 to 23:59.

Usage guidelines

This command enables the device to log successful IPS signature library update and rollback events and to output the logs at the specified time.

The device supports outputting IPS signature library update and rollback logs only as fast logs to log hosts. For the IPS logs to be output correctly, make sure the following requirements are met:

- Fast log output of IPS logs in SGCC format are enabled by using the **customlog format dpi ips sgcc** command.
- The log hosts where the IPS logs should be sent are configured by using the **customlog host** command.

For more information about the preceding commands, see fast log output commands in *Network Management and Monitoring Command Reference*.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Enable logging for IPS signature library update and rollback events and set the daily output time to 12:12.

```
<Sysname> system-view
[Sysname] ips signature update-log send-time 12:12
```

ips signature user-defined

Use **ips signature user-defined** create a user-defined IPS signature and enter its view, or enter the view of an existing user-defined IPS signature.

Use **undo ips signature user-defined** to delete user-defined IPS signatures.

Syntax

ips signature user-defined name *signature-name*

undo ips signature user-defined { **all** | **name** *signature-name* }

Default

No user-defined IPS signatures exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

signature-name: Specifies the IPS signature name, a case-insensitive string of 1 to 63 characters.

all: Deletes all user-defined signatures that are manually configured.

Usage guidelines

Repeat this command to create multiple user-defined IPS signatures, which are user-configured signatures and different from Snort signatures imported from an IPS signature file in the Snort format.

When you delete a user-configured signature, all the configurations for the signature will also be deleted.

Examples

Create user-defined IPS signature **mysignature** and enter its view.

```
<Sysname> system-view
[Sysname] ips signature user-defined name mysignature
[Sysname-ips-signature-mysignature]
```

Related commands

display ips signature user-defined user-config

ips whitelist

Use **ips whitelist** to create an IPS whitelist entry and enter its view, or enter the view of an existing IPS whitelist entry.

Use **undo ips whitelist** to delete an IPS whitelist entry.

Syntax

ips whitelist *entry-id*

undo ips whitelist *entry-id*

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

entry-id: Specifies the IPS whitelist entry ID, in the range of 1 to 2048.

Usage guidelines

If false alarms exist in IPS logs, you can enable the IPS whitelist feature, and add the detected IPS signature IDs or URLs to the IPS whitelist. The device permits packets matching the IPS signatures or URLs on the IPS whitelist to pass through, reducing false alarms.

Examples

Create IPS whitelist entry **1** and enter its view.

```
<Sysname> system-view
[Sysname] ips whitelist 1
[Sysname-ips-whitelist-1]
```

Related commands

ips whitelist activate

ips whitelist activate

Use **ips whitelist activate** to activate the IPS whitelist configuration.

Syntax

ips whitelist activate

Default

The creation and editing of an IPS whitelist entry does not take effect immediately if the entry contains a URL.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

After you create or edit an IPS whitelist entry that contains a URL, you must execute this command to have the configuration take effect.

Examples

Activate the IPS whitelist configuration.

```
<Sysname> system-view
[Sysname] ips whitelist activate
```

Related commands

url

ips whitelist enable

Use **ips whitelist enable** to enable the IPS whitelist feature.

Use **undo ips whitelist enable** to disable the IPS whitelist feature.

Syntax

ips whitelist enable

undo ips whitelist enable

Default

The IPS whitelist feature is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

If false alarms exist in IPS logs, you can enable the IPS whitelist feature, and add the detected IPS signature IDs or URLs to the IPS whitelist. The device permits packets matching the IPS signatures or URLs on the IPS whitelist to pass through, reducing false alarms.

Examples

Enable the IPS whitelist feature.

```
<Sysname> system-view
[Sysname] ips whitelist enable
```

log

Use **log** to specify the log output method.

Use **undo log** to restore the default.

Syntax

log { **email** | **syslog** }

undo log { **email** | **syslog** }

Default

The IPS log output method is **syslog**.

Views

IPS policy view

Predefined user roles

network-admin

context-admin

Parameters

email: Emails the IPS logs to an email receiver.

syslog: Exports the IPS logs to the information center.

Usage guidelines

This command takes effect only after the global parameter profiles are disabled by the **undo global-parameter enable** command.

If you specify the email log output method, you can specify a parameter profile used by the email action.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the log output method as **email** in IPS policy **policy1**.

```
<Sysname> system-view
[Sysname] ips policy policy1
[Sysname-ips-policy-policy1] log email
```

Related commands

email parameter-profile

global-parameter enable

object-dir

Use **object-dir** to specify a direction criterion to filter IPS signatures in an IPS policy.

Use **undo object-dir** to restore the default.

Syntax

object-dir { **client** | **server** } *

undo object-dir

Default

The direction attribute is not used for IPS signature filtering.

Views

IPS policy view

Predefined user roles

network-admin

context-admin

Parameters

client: Specifies the server to client direction.

server: Specifies the client to server direction.

Usage guidelines

Each IPS signature has a direction attribute that defines the traffic direction to which the signature applies. The direction attribute values include **To-server**, **To-client**, and **Any**.

IPS signatures with the **Any** direction attribute are always used by an IPS policy, regardless of the settings of this command. For example, if you configure the **object-dir client** command for an IPS policy, the policy will use IPS signatures with both the **To-client** and **Any** direction attributes.

If you execute this command in an IPS policy multiple times, the most recent configuration takes effect.

Examples

Configure IPS policy **test** to use IPS signatures with the **To-client** and **Any** direction attributes.

```
<Sysname> system-view
[Sysname] ips policy test
[Sysname-ips-policy-test] object-dir client
```

override-current

Use **override-current** to configure the device to overwrite the current IPS signature library without backing up the library during an automatic signature library update.

Use **undo override-current** to restore the default.

Syntax

override-current

undo override-current

Default

Before performing an automatic IPS signature library update, the device backs up the current IPS signature library as the previous version.

Views

Automatic IPS signature library update configuration view

Predefined user roles

network-admin

context-admin

Usage guidelines

Backing up the current IPS signature library requires additional storage space but enables signature library rollback. As a best practice, enable the backup function if there is sufficient storage space.

Examples

Configure the device to overwrite the current IPS signature library without backing up the library during an automatic signature library update.

```
<Sysname> system-view
[Sysname] ips signature auto-update
[Sysname-ips-autoupdate] override-current
```

Related commands

ips signature auto-update

protect-target

Use **protect-target** to set a target criterion to filter the IPS signatures in an IPS policy.

Use **undo protect-target** to remove a target criterion.

Syntax

protect-target { *target* [*subtarget*] | **all** }

undo protect-target { *target* [*subtarget*] | **all** }

Default

The protected target attribute is not used for IPS signature filtering.

Views

IPS policy view

Predefined user roles

network-admin

context-admin

Parameters

target: Specifies a target.

subtarget: Specifies a subtarget of the target. If you do not specify a subtarget, this command matches any IPS signatures with a subtarget of the specified target.

all: Specifies all targets.

Usage guidelines

This command filters the IPS signatures that an IPS policy uses based on the protected target attribute of the signatures.

You can execute this command multiple times to specify multiple target criteria in an IPS policy. The IPS policy uses an IPS signature if the signature matches any of the configured target criteria.

Examples

Configure IPS policy **test** to use IPS signatures with the **WebLogic** subtarget of the **WebServer** target.

```
<Sysname> system-view
[Sysname] ips policy test
[Sysname-ips-policy-test] protect-target WebServer WebLogic
```

rule

Use **rule** to create a user-defined IPS signature rule and enter its view, or enter the view of an existing user-defined IPS signature rule.

Use **undo rule** to delete user-defined IPS signature rules.

Syntax

rule *rule-id* **l4-protocol** *l4-protocol-name* **l5-protocol** *l5-protocol-name* **pattern-type** { **keyword** | **integer** }

undo rule { *rule-id* | **all** }

Default

No user-defined IPS signature rules exist.

Views

User-defined IPS signature view

Predefined user roles

network-admin

context-admin

Parameters

rule-id: Specifies the rule ID, in the range of 1 to 8.

l4-protocol *l4-protocol-name*: Specifies the transport layer protocol by its name. To view the names of supported protocols, enter a question mark (?) after the **l4-protocol** keyword.

l5-protocol *l5-protocol-name*: Specifies the application layer protocol by its name. To view the names of supported protocols, enter a question mark (?) after the **l5-protocol** keyword.

pattern-type: Specifies the match pattern type for the rule.

keyword: Specifies the keyword type.

integer: Specifies the integer type.

all: Deletes all user-defined IPS signature rules.

Usage guidelines

You can configure multiple rules in a user-defined signature. To configure the logical operator between rules, use the **rule-logic** command.

You cannot execute this command multiple times to change any configurations of a rule. If you want to modify the rule configuration, use the **undo rule** command to delete the rule first.

Examples

Create user-defined IPS signature rule 1 and enter its view. Set the rule to match TCP and HTTP packets, and specify the keyword match pattern type.

```
<Sysname> system-view
[Sysname] ips signature user-defined name mysignature
[Sysname-ips-signature-mysignature] rule 1 l4-protocol tcp l5-protocol http pattern-type keyword
[Sysname-ips-signature-mysignature-rule-1]
```

rule-logic

Use **rule-logic** to define the logical operator between the rules in a user-defined IPS signature.

Use **undo rule-logic** to restore the default.

Syntax

rule-logic { **and** | **or** }

undo rule-logic

Default

The logical operator between the rules in a user-defined IPS signature is **or**.

Views

User-defined IPS signature view

Predefined user roles

network-admin

context-admin

Parameters

and: Specifies the logical AND operator.

or: Specifies the logical OR operator.

Usage guidelines

If the logical AND operator is specified between rules in a user-defined signature, a packet matches the signature only when the packet matches all rules in the signature.

If the logical OR operator is specified between rules in a user-defined signature, a packet matches the signature when the packet matches any rule in the signature.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

In user-defined IPS signature **mysignature**, specify the logical AND operator between the rules.

```
<Sysname> system-view
[Sysname] ips signature user-defined name mysignature
[Sysname-ips-signature-mysignature] rule-logic and
```

severity-level (IPS policy view)

Use **severity-level** to set a severity level criterion to filter the IPS signatures in an IPS policy.

Use **undo severity-level** to restore the default.

Syntax

severity-level { **critical** | **high** | **low** | **medium** } *

undo severity-level

Default

The severity level attribute is not used for IPS signature filtering.

Views

IPS policy view

Predefined user roles

network-admin

context-admin

Parameters

critical: Specifies the critical severity level.

high: Specifies the high severity level.

low: Specifies the low severity level.

medium: Specifies the medium severity level.

Usage guidelines

Each IPS signature has a severity level attribute, which indicates the severity level of the attacks matching the signature.

This command filters the IPS signatures that an IPS policy uses based on the severity level attribute of the signatures.

You can specify multiple severity levels in a severity level criterion. The IPS policy uses an IPS signature if the signature matches any of the specified severity levels.

If you execute this command in an IPS policy multiple times, the most recent configuration takes effect.

Examples

Configure IPS policy **test** to use IPS signatures with the critical and medium severity levels.

```
<Sysname> system-view
[Sysname] ips policy test
[Sysname-ips-policy-test] severity-level critical medium
```

severity-level (IPS signature view)

Use **severity-level** to set a severity level criterion for a user-defined IPS signature.

Use **undo severity-level** to restore the default.

Syntax

severity-level { **critical** | **high** | **low** | **medium** }

undo severity-level

Default

The severity level of a user-defined IPS signature is **low**.

Views

User-defined IPS signature view

Predefined user roles

network-admin

context-admin

Parameters

critical: Specifies the critical severity level.

high: Specifies the high severity level.

low: Specifies the low severity level.

medium: Specifies the medium severity level.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the severity level to **medium** for user-defined IPS signature **mysignature**.

```
<Sysname> system-view
[Sysname] ips signature user-defined name mysignature
[Sysname-ips-signature-mysignature] severity-level medium
```

signature override

Use **signature override** to change the status and actions for an IPS signature in an IPS policy.

Use **undo signature override** to restore the default status and actions for an IPS signature in an IPS policy.

Syntax

signature override { **pre-defined** | **user-defined** } *signature-id* { { **disable** | **enable** } [{ **block-source** | **drop** | **permit** | **redirect** | **reset** } | **capture** | **logging**] * }

undo signature override { **pre-defined** | **user-defined** } *signature-id*

Default

Predefined IPS signatures use the actions and states defined by the system.

User-defined IPS signatures use the actions and states defined in the IPS signature file from which the signatures are imported.

Views

IPS policy view

Predefined user roles

network-admin

context-admin

Parameters

pre-defined: Specifies a predefined IPS signature.

user-defined: Specifies a user-defined IPS signature.

signature-id: Specifies an IPS signature ID. For a predefined IPS signature, the value range is 1 to 536870911. For a user-defined IPS signature, the value range is 536870913 to 1073741823.

disable: Disables the IPS signature.

enable: Enables the IPS signature.

block-source: Drops matching packets and adds the sources of the packets to the IP blacklist. If the IP blacklist feature is enabled, packets from the blacklisted sources will be blocked for a duration set by the **block-period** command. If the IP blacklist feature is not enabled, packets from the blacklisted sources are not blocked. For more information about the IP blacklist feature, see *Security Configuration Guide*. For information about configuring the block period, see "DPI engine commands."

drop: Drops matching packets.

permit: Permits matching packets to pass.

redirect: Redirects matching packets to a webpage.

reset: Closes the TCP connections for matching packets by sending TCP reset messages.

capture: Captures matching packets.

logging: Logs matching packets.

Usage guidelines

This command is available only for user-defined IPS policies. The signature actions and status in the default IPS policy cannot be modified.

If you execute this command for a signature in an IPS policy multiple times, the most recent configuration takes effect.

Examples

Enable predefined signature 2 for IPS policy **ips1**. Specify the **drop**, **capture**, and **logging** actions for the signature.

```
<Sysname> system-view
[Sysname] ips policy ips1
[Sysname-ips-policy-ips1] signature override pre-defined 2 enable drop capture logging
```

Related commands

blacklist enable (security zone view) (*Security Command Reference*)

blacklist global enable (*Security Command Reference*)

ips parameter-profile

ips policy

signature override all

signature override all

Use **signature override all** to specify the IPS actions for an IPS policy.

Use **undo signature override all** to restore the default.

Syntax

signature override all { { **block-source** | **drop** | **permit** | **redirect** | **reset** } | **capture** | **logging** } *

undo signature override all

Default

No actions are specified for an IPS policy and the default actions of IPS signatures are applied to matching packets.

Views

IPS policy view

Predefined user roles

network-admin

context-admin

Parameters

block-source: Drops matching packets and adds the sources of the packets to the IP blacklist. If the IP blacklist feature is enabled, packets from the blacklisted sources will be blocked for a duration set by the **block-period** command. If the IP blacklist feature is not enabled, packets from the blacklisted sources are not blocked. For more information about the IP blacklist feature, see *Security Configuration Guide*. For information about configuring the block period, see "DPI engine commands."

drop: Drops matching packets.

permit: Permits matching packets to pass.

redirect: Redirects matching packets to a webpage.

reset: Closes the TCP connections for matching packets by sending TCP reset messages.

capture: Captures matching packets.

logging: Logs matching packets.

Usage guidelines

Use this command to specify the global packet processing actions for an IPS policy.

Each IPS signature is defined with default actions for matching packets. You can change the default actions for individual signatures in an IPS policy.

The system selects the actions for packets matching an IPS signature in the following order:

1. Actions configured for the IPS signature in the IPS policy (by using the **signature override** command).
2. Actions configured for the IPS policy.
3. Default actions of the IPS signature.

Examples

Specify actions **drop**, **logging**, and **capture** for IPS policy **test**.

```
<Sysname> system-view
[Sysname] ips policy test
[Sysname-ips-policy-test] signature override all drop logging capture
```

Related commands

blacklist enable (security zone view) (*Security Command Reference*)

blacklist global enable (*Security Command Reference*)

ips parameter-profile

signature override

signature version-baseline

Use **signature version-baseline** to specify an IPS signature library baseline version.

Use **undo signature version-baseline** to restore the default.

Syntax

signature version-baseline *version-number*

undo signature version-baseline

Default

No IPS signature library baseline version is specified.

Views

IPS policy view

Predefined user roles

network-admin

context-admin

Parameters

version-number: Specifies an IPS signature library version number. To obtain the version number of the current version and the previous version, use the **display ips signature library** command. To obtain history signature library version numbers, access the signature database services on the company's website.

Usage guidelines

This command sets an IPS signature library version as the baseline version and enables the device to match packets only with the signatures in the baseline version. With this command, the device compares the current IPS signature library with the baseline signature library. If a signature is included in the current signature library but does not included in the baseline signature library, the device sets the signature to ineffective state. Signatures in ineffective state cannot match packets.

This command allows the device to match packets only with the signatures in the baseline version without rolling back the signature library to the baseline version.

To separately activate an ineffective signature after this command is used, perform the following tasks:

1. On the Web interface of the device, obtain the IDs of all ineffective signatures.
2. Use this command again to change the IPS signature library baseline version to the version that contains the signature.
3. Execute the **signature override** command to disable all signatures that were in ineffective state when the previous signature library baseline version was used, except the signature to be activated.

If you execute the **signature version-baseline** command multiple times, the most recent configuration takes effect.

Examples

In IPS policy test, set the signature library baseline version to 1.0.88.

```
<Sysname> system-view
[Sysname] ips policy test
[Sysname-ips-policy-test] signature version-baseline 1.0.88
```

Related commands

display ips signature library

signature-id

Use **signature-id** to add an IPS signature ID to an IPS whitelist entry.

Use **undo signature-id** to restore the default.

Syntax

signature-id *sig-id*

undo signature-id

Default

No signature ID exists in an IPS whitelist entry.

Views

IPS whitelist entry view

Predefined user roles

network-admin

context-admin

Parameters

sig-id: Specifies an IPS signature ID, in the range of 1 to 4294967294.

Usage guidelines

If false alarms exist in IPS logs, use this command to add an IPS signature ID to an IPS whitelist entry. The IPS signature ID is recorded in the IPS log. The device permits packets matching the IPS signatures on the IPS whitelist to pass through, reducing false alarms.

If both a signature ID and URL exist in the IPS whitelist entry, a packet matches the IPS whitelist entry only when both the signature ID and URL are matched.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Add IPS signature 936 to IPS whitelist entry 1.

```
<Sysname> system-view
[Sysname] ips whitelist 1
[Sysname-ips-whitelist-1] signature-id 936
```

Related commands

source-address (IPS whitelist entry view)

url

source-address (IPS whitelist entry view)

Use **source-address** to add a source IP address to an IPS whitelist entry.

Use **undo source-address** to restore the default.

Syntax

source-address { **ip** *ipv4-address* | **ipv6** *ipv6-address* }

undo source-address

Default

No source IP address exists in an IPS whitelist entry.

Views

IPS whitelist entry view

Predefined user roles

network-admin

context-admin

Parameters

ip *ipv4-address*: Specifies an IPv4 address.

ipv6 *ipv6-address*: Specifies an IPv6 address.

Usage guidelines

If false alarms exist in IPS logs, use this command to add a source IP address to an IPS whitelist entry. The source IP address is recorded in the IPS log. The device permits packets matching the source IP addresses on the IPS whitelist to pass through, reducing false alarms.

If an IPS whitelist entry contains a signature ID, URL, and source IP address, or two of them, a packet matches this entry only when it matches all configured criteria.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Add source IP address 192.168.0.1 to IPS whitelist entry 1.

```
<Sysname> system-view
[Sysname] ips whitelist 1
[Sysname-ips-whitelist-1] source-address ip 192.168.0.1
```

Related commands

signature-id
url

source-address (user-defined IPS signature rule view)

Use **source-address** to specify a source address filtering criterion in a user-defined IPS signature rule.

Use **undo source-address** to restore the default.

Syntax

source-address ip *ip-address*

undo source-address

Default

No source IP address exists.

Views

User-defined IPS signature rule view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies an IPv4 address. It is used to match the packet source IPv4 address.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

In rule 1 of user-defined IPS signature **mysignature**, specify the keyword type as the match pattern type and specify source IP address 10.1.1.1 as a filtering criterion.

```
<Sysname> system-view
[Sysname] ips signature user-defined name mysignature
[Sysname-ips-signature-mysignature] rule 1 l4-protocol tcp l5-protocol http pattern-type keyword
[Sysname-ips-signature-mysignature-rule-1] source-address ip 10.1.1.1
```

source-port

Use **source-port** to specify a source port filtering criterion in a user-defined signature rule.

Use **undo source-port** to restore the default.

Syntax

source-port *start-port* [**to** *end-port*]

undo source-port

Default

No source ports are specified as the filtering criteria in a user-defined signature rule.

Views

User-defined IPS signature rule view

Predefined user roles

network-admin

context-admin

Parameters

start-port: Specifies the start port number of a source port range, in the range of 1 to 65535.

to *end-port*: Specifies the end port number of a source port range, in the range of 1 to 65535. If you do not specify this option, only the start port number is specified.

Usage guidelines

The port numbers are used to match the source port numbers of the specified transport layer protocol.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

In rule 1 of user-defined IPS signature **mysignature**, specify the keyword type as the match pattern type and specify the source port range as 1 to 3550.

```
<Sysname> system-view
[Sysname] ips signature user-defined name mysignature
[Sysname-ips-signature-mysignature] rule 1 l4-protocol tcp l5-protocol http pattern-type keyword
[Sysname-ips-signature-mysignature-rule-1] source-port 1 to 3550
```

statistics signature-hit enable

Use **statistics signature-hit enable** to enable IPS signature hit counting.

Use **undo statistics signature-hit enable** to disable IPS signature hit counting.

Syntax

statistics signature-hit enable

undo statistics signature-hit enable

Default

IPS signature hit counting is disabled.

Views

IPS policy view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command enables the device to collect hit statistics for each IPS signature. You can view IPS signature hit statistics on the Web interface of the device.

Examples

Enable IPS signature hit counting in IPS policy **policy**.

```
<Sysname> system-view
[Sysname] ips policy policy
[Sysname-ips-policy-policy] statistics signature-hit enable
```

status

Use **status** to specify a default status criterion to filter IPS signatures in an IPS policy.

Use **undo status** to restore the default.

Syntax

status { **disabled** | **enabled** } *

undo status

Default

The default status attribute is not used for IPS signature filtering.

Views

IPS policy view

Predefined user roles

network-admin

context-admin

Parameters

disabled: Specifies the signatures that are not recommended in the IPS signature library by default.

enabled: Specifies the signatures that are recommended in the IPS signature library by default.

Usage guidelines

This command filters the IPS signatures that an IPS policy uses based on the default status attribute of the IPS signatures.

The default status of an IPS signature indicates whether or not the IPS signature is recommended in the IPS signature library by default.

- **Disabled IPS signatures**—Not recommended IPS signatures, which apply only to special scenarios and are not universally applied.
- **Enabled IPS signatures**—Recommended IPS signatures, which are universally applied.

You can specify both default states. The IPS policy uses an IPS signature if the IPS signature matches either of the configured default status criteria.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure IPS policy **policy** to use IPS signatures in **enabled** default status .

```
<Sysname> system-view
[Sysname] ips policy policy
[Sysname-ips-policy-policy] status enabled
```

trigger

Use **trigger** to create a detection trigger condition in a user-defined IPS signature rule.

Use **undo trigger** to delete a detection trigger condition from the user-defined IPS signature rule.

Syntax

trigger field *field-name* **include** { **hex** *hex-string* | **text** *text-string* } [**offset** *offset-value*] [**depth** *depth-value*]

undo trigger

Default

No detection trigger condition exists.

Views

User-defined IPS signature rule view

Predefined user roles

network-admin

context-admin

Parameters

field-name: Specifies a protocol field by its name, in a case-insensitive string. To view the names of supported protocol fields, enter a question mark (?) after the **field** keyword.

include: Matches contents that include the specified string.

hex *hex-string*: Specifies a case-sensitive hexadecimal string of 8 to 254 characters. Valid characters contain integers, and letters of A to F and a to f. An even number of characters are required, and enclose the characters with two vertical bars (|), for example |1234f5b6|.

text *text-string*: Specifies a case-insensitive text string of 3 to 255 characters.

offset *offset-value*: Specifies an offset in bytes after which the match operation starts, in the range of 1 to 65535. If you do not specify *offset-value* argument, the match operation starts from the beginning of the protocol field.

depth *depth-value*: Specifies the number of bytes to match, in the range of 3 to 65535. If you do not specify *depth-value* argument, the detection trigger condition detects the whole protocol field.

Usage guidelines

This command is available only for a user-defined signature rule of the keyword match pattern type. The device continues to compare a packet with detection items only after the packet matches the detection trigger condition in a rule. If a packet fails to match the detection trigger condition, the rule matching fails, and the detection items will not be compared.

In a signature rule of the keyword match pattern type, a detection trigger condition must be configured before detection item configuration.

If you delete the detection trigger condition, all detection items in the rule will also be deleted.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

In user-defined IPS signature **mysignature**, create rule 1 for TCP and HTTP protocols and specify the keyword match pattern type. Create a detection item in the rule to match packets whose **http.host** field includes **abc**. Specify the offset and depth as 10 bytes and 50 bytes, respectively.

```
<Sysname> system-view
[Sysname] ips signature user-defined name mysignature
[Sysname-ips-signature-mysignature] rule 1 l4-protocol tcp l5-protocol http pattern-type keyword
[Sysname-ips-signature-mysignature-rule-1] trigger field http.host include text abc offset 10 depth 50
```

update schedule

Use **update schedule** to schedule the time for automatic IPS signature library update.

Use **undo update schedule** to restore the default.

Syntax

update schedule { **daily** | **weekly** { **fri** | **mon** | **sat** | **sun** | **thu** | **tue** | **wed** } } **start-time** *time* **tingle** *minutes*

undo update schedule

Default

The device starts updating the IPS signature library at a random time between 01:00:00 and 03:00:00 every day.

Views

Automatic IPS signature library update configuration view

Predefined user roles

network-admin

context-admin

Parameters

daily: Updates the IPS signature library every day.

weekly: Updates the IPS signature library every week.

fri: Updates the IPS signature library every Friday.

mon: Updates the IPS signature library every Monday.

sat: Updates the IPS signature library every Saturday.

sun: Updates the IPS signature library every Sunday.

thu: Updates the IPS signature library every Thursday.

tue: Updates the IPS signature library every Tuesday.

wed: Updates the IPS signature library every Wednesday.

start-time *time*: Specifies the start time in the hh:mm:ss format. The value range is 00:00:00 to 23:59:59.

tingle *minutes*: Specifies the tolerance time in minutes. The value range is 0 to 120. An automatic library update will occur at a random time between the following time points:

- Start time minus half the tolerance time.
- Start time plus half the tolerance time.

Examples

Configure the device to automatically update the IPS signature library every Monday at a random time between 20:25:00 and 20:35:00.

```
<Sysname> system-view
[Sysname] ips signature auto-update
[Sysname-ips-autoupdate] update schedule weekly mon start-time 20:30:00 tingle 10
```

Related commands

ips signature auto-update

url

Use **url** to add a URL to an IPS whitelist entry.

Use **undo url** to restore the default.

Syntax

url match-type { **accurate** | **substring** } *url-text*

undo url

Default

No URL exists in an IPS whitelist entry.

Views

IPS whitelist entry view

Predefined user roles

network-admin

context-admin

Parameters

match-type: Specifies the match type.

accurate: Specifies the exact match. A match is found if the URL in the packet is exactly the same as the configured URL.

substring: Specifies the substring match. A match is found if the URL in the packet contains the configured URL.

url-text: Specifies a URL, a case-insensitive string of 3 to 460 characters.

Usage guidelines

If false alarms exist in IPS logs, use this command to add a URL to an IPS whitelist entry. The URL is recorded in the IPS log. The device permits packets matching the URLs on the IPS whitelist to pass through, reducing false alarms.

If both a signature ID and URL exist in the IPS whitelist entry, a packet matches the IPS whitelist entry only when both the signature ID and URL are matched.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Add URL **baidu.com** to IPS whitelist entry 1, and specify the exact match type as the match type.

```
<Sysname> system-view
[Sysname] ips whitelist 1
[Sysname-ips-whitelist-1] url match-type accurate baidu.com
```

Related commands

ips whitelist activate

signature-id

source-address (IPS whitelist entry view)

Contents

URL filtering commands

add

Use **add** to add a blacklist or whitelist rule to a URL filtering policy.

Use **undo add** to delete a blacklist or whitelist rule from a URL filtering policy.

Syntax

add { **blacklist** | **whitelist** } [*id*] **host** { **regex** *host-regex* | **text** *host-name* } [**uri** { **regex** *uri-regex* | **text** *uri-name* }]

undo add { **blacklist** | **whitelist** } { *id* | **all** }

Default

No blacklist or whitelist rules exist in a URL filtering policy.

Views

URL filtering policy view

Predefined user roles

network-admin

context-admin

Parameters

blacklist: Specifies the blacklist rule type.

whitelist: Specifies the whitelist rule type.

id: Specifies a rule ID. The value must be an integer in the range of 1 to 65535. The ID of a blacklist or whitelist rule must be unique among all rules of the same type. If you do not specify a rule ID, the system automatically assigns an available ID to the rule according to the largest rule ID *N* used on the device:

- If *N* is smaller than 65535, the smallest available ID that is larger than *N* is used.
- If *N* equals to 65535, the smallest available ID is used.

host: Matches the host field in the URL.

uri: Matches the URI field in the URL.

regex *regex*: Specifies a case-sensitive regular expression string pattern. The string can start with only letters, digits, or underscores (_), and it must contain a minimum of three consecutive non-wildcard characters.

- If the **host** keyword is specified, the string can contain 3 to 224 characters.
- If the **uri** keyword is specified, the string can contain 3 to 245 characters.

text *string*: Specifies a case-insensitive text string pattern, which must contain a minimum of three consecutive non-wildcard characters.

- If the **host** keyword is specified, the string can contain 3 to 224 characters. Valid characters are letters, digits, underscores (_), hyphens (-), colons (:), left square brackets ([), right square brackets (]), dots (.), and asterisk (*).
- If the **uri** keyword is specified, the string can contain 3 to 245 characters.

all: Specifies all rules of the specified type.

Usage guidelines

The device supports using URL-based whitelist and blacklist rules to filter HTTP packets. If the URL in an HTTP packet matches a blacklist rule, the packet is dropped. If the URL matches a whitelist rule, the packet is permitted to pass through.

Follow these guidelines when you use the asterisk character (*) in the text string pattern for hostname or URI matching:

- For hostname matching, the asterisk (*) can appear only at the beginning or end of the text string pattern as a wildcard character to match zero or more characters.
- For URI matching, the asterisk (*) can appear at the beginning or end of the text string pattern as a wildcard character to match zero or more characters, or appear in the middle as a non-wildcard character.

When you configure a regular expression in a blacklist or whitelist rule, follow these restrictions and guidelines:

- The regular expression pattern can contain a maximum of four branches. For example, **'abc(c|d|e|\x3D)'** is valid, and **'abc(c|onreset|onselect|onchange|style\x3D)'** is invalid.
- Nested braces are not allowed. For example, **'ab((abcs*?))'** is invalid.
- A branch cannot be specified after another branch. For example, **'ab(a|b)(c|d)^\\r\\n]+?'** is invalid.
- A minimum of four non-wildcard characters must exist before an asterisk (*) or question mark (?). For example, **'abc*'** is invalid and **'abcd*DoS\x2d\d{5}\x20\x2bxi\\r\\nJOIN'** is valid.

Examples

In URL filtering policy **news**, add a blacklist rule to match URLs with the host field starting with **games.com**.

```
<Sysname> system-view
[Sysname] url-filter policy news
[Sysname-url-filter-policy-news] add blacklist 1 host text games.com*
```

category action

Use **category action** to specify actions for a URL category.

Use **undo category** to remove the action setting from a URL category.

Syntax

category *category-name* **action** { **block-source** [**parameter-profile** *parameter-name*] | **drop** | **permit** | **redirect parameter-profile** *parameter-name* | **reset** } [**logging** [**parameter-profile** *parameter-name*]]

undo category *category-name*

Default

A URL category does not have any action specified.

Views

URL filtering policy view

Predefined user roles

network-admin

context-admin

Parameters

category-name: Specifies a URL category by its name, a case-insensitive string of 1 to 63 characters.

action: Specifies the action for the matching packets.

block-source: Drops matching packets and adds the sources of the packets to the IP blacklist. If the IP blacklist feature is enabled, packets from the blacklisted sources will be blocked for a duration set by the **block-period** command. If the IP blacklist feature is not enabled, packets from the blacklisted sources are not blocked. For more information about the IP blacklist feature, see *Security Configuration Guide*. For information about configuring the block period, see "DPI engine commands."

drop: Drops matching packets.

permit: Permits matching packets to pass.

redirect: Redirects matching packets to a webpage.

reset: Disconnects the TCP connection for matching packets.

logging: Logs matching packets.

parameter-profile *parameter-name*: Specifies a parameter profile by its name, a case-insensitive string of 1 to 63 characters. If you do not specify a profile, or if the specified profile does not exist, the URL filtering action uses the default parameter settings. For information about configuring parameter profiles, see "DPI engine commands."

Usage guidelines

If an HTTP packet matches a URL filtering rule in a URL category, the action specified for the category applies to the packet.

If the packet matches none of URL filtering rules in the URL filtering policy, the default action specified for the policy applies to the packet. If the default action is not configured, the device permits the packet to pass.

If you execute this command for a URL category multiple times, the most recent configuration takes effect.

Examples

In the URL filtering policy **news**, specify the **drop** action for the URL category **sina**.

```
<Sysname> system-view
[Sysname] url-filter policy news
[Sysname-url-filter-policy-news] category sina action drop
```

Related commands

inspect block-source parameter-profile

inspect redirect parameter-profile

url-filter category

url-filter policy

cloud-query enable

Use **cloud-query enable** to enable cloud query for URL filtering.

Use **undo cloud-query enable** to disable cloud query for URL filtering.

Syntax

cloud-query enable

undo cloud-query enable

Default

URL filtering cloud query is disabled.

Views

URL filtering policy view

Predefined user roles

network-admin

context-admin

Usage guidelines

With cloud query enabled in a URL filtering policy, URLs that do not match any URL filtering rules in the policy are sent to the cloud server for further query. The device determines the actions for an HTTP packet based on the URL query results returned from the cloud server:

- If a matching rule is found, the rule and the name of URL category to which the rule belongs are returned. The device executes the actions specified for the URL category. If no actions are specified for the URL category, the default action of the policy is executed.
- If no matching rule is found, the device executes the default action of the policy.

Examples

Enable URL filtering cloud query in URL filtering policy **news**.

```
<Sysname> system-view
[Sysname] url-filter policy news
[Sysname-url-filter-policy-news] cloud-query enable
```

Related commands

url-filter policy

default-action

Use **default-action** to specify the default action for a URL filtering policy.

Use **undo default-action** to restore the default.

Syntax

default-action { **block-source** [**parameter-profile** *parameter-name*] | **drop** | **permit** | **redirect parameter-profile** *parameter-name* | **reset** } [**logging** [**parameter-profile** *parameter-name*]]

undo default-action

Default

A URL filtering policy does not have any default action.

Views

URL filtering policy view

Predefined user roles

network-admin

context-admin

Parameters

block-source: Drops matching packets and adds the sources of the packets to the IP blacklist. If the IP blacklist feature is enabled, packets from the blacklisted sources will be blocked for a duration set by the **block-period** command. For more information about the IP blacklist feature, see *Security Configuration Guide*. For information about configuring the block period, see "DPI engine commands."

drop: Drops matching packets.

permit: Permits packets to pass.

redirect: Redirects matching packets to a webpage.

reset: Disconnects the TCP connection for matching packets.

logging: Logs matching packets.

parameter-profile *parameter-name*: Specifies a DPI action parameter profile by its name, a case-insensitive string of 1 to 63 characters. If you do not specify a profile, or if the specified profile does not exist, the DPI action uses the default parameter settings. For information about configuring parameter profiles for DPI actions, see "DPI engine commands."

Usage guidelines

The default action applies to packets that do not match any URL filtering rules.

Examples

Set the default action to **drop** for URL filtering policy **cmcc**.

```
<Sysname> system-view
[Sysname] url-filter policy cmcc
[Sysname-url-filter-policy-cmcc] default-action drop
```

Related commands

inspect block-source parameter-profile

inspect redirect parameter-profile

url-filter policy

description

Use **description** to configure a description for a URL category.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

A user-defined URL category does not have a description.

Views

URL category view

Predefined user roles

network-admin

context-admin

Parameters

text: Specifies a description, a case-insensitive string of 1 to 255 characters. Spaces are allowed.

Usage guidelines

Use this command to configure descriptions for URL categories for easy maintenance.

Examples

Configure the description as **News information** for URL category **news**.

```
<Sysname> system-view
[Sysname] url-filter category news
[Sysname-url-filter-category-news] description News information
```

display url-filter cache

Use **display url-filter cache** to display URL filtering cache information.

Syntax

display url-filter cache [**category** *category-name*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

category *category-name*: Specify a URL category by its name, a case-insensitive string of 1 to 63 characters.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all member devices.

Usage guidelines

This command displays the cached entries in the URL filtering cache and the cloud query information.

Examples

Display all URL filtering rules in the URL filtering cache.

```
<Sysname> display url-filter cache
Slot 1 :
Url-filter cache information:
Cloud-query status: Enabled
Total cached entries: 35
Min update interval: 906 seconds
Max update interval: 46760 seconds
Last query message sent: 906 seconds ago
Last query result received: 906 seconds ago
```

Slot 1 :

```
Url-filter cache verbose:
Host: 192.168.56.99
URI: /wnm/get.j?sessionid=200001a5de59aebeb0877f982e5c31f58728
Hit count: 15
Time elapsed since last update: 906 seconds
Category ID: 152
Cache query state: Query ended
```

Table 1 Command output

Field	Description
Url_filter cache information	URL filtering cache information.
Cloud-query status	Whether cloud query is enabled or disabled.
Total cached entries	Total number of cached URL entries.
Min update interval	Minimum interval that a cached entry was updated, in seconds.
Max update interval	Maximum interval that a cached entry was updated, in seconds.
Last query message sent	Number of seconds elapsed since the last query message was sent.
Last query result received	Number of seconds elapsed since the last query result was received.
Url-filter cache verbose	Detailed information about a cached URL entry.
Host	Host field of the cached URL.
URI	URI field of the cached URL.
Hit count	Number of times the URL filtering rule has been matched.
Time elapsed since last update	Number of seconds elapsed since the cached entry was last updated.
Category ID	ID of the URL category to which the matching URL filtering rule belongs. This field is empty if no matching URL filtering rule is found for the URL. If the matching URL filtering rule belongs to multiple URL categories, the URL category IDs are displayed in a space-separated list.
Cache query state	Query state of the URL: • **In the cloud query**—Cloud query is in progress. • **Query end**—Cloud query is completed.

Related commands

`url-filter category`

display url-filter category

Use **`display url-filter category`** to display URL category information.

Syntax

`display url-filter` { **`category`** | **`parent-category`** } [**`verbose`**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

`category`: Specifies child URL categories.

`parent-category`: Specifies parent URL categories.

`verbose`: Display detailed URL category information. If you do not specify this keyword, this command displays the summarized URL category information.

Usage guidelines

The device supports two levels of predefined URL categories: child URL category and parent URL category. A predefined parent URL category contains only predefined child URL categories.

Examples

Display information about child URL categories.

```
<Sysname> display url-filter category
URL category statistics:
  Predefined categories: 53
  Predefined rules: 2000
  User-defined categories: 5
  User-defined rules: 4

URL categories:
  Name : 23
  Name : 24
  Name : 33
  Name : Pre-AdvertisementsAndPop-Ups
  Name : Pre-AlcoholAndTobacco
  Name : Pre-Anonymizers
  Name : Pre-Arts
  Name : Pre-Business
  Name : Pre-Chat
  Name : Pre-ComputersAndTechnology
  Name : Pre-CriminalActivity
  Name : Pre-Cults
  Name : Pre-DatingAndPersonals
  Name : Pre-DownloadSites
  Name : Pre-Education
  Name : Pre-Entertainment
  Name : Pre-FashionAndBeauty
…
```

Display detailed information about child URL categories.

```
<Sysname> display url-filter category verbose
URL category statistics:
  Predefined categories: 53
```

```
  Predefined rules: 2000
  User-defined categories: 5
  User-defined rules: 4

URL category details:
  Name: 23
  Type: User defined
  Severity: 1001
  Rules: 1
  Description:
  Name: 24
  Type: User defined
  Severity: 1002
  Rules: 1
  Description:
  Name: Pre-AdvertisementsAndPop-Ups
  Type: Predefined
  Severity: 300
  Rules: 32
  Description: Sites that provide advertising graphics or other ad content fi
               les such as banners and pop-ups.
  Name: Pre-AlcoholAndTobacco
  Type: Predefined
  Severity: 960
  Rules: 7
  Description: Sites that promote or sell alcohol- or tobacco-related product
                 s or services.
…
```

Table 2 Command output

Field	Description
Predefined categories	Number of predefined child URL categories.
Predefined rules	Number of predefined URL filtering rules.
User-defined categories	Number of user-defined child URL categories.
User-defined rules	Number of user-defined URL filtering rules.
URL category details	Detailed information about the child URL categories.
Name	Name of the child URL category.
Type	Type of the child URL category, **Predefined** or **User Defined**.
Severity	Severity level of the child URL category.
Rules	Number of rules in the child URL category.

Display information about parent URL categories.

```
<Sysname> display url-filter parent-category
URL parent category statistics:
  Predefined parent categories: 40
  Included predefined categories: 14
```

```
URL parent categories:
  Parent category name: SearchEngineAndPortal
  Parent category name: P2PAndDownload
  Parent category name: OrdinaryDownload
  Parent category name: House
  Parent category name: EducationAndScientificResearch
  Parent category name: Finance
  Parent category name: StreamMediaAndVideo
  Parent category name: Shopping
  Parent category name: TransportationVehicle
  Parent category name: Travel

…
```

Display detailed information about parent URL categories.

```
<Sysname> display url-filter parent-category verbose
URL parent category statistics:
  Predefined parent categories: 46
  Included predefined categories: 139
URL parent category details:
  Parent category name: Pre-Adult
  Type: Predefined
  Description: Adult
  Included categories: 7
    Pre-Abortion
    Pre-AdultSuppliers
    Pre-Homosexual
    Pre-Nudity
    Pre-OtherAdult
    Pre-SexualHealth
    Pre-Vulgar
  Parent category name: Pre-Arts
  Type: Predefined
  Description: Arts
  Included categories: 1
    Pre-Arts
…
```

Table 3 Command output

Field	Description
Predefined parent categories	Number of predefined parent URL categories.
Included predefined categories	Total number of predefined URL categories included in all parent URL categories.
URL parent category details	Detailed information about the parent URL categories.
Parent category name	Name of the parent URL category.
Type	Type of the parent URL category. The device supports only predefined parent URL categories.
Description	Description of the parent URL category.

Field	Description
Included categories	Number of child URL categories in the parent URL category.

display url-filter signature library

Use **display url-filter signature library information** to display information about the URL signature library.

Syntax

display url-filter signature library

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display information about the URL signature library.

```
<Sysname> display url-filter signature library
URL filter signature library information:
Type      SigVersion         ReleaseTime               Size
Current   1.0.0              Wed Jan 21 06:43:53 2015  36096
(null)    -                  -                         -
Factory   1.0.0              Wed Jan 21 06:43:53 2015  36096
```

Table 4 Command output

Field	Description
Type	Version of the URL signature library: • **Current**—Current version. • **Last**—Previous version. • **Factory**—Factory default version.
SigVersion	Version number.
ReleaseTime	Time when the URL signature library was released.
Size	Size of the URL signature library, in bytes.

display url-filter statistics

Use **display url-filter statistics** to display URL filtering statistics.

Syntax

display url-filter statistics

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display URL filtering statistics.

```
<Sysname> display url-filter statistics
-------------------------------------------------------
Slot 1 :
Total HTTP requests                         : 0
Total HTTPS handshakes                      : 0
Total logged requests                       : 0
Total logging rate                          : 0/s
Total permitted requests and handshakes     : 0
Total denied requests                       : 0
Requests that matched the blacklist         : 0
Requests that matched the whitelist         : 0
Requests that matched the referer-whitelist : 0
Requests that matched a user-defined rule   : 0
Requests that matched a predefined rule     : 0
Requests that matched a cached rule         : 0
Requests that matched the default action    : 0
Predefined URL filtering rules              : 2000
-------------------------------------------------------
```

Table 5 Command output

Field	Description
Total HTTP requests	Total number of HTTP packets.
Total HTTPS handshakes	Total number of encrypted traffic hits.
Total logged HTTP requests	Total number of logged HTTP packets.
Total HTTP logging rate	Logging rate for HTTP packets.
Total permitted HTTP requests	Total number of permitted HTTP packets.
Total denied HTTP requests	Total number of denied HTTP packets.
Requests that matched the blacklist	Number of HTTP packets that matched a blacklist rule.
Requests that matched the whitelist	Number of HTTP packets that matched a whitelist rule.
Requests that matched the referer-whitelist	Number of HTTP packets with a referer header that matched a whitelist rule.
Requests that matched a user-defined rule	Number of HTTP packets that matched a user-defined URL filtering rule.
Requests that matched a predefined rule	Number of HTTP packets that matched a predefined URL filtering rule.
Requests that matched a cached rule	Number of HTTP packets that matched a cached URL filtering rule.

Field	Description
Requests that matched the default action	Number of HTTP packets on which the default action is executed.
Predefined URL filtering rules	Total number of predefined URL filtering rules.

https-filter enable

Use **`https-filter enable`** to enable HTTPS URL filtering.

Use **`undo https-filter enable`** to disable HTTPS URL filtering.

Syntax

`https-filter enable`

`undo https-filter enable`

Default

HTTPS URL filtering is disabled.

Views

URL filtering policy view

Predefined user roles

network-admin

context-admin

Usage guidelines

By default, the device supports only the HTTP URL filtering. To enable filtering on HTTPS traffic, use either of the following methods:

- Use SSL decryption to decrypt the HTTPS traffic and then perform HTTP URL filtering on the decrypted traffic. For more information about SSL decryption, see proxy policy configuration in *DPI Configuration Guide*.

  SSL decryption involves a large number of encryption and decryption operations, which might downgrade device forwarding performance. As a best practice, use this method only when the device must perform URL filtering on HTTPS traffic.
- Enable HTTPS URL filtering. This feature performs URL filtering on undecrypted HTTPS traffic. The device directly detects the Client Hello message from the client, and extracts the server name from the Sever Name Indication (SNI) extension to match the URL filtering policy.

If SSL decryption is configured, this command does not take effect. For more information about SSL decryption, see proxy policy configuration in *DPI Configuration Guide*.

In HTTPS URL filtering, only the hostname match criterion in a URL filtering rule takes effect. The URI match criterion does not take effect.

This feature takes effect only when the hostname field in the URL is the server's domain name. This feature does not apply to the HTTPS traffic if the hostname field is an IP address.

This feature does not take effect in the following situations:

- The client browser enables TLS 1.3 downgrade enhancement mechanism, because the SNI extension will be encrypted.
- The HTTPS packets do not have the SNI extension.

Examples

Enable HTTPS URL filtering in URL filtering policy **news**.

```
<Sysname> system-view
[Sysname] url-filter policy news
[Sysname-url-filter-policy-news] https-filter enable
```

Related commands

action ssl-decrypt

include pre-defined

Use **include pre-defined** to add the URL filtering rules of a predefined URL category to a user-defined URL category.

Use **undo include pre-defined** to restore the default.

Syntax

include pre-defined *category-name*

undo include pre-defined

Default

A user-defined URL category does not contain the URL filtering rules of any predefined URL category.

Views

URL category view

Predefined user roles

network-admin

context-admin

Parameters

category-name: Specifies a predefined URL category by its name, a case-sensitive string of 1 to 63 characters. The specified URL category must exist on the device.

Usage guidelines

To simplify URL category configuration, you can use this command to add the URL filtering rules of a predefined URL category to a user-defined URL category.

You can add URL filtering rules of only one predefined URL category to a user-defined URL category. If you execute this command for a URL category multiple times, the most recent configuration takes effect.

Examples

Add the URL filtering rules of predefined URL category **Pre-Arts** to URL category **news**.

```
<Sysname> system-view
[Sysname] url-filter category news
[Sysname-url-filter-category-news] include pre-defined Pre-Arts
```

referer-whitelist enable

Use **referer-whitelist enable** to enable referer whitelist.

Use **undo referer-white enable** to disable referer whitelist.

Syntax

referer-whitelist enable

undo referer-whitelist enable

Default

Referer whitelist is enabled.

Views

URL filtering policy view

Predefined user roles

network-admin

context-admin

Usage guidelines

The referer whitelist is useful when you want to allow users to access links on the webpages that match the whitelist rules.

If this feature is disabled, the users can visit a webpage when the URL of the webpage matches a whitelist rule, but other links on the accessed webpage are inaccessible. To solve the preceding problem, you can enable this feature. It allows the device to extract the referer header of an HTTP or HTTPS request and compare the referer header with whitelist rules. If a match is found, the device permits the HTTP or HTTPS request to pass through. If no match is found, the device drops the HTTP or HTTPS request.

Examples

Enable referer whitelist in URL filtering policy **news**.

```
<Sysname> system-view
[Sysname] url-filter policy news
[Sysname-url-filter-policy-news] referer-whitelist enable
```

Related commands

add

rename (URL category view)

Use **rename** to rename a URL category.

Syntax

rename *new-name*

Views

URL category view

Predefined user roles

network-admin

context-admin

Parameters

new-name: Specify a new name for the URL category, a case-insensitive string of 1 to 63 characters.

Usage guidelines

If you change the name for a URL category that is used by a URL filtering policy, the URL category name in the policy is also changed.

Examples

Rename URL category **news** to **hello**, and enter the view of URL category **hello**.

```
<Sysname> system-view
[Sysname] url-filter category news
[Sysname-url-filter-category-news] rename hello
[Sysname-url-filter-category-hello]
```

rename (URL filtering policy view)

Use **rename** to rename a URL filtering policy.

Syntax

rename *new-name*

Views

URL filtering policy view

Predefined user roles

network-admin

context-admin

Parameters

new-name: Specify a new name for the URL filtering policy, a case-insensitive string of 1 to 31 characters.

Usage guidelines

If you change the name of a URL filtering policy that has been assigned to a DPI application profile, the policy name in the DPI application profile is also changed.

Examples

Rename URL filtering policy **news** to **hello**, and enter the view of URL filtering policy **hello**.

```
<Sysname> system-view
[Sysname] url-filter policy news
[Sysname-url-filter-policy-news] rename hello
[Sysname-url-filter-policy-hello]
```

reset url-filter statistics

Use **reset url-filter statistics** to clear URL filtering statistics.

Syntax

reset url-filter statistics

Views

User view

Predefined user roles

network-admin

context-admin

Examples

Clear URL filtering statistics.

```
<Sysname> reset url-filter statistics
```

Related commands

display url-filter statistics

rule

Use **rule** to create a URL filtering rule for a user-defined URL category.

Use **undo rule** to delete a URL filtering rule from a user-defined URL category.

Syntax

rule *rule-id* **host** { **regex** *regex* | **text** *string* } [**uri** { **regex** *regex* | **text** *string* }]

undo rule *rule-id*

Default

A user-defined URL category does not have any URL filtering rules.

Views

URL category view

Predefined user roles

network-admin

context-admin

Parameters

rule-id: Assigns an ID to the URL filtering rule, in the range of 1 to 65535.

host: Matches URLs by the hostname field.

uri: Matches URLs by the URI field.

regex *regular-expression*: Specifies a case-sensitive regular expression string pattern. The string can start with only letters, digits, or underscores (_), and it must contain a minimum of three consecutive non-wildcard characters.

- If the **host** keyword is specified, the string can contain 3 to 224 characters.
- If the **uri** keyword is specified, the string can contain 3 to 253 characters.

text *string*: Specifies a case-insensitive text string pattern, which must contain a minimum of three consecutive non-wildcard characters.

- If the **host** keyword is specified, the string can contain 3 to 224 characters. Valid characters are letters, digits, underscores (_), hyphens (-), colons (:), left square brackets ([), right square brackets (]), dots (.), and asterisk (*).
- If the **uri** keyword is specified, the string can contain 3 to 255 characters.

Usage guidelines

A URL filtering rule supports the following URL matching methods:

- **Text-based matching**—Matches the hostname and URI fields of a URL against text string patterns.

  When performing text-based matching for the hostname field of a URL, the device first determines if the text string pattern contains the asterisk (*) wildcard character at the beginning or end.

- If the text string pattern does not contain the asterisk (*) wildcard character at the beginning or end, the hostname matching succeeds if the hostname of the URL matches the text string pattern.
- If the text string pattern contains the asterisk (*) wildcard character at the beginning, the hostname matching succeeds if the hostname of the URL matches or ends with the text string pattern without the wildcard character.
- If the text string pattern contains the asterisk (*) wildcard character at the end, the hostname matching succeeds if the hostname of the URL matches or starts with the text string pattern without the wildcard character.
- If the text string pattern contains the asterisk (*) wildcard character at both the beginning and the end, the hostname matching succeeds if the hostname of the URL matches or includes the text string pattern without the wildcard characters.

Text-based matching for the URI field works in the same way that text-based matching for the hostname field works.

- **Regular expression-based matching**—Matches the hostname and URI fields of a URL against regular expressions. For example, if you set the regular expression for hostname matching to **sina.*cn**, URLs that carry the **news.sina.com.cn** hostname will be matched.

Follow these guidelines when you use the asterisk character (*) in the text string for hostname or URI matching:

- For hostname matching, the asterisk (*) can appear only at the beginning or end of the text string as a wildcard character to match zero or more characters.
- For URI matching, the asterisk (*) can appear at the beginning or end of the text string pattern as a wildcard character to match zero or more characters, or appear in the middle as a non-wildcard character.

When you configure a regular expression in a URL filtering rule, follow these restrictions and guidelines:

- The regular expression pattern can contain a maximum of four branches. For example, **'abc(c|d|e|\x3D)'** is valid, and **'abc(c|onreset|onselect|onchange|style\x3D)'** is invalid.
- Nested braces are not allowed. For example, **'ab((abcs*?))'** is invalid.
- A branch cannot be specified after another branch. For example, **'ab(a|b)(c|d)^\\r\\n]+?'** is invalid.
- A minimum of four non-wildcard characters must exist before an asterisk (*) or question mark (?). For example, **'abc*'** is invalid and **'abcd*DoS\x2d\d{5}\x20\x2bxi\\r\\nJOIN'** is valid.

Examples

In URL category **news**, create a URL filtering rule to match URLs with the host field starting with **sina.com**.

```
<Sysname> system-view
[Sysname] url-filter category news
[Sysname-url-filter-category-news] rule 10 host text sina.com*
```

Related commands

url-filter category

update schedule (automatic URL signature library update configuration view)

Use **update schedule** to configure a schedule for automatic URL signature library update.

Use **undo update schedule** to restore the default.

Syntax

update schedule { **daily** | **weekly** { **fri** | **mon** | **sat** | **sun** | **thu** | **tue** | **wed** } } **start-time** *time* **tingle** *minutes*

undo update schedule

Default

The device starts the URL signature library update at a random time between 01:00:00 and 03:00:00 every day.

Views

Automatic URL signature library update configuration view

Predefined user roles

network-admin

context-admin

Parameters

daily: Updates the URL signature library every day.

weekly: Updates the URL signature library every week.

fri: Updates the URL signature library every Friday.

mon: Updates the URL signature library every Monday.

sat: Updates the URL signature library every Saturday.

sun: Updates the URL signature library every Sunday.

thu: Updates the URL signature library every Thursday.

tue: Updates the URL signature library every Tuesday.

wed: Updates the URL signature library every Wednesday.

start-time *time*: Specifies the start time in hh:mm:ss format. The value range is 00:00:00 to 23:59:59.

tingle *minutes*: Specifies the tolerance time in minutes. The value range is 0 to 120. An automatic library update will occur at a random time between the following time points:

- Start time minus half the tolerance time.
- Start time plus half the tolerance time.

Examples

Configure the device to automatically update the URL signature library every Sunday at a random time between 20:25:00 and 20:35:00.

```
<Sysname> system-view
[Sysname] url-filter signature auto-update
[Sysname-url-filter-autoupdate] update schedule weekly sun start-time 20:30:00 tingle 10
```

Related commands

url-filter signatures auto-update

url-filter apply policy

Use **url-filter apply policy** to apply a URL filtering policy to a DPI application profile.

Use **undo url-filter apply policy** to remove the URL filtering policy from a DPI application profile.

Syntax

url-filter apply policy *policy-name*

undo url-filter apply policy

Default

No URL filtering policy is applied to a DPI application profile.

Views

DPI application profile view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies a URL filtering policy by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

A URL filtering policy takes effect only after it is applied to a DPI application profile.

You can apply only one URL filtering policy to a DPI application profile. If you execute this command multiple times, the most recent configuration takes effect.

Examples

Apply URL filtering policy **news** to DPI application profile **abc**.

```
<Sysname> system-view
[Sysname] app-profile abc
[Sysname-app-profile-abc] url-filter apply policy news
```

Related commands

app-profile

display app-profile

display url-filter policy

url-filter cache size

Use **url-filter cache size** to set the URL filtering cache size.

Use **undo url-filter cache size** to restore the default.

Syntax

url-filter cache size *cache-size*

undo url-filter cache size

Default

The URL filtering cache can cache a maximum of 16384 URL entries.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

cache-size: Specifies the cache size in the range of 8192 to 65535.

Usage guidelines

The device caches the URL filtering rules and categories returned from the cloud server. The cached rules can be used directly for subsequent URL filtering.

This command is supported only on the default context. For more information about contexts, see context configuration in *Virtual Technologies Configuration Guide*.

Examples

Set the URL filtering cache size to 20000.

```
<Sysname> system-view
[Sysname] url-filter cache size 20000
```

url-filter cache-time

Use **url-filter cache-time** to set the minimum cache time for a URL filtering rule.

Use **undo url-filter cache-time** to restore the default.

Syntax

url-filter cache-time *value*

undo url-filter cache-time

Default

The minimum cache time of a URL filtering rule is 10 minutes.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

value: Specifies the minimum cache time in minutes. The value range is 10 to 720.

Usage guidelines

Setting the minimum cache time for URL filtering rules ensures that the cached rules will not be deleted during the specified period of time.

When the URL filtering cache is full, the system identifies the cache time of the oldest URL filtering rule to determine whether to overwrite it:

- If the cache time of the rule is equal to or less than the minimum cache time, the system does not delete the rule. The new rule is not cached.
- If the cache time of the rule is greater than the minimum cache time, the system overwrites the rule with the new rule.

This command is supported only on the default context. For more information about contexts, see context configuration in *Virtual Technologies Configuration Guide*.

Examples

Set the minimum cache time to 36 minutes for URL filtering rules.

```
<Sysname> system-view
[Sysname] url-filter cache-time 36
```

url-filter category

Use **url-filter category** to create a user-defined URL category and enter its view, or enter the view of an existing URL category.

Use **undo url-filter category** to delete a URL category.

Syntax

url-filter category *category-name* [**severity** *severity-level*]

undo url-filter category *category-name*

Default

The device has only predefined URL categories with the name prefix **Pre-**.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

category-name: Specify the URL category name, a case-insensitive string of 1 to 63 characters. Valid characters are letters, digits, underscores (_), hyphens (-), and dots (.). The category name cannot start with **Pre-**.

severity *severity-value*: Specifies a severity level for the URL category. The value range is 1000 to 65535, and the default is 65535. The larger the value, the higher the severity level. The severity level of each user-defined URL category must be unique. This option is required when you create a URL category.

Usage guidelines

URL filtering provides the URL categorization feature to facilitate filtering rule management.

You can classify multiple URL filtering rules into a URL category and specify an action for the category. If a matching rule is in multiple URL categories, the system takes the action for the category with the highest severity level.

URL filtering supports the following types of URL categories:

- Predefined URL categories.

  The predefined URL categories contain the predefined URL filtering rules. Each predefined URL category has a unique severity level in the range of 1 to 999, and a category name that begins with **Pre**-. Predefined URL categories cannot be modified.

- User-defined URL categories.

  You can create user-defined URL categories and configure filtering rules for them. The severity level of a user-defined URL category is in the range of 1000 to 65535. You can edit the filtering rules and change the severity level for a user-defined URL category.

Examples

Create a URL category named **news** and set its severity level to 2000.

```
<Sysname> system-view
[Sysname] url-filter category news severity 2000
```

```
[Sysname-url-filter-category-news]
```

Related commands

display url-filter category

url-filter copy category

Use **url-filter copy policy** to copy a URL category.

Syntax

url-filter copy category *old-name new-name* **severity** *severity-level*

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

old-name: Specifies the name of the URL category to be copied. The specified URL category must already exist.

new-name: Specifies a name for the new URL category. The name is a case-insensitive string of 1 to 63 characters and cannot begin with **Pre**.

severity *severity-level*: Assigns a unique severity level to the new URL category. The value range is 1000 to 65535. The larger the value, the higher the severity level.

Usage guidelines

This command allows you to create a new URL category by copying an existing one.

The device supports copying only user-defined URL categories.

Examples

Create URL category **test** by copying URL category **news**.

```
<Sysname> system-view
[Sysname] url-filter copy category news test severity 1001
[Sysname-url-filter-category-test]
```

Related commands

url-filter category

url-filter copy policy

Use **url-filter copy policy** to copy a URL filtering policy.

Syntax

url-filter copy policy *old-name new-name*

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

old-name: Specifies the name of the URL filtering policy to be copied, a case-insensitive string of 1 to 31 characters.

new-name: Specifies a name for the new URL filtering policy, a case-insensitive string of 1 to 31 characters.

Usage guidelines

This command allows you to create a new URL filtering policy by copying an existing one.

Examples

Create two URL filtering policies by copying URL filtering policy **news**.

```
<Sysname> system-view
[Sysname] url-filter copy policy news news1
[Sysname-url-filter-policy-news_1] quit
[Sysname] url-filter copy policy news new2
[Sysname-url-filter-policy-news_2] quit
```

Related commands

url-filter policy

url-filter log directory root

Use **url-filter log directory root** to configure URL filtering to log only access to resources in the root directories of websites.

Use **undo url-filter log directory root** to restore the default.

Syntax

url-filter log directory root

undo url-filter log directory root

Default

URL filtering logs access to Web resources in all directories.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

After this command is configured, the **url-filter log except pre-defined** and **url-filter log except user-defined** commands become invalid.

Examples

Configure URL filtering to log only access to resources in the root directories of websites.

```
<Sysname> system-view
[Sysname] url-filter log directory root
```

Related commands

category action logging

default-action logging

url-filter log except pre-defined

url-filter log except user-defined

url-filter log enable

Use **url-filter log enable** to enable DPI engine logging.

Use **undo url-filter log enable** to disable DPI engine logging.

Syntax

url-filter log enable

undo url-filter log enable

Default

DPI engine logging is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

You can enable DPI engine logging for audit. Log messages generated by DPI engine are output to the device information center. The information center then sends the messages to designated destinations based on log output rules. For more information about the information center, see *Network Management and Monitoring Configuration Guide*.

DPI engine logging is memory intensive. To guarantee system performance, enable DPI engine logging only when necessary.

Examples

Enable DPI engine logging.

```
<Sysname> system-view
[Sysname] url-filter log enable
```

url-filter log except pre-defined

Use **url-filter log except pre-defined** to disable URL filtering logging for access to resources of a predefined resource type.

Use **undo url-filter log except pre-defined** to enable URL filtering logging for access to resources of a predefined resource type.

Syntax

url-filter log except pre-defined { **css** | **gif** | **ico** | **jpg** | **js** | **png** | **swf** | **xml** }

undo url-filter log except pre-defined { **css** | **gif** | **ico** | **jpg** | **js** | **png** | **swf** | **xml** }

Default

URL filtering does not log access to resources of the predefined resource types (CSS, GIF, ICO, JPG, JS, PNG, SWF, and XML resources).

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

`css`: Specifies the CSS resource type.

`gif`: Specifies the GIF resource type.

`ico`: Specifies the ICO resource type.

`jpg`: Specifies the JPG resource type.

`js`: Specifies the JS resource type.

`png`: Specifies the PNG resource type.

`swf`: Specifies the SWF resource type.

`xml`: Specifies the XML resource type.

Usage guidelines

Repeat this command to disable URL filtering logging for access to multiple types of predefined resources.

This command does not take effect if the **`url-filter log directory root`** command is configured. To validate this command, you must execute **`undo url-filter log directory root`** command.

Examples

Disable URL filtering logging for access to CSS resources.

```
<Sysname> system-view
[Sysname] url-filter log except pre-defined css
```

Related commands

`category action logging`

`default-action logging`

`url-filter log directory root`

`url-filter log except user-defined`

url-filter log except user-defined

Use **`url-filter log except user-defined`** to disable URL filtering logging for access to resources of a user-defined resource type.

Use **`undo url-filter log except user-defined`** to enable URL filtering logging for access to resources of a user-defined resource type.

Syntax

`url-filter log except user-defined` *`text`*

undo url-filter log except user-defined [*text*]

Default

URL filtering logs access to all resources except for resources of the predefined types.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

text: Specifies a Web resource type. The value is a case-insensitive string of 1 to 63 characters.

Usage guidelines

Repeat this command to disable URL logging for access to multiple types of user-defined resources.

This command does not take effect if the **url-filter log directory root** command is configured. To validate this command, you must execute **undo url-filter log directory root** command.

Executing the **undo url-filter log except user-defined** command without the *text* parameter enables URL logging for access to all resources except resources of the predefined resource types.

Examples

Disable URL filtering logging for access to HTML resources.

```
<Sysname> system-view
[Sysname] url-filter log except user-defined html
```

Related commands

category action logging

default-action logging

url-filter log directory root

url-filter log except pre-defined

url-filter policy

Use **url-filter policy** to create a URL filtering policy and enter its view, or enter the view of an existing URL filtering policy.

Use **undo url-filter policy** to delete a URL filtering policy.

Syntax

url-filter policy *policy-name*

undo url-filter policy *policy-name*

Default

No URL filtering policies exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Assigns a name to the URL filtering policy, a case-insensitive string of 1 to 31 characters.

Usage guidelines

In a URL filtering policy, you can specify an action for each URL category. You can also use the **default action** command to specify the default action for packets that do not match any URL filtering rules in the policy.

A URL filtering policy takes effect only after it is applied to a DPI application profile. For information about DPI application profiles, see *DPI Configuration Guide*.

Examples

Create a URL filtering policy named **news** and enter its view.

```
<Sysname> system-view
[Sysname] url-filter policy news
[Sysname-url-filter-policy-news]
```

url-filter signature auto-update

Use **url-filter signature auto-update** to enable automatic URL signature library update and enter automatic URL signature library update configuration view.

Use **undo url-filter signature auto-update** to disable automatic URL signature library update.

Syntax

url-filter signature auto-update

undo url-filter signature auto-update

Default

Automatic URL signature library update is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

The automatic update enables the device to periodically access the company's website to download the latest URL filtering signatures and update the local signature library.

You can schedule the time for automatic signature update by using the **update schedule** command.

Examples

Enable automatic URL signature library update and enter automatic URL signature library update configuration view.

```
<Sysname> system-view
[Sysname] url-filter signature auto-update
[Sysname-url-filter-autoupdate]
```

Related commands

update schedule

url-filter signature auto-update-now

Use **url-filter signature auto-update-now** to trigger an automatic URL signature library update manually.

Syntax

url-filter signature auto-update-now

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command immediately starts the automatic signature library update process. The device accesses the company's website to update the local URL signature library.

You can execute this command anytime you find a new version of signature library on the company's website.

Examples

Trigger an automatic URL signature library update manually.

```
<Sysname> system-view
[Sysname] url-filter signature auto-update-now
```

url-filter signature rollback

Use **url-filter signature rollback** to roll back the URL signature library.

Syntax

url-filter signature rollback { **factory** | **last** }

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

factory: Rolls back the URL signature library to the factory default version.

last: Rolls back the URL signature library to the previous version.

Usage guidelines

If a URL signature library update causes exceptions or a high false alarm rate, you can roll back the URL signature library.

Before rolling back the URL signature library, the device backs up the current signature library as the "previous version." For example, the previous library version is V1 and the current library version is V2. If you perform a rollback to the previous version, library version V1 becomes the current version and library version V2 becomes the previous version. If you perform a rollback to the previous version again, the library rolls back to library version V2.

Examples

Roll back the URL signature library to the previous version.

```
<Sysname> system-view
[Sysname] url-filter signature rollback last
```

url-filter signature update

Use **`url-filter signature update`** to manually update the URL signature library.

Syntax

`url-filter signature update` *`file-path`*

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

`file-path`: Specifies the URL filtering signature file path, a string of 1 to 255 characters.

Usage guidelines

△ **CAUTION:**

Select a signature file according to the memory size and software version of the device. NSFOCUS provides signature files separately for high-memory (equal to or higher than 8 GB) and low-memory (lower than 8 GB) devices and for different software versions. If you use a signature file applicable to high-memory devices to update the URL filtering signature library on a low-memory device, exceptions might occur on the low-memory device. As a best practice, use a signature file that is compatible with the software version and memory size of the device to update the URL filtering signature library on the device.

If the device cannot access the company's website, use one of the following methods to manually update the URL signature library:

- **Local update**—Updates the URL signature library on the device by using the locally stored update URL filtering signature file.

  Store the update file on the master device for successful signature library update.

  The following describes the format of the *`file-path`* parameter for different update scenarios.

Update scenario	Format of *file-path*	Remarks
The update file is stored in the current working directory.	*filename*	To display the current working directory, use the **pwd** command (see file system management in *Fundamentals Command Reference)*.
The update file is stored in a different directory on the same storage medium.	*filename*	Before updating the signature library, you must first use the **cd** command to open the directory where the file is stored. For information about the **cd** command, see file system management in *Fundamentals Command Reference.*
The update file is stored on a different storage medium.	*path/filename*	Before updating the signature library, you must first use the **cd** command to open the root directory of the storage medium where the file is stored. For information about the **cd** command, see file system management in *Fundamentals Command Reference.*

- **FTP/TFTP update**—Updates the URL signature library on the device by using the file stored on the FTP or TFTP server.

  The following describes the format of the *file-path* parameter for different update scenarios.

Update scenario	Format of *file-path*	Remarks
The update file is stored on an FTP server.	*ftp://username:password@ server address/filename*	The *username* parameter represents the FTP login username. The *password* parameter represents the FTP login password. The *server address* parameter represents the IP address or host name of the FTP server. Replace the following special characters in the FTP login username and password with their respective escape characters: • **Colon (:)**—%3A or %3a. • **At sign (@)**—%40. • **Forward slash (/)**—%2F or %2f.
The update file is stored on a TFTP server.	*tftp://server address/filename*	The *server address* parameter represents the IP address or host name of the TFTP server.

NOTE:

To update the signature library successfully, make sure the device and the FTP or TFTP server can reach each other. If you specify the FTP or TFTP server by its host name, you must also make sure the device can resolve the host name into an IP address through static or dynamic DNS. For more information about DNS, see *Layer 3—IP Services Configuration Guide*.

Examples

Manually update the local URL signature library by using a signature file stored on a TFTP server.

```
<Sysname> system-view
[Sysname] url-filter signature update tftp://192.168.0.10/url-filter-1.0.2-en.dat
```

Manually update the local URL signature library by using a signature file stored on an FTP server. The FTP login username and password are **user:123** and **user@abc/123**, respectively.

```
<Sysname> system-view
[Sysname] url-filter signature update
ftp://user%3A123:user%40abc%2F123@192.168.0.10/url-filter-1.0.2-en.dat
```

Manually update the local URL signature library by using a signature file stored on the device. The file is stored in directory **cfa0:/url-filter-1.0.23-en.dat**, and the current working directory is **cfa0:**.

```
<Sysname> system-view
[Sysname] url-filter signature update url-filter-1.0.23-en.dat
```

Manually update the local URL signature library by using a signature file stored on the device. The file is stored in directory **cfa0:/dpi/url-filter-1.0.23-en.dat**, and the current working directory is **cfa0:**.

```
<Sysname> cd dpi
<Sysname> system-view
[Sysname] url-filter signature update url-filter-1.0.23-en.dat
```

Manually update the local URL signature library by using a signature file stored on the device. The file is stored in directory **cfb0:/dpi/url-filter-1.0.23-en.dat**, and the current working directory is **cfa0:**.

```
<Sysname> cd cfb0:/
<Sysname> system-view
[Sysname] url-filter signature update dpi/url-filter-1.0.23-en.dat
```

whitelist-only enable

Use **whitelist-only enable** to enable URL whitelist-only filtering.

Use **undo whitelist-only enable** to disable URL whitelist-only filtering.

Syntax

whitelist-only enable

undo whitelist-only enable

Default

URL whitelist-only filtering is disabled.

Views

URL filtering policy view

Predefined user roles

network-admin

context-admin

Usage guidelines

This feature allows only the HTTP or HTTPS requests that match the whitelist rules to pass through, and the other settings in the URL filtering policy will not take effect.

Examples

Enable URL whitelist-only filtering in URL filtering policy **news**.

```
<Sysname> system-view
[Sysname] url-filter policy news
[Sysname-url-filter-policy-news] whitelist-only enable
```

Related commands

add

Contents

Data filtering commands

action

Use **action** to specify actions for a data filtering rule.

Use **undo action** to remove the action setting from a data filtering rule.

Syntax

action { **drop** | **permit** } [**logging**]

undo action

Default

The default action of a data filtering rule is **drop**.

Views

Data filtering rule view

Predefined user roles

network-admin

context-admin

Parameters

drop: Drops the matching packets.

permit: Permits the matching packets to pass.

logging: Logs the matching packets.

Usage guidelines

If a packet matches multiple data filtering rules, the device determines the actions as follows:

- If the matching rules have both the **permit** and **drop** actions, the device takes the **drop** action.
- If the **logging** action is specified for any of the matching rules, the device logs the packet.

Examples

Create data filtering policy **def**.

```
<Sysname> system-view
[Sysname] data-filter policy def
```

Specify action **permit** for data filtering rule **r1** in the policy.

```
[Sysname-data-filter-policy-def] rule r1
[Sysname-data-filter-policy-def-rule-r1] action permit
```

application

Use **application** to specify application layer protocols for a data filtering rule.

Use **undo application** to remove application layer protocols from a data filtering rule.

Syntax

application { **all** | **type** { **ftp** | **http** | **imap** | **nfs** | **pop3** | **rtmp** | **smb** | **smtp** } * }

undo application { **all** | **type** { **ftp** | **http** | **imap** | **nfs** | **pop3** | **rtmp** | **smb** | **smtp** } * }

Default

No application layer protocols are specified for a data filtering rule.

Views

Data filtering rule view

Predefined user roles

network-admin

context-admin

Parameters

all: Specifies all application layer protocols.

type: Specifies specific types of application layer protocols.

ftp: Specifies the FTP protocol.

http: Specifies the HTTP protocol.

imap Specifies the IMAP protocol.

nfs Specifies the NFS protocol. Only NFSv3 is supported.

pop3 Specifies the POP3 protocol.

rtmp Specifies the RTMP protocol.

smb Specifies the SMB protocol. Only SMBv1 and SMBv2 are supported.

smtp: Specifies the SMTP protocol.

Usage guidelines

Use this command to specify the application layer protocols to which a data filtering rule applies.

Examples

Create data filtering policy **def**.

```
<Sysname> system-view
[Sysname] data-filter policy def
```

Specify the HTTP protocol for data filtering rule **r1** in the policy.

```
[Sysname-data-filter-policy-def] rule r1
[Sysname-data-filter-policy-def-rule-r1] application type http
```

data-filter apply policy

Use **data-filter apply policy** to apply a data filtering policy to a DPI application profile.

Use **undo data-filter apply policy** to remove the data filtering policy from a DPI application profile.

Syntax

data-filter apply policy *policy-name*

undo data-filter apply policy

Default

No data filtering policy is applied to a DPI application profile.

Views

DPI application profile view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies a data filtering policy by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

A data filtering policy takes effect only after it is applied to a DPI application profile.

You can apply only one data filtering policy to a DPI application profile. If you execute this command for a DPI application profile multiple times, the most recent configuration takes effect.

Examples

Apply data filtering policy **def** to DPI application profile **abc**.

```
<Sysname> system-view
[Sysname] app-profile abc
[Sysname-app-profile-abc] data-filter apply policy def
```

Related commands

app-profile

data-filter policy

data-filter keyword-group

Use **data-filter keyword-group** to create a keyword group and enter its view, or enter the view of an existing keyword group.

Use **undo data-filter keyword-group** to delete a keyword group.

Syntax

data-filter keyword-group *keywordgroup-name*

undo data-filter keyword-group *keywordgroup-name*

Default

No keyword groups exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

keywordgroup-name: Assigns a name to the keyword group, a case-insensitive string of 1 to 31 characters.

Usage guidelines

A keyword group is a group of keyword match patterns. A packet matches a keyword group if it matches a pattern in the group.

Examples

Create a keyword group named **kg1** and enter its view.

```
<Sysname> system-view
[Sysname] data-filter keyword-group kg1
[Sysname-data-filter-keygroup-kg1]
```

data-filter policy

Use **data-filter policy** to create a data filtering policy and enter its view, or enter the view of an existing data filtering policy.

Use **undo data-filter policy** to delete a data filtering policy.

Syntax

data-filter policy *policy-name*

undo data-filter policy *policy-name*

Default

No data filtering policies exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Assigns a name to the data filtering policy, a case-insensitive string of 1 to 31 characters. Hyphens (-) are not allowed.

Usage guidelines

A data filtering policy can contain a maximum of 32 data filtering rules.

Examples

Create data filtering policy **def** and enter its view.

```
<Sysname> system-view
[Sysname] data-filter policy def
[Sysname-data-filter-policy-def]
```

Related commands

data-filter apply policy

description (data filtering policy view)

Use **description** to configure a description for a data filtering policy.

Use **undo description** to restore the default.

Syntax

description *string*

undo description

Default

A data filtering policy does not have a description.

Views

Data filtering policy view

Predefined user roles

network-admin

context-admin

Parameters

string: Specifies a description, a case-sensitive string of 1 to 255 characters.

Usage guidelines

Use this command to configure descriptions for data filtering policies for easy maintenance.

Examples

Configure the description as **The data filter** for data filtering policy **def**.

```
<Sysname> system-view
[Sysname] data-filter policy def
[Sysname-data-filter-policy-def] description The data filter
```

description (keyword group view)

Use **description** to configure a description for a keyword group.

Use **undo description** to restore the default.

Syntax

description *string*

undo description

Default

A keyword group does not have a description.

Views

Keyword group view

Predefined user roles

network-admin

context-admin

Parameters

string: Specifies a description, a case-sensitive string of 1 to 255 characters.

Usage guidelines

Use this command to configure descriptions for keyword groups for easy maintenance.

Examples

Configure the description as **The data filter keyword group** for keyword group **kg1**.

```
<Sysname> system-view
[Sysname] data-filter keyword-group kg1
[Sysname-data-filter-kgroup-kg1] description The data filter keyword group
```

direction

Use **direction** to specify the traffic direction for a data filtering rule.

Use **undo direction** to restore the default.

Syntax

direction { **both** | **download** | **upload** }

undo direction

Default

A data filtering rule applies to upload traffic.

Views

Data filtering rule view

Predefined user roles

network-admin

context-admin

Parameters

both: Specifies both the upload and download traffic directions.

download: Specifies the download traffic direction.

upload: Specifies the upload traffic direction.

Usage guidelines

Use this command to specify the traffic direction to which a data filtering rule applies.

Examples

Create data filtering policy **def**.

```
<Sysname> system-view
[Sysname] data-filter policy def
```

Specify the **download** traffic direction for data filtering rule **r1** in the policy.

```
[Sysname-data-filter-policy-def] rule r1
[Sysname-data-filter-policy-def-rule-r1] direction download
```

keyword-group

Use **keyword-group** to specify a keyword group for a data filtering rule.

Use **undo keyword-group** to restore the default.

Syntax

keyword-group *keygroup-name*

undo keyword-group

Default

A data filtering rule does not have a keyword group.

Views

Data filtering rule view

Predefined user roles

network-admin

context-admin

Parameters

keygroup-name: Specifies a keyword group by its name, a case-insensitive string of 1 to 31 characters. The specified keyword group must exist on the device.

Usage guidelines

A data filtering rule uses the keyword group to filter packets based on the application layer data.

You can specify only one keyword group for a data filtering rule. If you execute this command for a data filtering rule multiple times, the most recent configuration takes effect.

Examples

Create data filtering policy **def**.

```
<Sysname> system-view
[Sysname] data-filter policy def
```

Specify keyword group **kg1** for data filtering rule **r1** in the policy.

```
[Sysname-data-filter-policy-def] rule r1
[Sysname-data-filter-policy-def-rule-r1] keyword-group kg1
```

Related commands

data-filter keyword-group

pattern

Use **pattern** to configure a pattern for keyword matching.

Use **undo pattern** to delete a pattern.

Syntax

pattern *pattern-name* { **regex** | **text** } *pattern-string*

undo pattern *pattern-name*

Default

A keyword group does not contain any keyword match patterns.

Views

Keyword group view

Predefined user roles

network-admin

context-admin

Parameters

pattern-name: Assigns a name to the match pattern, a case-insensitive string of 1 to 31 characters.

regex *pattern-string*: Specifies a regular expression, a case-sensitive string of 3 to 245 characters. All printable characters are supported. The regular expression must include a minimum of three consecutive non-wildcard characters.

text *pattern-string*: Specifies a case-sensitive string of 3 to 245 characters for exact match. All printable characters are supported.

Usage guidelines

A pattern for keyword matching can be a regular expression or a text string.

A keyword group can contain a maximum of 32 keyword match patterns. A packet matches a keyword group if it matches a pattern in the group.

When you configure a regular expression pattern for keyword matching, follow these restrictions and guidelines:

- The regular expression pattern can contain a maximum of four branches. For example, **'abc(c|d|e|\x3D)'** is valid, and **'abc(c|onreset|onselect|onchange|style\x3D)'** is invalid.
- Nested braces are not allowed. For example, **'ab((abcs*?))'** is invalid.
- A branch cannot be specified after another branch. For example, **'ab(a|b)(c|d)^\\r\\n]+?'** is invalid.
- A minimum of four non-wildcard characters must exist before an asterisk (*) or question mark (?). For example, **'abc*'** is invalid and **'abcd*DoS\x2d\d{5}\x20\x2bxi\\r\\nJOIN'** is valid.

Examples

In keyword group **kg1**, configure a keyword match pattern with regular expression **(?i)^.***__abc.*__.

```
<Sysname> system-view
[Sysname] data-filter keyword-group kg1
[Sysname-data-filter-kgroup-kg1] pattern 1 regex (?i)^.*abc.*
```

pre-defined-pattern

Use **pre-defined-pattern** to enable a predefined pattern in a keyword group.

Use **undo pre-defined-pattern** to disable a predefined pattern in a keyword group.

Syntax

pre-defined-pattern name { **bank-card-number** | **credit-card-number** | **id-card-number** | **phone-number** }

undo pre-defined-pattern name { **bank-card-number** | **credit-card-number** | **id-card-number** | **phone-number** }

Default

No predefined patterns are enabled in a keyword group.

Views

Keyword group view

Predefined user roles

network-admin

context-admin

Parameters

name: Specifies a predefined pattern by its name.

bank-card-number: Specifies the bank card number pattern.

credit-card-number: Specifies the credit card number pattern.

id-card-number: Specifies the ID card number pattern.

phone-number: Specifies the phone number pattern.

Usage guidelines

To match packets that contain phone numbers, bank card numbers, credit card numbers, or ID card numbers in a keyword group, enable the corresponding predefined pattern in the keyword group.

You can execute this command multiple times in a keyword group to enable multiple predefined patterns.

Examples

Enable the phone number predefined pattern in keyword group **kg1** to match packets that contain phone numbers.

```
<Sysname> system-view
[Sysname] data-filter keyword-group kg1
[Sysname-data-filter-kgroup-kg1] pre-defined-pattern name phone-number
```

rule

Use **rule** to create a data filtering rule and enter its view, or enter the view of an existing data filtering rule.

Use **undo rule** to delete a data filtering rule.

Syntax

rule *rule-name*

undo rule *rule-name*

Default

No data filtering rules exist.

Views

Data filtering policy view

Predefined user roles

network-admin

context-admin

Parameters

rule-name: Assigns a name to the data filtering rule, a case-insensitive string of 1 to 31 characters.

Usage guidelines

A data filtering rule contains a set of filtering criteria and the actions for matching packets. The filtering criteria include keyword group, traffic direction, and application layer protocol. The actions include drop, permit, and logging. A packet must match all the filtering criteria for the actions specified for the rule to apply.

Examples

In data filtering policy **def**, create a data filtering rule named **r1** and enter its view.

```
<Sysname> system-view
[Sysname] data-filter policy def
[Sysname-data-filter-policy-def] rule r1
[Sysname-data-filter-policy-def-rule-r1]
```

Contents

File filtering commands

action

Use **action** to specify actions for a file filtering rule.

Use **undo action** to remove the action setting from a file filtering rule.

Syntax

action { **drop** | **permit** } [**logging**]

undo action

Default

The default action of a file filtering rule is **drop**.

Views

File filtering rule view

Predefined user roles

network-admin

context-admin

Parameters

drop: Drops the matching packets.

permit: Permits the matching packets to pass.

logging: Logs the matching packets.

Usage guidelines

If a packet matches only one file filtering rule, the device takes the actions specified for the rule.

If a packet matches multiple file filtering rules, the device determines the actions as follows:

- If the matching rules have both the **permit** and **drop** actions, the device takes the **drop** action.
- If the **logging** action is specified for any of the matching rules, the device logs the packet.

Examples

Create file filtering policy **def**.

```
<Sysname> system-view
[Sysname] file-filter policy def
```

Specify action **permit** for file filtering rule **ch1** in the policy.

```
[Sysname-file-filter-policy-def] rule ch1
[Sysname-file-filter-policy-def-rule-ch1] action permit
```

application

Use **application** to specify application layer protocols for a file filtering rule.

Use **undo application** to remove application layer protocols from a file filtering rule.

Syntax

application { **all** | **type** { **ftp** | **http** | **imap** | **nfs** | **pop3** | **rtmp** | **smb** | **smtp** } * }

undo application { **all** | **type** { **ftp** | **http** | **imap** | **nfs** | **pop3** | **rtmp** | **smb** | **smtp** } * }

Default

No application layer protocols are specified for a file filtering rule.

Views

File filtering rule view

Predefined user roles

network-admin

context-admin

Parameters

all: Specifies all application layer protocols.

type: Specifies specific types of application layer protocols.

ftp: Specifies the FTP protocol.

http: Specifies the HTTP protocol.

imap Specifies the IMAP protocol.

nfs Specifies the NFS protocol. Only NFSv3 is supported.

pop3 Specifies the POP3 protocol.

rtmp Specifies the RTMP protocol.

smb Specifies the SMB protocol. Only SMBv1 and SMBv2 are supported.

smtp: Specifies the SMTP protocol.

Usage guidelines

Use this command to specify the application layer protocols to which a file filtering rule applies.

Examples

Create file filtering policy **def**.

```
<Sysname> system-view
[Sysname] file-filter policy def
```

Specify the HTTP protocol for file filtering rule **ch1** in the policy.

```
[Sysname-file-filter-policy-def] rule ch1
[Sysname-file-filter-policy-def-rule-ch1] application type http
```

description (file filtering policy view)

Use **description** to configure a description for a file filtering policy.

Use **undo description** to restore the default.

Syntax

description *string*

undo description

Default

A file filtering policy does not have a description.

Views

File filtering policy view

Predefined user roles

network-admin

context-admin

Parameters

string: Specifies a description, a case-sensitive string of 1 to 255 characters.

Usage guidelines

Use this command to configure descriptions for file filtering policies for easy maintenance.

Examples

Configure the description as **The file filter** for file filtering policy **def**.

```
<Sysname> system-view
[Sysname] file-filter policy def
[Sysname-file-filter-policy-def] description The file filter
```

Related commands

file-filter policy

description (file type group view)

Use **description** to configure a description for a file type group.

Use **undo description** to restore the default.

Syntax

description *string*

undo description

Default

A file type group does not have a description.

Views

File type group view

Predefined user roles

network-admin

context-admin

Parameters

string: Specifies a description, a case-sensitive string of 1 to 255 characters.

Usage guidelines

Use this command to configure descriptions for file type groups for easy maintenance.

Examples

Configure the description as **def** for file type group **abc**.

```
<Sysname> system-view
```

```
[Sysname] file-filter filetype-group abc
[Sysname-file-filter-fgroup-abc] description def
```

Related commands

file-filter filetype-group

direction

Use **direction** to specify the traffic direction for a file filtering rule.

Use **undo direction** to restore the default.

Syntax

direction { **both** | **download** | **upload** }

undo direction

Default

A file filtering rule applies to upload traffic.

Views

File filtering rule view

Predefined user roles

network-admin

context-admin

Parameters

both: Specifies both the upload and download traffic directions.

download: Specifies the download traffic direction.

upload: Specifies the upload traffic direction.

Usage guidelines

Use this command to specify the traffic direction to which a file filtering rule applies.

For FTP and SMTP, the upload and download directions refer to the upload and download directions of the FTP or SMTP session.

For HTTP, the upload direction refers to HTTP POST requests, and the download direction refers to HTTP GET requests.

Examples

Create file filtering policy **def**.

```
<Sysname> system-view
[Sysname] file-filter policy def
```

Specify the **download** traffic direction for file filtering rule **ch1** in the policy.

```
[Sysname-file-filter-policy-def] rule ch1
[Sysname-file-filter-policy-def-rule-ch1] direction download
```

file-filter apply policy

Use **data-filter apply policy** to apply a file filtering policy to a DPI application profile.

Use **undo data-filter apply policy** to remove the file filtering policy from a DPI application profile.

Syntax

file-filter apply policy *policy-name*

undo file-filter apply policy

Default

No file filtering policy is applied to a DPI application profile.

Views

DPI application profile view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies a file filtering policy by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

A file filtering policy takes effect only after it is applied to a DPI application profile.

You can apply only one file filtering policy to a DPI application profile. If you execute this command for a DPI application profile multiple times, the most recent configuration takes effect.

Examples

Apply file filtering policy **def** to DPI application profile **abc**.

```
<Sysname> system-view
[Sysname] app-profile abc
[Sysname-app-profile-abc] file-filter apply policy def
```

Related commands

app-profile

data**-filter policy**

file-filter false-extension action

Use **file-filter false-extension action** to set the action for packets with files carrying false extensions.

Use **undo file-filter false-extension action** to restore the default.

Syntax

file-filter false-extension action { **drop** | **permit** }

undo file-filter false-extension action

Default

The default action is **permit**, which enables the device to determine the packet processing action based on the real file extension.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

drop: Drops the packet.

permit: Permits the packet to pass so the action for the packet can be determined based on the real file extension.

Usage guidelines

A packet might contain files that carry false extensions. For example, a file that carries the .exe file extension might actually be a .txt file.

Use this command to specify the action for packets with files carrying false extensions. To perform file filtering inspection based on the real file extension, set the action to **permit**. To discard such packets directly, set the action to **drop**.

Examples

Set the action to drop for packets with files carrying false extensions.

```
<Sysname> system-view
[Sysname] file-filter false-extension action drop
```

file-filter filetype-group

Use **file-filter filetype-group** to create a file type group and enter its view, or enter the view of an existing file type group.

Use **undo file-filter filetype-group** to delete a file type group.

Syntax

file-filter filetype-group *group-name*

undo file-filter filetype-group *group-name*

Default

No file type groups exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Assigns a name to the file type group, a case-insensitive string of 1 to 31 characters.

Usage guidelines

A file type group is a group of file type match patterns. A file matches a file type group if it matches a pattern in the group.

Examples

Create a file type group named **fg1** and enter its view.

```
<Sysname> system-view
[Sysname] file-filter filetype-group fg1
[Sysname-file-filter-fgroup-fg1]
```

file-filter policy

Use **file-filter policy** to create a file filtering policy and enter its view, or enter the view of an existing file filtering policy.

Use **undo file-filter policy** to delete a file filtering policy.

Syntax

file-filter policy *policy-name*

undo file-filter policy *policy-name*

Default

No file filtering policies exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Assigns a name to the file filtering policy, a case-sensitive string of 1 to 31 characters. Hyphens (-) are not allowed.

Usage guidelines

A file filtering policy can contain a maximum of 32 file filtering rules.

Examples

Create file filtering policy **def** and enter its view.

```
<Sysname> system-view
[Sysname] file-filter policy def
[Sysname-file-filter-policy-def]
```

Related commands

file-filter apply policy

filetype-group

Use **filetype-group** to apply a file type group to a file filtering rule.

Use **undo filetype-group** to restore the default.

Syntax

filetype-group *group-name*

undo filetype-group

Default

A file filtering rule does not have a file type group.

Views

File filtering rule view

Predefined user roles

network-admin

context-admin

Parameters

keygroup-name: Specifies a file type group by its name, a case-sensitive string of 1 to 31 characters. The specified file type group must exist on the device.

Usage guidelines

A file filtering rule uses the file type group to filter files based on the file extension.

You can specify only one file type group for a file filtering rule. If you execute this command for a file filtering rule multiple times, the most recent configuration takes effect.

Examples

Create file filtering policy **def**.

```
<Sysname> system-view
[Sysname] file-filter policy def
```

Specify file type group **fg1** for file filtering rule **ch1** in the policy.

```
[Sysname-file-filter-policy-def] rule ch1
[Sysname-file-filter-policy-def-rule-ch1] filetype-group fg1
```

Related commands

file-filter filetype-group

pattern

Use **pattern** to configure a pattern for file type matching.

Use **undo pattern** to delete a pattern.

Syntax

pattern *pattern-name* **text** *pattern-string*

undo pattern *pattern-name*

Default

A file type group does not contain any file type match patterns.

Views

File type group view

Predefined user roles

network-admin

context-admin

Parameters

pattern-name: Assigns a name to the match pattern, a case-insensitive string of 1 to 31 characters.

text *pattern-string*: Specifies a file extension, a case-insensitive string of 1 to 8 characters.

Usage guidelines

File filtering uses file type match patterns to identify files based on the file extension.

A file type group can contain a maximum of 32 file type match patterns. A file matches a file type group if it matches a pattern in the group.

Examples

In file type group **fg1**, configure a file type match pattern to match files that use the **doc** extension.

```
<Sysname> system-view
[Sysname] file-filter filetype-group fg1
[Sysname-file-filter-fgroup-fg1] pattern 1 text doc
```

rule

Use **rule** to create a file filtering rule and enter its view, or enter the view of an existing file filtering rule.

Use **undo rule** to delete a file filtering rule.

Syntax

rule *rule-name*

undo rule *rule-name*

Default

No file filtering rules exist.

Views

File filtering policy view

Predefined user roles

network-admin

context-admin

Parameters

rule-name: Assigns a name to the file filtering rule, a case-insensitive string of 1 to 31 characters.

Usage guidelines

A file filtering rule contains a set of filtering criteria and the actions for matching files. The filtering criteria include file type group, traffic direction, and application layer protocol. The actions include drop, permit, and logging.

A file must match all the filtering criteria for the actions specified for the rule to apply.

A file filtering policy can contain a maximum of 32 filtering rules.

Examples

In file filtering policy **def**, create a file filtering rule named **ch1** and enter its view.

```
<Sysname> system-view
[Sysname] file-filter policy def
[Sysname-file-filter-policy-def]rule ch1
[Sysname-file-filter-policy-def-rule-ch1]
```

Contents

Anti-virus commands

anti-virus apply policy

Use **anti-virus apply policy** to apply an anti-virus policy to a DPI application profile.

Use **undo anti-virus apply policy** to remove the application.

Syntax

anti-virus apply policy *policy-name* **mode** { **alert** | **protect** }

undo anti-virus apply policy

Default

No anti-virus policy is applied to a DPI application profile.

Views

DPI application profile view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies an anti-virus policy by its name, a case-insensitive string of 1 to 63 characters.

mode: Specifies an anti-virus policy mode.

alert: Only logs matching packets.

protect: Takes the action specified in the anti-virus policy on matching packets.

Usage guidelines

An anti-virus policy takes effect only after it is applied to a DPI application profile. You can apply only one anti-virus policy to a DPI application profile. If you execute this command multiple times, the most recent configuration takes effect.

Examples

Apply anti-virus policy **abc** to DPI application profile **sec**. Set the anti-virus policy mode to **protect**.

```
<Sysname> system-view
[Sysname] app-profile sec
[Sysname-app-profile-sec] anti-virus apply policy abc mode protect
```

anti-virus cache min-time

Use **anti-virus cache min-time** to set the minimum cache period for an anti-virus MD5 entry.

Use **undo anti-virus cache min-time** to restore the default.

Syntax

anti-virus cache min-time *value*

undo anti-virus cache min-time

Default

The minimum cache period of an anti-virus MD5 entry is 10 minutes.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

value: Specifies the minimum cache period in minutes. The value range is 10 to 720.

Usage guidelines

When anti-virus cloud query is required, the device performs the following tasks:

1. Creates an MD5 entry in the cache.
2. Submits the MD5 value to the cloud server.
3. Updates the cached MD5 entry with the returned cloud query result.

Setting the minimum cache period for anti-virus MD5 entries ensures that the cached entries will not be overwritten by new entries during the specified period of time.

When the anti-virus cache is full, the system identifies the cache period of the oldest MD5 entry to determine whether to overwrite it with a new entry that requires cloud query:

- If the cache period of the entry is equal to or shorter than the minimum cache period, the system does not delete the entry. The new entry is not cached and cloud query will not be performed.
- If the cache period of the entry is longer than the minimum cache period, the system overwrites it with the new entry and submits the new entry to the cloud server.

After the **anti-virus cache size** command sets a smaller cache size, the system will delete the exceeding oldest entries immediately without checking their minimum cache periods.

Examples

Set the minimum cache period for an anti-virus MD5 entry to 36 minutes.

```
<Sysname> system-view
[Sysname] anti-virus cache min-time 36
```

Related commands

anti-virus cache size

anti-virus cache size

Use **anti-virus cache size** to set the anti-virus cache size.

Use **undo anti-virus cache size** to restore the default.

Syntax

anti-virus cache size *cache-size*

undo anti-virus cache size

Default

The anti-virus cache can cache a maximum of 100000 entries.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

cache-size: Specifies the cache size in the range of 100000 to 200000.

Usage guidelines

The device caches the anti-virus query result returned from the cloud server for subsequent virus detection. The query result identifies whether or not the MD5 value submitted for cloud query is a virus.

If you set a smaller anti-virus cache size, the system will delete the existing oldest entries without checking their minimum cache periods.

Examples

Set the anti-virus cache size to 20000.

```
<Sysname> system-view
[Sysname] anti-virus cache size 200000
```

Related commands

anti-virus cache min-time

anti-virus policy

Use **anti-virus policy** to create an anti-virus policy and enter its view, or enter the view of an existing anti-virus policy.

Use **undo anti-virus policy** to delete an anti-virus policy.

Syntax

anti-virus policy *policy-name*

undo anti-virus policy *policy-name*

Default

An anti-virus policy named **default** exists.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies the anti-virus policy name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

All virus signatures in the virus signature library are available for an anti-virus policy, whether the policy is the default policy or a user-defined policy.

The default anti-virus policy cannot be modified or deleted.

Examples

Create anti-virus policy **abc** and enter its view.

```
<Sysname> system-view
[Sysname] anti-virus policy abc
[Sysname-anti-virus-policy-abc]
```

anti-virus parameter-profile

Use **anti-virus parameter-profile** to specify a parameter profile for an anti-virus action.

Use **undo anti-virus parameter-profile** to remove the parameter profile specified for an anti-virus action.

Syntax

anti-virus { **email** | **logging** | **redirect** } **parameter-profile** *profile-name*

undo anti-virus { **email** | **logging** | **redirect** } **parameter-profile**

Default

No parameter profile is specified for an anti-virus action.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

email: Specifies the email action.

logging: Specifies the logging action.

redirect: Specifies the redirect action.

parameter-profile *parameter-name*: Specifies a parameter profile by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

Before you can specify a parameter profile for an anti-virus action, configure the parameter profile in the DPI engine. For more information, see DPI engine configuration in *DPI Configuration Guide*.

A parameter profile defines the parameters for executing an action. For example, you can configure parameters such as the email server address and email recipients in the email parameter profile, and then apply the profile to the email action.

If no parameter profile is specified for an anti-virus action, or if the specified parameter profile does not exist, the default parameter settings of the action are used.

Examples

Create an email parameter profile named **av1** and specify a plaintext login password (**abc123**) in the parameter profile.

```
<Sysname> system-view
[Sysname] inspect email parameter-profile av1
[Sysname-inspect-email-av1] password simple abc123
[Sysname-inspect-logging-av1] quit
```

Specify parameter profile **av1** for the email action.

```
[Sysname] anti-virus email parameter-profile av1
```

Related commands

inspect email parameter-profile

inspect logging parameter-profile

inspect redirect parameter-profile

anti-virus signature auto-update

Use **anti-virus signature auto-update** to enable automatic virus signature library update and enter automatic virus signature library update configuration view.

Use **undo anti-virus signature auto-update** to disable automatic virus signature library update.

Syntax

anti-virus signature auto-update

undo anti-virus signature auto-update

Default

Automatic virus signature library update is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

To automatically update the virus signature library, make sure the device can access the NSFOCUS website.

Examples

Enable automatic virus signature library update and enter automatic virus signature library update configuration view.

```
<Sysname> system-view
[Sysname] anti-virus signature auto-update
[Sysname-anti-virus-autoupdate]
```

Related commands

update schedule

anti-virus signature auto-update-now

Use **anti-virus signature auto-update-now** to manually trigger an automatic signature library update.

Syntax

anti-virus signature auto-update-now

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

After you execute this command, the device immediately starts the automatic signature library update process whether automatic signature library update is enabled or not. The device automatically backs up the current signature library before overwriting it.

You can execute this command anytime you find a new version of signature library on the NSFOCUS website.

Examples

Manually trigger an automatic signature library update.

```
<Sysname> system-view
[Sysname] anti-virus signature auto-update-now
```

anti-virus signature rollback

Use **anti-virus signature rollback** to roll back the virus signature library.

Syntax

anti-virus signature rollback { **factory** | **last** }

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

factory: Rolls back the virus signature library to the factory default version.

last: Rolls back the virus signature library to the previous version.

Usage guidelines

If a virus signature library update causes abnormal situations or a high false alarm rate, you can roll back the virus signature library.

Before performing a virus signature library rollback, the device backs up the current virus signature library as the previous version. For example, the previous version is V1 and the current version is V2. If you perform a rollback to the previous version, version V1 becomes the current version and version V2 becomes the previous version. If you perform a rollback to the previous version again, version V2 becomes the current version and version V1 becomes the previous version.

Examples

Roll back the virus signature library to the previous version.

```
<Sysname> system-view
[Sysname] anti-virus signature rollback last
```

anti-virus signature update

Use **anti-virus signature update** to manually update the virus signature library.

Syntax

anti-virus signature update *file-path*

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

file-path: Specifies the virus signature file path, a string of 1 to 255 characters.

Usage guidelines

CAUTION:

The NSFOCUS website provides different signature libraries for devices with different memory sizes and software versions. You must obtain the signature library that is suitable for your device. If your device has a small memory (8 GB or less) but you choose a signature library that is for a large memory (more than 8 GB), the signature update might result in device anomaly.

If the device cannot access the NSFOCUS website, use one of the following methods to manually update the virus signature library:

- **Local update**—Updates the virus signature library by using the locally stored virus signature file.

  Store the update file on the master device for successful signature library update.

  The following table describes the format of the *file-path* argument for different update scenarios.

Update scenario	Format of *file-path*	Remarks
The signature file is stored in the current working directory.	*filename*	To display the current working directory, use the **pwd** command. For information about the **pwd** command, see file system management in *Fundamentals Command Reference*.
The signature file is stored in a different directory on the same storage medium.	*filename*	Before updating the signature library, you must first use the **cd** command to open the directory where the file is stored. For information about the **cd** command, see file system management in *Fundamentals Command Reference*.
The signature file is stored on a different storage medium.	*path/filename*	Before updating the signature library, you must first use the **cd** command to open the root directory of the storage medium where the file is stored. For information about the **cd** command, see file system management in *Fundamentals Command Reference.*

- **FTP/TFTP update**—Updates the virus signature library by using the virus signature file stored on an FTP or TFTP server.

  The following table describes the format of the *file-path* argument for different update scenarios.

Update scenario	Format of *file-path*	Remarks
The signature file is stored on an FTP server.	*ftp://username:password@server/filename*	The *username* argument represents the FTP login username. The *password* argument represents the FTP login password. The *server* argument represents the IP address or host name of the FTP server. If a colon (:), at sign (@), or forward slash (/) exists in the username or password, you must convert it into its escape characters. The escape characters are %3A or %3a for a colon, %40 for an at sign, and %2F or %2f for a forward slash.
The signature file is stored on a TFTP server.	*tftp://server/filename*	The *server* argument represents the IP address or host name of the TFTP server.

NOTE:

To update the signature library successfully, make sure the device and the FTP or TFTP server can reach each other. If you specify the FTP or TFTP server by its host name, you must also make sure the device can resolve the host name into an IP address through static or dynamic DNS. For more information about DNS, see *Layer 3—IP Services Configuration Guide*.

Examples

Manually update the virus signature library by using a virus signature file stored on a TFTP server.

```
<Sysname> system-view
[Sysname] anti-virus signature update tftp://192.168.0.10/av-1.0.2-en.dat
```

Manually update the virus signature library by using a virus signature file stored on an FTP server. The FTP login username and password are **user:123** and **user@abc/123**, respectively.

```
<Sysname> system-view
[Sysname] anti-virus signature update
ftp://user%3A123:user%40abc%2F123@192.168.0.10/av-1.0.2-en.dat
```

Manually update the virus signature library by using a virus signature file stored on the device. The file is stored in directory **cfa0:/av-1.0.23-en.dat**. The current working directory is **cfa0:**.

```
<Sysname> system-view
[Sysname] anti-virus signature update av-1.0.23-en.dat
```

Manually update the virus signature library by using a virus signature file stored on the device. The file is stored in directory **cfa0:/dpi/av-1.0.23-en.dat**. The current working directory is **cfa0:**.

```
<Sysname> cd dpi
<Sysname> system-view
[Sysname] anti-virus signature update av-1.0.23-en.dat
```

Manually update the virus signature library by using a virus signature file stored on the device. The file is stored in directory **cfb0:/dpi/av-1.0.23-en.dat**. The current working directory is the **cfa0:**.

```
<Sysname> cd cfb0:/
<Sysname> system-view
```

```
[Sysname] anti-virus signature update dpi/av-1.0.23-en.dat
```

cloud-query enable

Use **cloud-query enable** to enable MD5 value-based anti-virus cloud query.

Use **undo cloud-query enable** to disable MD5 value-based anti-virus cloud query.

Syntax

cloud-query enable

undo cloud-query enable

Default

MD5 value-based anti-virus cloud query is disabled.

Views

Anti-virus policy view

Predefined user roles

network-admin

context-admin

Usage guidelines

You can enable cloud query in an anti-virus policy. If no virus is found in the file, the device will send the MD5 value of the file to the cloud server for cloud query. The cloud server determines whether the MD5 value is a virus and returns the result to the device so appropriate action can be taken. The anti-virus module will save the result returned from the cloud server to the anti-virus buffer so the virus detection for subsequent packets can be performed locally.

Examples

Enable MD5 value-based anti-virus cloud query in anti-virus policy **news**.

```
<Sysname> system-view
[Sysname] anti-virus policy news
[Sysname-anti-virus-policy-news] cloud-query enable
```

description

Use **description** to configure a description for an anti-virus policy.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

An anti-virus policy does not have a description.

Views

Anti-virus policy view

Predefined user roles

network-admin

context-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 255 characters. The description can contain spaces.

Usage guidelines

A description can identify an anti-virus policy or provide details about an anti-virus policy. Policies with descriptions can be easily maintained.

Examples

Configure **"RD Department anti-virus policy"** as the description of anti-virus policy **abc**.

```
<Sysname> system-view
[Sysname] anti-virus policy abc
[Sysname-anti-virus-policy-abc] description "RD Department anti-virus policy"
```

display anti-virus cache

Use **display anti-virus cache** to display anti-virus cache information.

Syntax

display anti-virus cache [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all member devices.

Usage guidelines

The anti-virus cache contains the anti-virus query results returned from the cloud server. For anti-virus to cache the cloud query results, cloud query must be enabled in a minimum of one anti-virus policy.

If the file in a flow does not match any rule in the local virus signature library, the device will send the MD5 value of the file to the cloud server for cloud query.

- If the MD5 value matches a virus rule, the result will be cached as an entry on the hit entry list.
- If the MD5 value does not match any virus rule or if it matches a non-virus rule, the result will be cached as an entry on the non-hit entry list.

Examples

Display anti-virus cache information.

```
<Sysname> display anti-virus cache
Slot 1:
Anti-virus cache information:
 Cloud-query state: Disabled
 Total cached non-hit entries: 0
 Total cached hit entries: 0
```

```
Non-hit list min update interval: 0 seconds
Non-hit list max update interval: 0 seconds
Hit list min update interval: 0 seconds
Hit list max update interval: 0 seconds
Last query message sent: 0 seconds ago
Last query result received: 0 seconds ago
```

Table 1 Command output

Field	Description
Cloud-query state	Enabling state of the cloud query.
Total cached non-hit entries	Number of entries on the non-hit entry list.
Total cached hit entries	Number of entries on the hit entry list.
Non-hit list min update interval	Time elapsed since the last update on the non-hit entry list, in seconds.
Non-hit list max update interval	Time elapsed since the first entry was created on the non-hit entry list, in seconds.
Hit list min update interval	Time elapsed since the last update on the hit entry list, in seconds.
Hit list max update interval	Time elapsed since the first entry was created on the hit entry list, in seconds.
Last query message sent	Time elapsed since the last query request was sent, in seconds.
Last query result received	Time elapsed since the last query result was received, in seconds.

Related commands

`cloud-query enable`

display anti-virus signature

Use **`display anti-virus signature`** to display virus signature information.

Syntax

`display anti-virus signature` [[*`signature-id`*] | [**`severity`** { **`critical`** | **`high`** | **`low`** | **`medium`** }]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

`signature-id`: Specifies a signature by its ID in the range of 1 to 4294967294. If you do not specify a signature ID, this command displays the total number of virus signatures in the virus signature library.

`severity`: Specifies a severity level of virus signatures.

`critical`: Specifies the critical severity level.

high: Specifies the high severity level.

low: Specifies the low severity level.

medium: Specifies the medium severity level.

Usage guidelines

You can use this command to display the severity level of virus signatures for a better use of the **signature severity enable** command.

Examples

Display information about virus signature 10000001.

```
<Sysname> display anti-virus signature 10000001
Signature ID: 10000001
Name        : Trojan [Downloader].VBS.Agent
Severity    : Medium
```

Table 2 Command output

Field	Description
Signature ID	ID of the virus signature.
Name	Name of the virus signature.
Severity	Severity level of the virus signature: **Low**, **Medium**, **High**, or **Critical**.

Display the total number of virus signatures and the number of virus signatures failed to be deployed from the virus signature library to the DPI engine.

```
<Sysname> display anti-virus signature
 Total count:9206
 failed:0
```

display anti-virus signature family-info

Use **display anti-virus signature family-info** to display virus signature family information.

Syntax

display anti-virus signature family-info

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display virus signature family information.

```
<Sysname> display anti-virus signature family-info
 Total count: 6373
 Family ID  Family name
 1          Virus.Win32.Virut.ce
```

```
2          Trojan.Win32.SGeneric
3          Virus.Win32.Nimnul.a
4          Virus.Win32.Virlock.j
```

Table 3 Command output

Field	Description
Total count	Total number of virus signature families.
Family ID	ID of the virus signature family.
Family name	Name of the virus signature family.

display anti-virus signature library

Use **display anti-virus signature library** to display virus signature library information.

Syntax

display anti-virus signature library

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display virus signature library information.

```
<Sysname> display anti-virus signature library
Anti-Virus signature library information:
Type      SigVersion         ReleaseTime               Size
Current   1.0.9              Wed Apr 22 09:51:13 2015  976432
Last      -                  -                         -
Factory   1.0.0              Fri Dec 31 16:00:00 1999  20016
```

Table 4 Command output

Field	Description
Type	Version type of the virus signature library: • **Current**—Current version. • **Last**—Previous version. • **Factory**—Factory default version.
SigVersion	Version number of the virus signature library.
ReleaseTime	Release time of the virus signature library.
Size	Size of the virus signature library in bytes.

display anti-virus statistics

Use **display anti-virus statistics** to display anti-virus statistics.

Syntax

display anti-virus statistics [**policy** *policy-name*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

policy *policy-name*: Specifies an anti-virus policy by its name, a case-insensitive string of 1 to 63 characters. If you do not specify an anti-virus policy, this command displays anti-virus statistics for all anti-virus policies.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays anti-virus statistics for all member devices.

Examples

Display anti-virus statistics for slot 4.

```
<Sysname> display anti-virus statistics slot 4 cpu 1
CPU 1 on slot 4:
Total Block:    0
Total Redirect: 0
Total Alert:    0
Type           http      ftp       smtp      pop3      imap
Block           0         0         0         0         0
Redirect        0         0         0         0         0
Alert+Permit    0         0         0         0         0
```

Table 5 Command output

Field	Description
Total Block	Total number of times that the block action is taken.
Total Redirect	Total number of times that the redirect action is taken.
Total Alert	Total number of times that the alert action is taken.
Type	Action type: • **Block**—Blocks and logs matching packets. • **Redirect**—Redirects matching HTTP connections to a URL and generates logs. • **Alert+Permit**—Permits and logs matching packets.
http	Number of times that the action is taken on HTTP packets.
ftp	Number of times that the action is taken on FTP packets.
smtp	Number of times that the action is taken on SMTP packets.

Field	Description
pop3	Number of times that the action is taken on POP3 packets.
imap	Number of times that the action is taken on IMAP packets.

exception application

Use **exception application** to set an application as an application exception and specify an anti-virus action for the application exception.

Use **undo exception application** to remove an application exception or all application exceptions.

Syntax

exception application *application-name* **action** { **alert** | **block** | **permit** }

undo exception application { *application-name* | **all** }

Default

No application exceptions exist.

Views

Anti-virus policy view

Predefined user roles

network-admin

context-admin

Parameters

application-name: Specifies the application name.

action: Specifies an action for the application exception.

all: Specifies all application exceptions.

alert: Permits and logs matching packets.

block: Blocks and logs matching packets.

permit: Permits matching packets.

Usage guidelines

By default, an anti-virus action is protocol specific and applies to all applications carried by the protocol. To take a different action on an application, you can set the application as an exception and specify a different anti-virus action for the application. Application exceptions use application-specific actions and the other applications use protocol-specific actions. For example, the anti-virus action for HTTP is alert. To block the games carried by HTTP, you can set the games as application exceptions and specify the block action for them.

Examples

Set the **163Email** application as an application exception. Specify alert as the anti-virus action for the application exception.

```
<Sysname> system-view
[Sysname] anti-virus policy abc
[Sysname-anti-virus-policy-abc] exception application 163Email action alert
```

exception md5

Use **exception md5** to set an MD5 value as an MD5 exception.

Use **undo exception md5** to remove an MD5 exception or all MD5 exceptions.

Syntax

exception md5 *md5-value*

undo exception md5 { *md5-value* | **all** }

Default

No MD5 exceptions exist.

Views

Anti-virus policy view

Predefined user roles

network-admin

context-admin

Parameters

md5-value: Specifies an MD5 value.

all: Specifies all MD5 exceptions.

Usage guidelines

If false positives occur for a virus, you can set the MD5 value of the virus as an MD5 exception. The device will permit subsequent packets matching the MD5 exception to pass.

You can get the MD5 value of the virus through the threat log.

Examples

In anti-virus policy abc, set MD5 value **2b9c5137769b613f0ea11bd51c324afc** as an MD5 exception.

```
<Sysname> system-view
[Sysname] anti-virus policy abc
[Sysname-anti-virus-policy-abc] exception md5 2b9c5137769b613f0ea11bd51c324afe
```

exception signature

Use **exception signature** to set a signature as a signature exception.

Use **undo exception signature** to remove a signature exception or all signature exceptions.

Syntax

exception signature *signature-id*

undo exception signature { *signature-id* | **all** }

Default

No signature exceptions exist.

Views

Anti-virus policy view

Predefined user roles

network-admin

context-admin

Parameters

signature-id: Specifies the signature ID in the range of 1 to 4294967292.

all: Specifies all signature exceptions.

Usage guidelines

If a virus proves to be a false alarm, you can set the virus signature as a signature exception. Packets matching the signature exception are permitted to pass.

Examples

Set virus signature 101000 as a signature exception.

```
<Sysname> system-view
[Sysname] anti-virus policy abc
[Sysname-anti-virus-policy-abc] exception signature 101000
```

Related commands

display anti-virus signature

inspect

Use **inspect** to configure anti-virus for an application layer protocol.

Use **undo inspect** to cancel anti-virus for an application layer protocol.

Syntax

inspect { **ftp** | **http** | **imap** | **nfs** | **pop3** | **smb** | **smtp** } **direction** { **both** | **download** | **upload** } [**cache-file-size** *file-size*] **action** { **alert** | **block** | **redirect** }

undo inspect { **ftp** | **http** | **imap** | **nfs** | **pop3** | **smb** | **smtp** }

Default

The device performs virus detection on the following packets:

- Upload and download packets for FTP, HTTP, SMB, NFS, and IMAP.
- Download packets for POP3.
- Upload packets for SMTP.

The anti-virus action for FTP, HTTP, NFS, and SMB is block and for IMAP, SMTP, and POP3 is alert.

The maximum size for the file that can be cached for virus detection is 1 MB.

Views

Anti-virus policy view

Predefined user roles

network-admin

context-admin

Parameters

ftp: Specifies the FTP protocol.

http: Specifies the HTTP protocol.

imap: Specifies the IMAP protocol.

nfs: Specifies the NFS protocol. Only NFSv3 is supported.

pop3: Specifies the POP3 protocol.

smb: Specifies the SMB protocol. Only SMBv1 and SMBv2 are supported.

smtp: Specifies the SMTP protocol.

direction: Specifies the anti-virus detection direction. You cannot specify this keyword for POP3 and SMTP because POP3 supports only **download** and SMTP supports only **upload**.

both: Specifies the upload and download directions.

download: Specifies the download direction.

upload: Specifies the upload direction.

cache-file-size *file-size*: Specifies the size of a file that can be cached for virus detection. The file size is in the range of 1 to 24 MB. Only the HTTP protocol supports this option.

action: Specifies an anti-virus action. The anti-virus action for IMAP can only be **alert**.

alert: Permits and logs matching packets.

block: Blocks and logs matching packets.

redirect: Redirects matching HTTP connections to a URL and generates logs. This keyword is applicable to only uploading connections.

Usage guidelines

After you configure this command, the device performs virus detection on packets from the specified direction for the specified protocol. If viruses are detected, the device takes the specified action on the virus packets.

The **direction** keyword is not available for the POP3 and SMTP protocols because the POP3 protocol supports only the download direction and the SMTP protocol supports only the upload direction.

With the HTTP protocol and the **block** action configured, in addition to blocking and logging matching packets, the device also supports displaying an alarm message on the client browser. A default message is predefined. To configure a user-defined alarm message, you can execute the **import block warning-file** command to import the message from a file. For more information about the warning file, see DPI engine configuration in *DPI Configuration Guide*.

Connections of the protocols that anti-virus supports are all initiated by clients. For connections to be established successfully and anti-virus to function correctly, make sure the security zone or the zone pair is correctly configured. The security zone that the clients reside in must be the source security zone and the security zone that the servers reside in must be the destination security zone.

Examples

Configure anti-virus for HTTP. Specify the direction as download and the anti-virus action as alert.

```
<Sysname> system-view
[Sysname] anti-virus policy abc
[Sysname-anti-virus-policy-abc] inspect http direction download action alert
```

Cancel anti-virus for HTTP.

```
<Sysname> system-view
[Sysname] anti-virus policy abc
[Sysname-anti-virus-policy-abc] undo inspect ftp
```

Related commands

import block warning-file

signature severity enable

Use **signature severity enable** to enable the virus signatures at and above a severity level.

Use **undo signature severity enable** to restore the default.

Syntax

signature severity { **critical** | **high** | **medium** } **enable**

undo signature severity enable

Default

Virus signatures of all severity levels are enabled.

Views

Anti-virus policy view

Predefined user roles

network-admin

context-admin

Parameters

critical: Specifies the critical severity level.

high: Specifies the high severity level.

medium: Specifies the medium severity level.

Usage guidelines

After you configure this command, only the virus signatures at and above the specified severity level take effect.

Examples

Enable the virus signatures at and above the high level.

```
<Sysname> system-view
[Sysname] anti-virus policy abc
[Sysname-anti-virus-policy-abc] signature severity high enable
```

update schedule

Use **update schedule** to schedule the automatic virus signature library update.

Use **undo update schedule** to restore the default.

Syntax

update schedule { **daily** | **weekly** { **mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun** } } **start-time** *time* **tingle** *minutes*

undo update schedule

Default

The device starts updating the virus signature library at a random time between 02:01:00 and 04:01:00 every day.

Views

Automatic virus signature library update configuration view

Predefined user roles

network-admin

context-admin

Parameters

daily: Updates the virus signature library every day.

weekly: Updates the virus signature library every week.

mon: Updates the virus signature library every Monday.

tue: Updates the virus signature library every Tuesday.

wed: Updates the virus signature library every Wednesday.

thu: Updates the virus signature library every Thursday.

fri: Updates the virus signature library every Friday.

sat: Updates the virus signature library every Saturday.

sun: Updates the virus signature library every Sunday.

start-time *time*: Specifies the start time in the hh:mm:ss format. The value range is 00:00:00 to 23:59:59.

tingle *minutes*: Specifies the tolerance time in minutes. The value range is 0 to 120. An automatic library update will occur at a random time between the following time points:

- Start time minus half the tolerance time.
- Start time plus half the tolerance time.

Examples

Configure the device to automatically update the virus signature library every Monday at a random time between 20:25:00 and 20:35:00.

```
<Sysname> system-view
[Sysname] anti-virus signature auto-update
[Sysname-anti-virus-autoupdate] update schedule weekly mon start-time 20:30:00 tingle 10
```

Related commands

anti-virus signature auto-update

warning parameter-profile

Use **warning parameter-profile** to apply a warning parameter profile to an anti-virus policy, and enable sending the alarm message defined in the profile.

Use **undo warning parameter-profile** to restore the default.

Syntax

warning parameter-profile *profile-name*

undo warning parameter-profile

Default

No warning parameter profile is applied and the device does not support sending alarm messages.

Views

Anti-virus policy view

Predefined user roles

network-admin

context-admin

Parameters

profile-name: Specifies a warning parameter profile by its name, a case-insensitive string of 1 to 63 characters. Valid characters are letters, digits, underscores (_).

Usage guidelines

If an endpoint user visits a virus-infected website, the device will display an alarm message on the user's browser. The alarm message is stored in the warning parameter profile applied to the policy. For more information about configuring a warning parameter profile, see DPI engine configuration in *DPI Configuration Guide*.

Examples

Apply warning parameter profile **av1** to anti-virus policy **abc** and enable the sending of alarm message defined in the profile.

```
<Sysname> system-view
[Sysname] anti-virus policy abc
[Sysname-anti-virus-policy-abc] warning parameter-profile av1
```

Related commands

inspect warning parameter-profile

Contents

Data analysis center commands

dac email-server client-authentication enable

Use **dac email-server client-authentication enable** to enable email client authentication.

Use **undo dac email-server client-authentication enable** to disable email client authentication.

Syntax

dac email-server client-authentication enable

undo dac email-server client-authentication enable

Default

Email client authentication is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

Enable email client authentication on the device if the email server (specified by the **dac email-server server-address** command) requires client identity authentication.

For successful email client authentication, you must configure the correct username and password for connecting to the email server.

Examples

Enable email client authentication.

```
<Sysname> system-view
[Sysname] dac email-server client-authentication enable
```

Related commands

dac email-server server-address

dac email-server username

dac email-server password

dac email-server password

Use **dac email-server password** to set the password for connecting to the email server.

Use **unto dac email-server password** to restore the default.

Syntax

dac email-server password { **cipher** | **simple** } *string*

undo dac email-server password

Default

The password for connecting to the email server is not specified.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 63 characters. Its encrypted form is a case-sensitive string of 1 to 117 characters.

Usage guidelines

Both the username and password for connecting to the email server are required if email client authentication is enabled.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify **abc123** as the password for connecting to the email server.

```
<Sysname> system-view
[Sysname] dac email-server password simple abc123
```

Related commands

dac email-server client-authentication enable

dac email-server username

dac email-server secure-authentication enable

Use **dac email-server secure-authentication enable** to enable secure transmission of authentication credentials.

Use **undo dac email-server secure-authentication enable** to disable secure transmission of authentication credentials.

Syntax

dac email-server secure-authentication enable

undo dac email-server secure-authentication enable

Default

Secure transmission of authentication credentials is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command enables the device to transmit email client authentication credentials to the email server over a secure channel.

This command takes effect only after email client authentication is enabled.

Examples

Enable secure transmission of authentication credentials.

```
<Sysname> system-view
[Sysname] dac email-server secure-authentication enable
```

Related commands

dac email-server client-authentication enable

dac email-server sender

Use **dac email-server sender** to specify the email sender address.

Use **undo dac email-server sender** to restore the default.

Syntax

dac email-server sender *address-string*

undo dac email-server sender

Default

The email sender address is not specified.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

address-string: Specifies the email sender address, as case-sensitive string of 3 to 63 characters.

Usage guidelines

The data analysis center (DAC) uses the specified email sender address send emails.

Examples

Specify **mailto:abc@123.com** as the email sender address.

```
<Sysname> system-view
[Sysname] dac email-server sender abc@123.com
```

Related commands

dac email-server server-address

dac email-server server-address

Use **dac email-server server-address** to specify the email server address for the DAC.

Use undo **dac email-server server-address** to restore the default.

Syntax

dac email-server server-address *address-string*

undo dac email-server server-address

Default

No email server is specified for the DAC.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

address-string: Specifies the IP address or host name of the email server. The host name is a case-sensitive string of 3 to 63 characters.

Usage guidelines

The DAC can send emails only after the both email server address and email sender address are configured.

If you specify the host name of the email server, make sure the device can obtain the IP address of the email server through a static or dynamic domain name resolution method. The device must reach the IP address of the email server. For more information about domain name resolution, see DNS configuration in *Layer 3—IP Services*.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify 101.1.1.255 as email server address for the DAC.

```
<Sysname> system-view
[Sysname] dac email-server server-address 101.1.1.225
```

Related commands

dac email-server sender

dac email-server username

Use **dac email-server username** to set the username for connecting to the email server.

Use **undo dac email-server username** to restore the default.

Syntax

dac email-server username *username*

undo dac email-server username

Default

The username for connecting to the email server is not specified.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

username: Specifies the username, a case-sensitive string of 1 to 63 characters.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify **admin** as the username for connecting to the email server.

```
<Sysname> system-view
[Sysname] dac email-server username admin
```

Related commands

dac email-server client-authentication enable

dac email-server password

dac log-collect enable

Use **dac log-collect enable** to enable the log collection for a service that is registered to the DAC.

Use **undo dac log-collect enable** to disable the log collection for a service.

Syntax

dac log-collect service *service-type service-name* **enable**

undo dac log-collect service *service-type service-name* **enable**

Default

The log collection status for each service varies by service setting when the service module is registered to the DAC.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

service-type: Specifies the type of a service that is registered to the DAC. The service type name is a case-insensitive string. To view the supported service type, enter a question mark (?) for this argument.

service-name: Specifies the name of a service that is registered to the DAC. The service name is a case-insensitive string. To view the supported service name, enter a question mark (?) for this argument.

Usage guidelines

This command enables the log collection for a specific service. To collect the log messages for the traffic service, first enable the session statistics collection and then enable the log collection.

Repeat this command to enable log collection for multiple services.

Examples

Enable the log collection for the DPI traffic service.

```
<Sysname> system-view
[Sysname] dac log-collet service dpi traffic enable
```

Related commands

display dac log-collect

dac log-display enable

Use **dac log-display enable** to enable the real-time log display.

Use **undo dac log-collect enable** to disable the real-time log display.

Syntax

dac log-display service *service-type service-name* **enable**

undo dac log-display service *service-type service-name* **enable**

Default

The real-time log display for all services is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

service-type: Specifies the type of a service that is registered with the DAC. The service type name is a case-insensitive string. To view the supported service type, enter a question mark (?) for this argument.

service-name: Specifies the name of a service that is registered with the DAC. The service name is a case-insensitive string. To view the supported service name, enter a question mark (?) for this argument.

Usage guidelines

This command for a service takes effect only after the log collection for the service is enabled by the **dac log-collect enable** command.

With this feature enabled, you can see the real-time log messages displayed on the Web interface.

Repeat this command to enable real-time log display for multiple services.

DPI do not support this feature in the current software version.

Examples

Enable the real-time display for system logs.

```
<Sysname> system-view
[Sysname] dac log-display service syslog syslog enable
```

Related commands

dac log-collect enable

display dac log-display

dac report

Use **dac report** to configure the subscription parameters for a report type.

Use **undo dac report** to remove the subscription parameters for a report type.

Syntax

dac report type { **comparison** | **integrated** | **intelligent** | **summary** } **subscriber** *mail-address* [**language** { **chinese** | **english** }]

undo dac report type { **comparison** | **integrated** | **intelligent** | **summary** } [**subscriber** *mail-address*]

Default

No report subscription parameters are configured.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

comparison: Specifies the comparison report.

integrated: Specifies the integrated report.

intelligent: Specifies the intelligent report.

summary: Specifies the summary report.

subscriber *mail-address*: Specifies the email address of the report subscriber, a case-sensitive string of 3 to 63 characters. If you do not specify a subscriber, the **undo** command removes all subscribers for the specified report type.

language: Specifies a language for the reports. If you do not specify this keyword, Chinese is used in the reports.

chinese: Uses Chinese in the reports.

english: Uses English in the reports.

Usage guidelines

You can configure a maximum of 50 subscribers for each report type.

Examples

Specify **admin@qq.com** and English as the subscriber address and language for the summary report, respectively.

```
<Sysname> system-view
[Sysname] dac report type summary subscriber admin@qq.com language english
```

Remove subscriber address **admin@qq.com** for the summary report.

```
<Sysname> system-view
[Sysname] undo dac report type summary subscriber admin@qq.com
```

Related commands

display dac report

dac report export

Use **dac report export** to configure report export parameters.

Use **undo dac report export** to delete report export parameters.

Syntax

dac report export period { **day** | **hour** | **month** | **quarter** | **week** | **year** } **template** *template-name* [**mail-address** *mail-address*]

undo dac report export period { **day** | **hour** | **month** | **quarter** | **week** | **year** } **template** *template-name* [**mail-address** *mail-address*]

Default

No report export parameters are configured.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

period: Specifies the type of the periodic report.

day: Specifies the daily report.

hour: Specifies the hourly report.

month: Specifies the monthly report.

quarter: Specifies the quarterly report.

week: Specifies the weekly report.

year: Specifies the annual report.

template *template-name*: Specifies the template name, a case insensitive string of 1 to 63 characters.

mail-address *mail-address*: Specifies the mail address to which the reports are exported. The mail address is a case sensitive string of 3 to 63 characters. If you do not specify this option, the reports are exported to the local device.

Usage guidelines

This command enables the device to periodically export the reports of the specified types.

To export reports of multiple types to multiple mail addresses, repeat this command.

If you do not specify the mail address for the **undo** command, all mail addresses are deleted.

Examples

Configure the device to use template **template1** to export reports to the address www@126.com every week.

```
<Sysname> system-view
[Sysname] dac report export period week template template1 mail-address www@126.com
```

Related commands

display dac report export

dac report export template

dac report export template

Use **dac report export template** to create a report export template and enter its view, or enter the view of an existing report export template.

Use **undo dac report export template** to delete a report export template.

Syntax

dac report export template *template-name*

undo dac report export template *template-name*

Default

No report export template exists.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

template-name: Specifies the name of a report export template. The name is a case insensitive string of 1 to 63 characters.

Usage guidelines

In a report export template, you can define the following items:

- Report language.
- Statistics contents in the report.

Examples

Create a report export template named **template1**, and enter its view.

```
<Sysname> system-view
[Sysname] dac report export template template1
[Sysname-dac-report-export-template-template1]
```

Related commands

display dac report export template

dac storage

Use **dac storage** to configure the data storage limits for a service.

Use **undo dac storage** to restore the default.

Syntax

dac storage service *service-type service-name* **limit** { **hold-time** *time-value* | **usage** *usage-value* | **action** { **delete** | **log-only** } }

undo dac storage service *service-type service-name* **limit** { **hold-time** | **usage** | **action** }

Default

The service data can be saved for a maximum of 365 days.

The data of each service can occupy up to 20% of the total storage space.

If the storage time or storage space usage limit is exceeded, the system deletes the expired or the oldest data.

Views

System view

Predefined user roles

network-admin

Parameters

service-type: Specifies the type of a service that is registered with the DAC. The service type name is a case-insensitive string. To view the supported service type, enter a question mark (?) for this argument.

service-name: Specifies the name of a service that is registered with the DAC. The service name is a case-insensitive string. To view the supported service name, enter a question mark (?) for this argument.

limit: Configures the data storage limits for a service.

hold-time *time-value*: Specifies the storage time limit in days. The value range is 1 to 65535. The storage time limit should be longer than the number of days that the oldest service data has been stored for.

usage *usage-value*: Specifies the percentage of the total storage space the service data can occupy. The value range is 1 to 100. The storage usage limit should be higher than the current storage usage of the service.

action: Specifies the action to take when a data storage limit is exceeded.

delete: Deletes data collected on the oldest dates and generates a log message. The data of the current date cannot be deleted.

log-only: Generates a log message only. When a storage limit is exceeded, old data are not deleted and new data cannot be saved.

Usage guidelines

The DAC periodically checks the data of each service to determine if the storage time or storage space usage limit is exceeded.

- If a storage limit is exceeded and the action is **delete**, the system deletes the expired or the oldest service data. A log will be generated to report the event.
- If a storage limit is exceeded and the action is **log-only**, the system generates a log message. New data will not be saved.

If you execute this command to set the storage time limit for a service multiple times, the most recent configuration takes effect. The same is true for setting the storage space limit or storage limit-violated action for a service. You can view the storage space usage of each service on the Web interface.

This command is supported only on the default context. For more information about contexts, see context configuration in *Virtual Technologies Configuration Guide.*

Examples

Set the storage time limit, storage space limit, and the action to take when the limits are exceeded for the traffic service.

```
<Sysname> system-view
```

```
[Sysname] dac storage service dpi traffic limit hold-time 60
[Sysname] dac storage service dpi traffic limit usage 30
[Sysname] dac storage service dpi traffic limit action delete
```

dac traffic-statistic enable

Use **dac traffic-statistic enable** to enable real-time traffic statistics collection.

Use **undo dac traffic-statistic enable** to disable real-time traffic statistics collection.

Syntax

dac traffic-statistic { **application** | **user** } **enable** [**verbose**]

undo dac traffic-statistic { **application** | **user** } **enable**

Default

The real-time traffic statistics collection is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

application: Collects application traffic statistics in real time.

user: Collects user traffic statistics in real time.

verbose: Collects detailed traffic information in real time. If you do not specify this keyword, this command collects brief traffic information in real time.

Usage guidelines

Enable real-time traffic statistics collection with caution when large-volume service traffic exists. This feature is CPU intensive.

To collect the traffic statistics in real time, you must first enable the session statistics collection. For more information about the collected session statistics, see session management in *Security Configuration Guide*.

The detailed information about user traffic that is collected in real time provides used applications on a per-user basis.

The detailed information about application traffic that is collected in real time provides user information on a per-application basis.

Repeat this command to enable multiple collections of real-time traffic statistics.

Examples

Enable the collection of detailed user traffic statistics in real time.

```
<Sysname> system-view
[Sysname] dac traffic-statistic user enable verbose
```

Related commands

display dac traffic-statistic

display dac email-server

Use **display dac email-server** to display the email server configuration of the DAC.

Syntax

display dac email-server

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display the email server configuration of the DAC.

```
<Sysname> display dac email-server
Mail server address : 2.2.2.2
        Mail sender address : qqq@11.com
             Authentication : Enable
      secure-authentication : Enable
                  Username : lkx
                  password : ******
```

Table 1 Command output

Field	Description
Authentication	Enabling status of the email client authentication.
Secure-authentication	Enabling status of the secure transmission of authentication credentials.
Username	Username for connecting to the email server.
Password	Password for connecting to the email server.

display dac log-collect

Use **display dac log-collect** to display the log collection configuration for a service.

Syntax

display dac log-collect { **all** | **service** *service-type service-name* }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

all: Specifies all types of services that are registered with the DAC. The DAC provides functions only for services that have registered with the DAC.

service-type: Specifies the type of a service that is registered with the DAC. The service type name is a case-insensitive string. To view the supported service type, enter a question mark (?) for this argument.

service-name: Specifies the name of a service that is registered with the DAC. The service name is a case-insensitive string. To view the supported service name, enter a question mark (?) for this argument.

Examples

Display the log collection configuration for all services.

```
<Sysname> system-view
[Sysname] display dac log-collect all
Service type       Service              Status

Slot 1:
dpi                audit                Disabled
dpi                ffilter              Disabled
dpi                threat               Disabled
dpi                traffic              Enabled
dpi                uflt                 Disabled
```

Table 2 Command output

Field	Description
Service	Service name.
Status	Status of the log collection: **Disabled** or **Enabled**.

Related commands

dac log-collect enable

display dac log-display

Use **display dac log-display** to display the configuration of the real-time log display.

Syntax

display dac log-display { **all** | **service** *service-type service-name* }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

all: Specifies all types of services that are registered with the DAC. The DAC provides functions only for services that have registered with the DAC.

service-type: Specifies the type of a service that is registered with the DAC. The service type name is a case-insensitive string. To view the supported service type, enter a question mark (?) for this argument.

service-name: Specifies the name of a service that is registered with the DAC. The service name is a case-insensitive string. To view the supported service name, enter a question mark (?) for this argument.

Examples

Display the configuration of the real-time log display for all types of services.

```
<Sysname> system-view
[Sysname] display dac log-display all
Service type        Service             Status

Slot 1 :
lb                  linkapp             Disabled
lb                  protectwarning      Disabled
attack-defense      flood               Disabled
syslog              cfglog              Disabled
lb                  virtualserver       Disabled
lb                  overviewvs          Disabled
attack-defense      ipcar_statistics    Disabled
sandbox             log                 Disabled
lb                  virtualserverstatus Disabled
lb                  overviewsf          Disabled
lb                  domain              Disabled
lb                  protectattack       Disabled
attack-defense      scan                Disabled
packet-filter       security_policy     Disabled
lb                  serverfarm          Disabled
lb                  member              Disabled
lb                  nodewarning         Disabled
dlp                 dlp_file_upload     Disabled
dpi                 terminal            Disabled
dlp                 dlp_eventlog        Disabled
---- More ----
```

Table 3 Command output

Field	Description
Service	Service name.
Status	Status of the log collection: **Disabled** or **Enabled**.

Related commands

dac log-display enable

display dac report

Use **display dac report** to display report subscriber information.

Syntax

display dac report [**comparison** | **integrated** | **intelligent** | **summary**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

comparison: Specifies the comparison report.

integrated: Specifies the integrated report.

intelligent: Specifies the intelligent report.

summary: Specifies the summary report.

Usage guidelines

If you do not specify a report type, this command displays subscriber information for all report types.

Examples

Display subscriber information for all report types.

```
<Sysname> display dac report
Total subscribers:4
Summary subscribers:1
Comparison subscribers:1
Intelligent subscribers:1
Integrated subscribers:1
Report type       Language    Subscriber email
Summary           CH          124@123.com
Comparison        CH          111@123.com
Intelligent       EN          123@123.com
Integrated        EN          112@123.com
```

Table 4 Command output

Field	Description
Total subscribers	Total number of subscribers.
Summary subscribers	Number of subscribers for the summary report.
Comparison subscribers	Number of subscribers for the comparison report.
Intelligent subscribers	Number of subscribers for the intelligent report.
Integrated subscribers	Number of subscribers for the integrated report.
Language	Language used in the reports:

Field	Description
	• **CH**—Chinese. • **EN**—English.
Subscriber email	Email address of a report subscriber.

display dac report export

Use **display dac report export** to display report export configuration.

Syntax

display dac report export

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display report export configuration.

```
<Sysname> display dac report export
  Mail address:  ttt@126.com
  Period:        Week, Month, Year
  Template name: hhh

  Mail address:  123@126.com
  Period:        Day
  Template name: 111
```

Table 5 Command output

Field	Description
Mail-address	Mail address to which the reports are exported. If no mail address is specified, this field displays a hyphen (**-**), and the reports are exported to the local device.
Period	Type of the periodic report: • **hour**—Hourly report. • **day**—Daily report. • **week**—Weekly report. • **month**—Monthly report. • **quarter**—Quarterly report. • **year**—Annual report.
Template name	Name of the report export template.

Related commands

dac report export

display dac report export template

Use **display dac report export template** command to display report export templates.

Syntax

display dac report export template [*template-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

template-name: Specifies the name the report export template. The name is a case insensitive string of 1 to 63 characters. If you do not specify a template name, this command exports all report export templates.

Examples

Display all report export templates.

```
<Sysname> display dac report export template
Template name: template1
  Language:             English
  Export service:       lb-link
    Statistics content: app
    Link name:          lk
  Export service:       lb-vs
    Statistics content: class
    Virtual server:     lkvs
```

Table 6 Command output

Field	Description
Template name	Name of the report export template.
Language	Language used by the report: • Chinese. • English.
Export service	Service that the report is about: • lb-link—Load balancing link. • lb-vs—Load balancing virtual server.
Statistic content	Statistics content.
Link-name	Load balancing link name.
Virtual Server	Load balancing virtual server name.

display dac storage

Use **display dac storage** to display the data storage limit configuration for services.

Syntax

display dac storage [*service-type service-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

service-type: Specifies the type of a service that is registered with the DAC. The service type name is a case-insensitive string. To view the supported service type, enter a question mark (?) for this argument.

service-name: Specifies the name of a service that is registered with the DAC. The service name is a case-insensitive string. To view the supported service name, enter a question mark (?) for this argument.

Usage guidelines

If you do not specify a service, this command displays the data storage limit configuration for all services.

This command is supported only on the default context. For more information about contexts, see context configuration in *Virtual Technologies Configuration Guide*.

Examples

Displays the data storage limit configuration for all services.

```
<Sysname> display dac storage
Total services           :25

Service type     Service name            Time limit (days)       Usage limit
         Action
syslog           cfglog                  365                     20%
         delete
lb               virtualserver           365                     20%
         delete
lb               overviewvs              365                     20%
         delete
sandbox          log                     365                     20%
---- More ----
```

Table 7 Command output

Field	Description
Total services	Total number of services.
Time limit	Storage time limit in days.
Usage limit	Storage space usage limit in percentage.
Action	Action to take when the storage time limit or space limit is exceed.

Field	Description
	• **delete**—Delete the oldest data, and generates a log message. • **log-only**—Generate a log message only.

display dac traffic-statistic

Use **display dac traffic-statistic** to display the configuration of the real-time traffic statistics collection.

Syntax

display dac traffic-statistic [**application** | **user**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

application: Specifies the collection of the real-time application traffic statistics.

user: Specifies the collection of the real-time user traffic statistics.

Usage guidelines

If you do not specify any keyword, this command displays the configuration of the collection for all real-time traffic statistics.

Examples

Displays the configuration of the real-time user traffic statistics collection.

```
<Sysname> system-view
[Sysname] display dac traffic-statistic user
Slot 1:
Type               Status
User               Enabled (verbose)
```

Table 8 Command output

Field	Description
Type	Type of traffic collected in real time: • **Application**. • **User**.
Status	Status of the real-time traffic statistics collection: • **Disabled**—This feature is disabled. • **Enabled (brief)**—This feature is enabled, and the DAC collects brief traffic information. • **Enabled (verbose)**—This feature is enabled, and the DAC collects detailed traffic information.

Related commands

dac traffic-statistic enable

export-service

Use **export-service** to create the statistics report view of a service and enter the view.

Use **undo export-service** to delete the configuration in the specified statistics report view.

Syntax

export-service { **lb-link** | **lb-virtual-server** }

undo export-service { **lb-link** | **lb-virtual-server** }

Views

Report export template view

Predefined user roles

network-admin

context-admin

Parameters

lb-link: Specifies the LB link statistics.

lb-virtual-server: Specifies the LB virtual server statistics.

Usage guidelines

In the report view of a service, you can specify the statistics contents to be included in the report.

Examples

In report export template **template1**, enter the LB link statistics report view.

```
<Sysname> system-view
[Sysname] dac report export template template1
[Sysname-dac-template-template1] export-service lb-link
[Sysname-dac-template-template1-service-lblink]
```

Related commands

statistics content (LB link statistics report view)

statistics content (LB virtual server statistics report view)

statistics link

statistics virtual-server

language

Use **language** to specify the language used in exported reports.

Use **undo language** to restore the default.

Syntax

language { **chinese** | **english** }

undo language

Default

Chinese is used.

Views

Report export template view

Predefined user roles

network-admin

context-admin

Parameters

chinese: Specifies Chinese.

english: Specifies English.

Examples

In report export template **template1**, specify English as the language used in exported reports.

```
<Sysname> system-view
[Sysname] dac report export template template1
[Sysname-dac-template-template1] language english
```

statistics content (LB link statistics report view)

Use **statistics content** to specify the contents for the LB link statistics report.

Use **undo statistics content** to delete contents from the LB link statistics report.

Syntax

statistics content { abnormal-flow | app | connection-count | connection-rate | delay | packetloss | stability } *

undo statistics content { abnormal-flow | app | connection-count | connection-rate | delay | packetloss | stability } *

Default

No content is specified for the LB link statistics report.

Views

LB link statistics report view

Predefined user roles

network-admin

context-admin

Parameters

abnormal: Specifies abnormal traffic statistics.

app: Specifies application statistics.

connection-count: Specifies the connection count statistics.

connection-rate: Specifies the connection rate statistics.

delay: Specifies the delay statistics.

packetloss: Specifies the packet loss statistics.

stability: Specifies link state statistics.

Usage guidelines

This command is required for LB link statistics reports. If no contents are specified, no LB link statistics reports will be exported.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

In LB link statistics report view, specify the application statistics as the report content.

```
<Sysname> system-view
[Sysname] dac report export template template1
[Sysname-dac-template-template1] export-service lb-link
[Sysname-dac-template-template1-service-lblink] statistics content app
```

statistics content (LB virtual server statistics report view)

Use **statistics content** to specify the content for the LB virtual link statistics report.

Use **undo statistics content** to delete content from the LB virtual server statistics report.

Syntax

statistics content class

undo statistics content class

Default

No content is specified for the LB virtual server statistics report.

Views

LB virtual server statistics report view

Predefined user roles

network-admin

context-admin

Parameters

class: Specify the LB class. The report contains the packet matching statistics for LB classes.

Usage guidelines

This command is required for LB virtual server statistics reports. If no content is specified, no LB virtual server statistics reports will be exported.

Examples

In LB virtual server statistics report view, specify the LB classes as the content in LB virtual server statistics report.

```
<Sysname> system-view
[Sysname] dac report export template template1
[Sysname-dac-template-template1] export-service lb-virtual-server
[Sysname-dac-template-template1-service-lbvs] statistics content class
```

statistics link

Use **statistics link** to specify an LB link for the LB link statistics report.

Use **undo statistics link** to delete an LB link from the LB link statistics report.

Syntax

statistics link *name*

undo statistics link *name*

Default

No LB link is specified for the LB link statistics report.

Views

LB link statistics report view

Predefined user roles

network-admin

context-admin

Parameters

Name: Specifies the name of an LB link, a case insensitive string of 1 to 63 characters.

Usage guidelines

This command allows the DAC to export statistics report for the specified LB links.

Repeat this command to specify multiple object links.

Examples

In LB link statistics report view, specify **link1** and **link2** as the statistics objects.

```
<Sysname> system-view
[Sysname] dac report export template template1
[Sysname-dac-template-template1] export-service lb-link
[Sysname-dac-template-template1-service-lblink] statistics link link1
[Sysname-dac-template-template1-service-lblink] statistics link link2
```

Related commands

statistics content (LB link statistics report view)

statistics virtual-server

Use **statistics virtual-server** to specify a virtual server for the LB virtual server statistics report.

Use **undo statistics virtual-server** to delete a virtual server from the LB virtual server statistics report.

Syntax

statistics virtual-server *name*

undo statistics virtual-server *name*

Default

No LB virtual server object is specified for the LB virtual server statistics report.

Views

LB virtual server statistics report view

Predefined user roles

network-admin

context-admin

Parameters

Name: Specifies the name of the virtual server, a case insensitive of 1 to 63 characters.

Usage guidelines

This command allows the DAC to export statistics report for the specified LB virtual server.

Repeat this command to specify multiple LB virtual servers.

Examples

In LB virtual server statistics report view, specify **vs1** as the statistics object.

```
<Sysname> system-view
[Sysname] dac report export template template1
[Sysname-dac-template-template1] export-service lb-virtual-server
[Sysname-dac-template-template1-service-lbvs] statistics virtual-server vs1
```

Related commands

`statistics content` (LB virtual server statistics report view)

Contents

Proxy policy commands

action

Use **action** to set the action for traffic matching a proxy policy rule.

Use **undo action** to restore the default.

Syntax

action { **no-proxy** | **ssl-decrypt** | **tcp-proxy** }

undo action

Default

The no-proxy action is used.

Views

Proxy policy rule view

Predefined user roles

network-admin

context-admin

Parameters

no-proxy: Specifies the no-proxy action.

ssl-decrypt: Specifies the SSL decryption action.

tcp-proxy: Specifies the TCP proxy action.

Usage guidelines

The device supports the following actions for traffic matching a proxy policy rule:

- **No-proxy**—The device directly transmits the traffic without TCP or SSL proxy.
- **SSL-decryption**—The device acts as an SSL proxy to decrypt the SSL traffic and performs deep packet inspection and Layer 7 load balancing on the decrypted traffic. SSL decryption is implemented based on TCP proxy.
- **TCP-proxy**—The device acts as a TCP proxy and provides TCP-layer isolation between the TCP client and TCP server to effectively intercept malicious connections and attacks.

If you execute this command for a proxy policy rule multiple times, the most recent configuration takes effect.

Examples

Specify the **ssl-decrypt** action for proxy policy rule **rule1**.

```
<Sysname> system-view
[Sysname] app-proxy-policy
[Sysname-app-proxy-policy] rule 1 name rule1
[Sysname-app-proxy-policy-0-rule1] action ssl-decrypt
```

Related commands

display app-proxy-policy

rule

app-proxy internal-server-certificate delete

Use **app-proxy internal-server-certificate delete** to delete an internal server certificate.

Syntax

app-proxy internal-server-certificate delete md5 *md5-value*

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

md5 *md5-value*: Specifies the MD5 value of an internal server certificate.

Usage guidelines

When an internal server certificate expires or an internal server does not need to be protected, you can execute this command to delete the imported internal server certificate.

You can execute the **display app-proxy imported internal-server-certificate** command to view the MD5 values of the internal server certificates.

Examples

Delete the internal server certificate with the MD5 value **c4f5f2c41ca1de4258d893c9887bf287**.

```
<Sysname> system-view
[Sysname] app-proxy internal-server-certificate delete md5
c4f5f2c41ca1de4258d893c9887bf287
```

Related commands

display app-proxy imported internal-server-certificate

app-proxy internal-server-certificate import

Use **app-proxy internal-server-certificate import** to import an internal server certificate.

Syntax

app-proxy internal-server-certificate import { **p12** | **pem** } **filename** *filename*

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

p12: Specifies the PKCS#12 certificate file format.

pem: Specifies the PEM certificate file format.

filename *filename*: Specifies the certificate file name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

The internal server certificates are required in the scenario of protecting internal servers. With an internal server certificate imported, the device will decrypt the certificate and generate a CER file and a key file. The CER file is used to identify the server and the key file is used to encrypt and decrypt the packets in the subsequent SSL proxy process. The device will calculate the MD5 value of the CER file and use the MD5 value as the unique identifier of the file.

The SSL proxy process is as follows:

1. The device receives an internal server certificate and calculates the MD5 value of the certificate.
2. The device compares the calculated MD5 value with the MD5 value of the imported internal server certificate:
   - If they are the same, the certificate is trusted and the device will use the certificate to establish an SSL connection with the client.
   - If they are different, the certificate is untrusted.

You can import multiple internal server certificates. If two certificates have the same MD5 value, the new certificate will overwrite the old certificate.

Examples

Import a PKCS#12 certificate file as an internal server certificate.

```
<Sysname> system-view
[Sysname] app-proxy internal-server-certificate import p12 filename server.p12
Password:
```

Related commands

display app-proxy imported internal-server-certificate

app-proxy ssl whitelist activate

Use **app-proxy ssl whitelist activate** to activate SSL proxy whitelist settings.

Syntax

app-proxy ssl whitelist activate

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

The following SSL proxy whitelist settings must be manually activated by using this command:

- Adding or removing hostnames to or from the user-defined SSL hostname whitelist.
- Enabling or disabling hostnames on the predefined SSL hostname whitelist.

This command is supported only on the default context. For more information about contexts, see context configuration in *Virtual Technologies Configuration Guide.*

Examples

Add **example.com** to the user-defined SSL hostname whitelist and activate the setting.

```
<Sysname> system-view
[Sysname] app-proxy ssl whitelist user-defined-hostname example.com
To activate the setting, execute app-proxy ssl whitelist activate.
[Sysname] app-proxy ssl whitelist activate
```

Related commands

app-proxy ssl whitelist predefined-hostname enable

app-proxy ssl whitelist user-defined-hostname

app-proxy ssl whitelist predefined-hostname enable

Use **app-proxy ssl whitelist predefined-hostname enable** to enable hostnames on the predefined SSL hostname whitelist.

Use **undo app-proxy ssl whitelist predefined-hostname enable** to disable hostnames on the predefined SSL hostname whitelist.

Syntax

app-proxy ssl whitelist predefined-hostname { **chrome-hsts** [*hostname*] | *hostname* } **enable**

undo app-proxy ssl whitelist predefined-hostname { **chrome-hsts** [*hostname*] | *hostname* } **enable**

Default

The entire predefined SSL hostname whitelist is enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

chrome-hsts [*hostname*]: Specifies a hostname on the Chrome HSTS list. The *hostname* argument represents the hostname, a case-insensitive string of 1 to 63 characters. If the hostname contains spaces, enclose it in double quotation marks. For example, **"user for test"**. If you do not specify a hostname, this command applies to all hostnames on the Chrome HSTS list.

host-name: Specifies a hostname that is not on the Chrome HSTS list. The hostname is a case-insensitive string of 1 to 63 characters. If the hostname contains spaces, enclose it in double quotation marks. For example, **"user for test"**.

Usage guidelines

The Chrome HSTS list is a predefined list of server hostnames that are accessible to Web browsers only through HTTPS.

Follow these guidelines to enable or disable hostnames on the Chrome HSTS list:

- When the entire Chrome HSTS list is enabled, you can disable individual hostnames on the list.
- When the entire Chrome HSTS list is disabled, all hostnames on the list are disabled and cannot be enabled individually.

This command is supported only on the default context. For more information about contexts, see context configuration in *Virtual Technologies Configuration Guide.*

Examples

Disable the entire Chrome HSTS list.

```
<Sysname> system-view
[Sysname] undo app-proxy ssl whitelist predefined-hostname chrome-hsts enable
To activate the setting, execute app-proxy ssl whitelist activate.
```

Disable hostname **12306.cn** on the predefined SSL hostname whitelist.

```
<Sysname> system-view
[Sysname] undo app-proxy ssl whitelist predefined-hostname 12306.cn enable
To activate the setting, execute app-proxy ssl whitelist activate.
```

Related commands

app-proxy ssl whitelist activate

display app-proxy ssl whitelist

app-proxy ssl whitelist user-defined-hostname

Use **app-proxy ssl whitelist user-defined-hostname host-name** to add a hostname to the user-defined SSL hostname whitelist.

Use **undo app-proxy ssl whitelist user-defined-hostname** to remove hostnames from the user-defined SSL hostname whitelist.

Syntax

app-proxy ssl whitelist user-defined-hostname *host-name*

undo app-proxy ssl whitelist user-defined-hostname { *host-name* | **all** }

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

host-name: Specifies a hostname, a case-insensitive string of 1 to 63 characters. If the hostname contains spaces, enclose it in double quotation marks. For example, **"user for test"**.

all: Specifies all hostnames on the user-defined SSL hostname whitelist.

Usage guidelines

If the **DNS Name** or **Common Name** value in a server certificate contains a hostname on the SSL hostname whitelist, the device does not proxy the SSL connections destined for the server.

This command must be manually activated by using the **app-proxy ssl whitelist activate** command.

This command is supported only on the default context. For more information about contexts, see context configuration in *Virtual Technologies Configuration Guide.*

Examples

Add **example.com** to the user-defined SSL hostname whitelist and active the configuration.

```
<Sysname> system-view
[Sysname] app-proxy ssl whitelist user-defined-hostname example.com
To activate the setting, execute app-proxy ssl whitelist activate.
```

```
[Sysname] app-proxy ssl whitelist activate
```

Related commands

app-proxy ssl whitelist activate

display app-proxy ssl whitelist

app-proxy ssl-decrypt-certificate delete

Use **app-proxy ssl-decrypt-certificate delete** to delete an SSL decryption certificate.

Syntax

app-proxy ssl-decrypt-certificate delete filename *filename*

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

filename: Specifies an SSL decryption certificate by its file name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

The device, acting as an SSL proxy, requires the correct SSL decryption certificate to issue proxy server certificates to send to clients for server authentication. If the required SSL decryption certificate is not available, the device cannot set up a connection with the client and the SSL traffic will be transmitted directly without SSL decryption.

After an SSL decryption certificate is imported, its file extension will be changed to .cer, which must be appended to the file name when you delete the certificate.

Examples

Delete SSL decryption certificate **aaa.cer**.

```
<Sysname> system-view
[Sysname] app-proxy ssl-decrypt-certificate delete filename aaa.cer
```

Related commands

display app-proxy ssl-decrypt-certificate

app-proxy ssl-decrypt-certificate import

Use **app-proxy ssl-decrypt-certificate import** to import a CA certificate as a trusted or untrusted SSL decryption certificate.

Syntax

app-proxy ssl-decrypt-certificate import { **trusted** | **untrusted** } { **pem** | **p12** } **filename** *filename*

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

trusted: Imports the CA certificate as a trusted SSL decryption certificate.

untrusted: Imports the CA certificate as an untrusted SSL decryption certificate.

pem: Specifies the PEM certificate file format.

p12: Specifies the PKCS#12 certificate file format.

filename *filename*: Specifies the certificate file name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

The device supports a maximum of one trusted SSL decryption certificate and one untrusted SSL decryption certificate. When importing an SSL decryption certificate, you must mark the certificate as **Trusted** or **Untrusted**. If you import multiple trusted or multiple untrusted SSL decryption certificates to the device, the most recent configuration takes effect.

To use the same CA certificate as both the trusted and untrusted SSL decryption certificate, first import the certificate with the **Trusted** or **Untrusted** tag, and then add the other tag to the certificate by using the **app-proxy ssl-decrypt-certificate modify** command.

After an SSL decryption certificate is imported, its file extension will be changed to .cer.

After receiving the certificate of the real server, the device verifies the legitimacy of the server certificate on behalf of the SSL client.

- If the server certificate is legitimate, the device uses the trusted SSL decryption certificate to issue a new certificate to the client. A server certificate issued by the trusted SSL decryption certificate is trusted by the client.
- If the server certificate is illegitimate, the device uses the untrusted SSL decryption certificate to issue a new certificate to the client. A security alarm will be generated on the client and users must clear the alarm to continue the access.

The trusted SSL decryption certificate must be installed on the client browser. Otherwise, the client cannot trust the proxy server certificate signed by the trusted SSL decryption certificate and might display a warning or directly terminate proxied SSL connections without a warning.

A Firefox browser does not use the SSL decryption certificate in the Windows certificate store by default. To use the SSL decryption certificate on the Firefox browser, you can take the following methods:

- Import the SSL decryption certificate into the Firefox browser.
- Configure the Firefox browser to use the SSL decryption certificate in the Windows certificate store through the following steps:
  a. Enter **about:config** in the address bar.
  b. In the **Search** box, enter **security.enterprise_roots.enabled**.
  c. Locate this entry, and double-click or right-click its value to change **false** to **true**.

Examples

Import a PKCS#12 certificate file as a trusted SSL decryption certificate.

```
<Sysname> system-view
[Sysname] app-proxy ssl-decrypt-certificate import trusted p12 filename aaa.p12
Password:
```

Related commands

display app-proxy ssl-decrypt-certificate certificate

app-proxy ssl-decrypt-certificate modify

Use **app-proxy ssl-decrypt-certificate modify** to add the **Trusted** or **Untrusted** tag to an SSL decryption certificate.

Use **undo app-proxy ssl-decrypt-certificate modify** to remove the **Trusted** or **Untrusted** tag from an SSL decryption certificate.

Syntax

app-proxy ssl-decrypt-certificate modify { **trusted** | **untrusted** } **filename** *filename*

undo app-proxy ssl-decrypt-certificate modify { **trusted** | **untrusted** }

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

trusted: Specifies the **Trusted** tag.

untrusted: Specifies the **Untrusted** tag.

filename: Specifies the SSL decryption certificate by its file name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

To use the same CA certificate as both the trusted and untrusted SSL decryption certificate, first import the certificate with the **Trusted** or **Untrusted** tag, and then use this command add the other tag to the certificate.

When you add the **Trusted** or **Untrusted** tag to an SSL decryption certificate, the system asks whether you want to overwrite the SSL decryption certificate with the same tag if such a certificate already exists.

Removing the **Trusted** or **Untrusted** tag from an SSL decryption certificate does not remove the certificate file from the system. You can use the **app-proxy ssl-decrypt-certificate modify** command to add the **Trusted** or **Untrusted** tag to the certificate again.

After an SSL decryption certificate is imported, its file extension will be changed to .cer. Append the .cer file extension when you specify the file containing the certificate whose credibility you want to change.

Examples

Add the **Trusted** tag to the CA certificate in certificate file **aaa**.

```
<Sysname> system-view
[Sysname] app-proxy ssl-decrypt-certificate modify trusted filename aaa.cer
[Sysname] A trusted CA certificate already exists. Overwrite the existing trusted CA
certificate with the specified certificate? [Y/N]:
```

Related commands

display app-proxy ssl-decrypt-certificate

app-proxy-policy

Use **app-proxy-policy** to enter proxy policy view.

Use **undo app-proxy-policy** to remove all proxy policy configurations.

Syntax

app-proxy-policy

undo app-proxy-policy

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

The device supports only one IPv4 proxy policy.

Examples

Enter proxy policy view.

```
<Sysname> system-view
[Sysname] app-proxy-policy
[Sysname-app-proxy-policy]
```

Related commands

display app-proxy-policy

default action

Use **default-action** to specify the default action for the proxy policy.

Use **undo default-action** to restore the default.

Syntax

default action { **no-proxy** | **ssl-decrypt** | **tcp-proxy** }

undo default action

Default

The proxy policy uses the no-proxy action.

Views

Proxy policy view

Predefined user roles

network-admin

context-admin

Parameters

no-proxy: Specifies the no-proxy action.

ssl-decrypt: Specifies the SSL decryption action.

tcp-proxy: Specifies the TCP proxy action.

Usage guidelines

The default action applies to packets that do not match any rules in the proxy policy.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the default action to **ssl-decrypt** for the proxy policy.

```
<Sysname> system-view
[Sysname] app-proxy-policy
[Sysname-app-proxy-policy] default action ssl-decrypt
```

default ssl-decrypt protect-mode

Use **default ssl-decrypt protect-mode** to specify an SSL decryption protection mode for the proxy policy.

Use **undo default ssl-decrypt protect-mode** to restore the default.

Syntax

default ssl-decrypt protect-mode { **client** | **server** }

undo default ssl-decrypt protect-mode

Default

The SSL decryption protection mode of the proxy policy is **client**.

Views

Proxy policy view

Predefined user roles

network-admin

context-admin

Parameters

client: Specifies client protection.

server: Specifies server protection.

Usage guidelines

The SSL decryption supports the following protection services:

- **Internal client protection**—The device is deployed at the exit of the network where the internal clients are. When the internal clients access an external server, the device acts as a proxy server to decrypt the packets and perform deep packet inspection on the decrypted packets. It protects the internal clients from being attacked by external malicious websites. In this scenario, the device requires imported SSL decryption certificates to establish SSL connections with the clients.
- **Internal server protection**—The device is deployed at the entrance of the network where the internal servers are. When the external clients access an internal server, the device acts as a proxy server to decrypt the packets and perform deep packet inspection on the decrypted packets. It protects the internal servers from being attacked by external malicious traffic. In this scenario, the device requires imported internal server certificates to establish SSL connections with the clients.

For more information about DPI, see "DPI overview."

By default, the SSL proxy protects the internal clients. You can select a protection service of the SSL decryption as required and import the corresponding certificates to the device for SSL connection establishment with the clients.

This command takes effect only when the SSL decryption action is used as the default action for the proxy policy.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify **server** as the SSL decryption protection mode for the proxy policy.

```
<Sysname> system-view
[Sysname] app-proxy-policy
[Sysname-app-proxy-policy] default ssl-decrypt protect-mode server
```

Related commands

display app-proxy-policy

destination-ip object-group

Use **destination-ip object-group** to configure an object group as a destination address filtering criterion in a proxy policy rule.

Use **undo destination-ip object-group** to remove destination address filtering criteria from a proxy policy rule.

Syntax

destination-ip object-group *object-group-name*

undo destination-ip object-group [*object-group-name*]

Default

A proxy policy rule does not contain any destination address filtering criterion.

Views

Proxy policy rule view

Predefined user roles

network-admin

context-admin

Parameters

object-group-name: Specifies an IP address object group by its name, a case-insensitive string of 1 to 63 characters. The object group must already exist and its name cannot be **any**.

Usage guidelines

You can repeat this command to set multiple destination address filtering criteria in a proxy policy rule. A packet passes the destination address filtering if it matches any of the configured destination address filtering criteria.

If you execute the **undo destination-ip object-group** command without specifying an object group, all destination address filtering criteria in the proxy policy rule will be deleted.

For more information about object groups, see object group configuration in *Security Configuration Guide*.

Examples

In proxy policy rule **rule1**, set IP address object groups **client1** and **client2** as destination address filtering criteria.

```
<Sysname> system-view
[Sysname] app-proxy-policy
[Sysname-app-proxy-policy] rule 1 name rule1
[Sysname-app-proxy-policy-0-rule1] destination-ip object-group client1
[Sysname-app-proxy-policy-0-rule1] destination-ip object-group client2
```

Related commands

display app-proxy-policy

object-group (*Security Command Reference*)

destination-zone

Use **destination-zone** to configure a destination security zone filtering criterion in a proxy policy rule.

Use **undo destination-zone** to remove destination security zone filtering criteria from a proxy policy rule.

Syntax

destination-zone *destination-zone-name*

undo destination-zone [*destination-zone-name*]

Default

A proxy policy rule does not contain any destination security zone filtering criterion.

Views

Proxy policy rule view

Predefined user roles

network-admin

context-admin

Parameters

destination-zone-name: Specifies a destination security zone by its name, a case-insensitive string of 1 to 31 characters. The destination security zone name cannot be **any**.

Usage guidelines

You can repeat this command to set multiple destination security zone filtering criteria in a proxy policy rule. A packet passes the destination security zone filtering if it matches any of the configured destination security zone filtering criteria.

You can specify a nonexistent security zone for a destination security zone filtering criterion. However, the destination security zone filtering criterion does not take effect until the security zone is configured.

If you execute the **undo destination-zone** command without specifying a security zone, all destination security zone filtering criteria in the proxy policy rule will be deleted.

For more information about security zones, see security zone configuration in *Security Configuration Guide*.

Examples

In proxy policy rule **rule1**, set security zones **trust** and **server** as destination security zone filtering criteria.

```
<Sysname> system-view
[Sysname] app-proxy-policy
[Sysname-app-proxy-policy] rule 1 name rule1
[Sysname-app-proxy-policy-0-rule1] destination-zone trust
[Sysname-app-proxy-policy-0-rule1] destination-zone server
```

Related commands

display app-proxy-policy

security-zone (*Security Configuration Guide*)

disable

Use **disable** to disable a proxy policy rule.

Use **undo disable** to enable a proxy policy rule.

Syntax

disable

undo disable

Default

A proxy policy rule is enabled.

Views

Proxy policy rule view

Predefined user roles

network-admin

context-admin

Usage guidelines

The device compares a packet against only the enabled proxy policy rules. The match process stops once a matching rule is found.

Examples

Disable proxy policy rule **rule1**.

```
<Sysname> system-view
[Sysname] app-proxy-policy
[Sysname-app-proxy-policy] rule 1 name rule1
[Sysname-app-proxy-policy-0-rule1] disable
```

Related commands

Rule

display app-proxy imported internal-server-certificate

Use **display app-proxy imported internal-server-certificate** to display information about imported internal server certificates.

Syntax

display app-proxy imported internal-server-certificate

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Usage guidelines

The information about the imported internal server certificates includes MD5 values, data, and signature algorithms.

Examples

Display information about imported internal server certificates.

```
<Sysname> display app-proxy imported internal-server-certificate
Certificate Md5: c4f5f2c41ca1de4258d893c9887bf287
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            aa:31:f8:3d:06:b0:9b:   Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=CN, ST=bj, L=cp, O=dpi, OU=sec, CN=trustca
        Validity
            Not Before: Sep  7 12:00:43 2017 GMT
            Not After : Aug 28 12:00:43 2057 GMT
        Subject: C=CN, ST=bj, L=cp, O=dpi, OU=sec, CN=trustca
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:ec:d7:73:af:03:07:07:86:e6:31:4d:e5:32:09:
                    20:7f:93:19:20:b2:25:c4:cc:32:8e:e4:29:fd:e0:
                    30:48:4c:8d:0a:83:66:28:af:6a:e0:69:81:08:58:
                    ca:cf:e4:3d:5a:e8:69:92:67:71:e3:c0:66:87:8e:
                    16:cc:6a:89:1d:d4:22:5f:93:14:47:bd:39:60:44:
                    3c:ee:0a:d1:8d:d4:16:84:65:e9:b7:b1:0f:6d:af:
                    6e:ef:21:b5:5a:02:4f:63:46:6e:8b:73:b5:95:70:
                    8a:ed:5d:23:8b:d8:0e:45:2d:8b:52:ab:34:6d:3b:
                    d5:85:ae:1c:d4:26:6e:fb:2c:1e:18:db:55:22:96:
                    d8:1f:1a:33:e9:ff:1f:8c:be:28:9d:de:77:d8:9b:
                    a7:27:0f:7e:e2:52:3e:bd:02:ee:c3:06:93:d0:16:
                    b0:c7:96:bb:c8:b1:96:8d:ee:ca:6e:76:63:1e:b1:
                    b6:fb:31:bf:d0:13:66:ad:f6:97:cf:0b:37:f7:6c:
                    f8:46:b6:76:f1:70:6f:24:6c:92:a6:dd:c2:3b:cf:
                    3c:35:c7:74:60:dd:db:a3:bf:70:b4:55:05:4b:d7:
```

```
                cd:dd:c1:1b:59:0d:41:e7:95:5a:79:44:9d:b0:8b:
                a7:f2:f4:67:0e:0c:4a:b6:35:97:1e:e6:99:88:fc:
                c8:e9
            Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                IP Address:1.1.1.1, DNS:trustca, email:1@3.com
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Subject Key Identifier:
                D4:35:A8:66:63:03:04:2B:CA:4E:91:06:11:F5:72:1C:26:E0:BE:33
            Netscape Cert Type:
                SSL CA
            Netscape Comment:
                example comment extension
    Signature Algorithm: sha1WithRSAEncryption
         b9:d2:eb:98:bd:f9:8d:7e:03:a8:0e:b4:29:cf:3a:a1:fd:f4:
         2a:fa:56:1c:cf:40:a4:9e:7f:5a:15:6b:88:8a:dd:86:d2:03:
         c3:38:49:7a:11:09:78:81:8c:8f:0a:3b:fb:d6:60:59:c4:0b:
         12:0e:38:b0:92:f3:2e:b5:96:ab:d3:a4:2d:cb:ef:fd:a0:97:
         d0:63:43:8e:91:1f:f1:fc:39:c8:cf:e5:ee:4b:e7:8c:8b:f8:
         3b:ff:5e:dc:00:df:5b:2f:98:53:f2:c7:da:fa:b8:2e:92:dd:
         33:6a:80:df:0e:22:62:62:5d:2f:6c:eb:4c:80:c4:56:c9:00:
         01:a6:82:60:e4:32:69:f7:7b:8f:6c:93:e5:c3:64:65:fe:aa:
         e1:0b:10:92:bd:ea:2f:2f:e5:b6:fd:b5:5b:df:34:c8:5d:5a:
         91:9a:0d:89:10:76:b8:ed:28:ef:6a:c4:7b:48:d7:88:57:7c:
         cf:4e:c8:38:84:ad:54:6d:3f:40:a0:38:d7:36:61:23:7a:82:
         62:34:41:3d:cc:b2:ee:4a:23:f1:7d:12:e2:23:26:10:df:c8:
         a1:6f:00:00:b7:c2:1f:ce:1b:63:60:e0:63:33:e0:59:31:78:
         bc:27:99:b6:27:40:95:da:1b:37:07:75:2f:99:97:56:33:f5:
         4f:ad:14:31
```

Figure 1 Command output

Field	Description
Certificate Md5	MD5 value of the certificate.
Certificate	Information about the certificate.
Version	Version number of the certificate.
Serial Number	Serial number of the certificate.
Signature Algorithm	Signature algorithm used in the certificate.
Issuer	Issuer of the certificate.
Validity	Validity of the certificate.

Field	Description
Subject	Identity of the entity to which the certificate belongs.
Subject Public Key Info	Public key information of the certificate subject.
Modulus	Modulus length of the key.
Exponent	Key exponent.
X509v3 extensions	X.509v3 extensions in the certificate.
X509v3 Subject Alternative Name	Alternative name of the certificate subject.
IP Address	IP address of the certificate subject.
DNS	DNS name of the certificate subject.
email	Email address of the certificate subject.
X509v3 Basic Constraints	Indicates whether the certificate belongs to a CA.
X509v3 Key Usage	Identifies the cryptographic operations which may be performed using the public key contained in the certificate.
X509v3 Subject Key Identifier	Key identifier of the certificate subject.
Netscape Cert Type	Netscape certificate type, an extension defined by Netscape to limit what the certificate can be used for.
Netscape Comment	Netscape comment that can be displayed in certain browsers.

Related commands

app-proxy server-certificate import

app-proxy server-certificate delete

display app-proxy server-certificate

Use **display app-proxy server-certificate** to display the SSL server certificates received by the device as the SSL proxy client.

Syntax

display app-proxy server-certificate [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays certificate information on all member devices.

Usage guidelines

When implementing the SSL proxy function, the device acts as the SSL proxy client to complete the SSL handshake and establish an SSL connection with the SSL server. This command displays information about the SSL server certificates received by the device as the SSL proxy client.

Examples

Display the SSL server certificates received by the device as the SSL proxy client on slot 1.

```
<Sysname> display app-proxy server-certificate slot 1
Slot1:
Total server certificates: --
Certificate info: /cn=nsfocus-https-self-signed-certificate-13a73249669cc70a
     Proxy count: 198
     Most recent proxy time: 2017/10/25 10:7:7
     First proxy at: 2017/10/23 15:52:59
```

Figure 2 Command output

Field	Description
Total server certificates	Total number of server certificates received by the device as the SSL proxy client.
Certificate info	Information about the certificate. This field displays the value in the **DNS Name** field (in the format of **example.com**) of the certificate. If the server certificate does not contain the **DNS Name** field, the value in the **Common Name** field (in the format of **/cn=example.com**) is displayed.
Proxy count	Number of times connections to the server had been proxied.
Most recent proxy time	Most recent time the device proxied a connection to the server.
First proxy at	First time the device proxied a connection to the server.

Related commands

reset app-proxy server-certificate

display app-proxy ssl whitelist hostname

Use **display app-proxy ssl whitelist hostname** to display the SSL hostname whitelist.

Syntax

display app-proxy ssl whitelist hostname { **predefined** | **user-defined** }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

`user-defined`: Displays the user-defined SSL hostname whitelist.

`predefined`: Displays the predefined SSL hostname whitelist.

Usage guidelines

This command is supported only on the default context. For more information about contexts, see context configuration in *Virtual Technologies Configuration Guide.*

Examples

Display the user-defined SSL hostname whitelist.

```
<Sysname> display app-proxy ssl whitelist hostname user-defined
Hostname
example1.com
example2.com
```

Display the predefined SSL hostname whitelist.

```
<Sysname> display app-proxy ssl whitelist hostname predefined
Chrome HSTS-defined hostnames:
  status      Hostname
  enabled     2mdn.net
  enabled     accounts.firefox.com
  enabled     aclu.org
  enabled     activiti.alfresco.com
  enabled     adamkostecki.de
  enabled     addvocate.com
  enabled     adsfund.org
  enabled     aie.de
  enabled     airbnb.com
  enabled     aladdinschools.appspot.com
  enabled     alexsexton.com
  enabled     alpha.irccloud.com
  enabled     android.com
  enabled     ansdell.net
  enabled     anycoin.me
  enabled     apadvantage.com
  enabled     api.intercom.io
  enabled     api.lookout.com
  enabled     api.mega.co.nz
  enabled     api.recurly.com
  enabled     api.simple.com
---- More ----
```

Figure 3 Command output

Field	Description
Chrome HSTS-defined hostnames	List of Chrome HSTS-defined hostnames accessible only through HTTPS.
Status	State of the hostname on the SSL hostname whitelist, **Enabled** or **Disabled**.

Related commands

app-proxy ssl whitelist predefined-hostname enable

app-proxy ssl whitelist user-defined-hostname

display app-proxy ssl whitelist { ipv4 | ipv6 }

Use **display app-proxy ssl whitelist** { **ipv4** | **ipv6** } to display the SSL IP address whitelist.

Syntax

display app-proxy ssl whitelist { **ipv4** | **ipv6** } { **all** [**slot** *slot-number*] | **ip-address** }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ipv4: Specifies the SSL IPv4 address whitelist.

ipv6: Specifies the SSL IPv6 address whitelist.

all: Specifies all IP addresses on the SSL IP address whitelist.

ip-address: Specifies the IP address of an SSL IP address whitelist entry to be displayed.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the SSL IP address whitelist information on all member devices.

Examples

Display the SSL IPv4 address whitelist on slot 1.

```
<Sysname> display app-proxy ssl whitelist ipv4 all slot 1
Slot 1:
IPv4 address              Port
10.1.1.1                443
10.10.1.1               443
```

Figure 4 Command output

Field	Description
IPv4 address	IPv4 address in an SSL IP address whitelist entry.
IPv6 address	IPv6 address in an SSL IP address whitelist entry.
Port	Port number of the SSL IP address whitelist entry. Connections destined for a server with the IP address and port number matching an IP address whitelist entry will not be proxied.

display app-proxy ssl-decrypt-certificate

Use **display app-proxy ssl-decrypt-certificate** to display SSL decryption certificate information.

Syntax

display app-proxy ssl-decrypt-certificate

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display SSL decryption certificate information.

```
<Sysname> display app-proxy ssl-decrypt-certificate
Trusted:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            aa:31:f8:3d:06:b0:9b:   Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=CN, ST=bj, L=cp, O=dpi, OU=sec, CN=trustca
        Validity
            Not Before: Sep  7 12:00:43 2017 GMT
            Not After : Aug 28 12:00:43 2057 GMT
        Subject: C=CN, ST=bj, L=cp, O=dpi, OU=sec, CN=trustca
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:ec:d7:73:af:03:07:07:86:e6:31:4d:e5:32:09:
                    20:7f:93:19:20:b2:25:c4:cc:32:8e:e4:29:fd:e0:
                    30:48:4c:8d:0a:83:66:28:af:6a:e0:69:81:08:58:
                    ca:cf:e4:3d:5a:e8:69:92:67:71:e3:c0:66:87:8e:
                    16:cc:6a:89:1d:d4:22:5f:93:14:47:bd:39:60:44:
                    3c:ee:0a:d1:8d:d4:16:84:65:e9:b7:b1:0f:6d:af:
                    6e:ef:21:b5:5a:02:4f:63:46:6e:8b:73:b5:95:70:
                    8a:ed:5d:23:8b:d8:0e:45:2d:8b:52:ab:34:6d:3b:
                    d5:85:ae:1c:d4:26:6e:fb:2c:1e:18:db:55:22:96:
                    d8:1f:1a:33:e9:ff:1f:8c:be:28:9d:de:77:d8:9b:
                    a7:27:0f:7e:e2:52:3e:bd:02:ee:c3:06:93:d0:16:
                    b0:c7:96:bb:c8:b1:96:8d:ee:ca:6e:76:63:1e:b1:
                    b6:fb:31:bf:d0:13:66:ad:f6:97:cf:0b:37:f7:6c:
                    f8:46:b6:76:f1:70:6f:24:6c:92:a6:dd:c2:3b:cf:
```

```
                3c:35:c7:74:60:dd:db:a3:bf:70:b4:55:05:4b:d7:
                cd:dd:c1:1b:59:0d:41:e7:95:5a:79:44:9d:b0:8b:
                a7:f2:f4:67:0e:0c:4a:b6:35:97:1e:e6:99:88:fc:
                c8:e9
            Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                IP Address:1.1.1.1, DNS:trustca, email:1@3.com
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Subject Key Identifier:
                D4:35:A8:66:63:03:04:2B:CA:4E:91:06:11:F5:72:1C:26:E0:BE:33
            Netscape Cert Type:
                SSL CA
            Netscape Comment:
                example comment extension
    Signature Algorithm: sha1WithRSAEncryption
         b9:d2:eb:98:bd:f9:8d:7e:03:a8:0e:b4:29:cf:3a:a1:fd:f4:
         2a:fa:56:1c:cf:40:a4:9e:7f:5a:15:6b:88:8a:dd:86:d2:03:
         c3:38:49:7a:11:09:78:81:8c:8f:0a:3b:fb:d6:60:59:c4:0b:
         12:0e:38:b0:92:f3:2e:b5:96:ab:d3:a4:2d:cb:ef:fd:a0:97:
         d0:63:43:8e:91:1f:f1:fc:39:c8:cf:e5:ee:4b:e7:8c:8b:f8:
         3b:ff:5e:dc:00:df:5b:2f:98:53:f2:c7:da:fa:b8:2e:92:dd:
         33:6a:80:df:0e:22:62:62:5d:2f:6c:eb:4c:80:c4:56:c9:00:
         01:a6:82:60:e4:32:69:f7:7b:8f:6c:93:e5:c3:64:65:fe:aa:
         e1:0b:10:92:bd:ea:2f:2f:e5:b6:fd:b5:5b:df:34:c8:5d:5a:
         91:9a:0d:89:10:76:b8:ed:28:ef:6a:c4:7b:48:d7:88:57:7c:
         cf:4e:c8:38:84:ad:54:6d:3f:40:a0:38:d7:36:61:23:7a:82:
         62:34:41:3d:cc:b2:ee:4a:23:f1:7d:12:e2:23:26:10:df:c8:
         a1:6f:00:00:b7:c2:1f:ce:1b:63:60:e0:63:33:e0:59:31:78:
         bc:27:99:b6:27:40:95:da:1b:37:07:75:2f:99:97:56:33:f5:
         4f:ad:14:31
```

Figure 5 Command output

Field	Description
Trusted	Credibility of the SSL decryption certificate, **Trusted** or **Untrusted**.
Version	Version number of the certificate.
Serial Number	Serial number of the certificate.
Signature Algorithm	Signature algorithm used in the certificate.
Issuer	Issuer of the certificate.
Validity	Validity of the certificate.
Subject	Identity of the entity to which the certificate belongs.

Field	Description
Subject Public Key Info	Public key information of the certificate subject.
Modulus	Modulus length of the key.
Exponent	Key exponent.
X509v3 extensions	X.509v3 extensions in the certificate.
X509v3 Subject Alternative Name	Alternative name of the certificate subject.
IP Address	IP address of the certificate subject.
DNS	DNS name of the certificate subject.
email	Email address of the certificate subject.
X509v3 Basic Constraints	Indicates whether the certificate belongs to a CA.
X509v3 Key Usage	Identifies the cryptographic operations which may be performed using the public key contained in the certificate.
X509v3 Subject Key Identifier	Key identifier of the certificate subject.
Netscape Cert Type	Netscape certificate type, an extension defined by Netscape to limit what the certificate can be used for.
Netscape Comment	Netscape comment that can be displayed in certain browsers.

display app-proxy-policy

Use **display app-proxy-policy** to display proxy policy information.

Syntax

display app-proxy-policy [**rule** *rule-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

rule *rule-name*: Specifies a proxy policy rule by its name, a case-insensitive string of 1 to 63 characters. If you do not specify a proxy policy rule, this command displays information about all proxy policy rules.

Examples

Display proxy policy information and all rules in the policy.

```
<Sysname> display app-proxy-policy
Default action: ssl-decrypt (Protect mode: server)
```

```
Rule with ID 0 and name rule0:
  Action: ssl-decrypt
  Status: Enabled
  Protect mode: server
  Match criteria:
   Source security zones: trust
   Destination security zones: trust
   Source IP address object groups: srcobj
   Destination IP address object groups: destobj
   Service object groups: serviceobj
   Users: user1
   User groups: usergroup1

  Rule with ID 2 and name rule2:
  Action: ssl-decrypt
  Status: Enabled
  Match criteria:
  source-zone: trust
  destination-zone: Untrust
  Protection mode: Client
```

Figure 6 Command output

Field	Description
Default action	Default action of the policy: • **no-proxy**. • **ssl-decrypt**. • **tcp-proxy**.
(Protect mode: XXX)	SSL decryption protection mode of the proxy policy: • **client**—Protects internal clients from attacks. • **server**—Protects internal servers from attacks. This field is available only when the SSL decryption action is used as the default action for the proxy policy.
Rule with ID *rule-id* and name *rule-name*	ID and name of a proxy policy rule.
Action	Action for traffic matching the proxy policy rule: • **no-proxy**. • **ssl-decrypt**. • **tcp-proxy**.
Protect mode	SSL decryption protection mode of the proxy policy rule: • **client**—Protects internal clients from attacks. • **server**—Protects internal clients from attacks.
Source security zones	Source security zones to which the proxy policy rule applies.
Destination security zones	Destination security zones to which the proxy policy rule applies.
Source IP address object groups	Source IP address object groups to which the proxy policy rule applies.
Destination IP address object groups	Destination IP address object groups to which the proxy policy rule applies.

Field	Description
Service object groups	Service object groups to which the proxy policy rule applies.
Users	Users to whom the proxy policy rule applies.
User groups	User groups to which the proxy policy rule applies.

reset app-proxy server-certificate

Use **reset app-proxy server-certificate** to clear information about the SSL server certificates received by the device as the SSL proxy client.

Syntax

reset app-proxy server-certificate

Views

User view

Predefined user roles

network-admin

context-admin

Examples

Clear information about the SSL server certificates received by the device as the SSL proxy client.

```
<Sysname> reset app-proxy server-certificate
```

Related commands

display app-proxy server-certificate

reset app-proxy ssl whitelist ip

Use **reset app-proxy ssl whitelist ip** to clear the SSL IP address whitelist.

Syntax

reset app-proxy ssl whitelist

Views

User view

Predefined user roles

network-admin

context-admin

Examples

Clear the SSL IP address whitelist.

```
<Sysname> reset app-proxy ssl whitelist ip
```

Related commands

display app-proxy ssl whitelist ip

rule

Use **rule** to create a proxy policy rule and enter its view, or enter the view of an existing proxy policy rule.

Use **undo rule** to remove a proxy policy rule.

Syntax

rule { *rule-id* | [*rule-id*] **name** *rule-name* }

undo rule { *rule-id* | **name** *rule-name* }

Views

Proxy policy view

Predefined user roles

network-admin

context-admin

Parameters

rule-id: Specifies a rule ID, which must be an integer in the range of 1 to 65535. If you do not specify a rule ID when creating a rule, the system automatically assigns a rule ID that is larger than that the largest rule ID already used. If rule ID 65535 is already used, the system assigns the smallest unused ID to the rule.

name *rule-name*: Specifies a rule name, a case-insensitive string of 1 to 63 characters. The rule name is required when you create a rule and it cannot be set to **default**.

Examples

Create rule 1 named **rule1**.

```
<Sysname> system-view
[Sysname] app-proxy-policy
[Sysname-app-proxy-policy] rule 1 name rule1
[Sysname-app-proxy-policy-1-rule1]
```

Related commands

display app-proxy-policy

rule move id

Use **rule move id** to move a proxy policy rule to a new position through rule IDs.

Syntax

rule move id *rule-id* **before** *insert-rule-id*

Views

Proxy policy view

Predefined user roles

network-admin

context-admin

Parameters

rule-id: Specifies the target rule to be moved by its ID in the range of 1 to 65535. The specified rule must already exist.

before *insert-rule-id*: Specifies the reference rule ID in the range of 1 to 65535. The target rule is moved to the position before the reference rule. To move the rule to the end of all rules, set the reference rule ID to 65535. The specified reference rule must already exist.

Examples

Move rule 5 to the position before rule 2.

```
<Sysname> system-view
[Sysname] app-proxy-policy
[Sysname-app-proxy-policy] rule move id 5 before 2
```

Related commands

rule

rule move name

Use **rule move name** to move a proxy policy rule to a new position through rule names.

Syntax

rule move name *rule-name1* { **before** [*rule-name2*] | **after** *rule-name2* }

Views

Proxy policy view

Predefined user roles

network-admin

context-admin

Parameters

rule-name1: Specifies the target rule to be moved by its name.

before [*rule-name2*]: Moves the target rule before another rule. If you do not specify a rule, the target rule is moved before all rules.

after [*rule-name2*]: Moves the target rule after another rule.

Usage guidelines

If the two rules are the same or one of the two rules does not exist, no move operation is performed.

Examples

Move rule **a** to the position before rule **b**.

```
<Sysname> system-view
[Sysname] app-proxy-policy
[Sysname-app-proxy-policy] rule move name a before b
```

service

Use **destination-zone** to configure a service filtering criterion in a proxy policy rule.

Use **undo destination-zone** to remove service filtering criteria from a proxy policy rule.

Syntax

service object-group { *object-group-name* }

undo service object-group [*object-group-name*]

Default

A proxy policy rule does not contain any service filtering criterion.

Views

Proxy policy rule view

Predefined user roles

network-admin

context-admin

Parameters

object-group-name: Specifies a service object group by its name, a case-insensitive string of 1 to 63 characters. The object group must already exist and its name cannot be **any**.

Usage guidelines

You can repeat this command to set multiple service filtering criteria in a proxy policy rule. A packet passes the service filtering if it matches any of the service filtering criteria.

If you execute the **undo service object-group** command without specifying an object group zone, all service filtering criteria in the proxy policy rule will be deleted.

Examples

In proxy rule **rule1**, specify object group **ftp** as a service filtering criterion.

```
<Sysname> system-view
[Sysname] app-proxy-policy
[Sysname-app-proxy-policy] rule 1 name rule1
[Sysname-app-proxy-policy-0-rule1] service object-group ftp
```

Related commands

display app-proxy-policy

object-group (*Security Command Reference*)

source-ip object-group

Use **source-ip object-group** to configure an object group as a source address filtering criterion in a proxy policy rule.

Use **undo source-ip object-group** to remove source address filtering criteria from a proxy policy rule.

Syntax

source-ip object-group *object-group-name*

undo source-ip object-group [*object-group-name*]

Default

A proxy policy rule does not contain any source address filtering criterion.

Views

Proxy policy rule view

Predefined user roles

network-admin

context-admin

Parameters

object-group-name: Specifies an IP address object group by its name, a case-insensitive string of 1 to 63 characters. The object group must already exist and its name cannot be **any**.

Usage guidelines

You can repeat this command to set multiple source address filtering criteria in a proxy policy rule. A packet passes the source address filtering if it matches any of the configured destination address filtering criteria.

If you execute the **undo source-ip object-group** command without specifying an object group, all source address filtering criteria in the proxy policy rule will be deleted.

For more information about object groups, see object group configuration in *Security Configuration Guide*.

Examples

In proxy policy rule **rule1**, specify IP address object groups **server1** and **server2** as source address filtering criteria.

```
<Sysname> system-view
[Sysname] app-proxy-policy
[Sysname-app-proxy-policy] rule 1 name rule1
[Sysname-app-proxy-policy-0-rule1] source-ip object-group server1
[Sysname-app-proxy-policy-0-rule1] source-ip object-group server2
```

Related commands

display app-proxy-policy

object-group (*Security Command Reference*)

source-zone

Use **source-zone** to configure a source security zone filtering criterion in a proxy policy rule.

Use **undo source-zone** to remove source security zone filtering criteria from a proxy policy rule.

Syntax

source-zone *source-zone-name*

undo source-zone [*source-zone-name*]

Default

A proxy policy rule does not contain any source security zone filtering criterion.

Views

Proxy policy rule view

Predefined user roles

network-admin

context-admin

Parameters

source-zone-name: Specifies a source security zone by its name, a case-insensitive string of 1 to 31 characters. The source security zone name cannot be **any**.

Usage guidelines

You can repeat this command to set multiple source security zone filtering criteria in a proxy policy rule. A packet passes the source security zone filtering if it matches any of the configured source security zone filtering criteria.

You can specify a nonexistent security zone for a source security zone filtering criterion. However, the source security zone filtering criterion does not take effect until the security zone is configured.

If you execute the **undo source-zone** command without specifying a security zone, all source security zone filtering criteria in the proxy policy rule will be deleted.

For more information about security zones, see security zone configuration in *Security Configuration Guide*.

Examples

In proxy policy rule **rule1**, specify security zones **trust** and **server** as source security zone filtering criteria.

```
<Sysname> system-view
[Sysname] app-proxy-policy
[Sysname-app-proxy-policy] rule 1 name rule1
[Sysname-app-proxy-policy-0-rule1] source-zone trust
[Sysname-app-proxy-policy-0-rule1] source-zone server
```

Related commands

display app-proxy-policy

security-zone (*Security Command Reference*)

ssl-decrypt protect-mode

Use **ssl-decrypt protect-mode** to specify an SSL decryption protection mode for a proxy policy rule.

Use **ssl-decrypt protect-mode** to restore the default.

Syntax

ssl-decrypt protect-mode { **client** | **server** }

undo ssl-decrypt protect-mode

Default

The SSL decryption protection mode of a proxy policy rule is **client**.

Views

Proxy policy rule view

Predefined user roles

network-admin

context-admin

Parameters

client: Specifies client protection.

server: Specifies server protection.

Usage guidelines

The SSL decryption supports the following protection services:

- **Internal client protection**—The device is deployed at the exit of the network where the internal clients are. When the internal clients access an external server, the device acts as a proxy server to decrypt the packets and perform deep packet inspection on the decrypted packets. It protects the internal clients from being attacked by external malicious websites. In this scenario, the device requires imported SSL decryption certificates to establish SSL connections with the clients.
- **Internal server protection**—The device is deployed at the entrance of the network where the internal servers are. When the external clients access an internal server, the device acts as a proxy server to decrypt the packets and perform deep packet inspection on the decrypted packets. It protects the internal servers from being attacked by external malicious traffic. In this scenario, the device requires imported internal server certificates to establish SSL connections with the clients.

For more information about DPI, see "DPI overview."

By default, the SSL proxy protects the internal clients. You can select a protection service of the SSL decryption as required and import the corresponding certificates to the device for SSL connection establishment with the clients.

This command takes effect only when the SSL decryption action is used as the default action for the proxy policy.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify **server** as the SSL decryption protection mode for proxy policy rule **rule1**.

```
<Sysname> system-view
[Sysname] app-proxy-policy
[Sysname-app-proxy-policy] rule 1 name rule1
[Sysname-app-proxy-policy-0-rule1] ssl-decrypt protect-mode server
```

Related commands

display app-proxy-policy

user

Use **user** to configure a user filtering criterion in a proxy policy rule.

Use **undo user** to remove user filtering criteria from a proxy policy rule.

Syntax

user *user-name* [**domain** *domain-name*]

undo user [*username* [**domain** *domain-name*]]

Default

A proxy policy rule does not contain any user filtering criterion.

Views

Proxy policy rule view

Predefined user roles

network-admin

context-admin

Parameters

username: Specify a username, a case-sensitive string of 1 to 55 characters. The username cannot be **a**, **al**, or **all**, and cannot contain special characters listed in Table 1.

Table 1 Special characters

Character name	Symbol
Backslash	\
Vertical bar	|
Forward slash	/
Colon	:
Asterisk	*
Question mark	?
Left angle bracket	<
Right angle bracket	>
At sign	@

domain *domain-name*: Specifies the name of the identity domain to which the user belongs. The identity domain name is a case-insensitive string of 1 to 255 characters which cannot contain special characters listed in Table 1.

Usage guidelines

You can repeat this command to set multiple user filtering criteria in a proxy policy rule. A packet passes the user filtering if it matches any of the user filtering criteria.

If the specified user does not exist for the following reasons, the configuration succeeds but does not take effect:

- The user does not exist.
- The domain does not exist.
- The user does not exist in the domain.

For successful user filtering criterion configuration, the user must exist and belong to the domain, if specified.

Follow these guidelines when you execute the **undo user** command:

- To remove all user filtering criteria in a proxy policy rule, do not specify any parameters.
- To remove a user in a domain as a user filtering criterion, specify the *username* parameter with the **domain** *domain-name* option.
- To remove a user that does not belong to any identity domains, specify the *username* parameter without the **domain** *domain-name* option.

Examples

In proxy rule **rule1**, specify users **usera** and **userb** in domain **test** as user filtering criteria.

```
<Sysname> system-view
[Sysname] app-proxy-policy
[Sysname-app-proxy-policy] rule 1 name rule1
[Sysname-app-proxy-policy-0-rule1] user usera domain test
[Sysname-app-proxy-policy-0-rule1] user userb domain test
```

Related commands

display app-proxy-policy

user-identity enable (*Security Command Reference*)

user-identity static-user (*Security Command Reference*)

user-group

Use **user-group** to configure a user group filtering criterion in a proxy policy rule.

Use **undo user-group** to remove user group filtering criteria from a proxy policy rule.

Syntax

user-group *user-group-name* [**domain** *domain-name*]

undo user-group [*user-group-name* [**domain** *domain-name*]]

Default

A proxy policy rule does not contain any user group filtering criterion.

Views

Proxy policy rule view

Predefined user roles

network-admin

context-admin

Parameters

user-group-name: Specify a user group by its name, a case-insensitive string of 1 to 200 characters.

domain *domain-name*: Specifies the name of the identity domain to which the user group belongs. The identity domain name is a case-insensitive string of 1 to 255 characters which cannot contain special characters listed in Table 2.

Table 2 Special characters

Character name	Symbol
Backslash	\
Vertical bar	|
Forward slash	/
Colon	:
Asterisk	*
Question mark	?
Left angle bracket	<
Right angle bracket	>
At sign	@

Usage guidelines

You can repeat this command to set multiple user group filtering criteria in a proxy policy rule. A packet passes the user group filtering if it matches any of the user group filtering criteria.

The command succeeds but does not take effect if the specified user group does not exist for the following reasons:

- The user does not exist.
- The domain does not exist.
- The user does not exist in the domain.

Follow these guidelines when you execute the **undo user-group** command:

- To remove all user group filtering criteria in a proxy policy rule, do not specify any parameters.
- To remove a user group in a domain as a user group filtering criterion, specify the *user-group-name* parameter with the **domain** *domain-name* option.
- To remove a user group that does not belong to any identity domains, specify the *user-group-name* parameter without the **domain** *domain-name* option.

For more information about user groups, see user identification configuration in *Security Configuration Guide*.

Examples

In proxy rule **rule1**, specify user groups **groupa** and **groupb** in domain **test** as user group filtering criteria.

```
<Sysname> system-view
[Sysname] app-proxy-policy
[Sysname-app-proxy-policy] rule 1 name rule1
[Sysname-app-proxy-policy-0-rule1] user-group groupa domain test
[Sysname-app-proxy-policy-0-rule1] user-group groupb domain test
```

Related commands

display app-proxy-policy

user-group (*Security Command Reference*)

NSFOCUS Firewall Series

NF NAT Command Reference

NSFOCUS Technologies, Inc.

Document version: 6W600-20230221

Preface

This command reference describes the commands for configuring NAT, NAT66, and AFT

This preface includes the following topics about the documentation:

- Audience.
- Conventions.

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators.

Conventions

The following information describes the conventions used in the documentation.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select a minimum of one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
CAUTION:	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Contents

NAT commands

Interface-based NAT is not supported on the NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280

action

Use **action** to specify an address translation method for a NAT rule.

Use **undo action** to delete the address translation method configuration for a NAT rule.

Syntax

Easy IP method:

action easy-ip

NO-NAT method:

action no-nat

NO-PAT method:

action address-group { *group-id* | **name** *group-name* } **no-pat** [**reversible**]

PAT method:

action address-group { *group-id* | **name** *group-name* } [**port-preserved**]

Default

No address translation method is specified in a NAT rule.

Views

NAT rule view

Predefined user roles

network-admin

context-admin

Parameters

address-group: Uses the NAT address group for address translation.

group-id: Specifies the ID of the address group. The value range for this argument is 0 to 65535.

name *group-name*: Specifies the name of the address group. The name is a case-sensitive string of 1 to 63 characters.

easy-ip: Uses the Easy IP method on the interface where the NAT rule is configured. The IP address of the interface is used as the NAT IP address.

no-nat: Disables the rule and its subsequent rules from translating matching packets.

no-pat: Uses the NO-PAT mode in which port numbers are not translated.

reversible: Allows reverse address translation. Reverse address translation uses existing NO-PAT entries to translate destination addresses for packets of connections actively initiated by external hosts to internal hosts.

port-preserved: Tries to preserve port number for PAT.

Usage guidelines

PAT supports TCP, UDP, and UDPLITE packets, and ICMP request packets.

A NAT address group cannot be used by both the PAT and NO-PAT methods.

If excessive NAT rules exist and you want to disable address translation for specific traffic temporarily, locate the NAT rule matching the traffic and specify the **no-nat** keyword in the rule.

Examples

Configure NAT rule **aaa** to use the PAT mode and NAT address group 0 for address translation.

```
<Sysname> system
[Sysname] nat policy
[Sysname-nat-policy] rule name aaa
[Sysname-nat-policy-rule-aaa] action address-group 0
```

Configure NAT rule **aaa** to use the NO-PAT mode and address group 0 for address translation.

```
<Sysname> system
[Sysname] nat policy
[Sysname-nat-policy] rule name aaa
[Sysname-nat-policy-rule-aaa] action address-group 0 no-pat
```

Configure NAT rule **aaa** to use Easy IP for address translation.

```
<Sysname> system
[Sysname] nat policy
[Sysname-nat-policy] rule name aaa
[Sysname-nat-policy-rule-aaa] action easy-ip
```

Disable NAT rule **aaa** and its subsequent rules from translating matching packets.

```
<Sysname> system
[Sysname] nat policy
[Sysname-nat-policy] rule name aaa
[Sysname-nat-policy-rule-aaa] action no-nat
```

Related commands

display nat all

display nat policy

nat address-group

action dnat (NAT64-type rule view)

Use **action dnat** to specify a destination address translation method for a NAT rule.

Use **undo action dnat** to delete the destination address translation method configuration for a NAT rule.

Syntax

Static NAT method:

action dnat static ip-address *local-ipv4-address* [*ipv6-***vrrp** *virtual-router-id*] [**vrf** *vrf-name*]

action dnat static ip-address *local-ipv6-address* [**ipv4-vrrp** *virtual-router-id*] [**vrf** *vrf-name*]

undo action dnat

Server mapping method:

action dnat server ip-address *local-ipv4-address* [**local-port** *local-port*] [**vrf** *vrf-name*]

action dnat server ip-address *local-ipv6-address* [**local-port** *local-port*] [**ipv4-vrrp** *virtual-router-id*] [**vrf** *vrf-name*]

undo action dnat

Prefix method:

action dnat prefix { **general v6tov4** | **nat64 v6tov4** } [**vrf** *vrf-name*]

action dnat prefix { **general v4tov6** *prefix-general prefix-length* | **ivi v4tov6** *prefix-ivi* } [**ipv4-vrrp** *virtual-router-id*] [**vrf** *vrf-name*]

undo action dnat

Default

No destination address translation method is specified in a NAT rule.

Views

NAT rule view

Predefined user roles

network-admin

context-admin

Parameters

static: Uses the static NAT method. Mappings between IPv6 and IPv4 addresses are manually configured.

server: Uses the internal server method for address translation.

ip-address: Specifies the IP address after translation.

local-ipv4-address: Specifies the internal destination IPv4 address after translation.

local-ipv6-address: Specifies the internal destination IPv6 address after translation.

local-port *port-number*: Specifies the internal destination port number after translation, in the range of 1 to 65535. If you do not specify this keyword, the destination port number is not translated. This feature is supported only for TCP, UDP, and ICMP query packets. Because ICMP IPv4/IPv6 packets do not have port numbers, the ICMP IDs in these packets are used as their destination port numbers.

prefix: Uses the prefix method for address translation.

general: Uses the general prefix method for destination address translation.

v4tov6: Translates IPv4 addresses to IPv6 addresses.

v6tov4: Translates IPv6 addresses to IPv4 addresses.

ivi: Uses the IVI prefix method for IPv6-to-IPv4 destination address translation.

prefix-ivi: Specifies an IVI prefix, which is fixed at 32.

nat64: Uses the NAT64 prefix method for destination address translation.

prefix-general: Specifies a general prefix.

general-prefix-length: Specifies the general prefix length. Available values include 32, 40, 48, 56, 64, and 96. When 96 is specified as the general prefix length, make sure the 64th bit through the 71st bit of the general prefix are 0.

ipv4-vrrp *virtual-router-id*: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

ipv6-vrrp *virtual-router-id*: Specifies an IPv6 VRRP group by its virtual router ID in the range of 1 to 255.

vrf *vrf-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, this command applies to IPv4 or IPv6 addresses after destination address translation on the public network.

Usage guidelines

When an IPv6 user accesses an IPv4 network, the following methods are available:

- **Static method**—In this method, you must manually configure the one-to-one IPv4-to-IPv6 address mappings. An IPv6 user uses the IPv6 address in the matching address mapping as the destination address, and the NAT64 device translates the destination IPv6 address to an IPv4 address according to the address mapping.
- **Internal server method**—In this method, an IPv4 server address and its port number are mapped to the IPv6 network. An IPv6 user can access the server in the IPv4 network through accessing the translated IPv6 address and port number.
- **Prefix method**—In this method, a NAT64 prefix or general prefix is used to translate a destination IPv6 address to an IPv4 address.

When an IPv4 user accesses an IPv6 network, the address translation procedure is similar to that when an IPv6 user accesses an IPv4 network.

In a hot backup system collaborating with VRRP, bind the translation actions in the following address translation methods to VRRP groups:

- **Static NAT**—Bind the IPv6-to-IPv4 destination address translation action to the VRRP group on the IPv6 side.
- **Static NAT**—Bind the IPv4-to-IPv6 destination address translation action to the VRRP group on the IPv4 side.
- **Server mapping**—Bind the IPv4-to-IPv6 destination address translation action to the VRRP group on the IPv4 side.
- **Prefix**—Bind the IPv4-to-IPv6 destination address translation action to the VRRP group on the IPv4 side.

If you do not bind the translation actions to VRRP groups, the uplink Layer 3 device directly connected to the hot backup system might send downlink packets to the backup device, causing service anomalies.

When you use this command together with the packet match criteria, if you first execute the **destination-ip** command and then the **action dnat static ip-address** command, you cannot repeatedly execute the **destination-ip** command to modify the packet match criteria.

To perform source and destination address translations simultaneously in a VPN environment, make sure the translated addresses belong to the same VPN instance. To perform address translation, execute the **action snat** and **action dnat** commands.

This command is available only in NAT rule view of the global NAT policy.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure NAT rule **rule1** to use the server mapping method to translate the destination IP address to 1.1.1.5.

```
<Sysname> system-view
[Sysname] nat global-policy
[Sysname-nat-global-policy] rule name rule1 type nat64
[Sysname-nat-global-policy-rule-nat64-rule1] action dnat ip-address 1.1.1.5
```

Related commands

action snat

destination-ip

action dnat (NAT66-type rule view)

Use **action dnat** to specify a destination address translation method for a NAT rule.

Use **undo action dnat** to delete the destination address translation method configuration for a NAT rule.

Syntax

Server mapping method:

action dnat ip-address *local-ipv6-address* [**local-port** *local-port*] [**vrf** *vrf-name*]

undo action dnat

NPTv6 method:

action dnat nptv6 *translated-ipv6-prefix prefix-length* [**vrf** *vrf-name*]

undo action dnat

NO-NAT method:

action dnat no-nat

undo action dnat

Default

No destination address translation method is specified in a NAT rule.

Views

NAT rule view

Predefined user roles

network-admin

context-admin

Parameters

static: Uses the static method for address translation. The mappings between destination IPv6 addresses before and after translation are manually configured.

ip-address *local-ipv6-address*: Specifies the internal destination IPv6 address after translation.

local-port *port-number*: Specifies the internal destination port number after translation, in the range of 1 to 65535. If you do not specify this keyword, the destination port number is not translated. This feature is supported only for TCP, UDP, and ICMPv6 query packets. Because ICMPv6 packets do not have port numbers, the ICMP IDs in these packets are used as their destination port numbers.

nptv6: Uses the NPTv6 method for IPv6 address prefix translation.

translated-ipv6-prefix prefix-length: Specifies the IPv6 address prefix after translation. The *translated-ipv6-prefix* argument indicates the address prefix. The *prefix-length* argument specifies the IPv6 address prefix length in the range of 1 to 112.

no-nat: Disables the rule and its subsequent rules from translating the destination IP address of the matching packets.

vrf *vrf-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, this command applies to IPv6 addresses after destination address translation on the public network.

Usage guidelines

This command is applicable to scenarios where a server in an internal network provides services (for example, Web or FTP service) for external networks. Through configuring mappings between internal servers and external servers in a NAT66-type rule, users in external networks can access servers in internal networks through the specified external network address.

If excessive NAT rules exist and you want to disable address translation for specific traffic temporarily, locate the NAT rule that matches the traffic and specify the **no-nat** keyword in the rule.

When you use this command together with packet match criteria, follow these restrictions and guidelines:

- When you use the **action dnat nptv6** command together with the **destination-ip** command, if you first execute the **destination-ip** command and then the **action dnat nptv6** command, you cannot repeatedly execute the **destination-ip** command to modify the packet match criteria.
- You cannot use this command together with the security zone match criteria. To use destination security zones as the packet match criteria for a NAT rule, first execute the **undo action dnat** command and then the **destination-zone** command.

To perform source and destination address translations simultaneously in a VPN environment, make sure the translated addresses belong to the same VPN instance. To perform address translation, execute the **action snat** and **action dnat** commands.

This command is available only in NAT rule view of the global NAT policy.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure NAT rule **rule1** to use the server mapping method to translate the destination IPv6 address to 3001::5.

```
<Sysname> system-view
[Sysname] nat global-policy
[Sysname-nat-global-policy] rule name rule1 type nat66
[Sysname-nat-global-policy-rule-nat66-rule1] action dnat ip-address 3001::5
```

Related commands

action snat

destination-ip

destination-zone

action dnat (NAT-type rule view)

Use **action dnat** to specify a destination address translation method for a NAT rule.

Use **undo action dnat** to delete the configuration of a destination address translation method for a NAT rule.

Syntax

Server mapping method:

action dnat { **ip-address** *local-address* | **object-group** *ipv4-object-group-name* } [**local-port** *local-port*] [**vrrp** *virtual-router-id*] [**vrf** *vrf-name*]

undo action dnat

NO-NAT method:

action dnat no-nat

undo action dnat

Default

No destination address translation method is specified in a NAT rule.

Views

NAT rule view

Predefined user roles

network-admin

context-admin

Parameters

ip-address *local-address*: Specifies a private destination IP address after translation.

object-group *ipv4-object-group-name*: Specifies an object group by its name. The name is a case-insensitive string of 1 to 63 characters, and it cannot be **any**. If spaces are included in the name, enclose the name in quotation marks ("), for example, "XXX XXX".

local-port *local-port*: Specifies a private destination port number after translation, in the range of 1 to 65535. If you do not specify this option, the device does not translate destination ports of the packets. Only TCP, UDP, and ICMP query packets are supported. For an ICMP packet, the ICMP ID is used as its destination port number.

no-nat: Disables the rule and its subsequent rules from translating the destination IP address of the matching packets.

vrrp *virtual-router-id*: Binds the destination translation method to a VRRP group. The *virtual-router-id* parameter represents the virtual router ID in the range of 1 to 255.

vrf *vrf-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, this command applies to IPv4 addresses after destination address translation on the public network.

Usage guidelines

When external users access an internal server, the NAT device translates the destination IP addresses and ports of the matching packets to the IP address and port of the internal server.

If excessive NAT rules exist and you want to disable address translation for specific traffic temporarily, locate the NAT rule that matches the traffic and specify the **no-nat** keyword in the rule.

In a hot backup system collaborating with VRRP, bind the destination address translation method on the primary device in the hot backup system to the VRRP group facing the external network. If you do not perform the binding, the uplink Layer 3 device directly connected to the hot backup system might send downlink packets to the backup device, causing service anomalies.

A NAT rule that uses the destination address translation method does support using a destination security zone as the packet match criterion. To use the destination security zone as the packet match criterion for the rule, execute the **undo action dnat** command first and then execute the **destination-zone** command.

To perform source and destination address translations simultaneously in a VPN environment, make sure the translated addresses belong to the same VPN instance. To perform address translation, execute the **action snat** and **action dnat** commands.

This command is available only in NAT rule view of the global NAT policy.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

For NAT rule **rule1**, specify the server mapping method and specify 1.1.1.5 as the destination address after translation.

```
<Sysname> system-view
[Sysname] nat global-policy
[Sysname-nat-global-policy] rule name rule1
[Sysname-nat-global-policy-rule-rule1] action dnat ip-address 1.1.1.5
```

Related commands

action snat

destination-zone

action snat (NAT64-type rule view)

Use **action snat** to specify a source address translation method for a NAT rule.

Use **undo action snat** to delete the source address translation method configuration for a NAT rule.

Syntax

NO-PAT method:

action snat object-group *ipv4-object-group-name* **no-pat** [**ipv4-vrrp** *virtual-router-id*] [**vrf** *vrf-name*]

action snat object-group *ipv6-object-group-name* **no-pat** [**vrf** *vrf-name*]

undo action snat

PAT method:

action snat object-group *ipv4-object-group-name* [**ipv4-vrrp** *virtual-router-id*] [**vrf** *vrf-name*]

action snat object-group *ipv6-object-group-name* [**vrf** *vrf-name*]

undo action snat

Prefix translation method:

action snat prefix { **general** { **v4tov6** *prefix-general general-prefix-length* | **v6tov4** } | **ivi v6tov4** | **nat64 v4tov6** *prefix-nat64 nat64-prefix-length* } [**vrf** *vrf-name*]

undo action snat

Static NAT method:

action snat static ip-address *global-ipv4-address* [**ipv4-vrrp** *virtual-router-id*] [**vrf** *vrf-name*]

action snat static ip-address *global-ipv6-address* [**ipv6-vrrp** *virtual-router-id*] [**vrf** *vrf-name*]

undo action snat

Default

No source address translation method is specified in a NAT rule.

Views

NAT rule view

Predefined user roles

network-admin

context-admin

Parameters

object-group: Specifies the address object group used for address translation.

ipv4-object-group-name: Specifies an IPv4 address object group by its name. The name is a case-insensitive string of 1 to 63 characters, and it cannot be **any**. If spaces are included in the name, enclose the name in quotation marks ("), for example, "XXX XXX".

ipv6-object-group-name: Specifies an IPv6 address object group by its name. The name is a case-insensitive string of 1 to 63 characters, and it cannot be **any**. If spaces are included in the name, enclose the name in quotation marks ("), for example, "XXX XXX".

prefix: Uses the prefix method for source address translation.

general: Uses the general prefix method for source address translation.

ivi: Uses the IVI prefix method for source address translation.

nat64: Uses the NAT64 prefix method for source address translation.

v4tov6: Translates IPv4 addresses to IPv6 addresses.

v6tov4: Translates IPv6 addresses to IPv4 addresses.

prefix-general: Specifies a general prefix.

general-prefix-length: Specifies the general prefix length. Available values include 32, 40, 48, 56, 64, and 96.

prefix-nat64: Specifies a NAT64 prefix.

nat64-prefix-length: Specifies the NAT64 prefix length. Available values include 32, 40, 48, 56, 64, and 96. When 96 is specified as the NAT64 prefix length, make sure the 64th bit through the 71st bit of the NAT64 prefix are 0.

static: Uses the static method for source address translation.

ip-address: Specifies the IP address after translation.

global-ipv4-address: Specifies the source IPv4 address after translation.

global-ipv6-address: Specifies source IPv6 address after translation.

ipv4-vrrp *virtual-router-id*: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

ipv6-vrrp *virtual-router-id*: Specifies an IPv6 VRRP group by its virtual router ID in the range of 1 to 255.

vrf *vrf-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, this command applies to IPv4 or IPv6 addresses after source address translation on the public network.

Usage guidelines

You can use different source IP address match criteria together with different source address translation methods to perform address translation. For example, when the **source-ip host** { *ipv4-address* | *ipv6-address* } command is used to configure packet match criteria for a NAT rule, the command can be used together with the **action snat static ip-address** { *global-ipv4-address* | *global-ipv6-address* } command to implement one-to-one static address translation.

When you use this command together with packet match criteria, follow these restrictions and guidelines:

- When you use the **action snat static ip-address** command together with the **source-ip** command, if you first execute the **source-ip** command and then the **action snat static ip-address** command, you cannot repeatedly execute the **source-ip** command to modify packet match criteria.
- When you use the static method for address translation, make sure the number of IP addresses in the packet match criteria for matching the source addresses of packets is the same as that in the static address translation method.

When a source address translation method references an address object group, follow these restrictions and guidelines:

- For an address object group to be successfully referenced by the source address translation method, make sure the objects in the referenced address object group are created through the following methods:
  - [*object-id*] **network host address** *ip-address*
  - [*object-id*] **network subnet** *ip-address* { *mask-length* | *mask* }
  - [*object-id*] **network range** *ip-address1 ip-address2*

  For more information about these commands, see object group commands in *Security Command Reference*.
- The number of IP addresses in the address object groups referenced by the source address translation method cannot exceed 65535.
- The address object group referenced by the static address translation method cannot contain excluded addresses.

In a hot backup system collaborating with VRRP, bind the translation actions in the following address translation methods to VRRP groups:

- **NO-PAT method**—Bind the IPv6-to-IPv4 source address translation action to the VRRP group on the IPv4 side.
- **PAT method**—Bind the IPv6-to-IPv4 source address translation action to the VRRP group on the IPv4 side.
- **Static NAT method**—Bind the IPv6-to-IPv4 source address translation action to the VRRP group on the IPv4 side.
- **Static NAT method**—Bind the IPv4-to-IPv6 source address translation action to the VRRP group on the IPv6 side.

If you do not bind the translation actions to VRRP groups, the uplink Layer 3 device directly connected to the hot backup system might send downlink packets to the backup device, causing service anomalies.

To perform source and destination address translations simultaneously in a VPN environment, make sure the translated addresses belong to the same VPN instance. To perform address translation, execute the **action snat** and **action dnat** commands.

This command is available only in NAT rule view of the global NAT policy.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure NAT rule **aaa** to use the PAT method and reference source IPv4 address object group **srcIP1**.

```
<Sysname> system
[Sysname] nat global-policy
[Sysname-nat-global-policy] rule name aaa type nat64
[Sysname-nat-global-policy-rule-nat64-aaa] action snat object-group srcIP1
```

Related commands

action dnat

display nat all

display nat global-policy

network (*Security Command Reference*)

action snat (NAT66-type rule view)

Use **action snat** to specify a source address translation method for a NAT rule.

Use **undo action snat** to delete the configuration of a source address translation method for a NAT rule.

Syntax

NO-PAT method:

action snat object-group *ipv6-object-group-name* **no-pat** [**vrf** *vrf-name*]

undo action snat

PAT method:

action snat object-group *ipv6-object-group-name* [**vrf** *vrf-name*]

undo action snat

Static NAT method:

action snat static ip-address *global-ipv6-address* [**ipv6-vrrp** *virtual-router-id*] [**vrf** *vrf-name*]

undo action snat

NPTv6 method:

action snat nptv6 *translated-ipv6-prefix prefix-length* [**vrf** *vrf-name*]

undo action snat

NO-NAT method:

action snat no-nat

undo action snat

Default

No source address translation method is specified in a NAT rule.

Views

NAT rule view

Predefined user roles

network-admin

context-admin

Parameters

object-group *ipv6-object-group-name*: Specifies an IPv6 address object group by its name for address translation. The name is a case-insensitive string of 1 to 63 characters, and it cannot be **any**. If spaces are included in the name, enclose the name in quotation marks ("), for example, "XXX XXX".

no-pat: Uses the NO-PAT mode in which port numbers are not translated.

static: Uses the static method for address translation. The mappings between source IPv6 addresses before and after translation are manually configured.

ipv6-address *global-ipv6-address*: Specifies the source IPv6 address after translation.

nptv6: Uses the NPTv6 method for IPv6 address prefix translation.

translated-ipv6-prefix nptv6-prefix-length: Specifies the IPv6 address prefix after translation. The *translated-ipv6-prefix* argument indicates the address prefix. The *nptv6-prefix-length* argument specifies the IPv6 address prefix length in the range of 1 to 112.

no-nat: Disables the rule and its subsequent rules from translating the source IP address of the matching packets.

ipv6-vrrp *virtual-router-id*: Specifies an IPv6 VRRP group by its virtual router ID in the range of 1 to 255.

vrf *vrf-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, this command applies to IPv6 addresses after source address translation on the public network.

Usage guidelines

You can use different source IP address match criteria together with different source address translation methods to perform address translation. For example, when the **source-ip host** { *ipv4-address* | *ipv6-address* } command is used to configure packet match criteria for a NAT rule, the command can be used together with the **action snat static ip-address** { *global-ipv4-address* | *global-ipv6-address* } command to implement one-to-one static address translation.

If you have configured a large number of NAT rules, to exclude some packets with addresses in a small range from source address translation, use the NO-PAT method.

When you use this command together with packet match criteria, follow these restrictions and guidelines:

- When you use the **action snat static ip-address** command together with the **source-ip** command, if you first execute the **source-ip** command and then the **action snat static ip-address** command, you cannot repeatedly execute the **source-ip** command to modify packet match criteria.
- The **action snat nptv6** command can be used together with only the **source-ip subnet** command. If you first execute the **source-ip subnet** command and then the **action snat nptv6** command, you cannot repeatedly execute the **source-ip** command to modify the packet match criteria.
- When you use the static method for address translation, make sure the number of IP addresses in the packet match criteria for matching the source addresses of packets is the same as that in the static address translation method.

When a source address translation method references an address object group, follow these restrictions and guidelines:

- For an address object group to be successfully referenced by the source address translation method, make sure the objects in the referenced address object group are created through the following methods:
  - [*object-id*] **network host address** *ip-address*
  - [*object-id*] **network subnet** *ip-address* { *mask-length* | *mask* }
  - [*object-id*] **network range** *ip-address1 ip-address2*

  For more information about these commands, see object group commands in *Security Command Reference*.

- The number of IP addresses in the address object group referenced by the source address translation method cannot exceed 65535.
- An address object group referenced by the static address translation method cannot contain excluded addresses.

In a hot backup system collaborating with VRRP, bind the static address translation action to the VRRP group on the IPv6 side. If you do not perform the binding, the uplink Layer 3 device directly connected to the hot backup system might send downlink packets to the backup device, causing service anomalies.

To perform source and destination address translations simultaneously in a VPN environment, make sure the translated addresses belong to the same VPN instance. To perform address translation, execute the **action snat** and **action dnat** commands.

This command is available only in NAT rule view of the global NAT policy.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure NAT rule **aaa** to use the NAT66 prefix method to translate the source IPv6 address prefix to 2101::/64 for packets whose source IP addresses match subnet fd9C:58ed:7d73:2::/64.

```
<Sysname> system
[Sysname] nat global-policy
[Sysname-nat-global-policy] rule name aaa type nat66
[Sysname-nat-global-policy-rule-nat66-aaa] source-ip subnet fd9C:58ed:7d73:2:: 64
[Sysname-nat-global-policy-rule-nat66-aaa] action snat prefix 2101:: 64
```

Related commands

action dnat

display nat all

display nat global-policy

source-ip

action snat (NAT-type rule view)

Use **action snat** to specify a source address translation method for a NAT rule.

Use **undo action snat** to delete the configuration of a source address translation method for a NAT rule.

Syntax

NO-PAT method:

action snat { **address-group** { *group-id* | **name** *group-name* } | **object-group** *ipv4-object-group-name* } **no-pat** [**reversible**] [**vrrp** *virtual-router-id*] [**vrf** *vrf-name*]

undo action snat

PAT method:

action snat { **address-group** { *group-id* | **name** *group-name* } | **object-group** *ipv4-object-group-name* } [**port-preserved**] [**vrrp** *virtual-router-id*] [**vrf** *vrf-name*]

undo action snat

Easy IP:

action snat easy-ip [**port-preserved**] [**vrf** *vrf-name*]

undo action snat

Static NAT:

action snat static { **ip-address** *global-address* | **object-group** *object-group-name* | **subnet** *subnet-ip-address mask-length* } [**vrrp** *virtual-router-id*] [**vrf** *vrf-name*]

undo action snat

NO-NAT method:

action snat no-nat

undo action snat

Default

No source address translation method is specified in a NAT rule.

Views

NAT rule view

Predefined user roles

network-admin

context-admin

Parameters

address-group: Uses the NAT address group for address translation.

group-id: Specifies the ID of the NAT address group. The value range is 0 to 65535.

name *group-name*: Specifies the name of an address group, a case-sensitive string of 1 to 63 characters.

easy-ip: Uses the Easy IP method. The IP address of the packet output interface is used as the NAT IP address.

ip-address *global-address*: Specifies a public IP address as the NAT IP address for source address translation.

no-nat: Disables the rule and its subsequent rules from translating the source IP address of the matching packets.

no-pat: Uses the NO-PAT mode in which port numbers are not translated.

reversible: Enables reverse address translation. Reverse address translation uses existing NO-PAT entries to translate the destination address for connections actively initiated from the internal network to the external network.

port-preserved: Tries to preserve port number for PAT.

static: Uses the static NAT method. Mappings between private and public addresses are manually configured.

object-group *object-group-name*: Specifies the name of an address object group. The name is a case-insensitive string of 1 to 63 characters, and it cannot be **any**. If spaces are included in the name, enclose the name in quotation marks ("), for example, "XXX XXX".

subnet *subnet-ip-address mask-length*: Specifies a subnet as NAT IP address resources for address translation. The *subnet-ip-address* argument specifies the subnet address. The *mask-length* argument specifies the mask length, which can be 8, 16, or an integer in the range of 24 to 31.

vrrp *virtual-router-id*: Binds the source translation method to a VRRP group. The *virtual-router-id* parameter represents the virtual router ID in the range of 1 to 255.

vrf *vrf-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, this command applies to IPv4 addresses after source address translation on the public network.

Usage guidelines

A NAT address group cannot be used by both the PAT and NO-PAT methods.

You can configure combinations between source IP address match criteria and source IP address translation methods. In each static combination, the number of IP addresses in the match criteria must equal the number of NAT IP addresses in the translation method. For example, the **action snat static ip-address** *global-address* command and the **source-ip host** *ip-address* command can define a one-to-one static source address translation.

If excessive NAT rules exist and you want to disable address translation for specific traffic temporarily, locate the NAT rule that matches the traffic and specify the **no-nat** keyword in the rule.

When the source address translation method references an address object group, follow these restrictions and guidelines:

- For an address object group to be successfully referenced by the source address translation method, make sure the objects in the referenced address object group are created through the following methods:
  - [*object-id*] **network host address** *ip-address*
  - [*object-id*] **network subnet** *ip-address* { *mask-length* | *mask* }
  - [*object-id*] **network range** *ip-address1 ip-address2*

  For more information about these commands, see object group commands in *Security Command Reference*.
- The number of IP addresses in the address object groups referenced by the source address translation method cannot exceed 65535.
- An address object group referenced by the static address translation method cannot contain excluded addresses.

In a hot backup system collaborating with VRRP, bind the source address translation method on the primary device in the hot backup system to the VRRP group facing the external network. If you do not perform the binding, the uplink Layer 3 device directly connected to the hot backup system might send downlink packets to the backup device, causing service anomalies.

For dual-active hot backup, select one of the following configuration methods:

- The two devices can share the same NAT address group. To prevent different master devices from using the same IP-port mapping for different hosts, specify the PAT translation mode and execute the **nat remote-backup port-alloc** command on the primary device.
- As a best practice to prevent different master devices from using the same IP-port mapping for different hosts, configure the two devices to use different public IP addresses for address translation. For example, if the two devices use different NAT addresses, user traffic with different source IP addresses is identified by source IP address match criteria in NAT rules. To enable different master devices to translate the forward user traffic, specify different gateway addresses for different internal users. To direct the reverse traffic to different master devices, configure VRRP group binding on the primary device for load sharing.

To perform source and destination address translations simultaneously in a VPN environment, make sure the translated addresses belong to the same VPN instance. To perform address translation, execute the **action snat** and **action dnat** commands.

This command is available only in NAT rule view of the global NAT policy.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure NAT rule **aaa** to use the PAT mode and NAT address group **0** for address translation.

```
<Sysname> system
[Sysname] nat global-policy
[Sysname-nat-global-policy] rule name aaa
[Sysname-nat-global-policy-rule-aaa] action address-group 0
```

Configure NAT rule **aaa** to use the NO-PAT mode and address group **0** for address translation.

```
<Sysname> system
[Sysname] nat global-policy
[Sysname-nat-global-policy] rule name aaa
[Sysname-nat-global-policy-rule-aaa] action address-group 0 no-pat
```

Configure NAT rule **aaa** to use the static NAT method to translate source IP address 1.1.1.1 to 100.10.0.1.

```
<Sysname> system
[Sysname] nat global-policy
[Sysname-nat-global-policy] rule name aaa
[Sysname-nat-global-policy-rule-aaa] source-ip host 1.1.1.1
[Sysname-nat-global-policy-rule-aaa] action snat static ip-address 100.10.0.1
```

Disable address translation for NAT rule **aaa**.

```
<Sysname> system
[Sysname] nat global-policy
[Sysname-nat-global-policy] rule name aaa
[Sysname-nat-global-policy-rule-aaa] action snat no-nat
```

Related commands

action dnat

display nat all

display nat policy

nat address-group

address

Use **address** to add an address range to a NAT address group.

Use **undo address** to remove an address range from a NAT address group.

Syntax

address *start-address end-address*

undo address *start-address end-address*

Default

No address ranges exist.

Views

NAT address group view

Predefined user roles

network-admin

context-admin

Parameters

start-address end-address: Specifies the start and end IP addresses of the address range. The end address must not be lower than the start address. If they are the same, the address range has only one IP address.

Usage guidelines

A NAT address group is a set of address ranges. The source address in a packet destined for an external network is translated into an address in one of the address ranges.

You can specify a maximum of 65535 addresses in one command execution. Make sure the address ranges do not overlap.

The **address** command and the **address interface** command are mutually exclusive for one NAT address group.

Examples

Add address ranges to an address group.

```
<Sysname> system-view
[Sysname] nat address-group 2
[Sysname-address-group-2] address 10.1.1.1 10.1.1.15
[Sysname-address-group-2] address 10.1.1.20 10.1.1.30
```

Related commands

address interface

nat address-group

block-size

Use **block-size** to set the port block size.

Use **undo block-size** to restore the default.

Syntax

block-size *block-size*

undo block-size

Default

The port block size is 256.

Views

NAT port block group view

Predefined user roles

network-admin

context-admin

Parameters

block-size: Specifies the number of ports for a port block. The value range for this argument is 1 to 65535.

Usage guidelines

Set an appropriate port block size based on the number of private IP addresses, the number of public IP addresses, and the port range in the port block group.

The port block size cannot be larger than the number of ports in the port range.

Examples

Set the port block size to 1024 for port block group **1**.

```
<Sysname> system-view
[Sysname] nat port-block-group 1
[Sysname-port-block-group-1] block-size 1024
```

Related commands

nat port-block-group

counting enable

Use **counting enable** to enable hit counting for a NAT rule.

Use **undo counting enable** to disable hit counting for a NAT rule.

Syntax

counting enable

undo counting enable

Default

NAT rule hit counting is disabled.

Views

NAT rule view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command enables the devices to count the number of times the rule is matched (or hit). To view hit statistics for the rule, execute the **display nat policy** command.

Examples

Enable hit counting for NAT rule **aaa** in the interface-based NAT policy.

```
<Sysname> system
[Sysname] nat policy
[Sysname-nat-policy] rule name aaa
[Sysname-nat-policy-rule-aaa] counting enable
```

Enable hit counting for NAT rule **aaa** in the global NAT policy.

```
<Sysname> system
[Sysname] nat global-policy
[Sysname-nat-global-policy] rule name aaa
[Sysname-nat-global-policy-rule-aaa] counting enable
```

Related commands

display nat all

display nat global-policy

display nat policy

description

Use **description** to configure a description for the NAT rule.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

A NAT rule does not have any description.

Views

NAT rule view

Predefined user roles

network-admin

context-admin

Parameters

text: Specifies the description, a case-sensitive string of 1 to 63 characters.

Examples

Configure a description for NAT rule **aaa** in the interface-based NAT policy.

```
<Sysname> system
[Sysname] nat policy
[Sysname-nat-policy] rule name aaa
[Sysname-nat-policy-rule-aaa] description This is a nat rule of abc policy
```

Configure a description for NAT rule **aaa** in the global NAT policy.

```
<Sysname> system
[Sysname] nat global-policy
[Sysname-nat-global-policy] rule name aaa
[Sysname-nat-global-policy-rule-aaa] description This is a nat rule of abc policy
```

destination-ip

Use **destination-ip** to specify a destination IP address match criterion in a NAT rule.

Use **undo destination-ip** to delete a destination IP address match criterion from a NAT rule.

Syntax

NAT-type rule view in the interface-based NAT policy:

destination-ip *ipv4-object-group-name*

undo destination-ip [*ipv4-object-group-name*]

NAT-type rule view in the global NAT policy:

destination-ip { **host** *ip-address* | **subnet** *subnet-ip-address mask-length* }

undo destination-ip { **host** [*ip-address*] | **subnet** [*subnet-ip-address mask-length*] }

NAT64-type rule view in the global NAT policy:

destination-ip { *ipv4-object-group-name* | *ipv6-object-group-name* }

undo destination-ip [*ipv4-object-group-name* | *ipv6-object-group-name*]

destination-ip { **host** { *ipv4-address* | *ipv6-address* } | **subnet** { *subnet-ipv4-address mask-length* | *ipv6-prefix prefix-length* } }

undo destination-ip { **host** [*ipv4-address* | *ipv6-address*] | **subnet** [*subnet-ipv4-address mask-length* | *ipv6-prefix prefix-length*] }

NAT66-type rule view in the global NAT policy:

destination-ip *ipv6-object-group-name*

undo destination-ip [*ipv6-object-group-name*]

destination-ip { **host** *ipv6-address* | **subnet** *ipv6-prefix prefix-length* }

undo destination-ip { **host** [*ipv6-address*] | **subnet** [*ipv6-prefix prefix-length*] }

Default

A NAT rule does not have any destination IP address match criteria.

Views

NAT rule view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-object-group-name: Specifies the name of an IPv4 address object group. The name is a case-insensitive string of 1 to 63 characters, and it cannot be **any**. If spaces are included in the name, enclose the name in quotation marks ("), for example, "XXX XXX".

ipv6-object-group-name: Specifies the name of an IPv6 address object group. The name is a case-insensitive string of 1 to 63 characters, and it cannot be **any**. If spaces are included in the name, enclose the name in quotation marks ("), for example, "XXX XXX".

host *ipv4-address*: Specifies an IPv4 address to match destination IP address. The IPv4 address cannot be an all-zero address, all-one address, Class D address, Class E address, or loopback address.

host *ipv6-address*: Specifies an IPv6 address to match destination IP address.

subnet *subnet-ipv4-address mask-length*: Specifies a subnet to match destination IPv4 addresses. The *subnet-ip-address* argument specifies the subnet address. The *mask-length* argument specifies the mask length, which can be 8, 16, or an integer in the range of 24 to 31.

subnet *ipv6-prefix prefix-length*: Specifies an IPv6 prefix for a NAT rule. The *ipv6-prefix* argument indicates an IPv6 prefix. The *prefix-length* argument indicates the prefix length in the range of 1 to 128.

Usage guidelines

The NAT device uses the destination IP addresses specified in this command to identify matching packets. Only packets with the matching destination IP addresses are translated.

To translate destination IP addresses of packets from the internal network to the external network, use this command with the **action dnat** command.

When referencing an address object group, follow these restrictions and guidelines:

- The address object group must already exist.
- For an address object group to be successfully referenced by the destination address translation method, make sure the objects in the referenced address object group are created through the following methods:
  - [*object-id*] **network host address** *ip-address*
  - [*object-id*] **network subnet** *ip-address* { *mask-length* | *mask* }
  - [*object-id*] **network range** *ip-address1 ip-address2*

  For more information about these commands, see object group commands in *Security Command Reference*.

If you do not specify any parameters in the **undo destination-ip** command, the command deletes all destination address match criteria in the NAT rule.

When you configure match criteria for a NAT rule, follow these restrictions and guidelines:

- A NAT rule can have a maximum of 256 destination address object groups.
- A NAT rule can have a maximum of 256 destination IP addresses.
- If you configure multiple packet match criteria in a NAT64-type rule, the IP address type in the later configured packet match criteria must be the same as that in the earlier configured packet match criteria. For example, if you first execute the **destination-ip host 192.168.1.1** command, the **destination-ip host 100::1** command executed later does not take effect. Select an IP type as needed.
- If you execute the following commands in the same NAT rule, the most recent configuration takes effect:
  - **destination-ip subnet**
  - **destination-ip**
  - **destination-ip host**

Examples

In the interface-based NAT policy, configure NAT rule **aaa** to use destination address object groups **desIP1**, **desIP2**, and **desIP3** as the packet match criteria.

```
<Sysname> system
[Sysname] nat policy
[Sysname-nat-policy] rule name aaa
[Sysname-nat-policy-rule-aaa] destination-ip desIP1
[Sysname-nat-policy-rule-aaa] destination-ip desIP2
[Sysname-nat-policy-rule-aaa] destination-ip desIP3
```

In the global NAT policy, configure NAT rule **aaa** to use destination address object groups **desIP1**, **desIP2**, and **desIP3** as the packet match criteria.

```
<Sysname> system-view
[Sysname] nat global-policy
[Sysname-nat-global-policy] rule name aaa
[Sysname-nat-global-policy-rule-aaa] destination-ip desIP1
[Sysname-nat-global-policy-rule-aaa] destination-ip desIP2
[Sysname-nat-global-policy-rule-aaa] destination-ip desIP3
```

Related commands

display nat all

display nat global-policy

display nat policy

object-group (*Security Command Reference*)

destination-zone

Use **destination-zone** to specify a destination security zone in a NAT rule.

Use **undo destination-zone** to delete a destination security zone from a NAT rule.

Syntax

destination-zone *destination-zone-name*

undo destination-zone [*destination-zone-name*]

Default

No destination security zones are specified in a NAT rule.

Views

NAT rule view

Predefined user roles

network-admin

context-admin

Parameters

destination-zone-name: Specifies the name of a destination security zone. The name is a case-insensitive string of 1 to 31 characters, and it cannot be **any**. You can specify a nonexistent security zone. This command takes effect after you use the **security-zone name** command to create the security zone. For more information about security zones, see *Security Configuration Guide*.

Usage guidelines

The NAT device uses the destination security zones specified in this command to identify matching packets. Only packets with the matching destination security zones are translated.

To translate source IP addresses of outgoing packets, use this command with the **action snat** command. This command cannot be used with the **action dnat** command.

This command does not support modifying destination security zones. To modify the destination security zone for a NAT rule, first execute the **undo destination-zone** command to delete the zone, and then execute the **destination-zone** command to specify a new one.

If you do not specify a destination security zone in the **undo destination-zone** command, the command deletes all destination security zones in the rule.

This command is available only in NAT-type rule view and NAT66-type rule view of the global NAT policy.

A NAT rule can have a maximum of 16 destination security zones.

Examples

Specify destination security zone **trust** for NAT rule **rule1**.

```
<Sysname> system-view
[Sysname] nat global-policy
[Sysname-nat-global-policy] rule name rule1
[Sysname-nat-global-policy-rule-rule1] destination-zone trust
```

Related commands

rule name

security-zone name (*Security Command Reference*)

disable

Use **disable** to disable a NAT rule.

Use **undo disable** to enable a NAT rule.

Syntax

disable

undo disable

Default

A NAT rule is enabled.

Views

NAT rule view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command does not delete a NAT rule, but makes the rule ineffective. You can use the **display nat policy** command or the **display nat global-policy** command to view the status of the NAT rules. If you want to delete a NAT rule, use the **undo rule name** command.

Examples

Disable the NAT rule **aaa** in the interface-based NAT policy.

```
<Sysname> system
[Sysname] nat policy
[Sysname-nat-policy] rule name aaa
[Sysname-nat-policy-rule-aaa] disable
```

Disable the NAT rule **aaa** in the global NAT policy.

```
<Sysname> system
[Sysname] nat global-policy
[Sysname-nat-global-policy] rule name aaa
[Sysname-nat-global-policy-rule-aaa] disable
```

Related commands

display nat all

display nat global-policy

display nat policy

display nat address-group

Use **display nat address-group** to display NAT address group information.

Syntax

display nat address-group [*group-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

group-id: Specifies the ID of a NAT address group. The value range for this argument is 0 to 65535. If you do not specify the *group-id* argument, this command displays information about all NAT address groups.

Examples

Display information about all NAT address groups.

```
<Sysname> display nat address-group
NAT address group information:
  Totally 5 NAT address groups.
  Address group ID: 1    Address group name: a
    Port range: 1-65535
    Address information:
      Start address         End address
      202.110.10.10         202.110.10.15

  Address group ID: 2
    Port range: 1-65535
    VRID      : 1
    Address information:
      Start address         End address
      202.110.10.20         202.110.10.25
      202.110.10.30         202.110.10.35

  Address group ID: 3
    Port range: 1024-65535
    Address information:
      Start address         End address
      202.110.10.40         202.110.10.50

  Address group ID: 4
    Port range: 10001-65535
    Port block size: 500
    Extended block number: 1
    Address information:
      Start address         End address
      202.110.10.60         202.110.10.65

  Address group ID: 5
    Port range: 1-1024
    Port block size: 500
    Address information:
      20.1.1.1 (GigabitEthernet1/0/1)
```

```
  Address group ID: 6
    Port range: 1-65535
    Address information:
      Start address         End address
      ---                   ---
```

Display information about NAT address group **1**.

```
<Sysname> display nat address-group 1
  Address group ID: 1    Address group name: a
    VRID      : 1
    Port range: 1-65535
    Address information:
      Start address         End address
      202.110.10.10         202.110.10.15
```

Table 1 Command output

Field	Description
NAT address group information	Information about the NAT address group
Address group ID	ID of the NAT address group.
Totally *n* NAT address groups	Total number of NAT address groups.
Address group name	Name of the NAT address group. If no address group name is configured, this field is not displayed.
VRID	Virtual router ID (VRRP group number). If no VRRP group is specified, this field is not displayed.
Port range	Port range for public IP addresses.
Port block size	Number of ports in a port block. This field is not displayed if the port block size is not set.
Extended block number	Number of extended port blocks. This field is not displayed if the number of extended port blocks is not set.

Address information	Information about the IP addresses in the address group.
	• For addresses added by using the **address** command:
	  ○ **Start address**—Start IP address of an address range. If you do not specify a start address for the range, this field displays hyphens (**---**).
	  ○ **End address**—End IP address of an address range. If you do not specify an end address for the range, this field displays hyphens (**---**).
	• For addresses added by using the **address interface** command:
	  ○ **20.1.1.1 (GigabitEthernet1/0/1)**—IP address 20.1.1.1 of GigabitEthernet 1/0/1 has been added to the NAT address group.
	  ○ **--- (GigabitEthernet1/0/2)**—Failed to add the IP address of GigabitEthernet 1/0/2 to the NAT address group because this interface does not have an IP address.

Related commands

nat address-group

display nat alg

Use **display nat alg** to display the NAT ALG status for all supported protocols.

Syntax

display nat alg

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display the NAT ALG status for all supported protocols.

```
<Sysname> display nat alg
NAT ALG:
  DNS         : Enabled
  FTP         : Disabled
  H323        : Disabled
  ICMP-ERROR  : Disabled
  ILS         : Disabled
  MGCP        : Disabled
  NBT         : Disabled
  PPTP        : Disabled
  RTSP        : Disabled
  RSH         : Disabled
  SCCP        : Disabled
  SCTP        : Disabled
  SIP         : Disabled
  SQLNET      : Disabled
  TFTP        : Disabled
  XDMCP       : Disabled
```

Related commands

display nat all

display nat all

Use **display nat all** to display all NAT configuration information.

Syntax

display nat all

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display all NAT configuration information.

```
<Sysname> display nat all
NAT address group information:
  Totally 5 NAT address groups.
  Address group 1:
    Port range: 1-65535
    Address information:
      Start address         End address
      202.110.10.10         202.110.10.15

  Address group 2:
    Port range: 1-65535
    Address information:
      Start address         End address
      202.110.10.20         202.110.10.25
      202.110.10.30         202.110.10.35

  Address group 3:
    Port range: 1024-65535
    Address information:
      Start address         End address
      202.110.10.40         202.110.10.50

  Address group 4:
    Port range: 10001-65535
    Port block size: 500
    Extended block number: 1
    Address information:
      Start address         End address
      202.110.10.60         202.110.10.65

  Address group 6:
    Port range: 1-65535
    Address information:
      Start address         End address
      ---                   ---

NAT server group information:
  Totally 3 NAT server groups.
  Group Number        Inside IP             Port        Weight
  1                   192.168.0.26          23          100
```

```
                    192.168.0.27          23          500
  2                 ---                   ---         ---
  3                 192.168.0.26          69          100

NAT global-policy information:
  Totally 1 NAT global-policy rules.
  Rule name: rule1
    Description            : global nat rule
    SrcIP object group     : srcObj1
    SrcIP object group     : srcObj2
    SrcIP object group     : srcObj3
    DestIP object group    : desObj1
    DestIP object group    : desObj2
    DestIP object group    : desObj3
    Service object group   : serviceObj1
    Service object group   : serviceObj2
    Service object group   : serviceObj3
    Source zone name       : Trust
    Destination zone name  : Local
    SNAT action:
      Address group ID: 2    Address group name: a
      NO-PAT: Y
      Reversible: N
      Port-preserved: N
    DNAT action:
      IP address: 1.1.2.1
      Port: 80
    NAT counting : 0
    Config status: Active

NAT policy information:
  Totally 1 NAT policy rules.
  Rule name: rule1
    Description            : first rule
    Routing-interface      : GigabitEthernet1/0/2
    SrcIP object group     : srcObj1
    SrcIP object group     : srcObj2
    SrcIP object group     : srcObj3
    DestIP object group    : desObj1
    DestIP object group    : desObj2
    DestIP object group    : desObj3
    Service object group   : serviceObj1
    Service object group   : serviceObj2
    Service object group   : serviceObj3
    Action
      Address group ID: 2    Address group name: a
      NO-PAT: Y
      Reversible: N
```

```
      Port-preserved: N
    Config status: Active

NAT inbound information:
  Totally 1 NAT inbound rules.
  Interface: GigabitEthernet1/0/1
    ACL: 2038
    Address group ID: 2
    Add route: Y        NO-PAT: Y  Reversible: N
    VPN instance: vpn_nat
    Rule name: abcdefg
    Priority: 1000
    Description: NatInbound1
    Config status: Active

NAT outbound information:
  Totally 2 NAT outbound rules.
  Interface: GigabitEthernet1/0/2
    ACL: 2036
    Address group ID: 1
    Port-preserved: Y        NO-PAT: N  Reversible: N
    Configuration mode  : NETCONF (action)
    Rule name: cdefg
    Priority: 1001
    Description: NatOutbound1
    Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: address group, and ACL.

  Interface: GigabitEthernet1/0/2
    ACL: 2037
    Address group ID: 1
    Port-preserved: N        NO-PAT: Y  Reversible: Y
    VPN instance: vpn_nat
    Rule name: blue
    Priority: 1002
    Config status: Active.

NAT internal server information (object-group):
  Totally 1 object-group-based NAT server rules.
  Rule name: aaa
    Interface: GigabitEthernet1/0/1
    Local IP/Port: 1.1.1.1/80
    DestIP Object group: abc
    NAT counting  : 0
    Config status : Active

NAT internal server information:
```

```
Totally 5 internal servers.
Interface: GigabitEthernet1/0/1
  Global ACL    : 2000
  Local IP/port : 192.168.10.1/23
  Rule name     : cdefgab
  Priority      : 1000
  Configuration mode  : NETCONF (action)
  NAT counting  : 0
  Description   : NatServerDescription1
  Config status : Active

Interface: GigabitEthernet1/0/2
  Protocol: 6(TCP)
  Global IP/port: 50.1.1.1/23
  Local IP/port : 192.168.10.15/23
  ACL           : 2000
  Rule name     : green
  NAT counting  : 0
  Config status : Active

Interface: GigabitEthernet1/0/3
  Protocol: 6(TCP)
  Global IP/port: 50.1.1.1/23-30
  Local IP/port : 192.168.10.15-192.168.10.22/23
  Global VPN    : vpn1
  Local VPN     : vpn3
  Rule name     : blue
  NAT counting  : 0
  Config status : Active

Interface: GigabitEthernet1/0/4
  Protocol: 255(Reserved)
  Global IP/port: 50.1.1.100/---
  Local IP/port : 192.168.10.150/---
  Global VPN    : vpn2
  Local VPN     : vpn4
  ACL           : 3000
  Rule name     : white
  NAT counting  : 0
  Config status : Inactive
  Reasons for inactive status:
    The following items don't exist or aren't effective: ACL.

Interface: GigabitEthernet1/0/5
  Protocol: 17(UDP)
  Global IP/port: 50.1.1.2/23
  Local IP/port : server group 1
                  192.168.0.26/23       (Connections: 10)
```

```
                  192.168.0.27/23       (Connections: 20)
    Global VPN    : vpn1
    Local VPN     : vpn3
    Rule name     : black
    NAT counting  : 0
    Config status : Active

Static NAT mappings:
  Totally 2 inbound static NAT mappings.
  Net-to-net:
    Global IP    : 2.2.2.1 – 2.2.2.255
    Local IP     : 1.1.1.0
    Netmask      : 255.255.255.0
    Global VPN   : vpn2
    Local VPN    : vpn1
    ACL          : 2000
    Reversible   : Y
    Rule name     : pink
    Priority      : 1000
    Config status: Active
    Global flow-table status: Active
    Local flow-table status: Active

  IP-to-IP:
    Global IP    : 5.5.5.5
    Local IP     : 4.4.4.4
    ACL          : 2001
    Reversible   : Y
    Rule name    : yellow
    Priority     : 1000
    Description  : NatStaticDescription1
    Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: ACL.
    Global flow-table status: Active
    Local flow-table status: Active

  Totally 2 outbound static NAT mappings.
  Net-to-net:
    Local IP     : 1.1.1.1 - 1.1.1.255
    Global IP    : 2.2.2.0
    Netmask      : 255.255.255.0
    ACL          : 2000
    Reversible   : Y
    Rule name    : grey
    Priority     : 1000
    Config status: Active
    Global flow-table status: Active
```

```
    Local flow-table status: Active

  IP-to-IP:
    Local IP     : 4.4.4.4
    Global IP    : 5.5.5.5
    ACL:         : 2001
    Reversible   : Y
    Rule name    : orange
    Priority     : 10000
    Description  : NatStaticDescription2
    Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: ACL.
    Global flow-table status: Active
    Local flow-table status: Active

Interfaces enabled with static NAT:
  Totally 2 interfaces enabled with static NAT.
  Interface: GigabitEthernet1/0/4
    Config status: Active

  Interface: GigabitEthernet1/0/6
    Config status: Active

NAT DNS mappings:
  Totally 2 NAT DNS mappings.
  Domain name  : www.server.com
  Global IP    : 6.6.6.6
  Global port  : 23
  Protocol     : TCP(6)
  Config status: Active

  Domain name  : www.service.com
  Global IP    : ---
  Global port  : 12
  Protocol     : TCP(6)
  Config status: Inactive
  Reasons for inactive status:
    The following items don't exist or aren't effective: interface IP address.

NAT logging:
  Log enable          : Enabled(ACL 2000)
  Flow-begin          : Disabled
  Flow-end            : Disabled
  Flow-active         : Enabled(10 minutes)
  Port-block-assign   : Disabled
  Port-block-withdraw : Disabled
  Alarm               : Disabled
```

```
  NO-PAT IP usage     : Disabled

NAT hairpinning:
  Totally 2 interfaces enabled with NAT hairpinning.
  Interface: GigabitEthernet1/0/4
    Config status: Active

  Interface: GigabitEthernet1/0/5
    Config status: Active

NAT mapping behavior:
  Mapping mode : Endpoint-Independent
  ACL          : 2050
  Config status: Active

NAT ALG:
  DNS        : Enabled
  FTP        : Enabled
  H323       : Enabled
  ICMP-ERROR : Enabled
  ILS        : Enabled
  MGCP       : Enabled
  NBT        : Enabled
  PPTP       : Enabled
  RTSP       : Enabled
  RSH        : Enabled
  SCCP       : Enabled
  SCTP       : Disabled
  SIP        : Enabled
  SQLNET     : Enabled
  TFTP       : Enabled
  XDMCP      : Disabled

NAT port block group information:
  Totally 3 NAT port block groups.
  Port block group 1:
    Port range: 1-65535
    Block size: 256
    Local IP address information:
      Start address        End address          VPN instance
      172.16.1.1           172.16.1.254         ---
      192.168.1.1          192.168.1.254        ---
      192.168.3.1          192.168.3.254        ---
    Global IP pool information:
      Start address        End address
      201.1.1.1            201.1.1.10
      201.1.1.21           201.1.1.25
```

```
  Port block group 2:
    Port range: 10001-30000
    Block size: 500
    Local IP address information:
      Start address        End address          VPN instance
      10.1.1.1             10.1.10.255          ---
    Global IP pool information:
      Start address        End address
      202.10.10.101        202.10.10.120

  Port block group 3:
    Port range: 1-65535
    Block size: 256
    Local IP address information:
      Start address        End address          VPN instance
      ---                  ---                  ---
    Global IP pool information:
      Start address        End address
      ---                  ---

NAT outbound port block group information:
  Totally 2 outbound port block group items.
  Interface: GigabitEthernet1/0/2
    port-block-group: 2
    Rule name: stone
    Config status   : Active

  Interface: GigabitEthernet1/0/2
    port-block-group: 10
    Config status   : Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: port block group.

Static NAT load balancing:     Disabled

NAT link-switch recreate-session: Disabled

NAT configuration-for-new-connection: Disabled
```

The output shows all NAT configuration information. Table 2 describes only the fields for the output of the **nat hairpin enable**, **nat mapping-behavior**, and **nat alg** commands.

Table 2 Command output

Field	Description
NAT address group information	Information about the NAT address group. See Table 1 for output description.
NAT server group information	Information about the internal server group. See Table 19 for output description.
NAT inbound information:	Inbound dynamic NAT configuration. See Table 6 for output

Field	Description
	description.
NAT outbound information	Outbound dynamic NAT configuration. See Table 10 for output description.
NAT internal server information	NAT server mapping configuration. See Table 18 for output description.
NAT global-policy information	Configuration of the global NAT policy. See Table 5 for output description.
NAT policy information	Configuration of the NAT policy. See Table 13 for output description.
Static NAT mappings	Static NAT mappings. See Table 21 for output description.
NAT DNS mappings	NAT DNS mappings. See Table 3 for output description.
NAT logging	NAT logging configuration. See Table 7 for output description.
NAT hairpinning	NAT hairpin configuration.
Totally *n* interfaces enabled NAT hairpinning	Number of interfaces with NAT hairpin enabled.
Interface	NAT hairpin-enabled interface.
Rule name	Name of the NAT rule.
Priority	Priority of the NAT rule.
Config status	Status of the NAT hairpin configuration: **Active** or **Inactive**.
NAT mapping behavior	Mapping behavior mode of PAT: **Endpoint-Independent** or **Address and Port-Dependent**.
ACL	ACL number or name. If no ACL is specified for NAT, this field displays hyphens (---).
Config status	Status of the NAT mapping behavior configuration: **Active** or **Inactive**.
Reasons for inactive status	Reasons why the NAT mapping behavior configuration does not take effect. This field is available when the **Config status** is **Inactive**.
NAT ALG	NAT ALG configuration for different protocols.
NAT port block group information	Configuration information about NAT port block groups. See Table 15 for output description.
NAT outbound port block group information	Configuration information about static outbound port block mapping rules. See Table 11 for output description.
Static NAT load balancing	Whether load balancing is enabled for static NAT on service engines: • Enabled. • Disabled.
NAT link-switch recreate-session	Whether NAT session recreation after link switchover is enabled: • Enabled. • Disabled.
NAT configuration-for-new-connection	Whether NAT configuration changes taking effect only on new connections is enabled: • Enabled. • Disabled.

display nat dns-map

Use **display nat dns-map** to display NAT DNS mappings.

Syntax

display nat dns-map

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display NAT DNS mappings.

```
<Sysname> display nat dns-map
NAT DNS mapping information:
  Totally 2 NAT DNS mappings.
  Domain name  : www.server.com
  Global IP    : 6.6.6.6
  Global port  : 23
  Protocol     : TCP(6)
  Config status: Active

  Domain name  : www.service.com
  Global IP    : ---
  Global port  : 12
  Protocol     : TCP(6)
  Config status: Inactive
  Reasons for inactive status:
    The following items don't exist or aren't effective: interface IP address.
```

Table 3 Command output

Field	Description
NAT DNS mapping information	Information about NAT DNS mappings.
Totally *n* NAT DNS mappings	Total number of NAT DNS mappings.
Domain name	Domain name of the internal server.
Global IP	Public IP address of the internal server. • If Easy IP is configured, this field displays the IP address of the specified interface. • If you do not specify a public IP address, this field displays hyphens (**---**).
Global port	Public port number of the internal server.
Protocol	Protocol name and number of the internal server.

Field	Description
Config status	Status of the DNS mapping: **Active** or **Inactive**.
Reasons for inactive status	Reasons why the DNS mapping does not take effect. This field is available when the **Config status** is **Inactive**.

Related commands

nat dns-map

display nat eim

Use **display nat eim** to display information about NAT Endpoint-Independent Mapping (EIM) entries.

Syntax

display nat eim [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays EIM entry information for all member devices.

Usage guidelines

EIM entries are created when PAT operates in EIM mode. An EIM entry is a 3-tuple entry, and it records the mapping between a private address/port and a public address/port.

The EIM entry provides the following functions:

- The same EIM entry applies to subsequent connections initiated from the same source IP and port.
- The EIM entries allow reverse translation for connections initiated from external hosts to internal hosts.

Examples

Display information about EIM entries for the specified slot.

```
<Sysname> display nat eim slot 1
Slot 1:
Local  IP/port: 192.168.100.100/1024
Global IP/port: 200.100.1.100/2048
Local  VPN: vpn1
Global VPN: vpn2
Protocol: TCP(6)

Local  IP/port: 192.168.100.200/2048
```

```
Global IP/port: 200.100.1.200/4096
Protocol: UDP(17)

Total entries found: 2
```

Table 4 Command output

Field	Description
Local VPN	MPLS L3VPN instance to which the private IP address belongs. If the private IP address does not belong to any VPN instance, this field is not displayed.
Global VPN	MPLS L3VPN instance to which the public IP address belongs. If the public IP address does not belong to any VPN instance, this field is not displayed.
Protocol	Protocol name and number.
Total entries found	Total number of EIM entries.

Related commands

nat mapping-behavior

nat outbound

display nat global-policy

Use **display nat global-policy** to display configuration of the global NAT policy.

Syntax

display nat global-policy [**rule-type** { **nat** | **nat64** | **nat66** }]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

rule-type: Specifies a NAT rule type. If you do not specify this keyword, this command displays information about all types of NAT rules.

nat: Specifies NAT-type rules.

nat64: Specifies NAT64-type rules.

nat66: Specifies NAT66-type rules.

Examples

Display configuration of all types of NAT rules in the global NAT policy.

```
<Sysname> display nat global-policy
NAT global-policy information:
  Totally 8 NAT global-policy rules.
```

```
Rule name: rule1
  Type                  : nat
  Description           : first rule
  SrcIP object group    : srcObj1
  SrcIP object group    : srcObj2
  SrcIP object group    : srcObj3
  DestIP object group   : desObj1
  DestIP object group   : desObj2
  DestIP object group   : desObj3
  Service object group  : serviceObj1
  Service object group  : serviceObj2
  Service object group  : serviceObj3
  Source-zone name      :  Trust
  Destination-zone name :  Local
  SNAT action:
    Address group ID: 2      Address group name: a
    NO-PAT: Y
    Reversible: N
    Port-preserved: N
  NAT counting : 0
  Config status: Active

Rule name: rule2
  Type                  : nat
  Description           : second rule
  SrcIP address         : 10.0.0.1
  SrcIP address         : 10.0.0.2
  DestIP address        : 100.0.0.11
  DestIP address        : 100.0.0.12
  Service object group  : serviceObj1
  Source-zone name      : Trust
  Destination-zone name : local
  SNAT action:
    Easy-IP
    NO-PAT: N
    Reversible: N
    Port-preserved: N
  NAT counting : 0
  Config status: Active

Rule name: rule3
  Type                  : nat
  Description           : third rule
  SrcIP object group    : srcObj1
  DestIP object group   : desObj1
  Service object group  : serviceObj1
  Service object group  : serviceObj2
  Service object group  : serviceObj3
```

```
  Source-zone name      : trust
  Vrf                   : vpn1
  SNAT action:
    Ipv4 address: 20.0.0.1
    Vrf: vpn2
  DNAT action:
    IPv4 address: 1.1.2.1
    Port: 80
    Vrf: vpn2
  NAT counting : 0
  Config status: Active

Rule name: rule4
  Type                  : nat
  Description           : third rule
  SrcIP subnet          : 10.1.1.0 24
  DestIP subnet         : 100.1.3.0 24
  SNAT action:
    Subnet: 20.0.0.0 24
  DNAT action:
    IPv4 address: 1.1.2.1
    Port: 80
  NAT counting : 0
  Config status: Active

Rule name: rule5
  Type                  : nat
  Description           : fifth rule
  SrcIP subnet          : 10.1.1.0 24
  DestIP subnet         : 100.1.3.0 24
  Source-zone name      : Trust
  VRID: 1
  SNAT action:
    Object group: obj1
  DNAT action:
    IPv4 address: 1.1.2.1
  NAT counting : 0
  Config status: Active

Rule name: 44_1
  Type                  : nat
  SrcIP address         : 10.1.1.10
  DestIP address        : 10.1.1.100
  SNAT action:
    IPv4 address: 2.1.1.100
    IPv4 VRRP VRID: 1
  DNAT action:
    IPv4 address: 2.1.1.15
```

```
    IPv4 VRRP VRID: 2
  NAT counting : 0
  Config status: Active

Rule name: 4to6_1
  Type                  : nat64
  SrcIP address         : 10.1.1.10
  DestIP address        : 10.1.1.100
  SNAT action:
    IPv6 address: 3003::100
    IPv6 VRRP VRID: 1
  DNAT action:
    IPv6 address: 3003::15
    IPv4 VRRP VRID: 2
  NAT counting : 0
  Config status: Active

Rule name: 66_1
  Type                  : nat66
  SrcIPV6 address       : 3001::10
  SNAT action:
    IPv6 address: 3003::800
    IPv6 VRRP VRID: 1
  NAT counting : 0
  Config status: Active
```

Table 5 Command output

Field	Description
NAT global-policy information	Configuration of the global NAT policy.
Totally *n* NAT global-policy rules	Total number of NAT rules in the policy.
Rule name	Name of the NAT rule.
Type	NAT rule type: • **nat**—NAT rule, which is used for translation between IPv4 addresses. • **nat64**—NAT64-type rule, which is used for translation between IPv4 addresses and IPv6 addresses. • **nat66**—NAT66-type rule, which is used for translation between IPv6 addresses or IPv6 address prefixes.
Description	Description of the NAT rule.
SrcIP object group	Source IP address object group in the NAT rule.
SrcIP address	IP address that the NAT rule uses to match packet source IP addresses.
SrcIP subnet	Subnet address that the NAT rule uses to match packet source IP addresses.
DestIP object group	Destination IP address object group in the NAT rule.
DestIP address	IP address that the NAT rule uses to match packet destination IP addresses.

Field	Description
DestIP subnet	Subnet address that the NAT rule uses to match packet destination IP addresses.
Service object group	Service object group in the NAT rule.
Source-zone name	Source security zone in the NAT rule.
Destination-zone name	Destination security zone in the NAT rule.
Vrf	VPN instance in the NAT rule.
IPv4 VRRP VRID	Virtual router ID (IPv4 VRRP group number) bound to the NAT rule.
IPv6 VRRP VRID	Virtual router ID (IPv6 VRRP group number) bound to the NAT rule.
SNAT action	Source address translation method in the NAT rule.
NO-NAT	No address translation.
Address group ID	ID of the NAT address group used in the NAT rule. If no NAT address group is specified, this field is not displayed.
Address group name	Name of the NAT address group used in the NAT rule. If no NAT address group is specified, this field is not displayed.
Easy-IP	Easy IP method used in the NAT rule. This field is not displayed if the Easy IP method is not specified.
IPv4 address	NAT IP address for source address translation. This field is not displayed if no translated source IP address is configured.
IPv6 address	NAT IPv6 address for source address translation. This field is not displayed if no translated source IPv6 address is configured.
Subnet	A range of NAT IP addresses for source address translation. This field is not displayed if no translated source subnet is configured.
NO-PAT	Whether NO-PAT or PAT is used: • **Y**—NO-PAT is used. • **N**—PAT is used.
Reversible	Whether reverse address translation is allowed: • **Y**—Reverse address translation is allowed. • **N**—Reverse address translation is not allowed.
Prefix	Prefix translation method used for source address translation in a NAT64-type rule: • **nat64 v4tov6**—Uses the NAT64 prefix to translate source IPv4 addresses to IPv6 addresses. • **General v4tov6**—Uses the general prefix to translate source IPv4 addresses to IPv6 addresses. • **General v6tov4**—Uses the general prefix to translate source IPv6 addresses to IPv4 addresses. This field is not displayed if the prefix method is not configured for source address translation.
Port-preserved	Whether to try to preserve the port numbers for PAT. • **Y**—Tries to preserve the port numbers. • **N**—Allows translating port numbers.
NPTv6	IPv6 address prefix used for source IPv6 address translation in NPTv6 method. The format is *translated-ipv6-prefix nptv6-prefix-length*, where the

Field	Description
	translated-ipv6-prefix argument indicates the address prefix and the *nptv6-prefix-length* argument specifies the IPv6 address prefix length. This field is not displayed if the NPTv6 method is not configured for source IPv6 address translation.
Vrf	VPN instance to which the source IP address after translation belongs.
DNAT action	Destination IP address translation method of the NAT rule.
IPv4 address	NAT IPv4 address for destination IP address translation.
IPv6 address	NAT IPv6 address for destination IP address translation.
Port	Translated port number for destination IP address translation.
Prefix	Prefix translation method used for destination address translation in a NAT64-type rule: • **nat64 v6tov4**—Uses the NAT64 prefix to translate destination IPv6 addresses to IPv4 addresses. • **General v4tov6**—Uses the general prefix to translate destination IPv4 addresses to IPv6 addresses. • **General v6tov4**—Uses the general prefix to translate destination IPv6 addresses to IPv4 addresses. • **IVI v4tov6**—Uses the IVI prefix to translate IPv4 addresses to IPv6 addresses. This field is not displayed if the prefix method is not configured for destination address translation.
NPTv6	IPv6 address prefix used for destination IPv6 address translation in NPTv6 method. The format is *translated-ipv6-prefix nptv6-prefix-length*, where the *translated-ipv6-prefix* argument indicates the address prefix and the *nptv6-prefix-length* argument specifies the IPv6 address prefix length. This field is not displayed if the NPTv6 method is not configured for source IPv6 address translation.
Vrf	VPN instance to which the destination IP address after translation belongs.
NAT counting	Number of times the NAT rule is matched.
Config status	Status of the global NAT policy: **Active** or **Inactive**.
Reasons for inactive status	Reasons why the NAT rule does not take effect. This field is available when the **Config status** is **Inactive**.

display nat inbound

Use **display nat inbound** to display inbound dynamic NAT configuration.

Syntax

display nat inbound

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display inbound dynamic NAT configuration.

```
<Sysname> display nat inbound
NAT inbound information:
  Totally 2 NAT inbound rules.
  Interface: GigabitEthernet1/0/2
    ACL: 2038
    Address group ID: 2
    Add route: Y            NO-PAT: Y  Reversible: N
    VPN instance: vpn1
    Rule name: abcd
    Priority: 1000
    Description: NatInbound1
    NAT counting: 0
    Config status: Active

Interface: GigabitEthernet1/0/3
    Address group ID: 1
    Add route: Y             NO-PAT: Y  Reversible: N
    Rule name: eif
    Priority: 1001
    NAT counting: 0
    Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: ACL.
```

Table 6 Command output

Field	Description
NAT inbound information	Information about inbound dynamic NAT configuration.
Totally *n* NAT inbound rules	Total number of inbound dynamic NAT rules.
Interface	Interface where the inbound dynamic NAT rule is configured.
ACL	ACL number or name.
Address group ID	ID of the NAT address group used by the inbound dynamic NAT rule.
Address group name	Name of the NAT address group. If no address group name is configured, this field is not displayed.
Add route	Whether to add a route when a packet matches the inbound dynamic NAT rule: • **Y**—Adds a route. • **N**—Does not add a route.
NO-PAT	Whether NO-PAT or PAT is used:

Field	Description
	• **Y**—NO-PAT is used. • **N**—PAT is used.
Reversible	Whether reverse address translation is allowed: • **Y**—Reverse address translation is allowed. • **N**—Reverse address translation is not allowed.
VPN instance	MPLS L3VPN instance to which the NAT address group belongs. If the NAT address group does not belong to any VPN instance, the field is not displayed.
Rule name	Name of the NAT rule.
Priority	Priority of the NAT rule.
Description	Description of the NAT rule. This field is not displayed if no description is configured for the rule.
NAT counting	Number of times the NAT rule is matched.
Config status	Status of the inbound dynamic NAT rule: **Active** or **Inactive**.
Reasons for inactive status	Reasons why the inbound dynamic NAT rule does not take effect: This field is available when the **Config status** is **Inactive**.

Related commands

`nat inbound`

display nat log

Use **`display nat log`** to display NAT logging configuration.

Syntax

`display nat log`

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display NAT logging configuration.

```
<Sysname> display nat log
NAT logging:
  Log enable          : Enabled(ACL 2000)
  Flow-begin          : Disabled
  Flow-end            : Disabled
  Flow-active         : Enabled(10 minutes)
  Port-block-assign   : Disabled
  Port-block-withdraw : Disabled
```

```
Alarm               : Disabled
NO-PAT IP usage     : Disabled
```

Table 7 Command output

Field	Description
NAT logging	NAT logging configuration.
Log enable	Enabling status of NAT logging. If an ACL is specified for NAT logging, this field also displays the ACL number or name.
Flow-begin	Enabling status of logging for NAT session establishment events.
Flow-end	Enabling status of logging for NAT session removal events.
Flow-active	Enabling status of logging for active NAT flows. If it is enabled, this field also displays the interval in minutes at which active flow logs are generated.
Port-block-assign	Enabling status of NAT444 user logging for port block assignment.
Port-block-withdraw	Enabling status of NAT444 user logging for port block withdrawal.
Alarm	Enabling status of logging for NAT444 alarms.
NO-PAT IP usage	Enabling status of logging for IP usage of NAT address groups when NO-PAT mode is used. If it is enabled, this field also displays IP usage for each configured NAT address group, in percentage.

Related commands

`nat log enable`

`nat log flow-active`

`nat log flow-begin`

`nat log no-pat ip-usage`

display nat no-pat

Use **`display nat no-pat`** command to display information about NAT NO-PAT entries.

Syntax

`display nat no-pat` { **`ipv4`** | **`ipv6`** } [**`slot`** *`slot-number`*]

Views

Any view

Default user roles

network-admin

network-operator

context-admin

context-operator

Parameters

`ipv4`: Displays NO-PAT entry information for IPv4 NAT sessions.

`ipv6`: Displays NO-PAT entry information for IPv6 NAT sessions.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays NO-PAT entry information for all member devices.

Usage guidelines

A NO-PAT entry records the mapping between a private address and a public address.

The NO-PAT entry provides the following functions:

- The same entry applies to subsequent connections initiated from the same source IP address.
- The NO-PAT entries allow reverse translation for connections initiated from external hosts to internal hosts.

Outbound and inbound NO-PAT address translations create their own NO-PAT tables. These two types of tables are displayed separately.

Examples

Display information about NO-PAT entries for IPv4 NAT sessions on the specified slot.

```
<Sysname> display nat no-pat ipv4 slot 1
Slot 1:
Global  IPv4: 200.100.1.100
Local   IPv4: 192.168.100.100
Global VPN: vpn2
Local  VPN: vpn1
Reversible: N
Type      : Inbound

Local   IPv4: 192.168.100.200
Global  IPv4: 200.100.1.200
Reversible: Y
Type      : Outbound

Total Ipv4 entries found: 2
```

Display information about NO-PAT entries for IPv6 NAT sessions on all cards.

```
<Sysname> display nat no-pat ipv6
Slot 0:
Global  IPv6: FD01:203:405::1
Local   IPv6: 2001:DB8:1::100
Global VPN: vpn2
Local  VPN: vpn1
Reversible: N
Type      : Inbound

Total Ipv6 entries found: 1
```

Display information about NO-PAT entries for IPv6 NAT sessions on the specified slot.

```
<Sysname> display nat no-pat slot 1 ipv6
Slot 1:
Global  IPv6: FD01:203:405::1
Local   IPv6: 2001:DB8:1::100
Global VPN: vpn2
Local  VPN: vpn1
Reversible: N
Type      : Inbound
```

```
Total Ipv6 entries found: 1
```

Table 8 Command output

Field	Description
Global IPv4	Public IPv4 address.
Local IPv4	Private IPv4 address.
Global IPv6	Public IPv6 address.
Local IPv6	Private IPv6 address.
Local VPN	MPLS L3VPN instance to which the private IP address belongs. If the private IP address does not belong to any VPN instance, this field is not displayed.
Global VPN	MPLS L3VPN instance to which the public IP address belongs. If the public IP address does not belong to any VPN instance, this field is not displayed.
Reversible	Whether reverse address translation is allowed: • **Y**—Reverse address translation is allowed. • **N**—Reverse address translation is not allowed.
Type	Type of the NO-PAT entry: • **Inbound**—A NO-PAT entry created during inbound dynamic NAT. • **Outbound**—A NO-PAT entry created during outbound dynamic NAT.
Total Ipv4 entries found	Total number of IPv4 NO-PAT entries.
Total Ipv6 entries found	Total number of IPv6 NO-PAT entries.

Related commands

nat inbound

nat outbound

display nat no-pat ip-usage

Use **display nat no-pat ip-usage** to display IP usage of NAT address groups or object groups in NO-PAT mode.

Syntax

display nat no-pat ip-usage [**address-group** { *group-id* | **name** *group-name* } | **object-group** *object-group-name*] [**slot** *slot-number*]

Views

Any view

Predefines user roles

network-admin

network-operator

context-admin

context-operator

Parameters

address-group: Displays the IP usage of the specified NAT address group. If you do not specify this keyword, the command displays the IP usage of each NAT address group.

group-id: Specifies the ID of a NAT address group. The value range is 0 to 65535.

name *group-name*: Specifies the name of a NAT address group, a case-insensitive string of 1 to 63 characters.

object-group *object-group-name*: Specifies the IP usage of the specified object group. The name is a case-insensitive string of 1 to 63 characters.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the IP usage of NAT address groups or object groups in NO-PAT mode for all member devices.

Examples

Display IP usage of address resources for all types in NO-PAT mode for the specified slot.

```
<Sysname> display nat no-pat ip-usage slot 1
```

CPU 0 on slot 1:

```
Totally 2 pieces of information about address usage.
  Address group 0:
    Total IP addresses   :10
    Used IP addresses    :9
    Unused IP addresses  :1
    NO-PAT IP usage      :90% (channel 0)

  Object group name: obj1
    Total IP addresses    :10
    Used IP addresses     :0
    Unused IP addresses   :10
    NO-PAT IP usage       :0%
```

Table 9 Command output

Field	Description
Address group	NAT address group ID.
NO-PAT IP usage	IP usage of the NAT address group or object group in NO-PAT mode.
channel	Field-programmable gate array (FPGA) ID.

Related commands

nat log no-pat ip-usage threshold

display nat outbound

Use **display nat outbound** to display outbound dynamic NAT configuration.

Syntax

display nat outbound

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display outbound dynamic NAT configuration.

```
<Sysname> display nat outbound
NAT outbound information:
  Totally 2 NAT outbound rules.
  Interface: GigabitEthernet1/0/1
    ACL: 2036
    Address group ID: 1
    Port-preserved: Y           NO-PAT: N  Reversible: N
    Configuration mode : NETCONF (action)
    Rule name: abefg
    Priority: 1000
    NAT counting: 0
    Config status: Active

  Interface: GigabitEthernet1/0/2
    ACL: 2037
    Address group ID: 2
    Port-preserved: N            NO-PAT: Y  Reversible: Y
    VPN instance: vpn_nat
    Rule name: cdefg
    Priority: 1001
    Description: NatOutbound1
    NAT counting: 0
    Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: ACL.

  Interface: GigabitEthernet1/0/1
    DS-Lite B4 ACL: 2100
    Address group ID: 2
    Port-preserved: N             NO-PAT: N  Reversible: N
    Priority: 0
    NAT counting: 0
    Config status: Active
```

Table 10 Command output

Field	Description
NAT outbound information	Information about outbound dynamic NAT configuration.
Totally *n* NAT outbound rules	Total number of outbound dynamic NAT rules.
Interface	Interface where the outbound dynamic NAT rule is configured.

Field	Description
ACL	IPv4 ACL number or name. If no IPv4 ACL is specified for outbound dynamic NAT rule, this field displays hyphens (**---**).
DS-Lite B4 ACL	Number or name of the IPv6 ACL used by DS-Lite B4 address translation.
Address group ID	ID of the address group used by the outbound dynamic NAT rule. If no address group is specified, the field displays hyphens (---).
Address group name	Name of the NAT address group. If no address group name is configured, this field is not displayed.
Port-preserved	Whether to try to preserve the port numbers for PAT. • **Y**—Tries to preserve the port numbers. • **N**—Allows translating port numbers.
NO-PAT	Whether NO-PAT is used: • **Y**—NO-PAT is used. • **N**—PAT is used.
Reversible	Whether reverse address translation is allowed: • **Y—**Reverse address translation is allowed. • **N—**Reverse address translation is not allowed.
VPN instance	MPLS L3VPN instance to which the NAT address group belongs. If the NAT address group does not belong to any VPN instance, the field is not displayed.
Rule name	Name of the NAT rule.
Priority	Priority of the NAT rule.
Description	Description of the NAT rule. This field is not displayed if no description is configured for the rule.
Configuration mode	Configuration method of the device. • This field displays **NETCONF (action)** if the device is configured by using a NETCONF action operation. • This field is not displayed if the device is configured by using other methods.
NAT counting	Number of times the NAT rule is matched.
Config status	Status of the outbound dynamic NAT rule: **Active** or **Inactive**.
Reasons for inactive status	Reasons why the outbound dynamic NAT rule does not take effect. This field is available when the **Config status** is **Inactive**.

Related commands

`nat outbound`

display nat outbound port-block-group

Use **`display nat outbound port-block-group`** to display static outbound port block mapping rules for NAT444.

Syntax

`display nat outbound port-block-group`

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display static outbound port block mapping rules for NAT444.

```
<Sysname> display nat outbound port-block-group
NAT outbound port block group information:
  Totally 2 outbound port block group items.
  Interface: GigabitEthernet1/0/2
    port-block-group: 2
    Rule name: abcdefg
    NAT counting: 0
    Config status   : Active

  Interface: GigabitEthernet1/0/2
    port-block-group: 10
    Rule name: abcfg
    NAT counting: 0
    Config status   : Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: port block group.
```

Table 11 Command output

Field	Description
NAT outbound port block group information	Information about static outbound port block mapping rules.
Totally *n* outbound port block group items	Total number of static outbound port block mapping rules.
Interface	Interface where the static outbound port block mapping rules configured.
port-block-group	ID of the port block group.
Rule name	Name of the static outbound port block mapping rule
NAT counting	Number of times the mapping rule is matched.
Config status	Status of the port block mapping rule: **Active** or **Inactive**.
Reasons for inactive status	Reasons why the port block mapping rule does not take effect. This field is available when the **Config status** is **Inactive**.

Related commands

`nat outbound port-block-group`

display nat periodic-statistics

Use **`display nat periodic-statistics`** to display periodic NAT statistics.

Syntax

display nat periodic-statistics { **address-group** [*group-id* | **name** *group-name*] | **ip** *global-ip* } [**slot** *slot-number*]

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280	No
NFNX5-HD6480, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	Yes

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

address-group: Displays periodic NAT statistics for the specified NAT address group.

group-id: Specifies the ID of a NAT address group. The value range for this argument is 0 to 65535.

name *group-name*: Specifies the name of a NAT address group. The name is a case-insensitive string of 1 to 63 characters.

ip *global-ip*: Displays periodic NAT statistics for the specified IP address. The *global-ip* argument specifies an IP address.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays periodic NAT statistics for all member devices.

Usage guidelines

If you do not specify the *group-id* argument or the **name** keyword, this command displays periodic NAT statistics for all NAT address groups.

Examples

Display periodic NAT statistics for address groups for slot 1.

```
<Sysname> display nat periodic-statistics address-group slot 1
Slot 1:
Totally 1 NAT address groups.
  Address group ID: 1     Address group name: abc
    NAT sessions                      : 10
    NAT port-block assign failures    : 0
```

Display periodic NAT statistics for IP address 202.38.6.12 for slot 1.

```
<Sysname> display nat periodic-statistics ip 202.38.6.12 slot 1
Slot 1:
  Global IP: 202.38.6.12
    NAT sessions                      : 10
```

```
    NAT port-block assign failures   : 0
```

Table 12 Command output

Field	Description
Address group ID	ID of the NAT address group. If no address group is specified, this field displays hyphens (**---**).
Totally *n* NAT address groups	Total number of NAT address groups.
Address group name	Name of the NAT address group. If no address group name is configured, this field is not displayed.
Global IP	IP address used for address translation. If the address is not in the specified address group, this field displays hyphens (**---**).
NAT sessions	Number of NAT sessions.
NAT port-block assign failures	Number of port block assignment failures.

Related commands

`nat periodic-statistics enable`

`nat periodic-statistics interval`

`reset nat periodic-statistics`

display nat policy

Use **`display nat policy`** to display the NAT policy configuration.

Syntax

`display nat policy`

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	No

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display the NAT policy configuration.

```
<Sysname> display nat policy
NAT policy information:
  Totally 1 NAT policy rules.
```

```
Rule name: rule1
  Description            : first rule
  Outbound-interface     : GigabitEthernet1/0/2
  SrcIP object group     : srcObj1
  SrcIP object group     : srcObj2
  SrcIP object group     : srcObj3
  DestIP object group    : desObj1
  DestIP object group    : desObj2
  DestIP object group    : desObj3
  Service object group   : serviceObj1
  Service object group   : serviceObj2
  Service object group   : serviceObj3
  Action:
    Address group ID: 2      Address group name: a
    NO-PAT: Y
    Reversible: N
    Port-preserved: N
  NAT counting : 0
  Config status: Active
```

Table 13 Command output

Field	Description
NAT policy information	Information about the NAT policy configuration.
Totally *n* NAT policy rules	Total number of NAT rules in the NAT policy.
Rule name	NAT rule name.
Description	Description of the NAT rule.
Outbound-interface	Direction of the traffic that the NAT rule applies.
SrcIP object group	Source IP address object group in the NAT rule.
DestIP object group	Destination IP address object group in the NAT rule.
Service object group	Service object group in the NAT rule.
Action	Address translation method in the NAT rule.
Easy-IP	Easy IP method.
NO-NAT	Address translation is disabled.
Address group ID	ID of the NAT address group in the NAT rule. If no NAT address group ID is configured, this field is not displayed.
Address group name	Name of the NAT address group. If no address group name is configured, this field is not displayed.
Reversible	Whether reverse address translation is allowed. • **Y**—Reverse address translation is allowed. • **N**—Reverse address translation is not allowed.
Port-preserved	Whether to try to preserve the port numbers for PAT: • **Y**—Tries to preserve the port numbers. • **N**—Allows translating port numbers.
NAT counting	Number of times the rule is matched.

Field	Description
Config status	Status of the NAT policy configuration: **Active** or **Inactive**.
Reasons for inactive status	Reasons why the NAT policy does not take effect. This field is available when the **Config status** is **Inactive**.

display nat port-block

Use **display nat port-block** to display NAT port block mappings.

Syntax

display nat port-block { **dynamic** [**address-group** { *group-id* | **name** *group-name* }] [**ds-lite-b4**] | **static** [**port-block-group** *group-id*] } [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

dynamic: Displays dynamic port block mappings.

address-group: Displays port block mappings for the specified address group. If you do not specify a NAT address group, this command displays port block mappings for all address groups.

group-id: Specifies the ID of the address group. The value range for this argument is 0 to 65535.

name *group-name*: Specifies the name of the address group. The name is a case-insensitive string of 1 to 63 characters.

ds-lite-b4: Displays port block mappings for DS-Lite B4 address translation.

static: Displays static port block mappings.

port-block-group *group-id*: Displays port block mappings for the specified port block group. The *group-id* argument specifies the ID of the port block group. The value range for the *group-id* argument is 0 to 65535. If you do not specify a port block group, this command displays port block mappings for all port block groups.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays port block mappings for all member devices.

Examples

Display static port block mappings for the specified slot.

```
<Sysname> display nat port-block static slot 1
Slot 1:
Local VPN     Local IP         Global IP        Port block   Connections
---           100.100.100.111  202.202.100.101  10001-10256  0
---           100.100.100.112  202.202.100.101  10257-10512  0
---           100.100.100.113  202.202.100.101  10513-10768  0
```

```
---           100.100.100.113  202.202.100.101  10769-11024  0
Total entries found: 4
```

Display dynamic port block mappings.

```
<Sysname> display nat port-block dynamic slot 1
Slot 1:
Local VPN     Local IP         Global IP        Port block   Connections
---           101.1.1.12       192.168.135.201  10001-11024  1
Total entries found: 1
```

Display port block mappings for DS-Lite B4 address translation.

```
<Sysname> display nat port-block dynamic ds-lite-b4 slot 1
Slot 1:
Local VPN     DS-Lite B4 addr  Global IP        Port block   Connections
---           2000::2          192.168.135.201  10001-11024  1
Total entries found: 1
```

Table 14 Command output

Field	Description
Local VPN	MPLS L3VPN instance to which the private IP address belongs. If the private IP address does not belong to any VPN instance, this field displays hyphens (**---**).
Local IP	Private IP address.
DS-Lite B4 addr	IPv6 address of the DS-Lite B4 element.
Global IP	Public IP address.
Port block	Port block defined by a start port number and an end port number.
Connections	Number of connections established by using the ports in the port block.

display nat port-block-group

Use **display nat port-block-group** to display NAT port block group configuration.

Syntax

display nat port-block-group [*group-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

group-id: Specifies the ID of a NAT port block group. The value range for this argument is 0 to 65535. If you do not specify this argument, the command displays configuration of all NAT port block groups.

Examples

Display configuration of all NAT port block groups.

```
<Sysname> display nat port-block-group
NAT port block group information:
  Totally 3 NAT port block groups.
  Port block group 1:
    VRID      : 2
    Port range: 1-65535
    Block size: 256
    Local IP address information:
      Start address        End address          VPN instance
      172.16.1.1           172.16.1.254         ---
      192.168.1.1          192.168.1.254        ---
      192.168.3.1          192.168.3.254        ---
    Global IP pool information:
      Start address        End address
      201.1.1.1            201.1.1.10
      201.1.1.21           201.1.1.25

  Port block group 2:
    Port range: 10001-30000
    Block size: 500
    Local IP address information:
      Start address        End address          VPN instance
      10.1.1.1             10.1.10.255          ---
    Global IP pool information:
      Start address        End address
      202.10.10.101        202.10.10.120

  Port block group 3:
    Port range: 1-65535
    Block size: 256
    Local IP address information:
      Start address        End address          VPN instance
      ---                  ---                  ---
    Global IP pool information:
      Start address        End address
      ---                  ---
```

Display information about NAT port block group **1**.

```
<Sysname> display nat port-block-group 1
  Port block group 1:
    VRID      : 2
    Port range: 1-65535
    Block size: 256
    Local IP address information:
      Start address        End address          VPN instance
      172.16.1.1           172.16.1.254         ---
      192.168.1.1          192.168.1.254        ---
```

```
  192.168.3.1          192.168.3.254        ---
Global IP pool information:
  Start address        End address
  201.1.1.1            201.1.1.10
  201.1.1.21           201.1.1.25
```

Table 15 Command output

Field	Description
NAT port block group information	Information about the port block group configuration.
Totally *n* NAT port block groups	Total number of port block groups.
Port block group	ID of the port block group.
VRID	Virtual router ID (VRRP group number). If no VRRP group is specified, this field is not displayed.
Port range	Port range for the public IP addresses.
Block size	Number of ports in a port block.
Local IP address information	Information about the private IP addresses.
Global IP pool information	Information about the public IP addresses.
Start address	Start IP address of a private or public IP address range. If no start IP address is specified for the address range, this field displays hyphens (**---**).
End address	End IP address of a private or public IP address range. If no end IP address is specified for the address range, this field displays hyphens (**---**).
VPN instance	MPLS L3VPN instance to which the private IP address range belongs. If no VPN instance is specified for the private address range, this field displays hyphens (**---**).

Related commands

nat port-block-group

display nat port-block-usage

Use **display nat port-block-usage** to display the port block usage for address groups.

Syntax

display nat port-block-usage [**address-group** *group-id*] [**slot** *slot-number*]

Views

System view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

address-group *group-id*: Specifies the ID of an address group. The value range for the *group-id* argument is 0 to 65535. If you do not specify an address group, this command displays the port block usage for all address groups.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the port block usage for all member devices.

Examples

Display the port block usage for address groups for slot 1.

```
<Sysname> display nat port-block-usage slot 1
Slot 1:
Address group 0 on channel 0:
  Total port block entries :10
  Active port block entries:9
  Current port block usage :90%
Total NAT address groups found: 1
```

Table 16 Command output

Field	Description
Address group	ID of the address group.
channel	Field-programmable gate array (FPGA) ID.
Total port block entries	Total number of port blocks in the address group.
Active port block entries	Total number of assigned port blocks in the address group.
Current port block usage	Port block usage in the address group.
Total NAT address groups found	Total number of address groups.

display nat probe address-group

Use **display nat probe address-group** to display NAT address group probe information.

Syntax

display nat probe address-group [*group-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

group-id: Specifies the address group ID. The value range for this argument is 0 to 65535. If you do not specify this argument, the command displays probe information for all address groups.

Usage guidelines

The excluded IP addresses displayed by this command only refers to those detected by the address group probe. The excluded IP addresses configured by the **exclude-ip** command are not included.

Examples

Display NAT address group probe information

```
<Sysname> display nat probe address-group
Address group ID: 1
Address-group name: dududu1
Address-group probe status: Partial available
Detected IP count: 5
Excluded IP count: 4
  IP address      Excluded  Excluded time
  1.1.1.1         YES       2017/12/26 09:30:39
  1.1.1.2         YES       2017/12/26 09:30:39
  1.1.1.3         YES       2017/12/26 09:30:39
  1.1.1.4         YES       2017/12/26 09:30:39
  1.1.1.5         NO        ----

Address group ID: 2
Address-group name: dududu2
Address-group probe status: Partial available
Detected IP count: 5
Excluded IP count: 4
  IP address      Excluded  Excluded time
  2.1.1.1         YES       2017/12/26 09:31:39
  2.1.1.2         YES       2017/12/26 09:31:39
  2.1.1.3         YES       2017/12/26 09:31:39
  2.1.1.4         YES       2017/12/26 09:31:39
  2.1.1.5         NO        ----
```

Display NAT address group probe information for slot 1.

```
<Sysname> display nat probe address-group 1
Address group ID: 1
Address-group name: dududu
Address-group probe status: Partial available
Detected IP count: 5
Excluded IP count: 4
  IP address      Excluded  Excluded time
  1.1.1.1         YES       2017/12/26 09:30:39
  1.1.1.2         YES       2017/12/26 09:30:39
  1.1.1.3         YES       2017/12/26 09:30:39
  1.1.1.4         YES       2017/12/26 09:30:39
  1.1.1.5         NO        ----
```

Table 17 Command output

Field	Description
Address group ID	ID of the NAT address group.
Address group name	Name of the address group. If the address group does not have a name, this field is not displayed.
Address-group probe status	Status of the address group status: • **Inactive**—The probe is not enabled. • **In progress**—The probe is in progress. • **All available**—All IP addresses in the group are available. • **Partial available**—Partial IP addresses are available. • **None available**—None of the IP addresses are available.
Detected IP count	Number of IP addresses that have been detected.
Excluded IP count	Number of IP addresses that are excluded from address translation.
IP address	IP addresses in the NAT address group.
Excluded	Whether the IP address is excluded from address translation: • **YES**—The IP address is excluded from address translation. • **NO**—The IP address is not excluded and can be used for address translation.
Excluded time	Time when the IP address is excluded from address translation.

Related commands

`exclude-ip`

`probe`

display nat server

Use **`display nat server`** to display NAT server mappings.

Syntax

`display nat server`

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display NAT server mappings.

```
<Sysname> display nat server
NAT internal server information (object-group):
  Totally 1 object-group-based NAT server rules.
  Rule name: aaa
```

```
    Interface: Vlan-interface1
    Local IP/Port: 1.1.1.1/80
    DestIP Object group: a1
    NAT counting  : 0
    Description   : NatServerDescription1
    Config status : Active


NAT internal server information:
  Totally 5 internal servers.
  Interface: GigabitEthernet1/0/1
    VRID          : 1
    Global ACL    : 2000
    Local IP/port : 192.168.10.1/23
    Rule name     : cdefgab
    Priority      : 1000
    Configuration mode  : NETCONF (action)
    NAT counting  : 0
    Config status : Active

  Interface: GigabitEthernet1/0/3
    Protocol: 6(TCP)
    Global IP/port: 50.1.1.1/23
    Local IP/port : 192.168.10.15/23
    Rule name     : ace
    NAT counting  : 0
    Config status : Inactive
    Reasons for inactive status:

  Interface: GigabitEthernet1/0/4
    Protocol: 6(TCP)
    Global IP/port: 50.1.1.1/23-30
    Local IP/port : 192.168.10.15-192.168.10.22/23
    Global VPN    : vpn1
    Local VPN     : vpn3
    Rule name     : abcdef
    NAT counting  : 0
    Config status : Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: ACL.

  Interface: GigabitEthernet1/0/4
    Protocol: 255(Reserved)
    Global IP/port: 50.1.1.100/---
    Local IP/port : 192.168.10.150/---
    Rule name     : cdefg
    NAT counting  : 0
    Config status : Active
```

```
Interface: GigabitEthernet1/0/5
  Protocol: 17(UDP)
  Global IP/port: 50.1.1.2/23
  Local IP/port : server group 1
                  1.1.1.1/21            (Connections: 10)
                  192.168.100.200/80    (Connections: 20)
  Rule name     : white
  NAT counting  : 0
  Config status : Active
```

Table 18 Command output

Field	Description
NAT internal server information (object-group)	Information about the object group-based NAT server mappings.
Totally *n* object-group-based NAT server rules	Total number of object group-based NAT server mappings.
Rule name	Name of the NAT server mapping.
Priority	Priority of the NAT server mapping.
Configuration mode	Configuration method of the device. • This field displays **NETCONF (action)** if the device is configured by using a NETCONF action operation. • This field is not displayed if the device is configured by using other methods.
NAT internal server information	Information about NAT server mapping.
Interface	Interface where the NAT server mapping is configured.
Protocol	Protocol number and name of the internal server.
VRID	Virtual router ID (VRRP group number). If no VRRP group is specified, this field is not displayed.
Global IP/port	Public IP address and port number of the internal server. • **Global IP**—A single IP address or an IP address range. If you use Easy IP, this field displays the IP address of the specified interface. If you do not specify an address for the interface, the **Global IP** field displays hyphens (**---**). • **port**—A single port number or a port number range. If no port number is in the specified protocol, the **port** field displays hyphens (**---**).
Local IP/port	For common NAT server mappings and object group-based NAT server mappings, this field displays the private IP address and port number of the internal server. • **Local IP**—A single IP address or an IP address range. • **port**—A single port number or a port number range. If no port number is in the specified protocol, the **port** field displays hyphens (---). For a load sharing NAT server mapping, this field displays the internal server group ID, IP address, port number, and number of connections of each member.
DestIP Object group	Destination IP object group used by the NAT server mapping.
Service Object group	Service object group used by the NAT server mapping.

Field	Description
Global VPN	MPLS L3VPN instance to which the public IP addresses belong. If the public IP addresses do not belong to any VPN instance, this field is not displayed.
Local VPN	MPLS L3VPN instance to which the private IP addresses belong. If the private IP addresses do not belong to any VPN instance, this field is not displayed.
ACL	ACL number or name. If no ACL is specified, this field is not displayed.
Rule name	Name of the NAT server mapping.
NAT counting	Number of times the NAT server mapping is matched.
Description	Description of the NAT server mapping. This field is not displayed if no description is configured for the mapping.
Config status	Status of the NAT server mapping: **Active** or **Inactive**.
Reasons for inactive status	Reasons why the NAT server mapping does not take effect. This field is available when the **Config status** is **Inactive**.

Related commands

nat server

display nat server-group

Use **display nat server-group** to display internal server group configuration.

Syntax

display nat server-group [*group-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

group-id: Specifies the ID of the internal server group. The value range for this argument is 0 to 65535. If you do not specify this argument, the command displays the configuration of all internal server groups.

Examples

Display the configuration of all internal server groups.

```
<Sysname> display nat server-group
NAT server group information:
  Totally 3 NAT server groups.
  Group Number        Inside IP             Port        Weight
  1                   192.168.0.26          23          100
                      192.168.0.27          23          500
  2                   ---                   ---         ---
```

```
  3                   192.168.0.26          69          100
```

Display the configuration of internal server group **1**.

```
<Sysname> display nat server-group 1
  Group Number        Inside IP             Port        Weight
  1                   192.168.0.26          23          100
                      192.168.0.27          23          500
```

Table 19 Command output

Field	Description
NAT server group information	Information about the NAT server group configuration.
Totally *n* NAT server groups	Total number of NAT server groups.
Group Number	ID of the internal server group.
Inside IP	Private IP address of a server in the internal server group. If no address is specified, this field displays hyphens (---).
Port	Private port number of a server in the internal server group. If no port number is specified, this field displays hyphens (**---**).
Weight	Weight of a server in the internal server group. If no weight value is specified, this field displays hyphens (**---**).

Related commands

`nat server-group`

display nat session

Use **`display nat session`** to display NAT sessions.

Syntax

`display nat session` [[**`responder`**] { **`source-ip`** *`source-ip`* | **`destination-ip`** *`destination-ip`* } * [**`vpn-instance`** *`vpn-instance-name`*]] [**`slot`** *`slot-number`*] [**`brief`** | **`verbose`**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

`responder`: Displays NAT sessions by responder. If you do not specify this keyword, this command displays NAT sessions by initiator.

`source-ip` *`source-ip`*: Displays NAT sessions for the source IP address specified by the *`source-ip`* argument. The IP address must be the source IP address of the packet that triggers the session establishment.

destination-ip *destination-ip*: Displays NAT sessions for the destination IP address specified by the *destination-ip* argument. The IP address must be the destination IP address of the packet that triggers the session establishment.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. The VPN must be the VPN inside the packet. If you do not specify a VPN instance, this command displays NAT sessions that do not belong to any VPN instance.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays NAT sessions for all member devices.

brief: Displays brief information about NAT sessions.

verbose: Displays detailed information about NAT sessions.

Usage guidelines

If you do not specify any parameters, this command displays detailed information about session initiators of all NAT sessions.

Examples

Display detailed information about NAT sessions for the specified slot.

```
<Sysname> display nat session slot 1 verbose
Slot 1:
Initiator:
  Source      IP/port: 192.168.1.18/1877
  Destination IP/port: 192.168.1.55/22
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: SrcZone
Responder:
  Source      IP/port: 192.168.1.55/22
  Destination IP/port: 192.168.1.10/1877
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: DestZone
State: TCP_SYN_SENT
Application: SSH
Rule ID: -/-/-
Rule name:
Start time: 2011-07-29 19:12:36  TTL: 28s
Initiator->Responder:         1 packets         48 bytes
Responder->Initiator:         0 packets          0 bytes

Total sessions found: 1
```

Display brief information about NAT sessions for the specified slot.

```
<Sysname> display nat session brief
Slot 1:
Protocol   Source IP/port         Destination IP/port    Global IP/port
```

```
TCP        2.1.1.20/1351          10.1.1.110/21          2.1.1.50/1025

Total sessions found: 1
```

Table 20 Command output

Field	Description
Initiator	Session information about the initiator.
Responder	Session information about the responder.
Source IP/port	Source IP address and port number.
Destination IP/port	Destination IP address and port number.
Global IP/port	Public IP address and port number.
DS-Lite tunnel peer	Destination address of the DS-Lite tunnel interface. If the session does not belong to any DS-Lite tunnel, this field displays a hyphen (**-**).
VPN instance/VLAN ID/Inline ID	The fields identify the following information: • **VPN instance**—MPLS L3VPN instance to which the session belongs. • **VLAN ID**—VLAN ID to which the session belongs for Layer 2 forwarding. • **Inline ID**——INLINE to which the session belongs for Layer 2 forwarding. If no VPN instance, VLAN ID, or inline ID is specified, a hyphen (-) is displayed for the related field.
Protocol	Transport layer protocol type: **DCCP**, **ICMP**, **Raw IP**, **SCTP**, **TCP**, **UDP**, or **UDP-Lite**.
Inbound interface	Input interface.
Source security zone	Security zone to which the input interface belongs. If the input interface does not belong to any security zone, this field displays a hyphen (**-**).
State	NAT session status.
Application	Application layer protocol type, such as **FTP** and **DNS**. This field displays **OTHER** for the protocol types identified by non-well-known ports.
Rule ID	ID of the security policy rule.
Rule name	Name of the security policy rule.
Start time	Time when the session starts.
TTL	Remaining NAT session lifetime in seconds.
Initiator->Responder	Number of packets and packet bytes from the initiator to the responder.
Responder->Initiator	Number of packets and packet bytes from the responder to the initiator.
Total sessions found	Total number of sessions.

Related commands

`reset nat session`

display nat static

Use **`display nat static`** to display static NAT mappings.

Syntax

display nat static

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display static NAT mappings.

```
<Sysname> display nat static
Static NAT mappings:
  Totally 2 inbound static NAT mappings.
  Net-to-net:
    VRID         : 1
    Global IP    : 1.1.1.1 - 1.1.1.255
    Local IP     : 2.2.2.0
    Netmask      : 255.255.255.0
    Global VPN   : vpn2
    Local VPN    : vpn1
    ACL          : 2000
    Reversible   : Y
    Rule name    : adefg
    Priority     : 1000
    NAT counting : 0
    Description  : NatStaticDescription1
    Config status: Active

  IP-to-IP:
    VRID         : 1
    Global IP   : 5.5.5.5
    Local IP     : 4.4.4.4
    ACL          : 2001
    Reversible   : Y
    Rule name    : abefg
    Priority     : 1000
    NAT counting : 0
    Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: ACL.

Totally 2 outbound static NAT mappings.
  Net-to-net:
    Local IP     : 1.1.1.1 - 1.1.1.255
    Global IP    : 2.2.2.0
```

```
    Netmask      : 255.255.255.0
    ACL          : 2000
    Reversible   : Y
    Rule name    : abcd
    Priority     : 1000
    NAT counting : 0
    Config status: Active

  IP-to-IP:
    Local IP     : 4.4.4.4
    Global IP    : 5.5.5.5
    ACL:         : 2000
    Rule name    : defg
    Priority     : 1000
    NAT counting : 0
    Reversible   : Y
    Description  : NatStaticDescription2
    Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: ACL.

Interfaces enabled with static NAT:
  Totally 1 interfaces enabled with static NAT.
  Interface: GigabitEthernet1/0/2
    Config status: Active
```

Table 21 Command output

Field	Description
Static NAT mappings	Information about static NAT mapping configuration.
Totally *n* inbound static NAT mappings	Total number of inbound static NAT mappings.
Totally *n* outbound static NAT mappings	Total number of outbound static NAT mappings.
Net-to-net	Net-to-net static NAT mapping.
IP-to-IP	One-to-one static NAT mapping.
Local IP	Private IP address or address range.
Global IP	Public IP address or address range.
Netmask	Network mask.
Local VPN	MPLS L3VPN instance to which the private IP addresses belong. If the private IP addresses do not belong to any VPN instance, this field is not displayed.
Global VPN	MPLS L3VPN instance to which the public IP addresses belong. If the public IP addresses do not belong to any VPN instance, this field is not displayed.
ACL	ACL number or name. If no ACL is specified, this field is not displayed.
Reversible	Whether reverse address translation is allowed. If reverse address translation is allowed, this field displays **Y**. If reverse address translation is not allowed, this field is not displayed.

Field	Description
Interfaces enabled with static NAT	Interfaces on which static NAT is enabled.
Totally *n* interfaces enabled with static NAT	Total number of interfaces where static NAT is enabled.
Interface	Interface on which static NAT is enabled.
Rule name	Name of the NAT rule.
Priority	Priority of the NAT rule.
VRID	Virtual router ID (VRRP group number). If no VRRP group is specified, this field is not displayed.
NAT counting	Number of times the NAT rule is matched.
Description	Description of the NAT rule. This field is not displayed if no description is configured for the rule.
Config status	Status of the static NAT mapping: **Active** or **Inactive**.
Reasons for inactive status	Reasons why the static NAT mapping does not take effect. This field is available when the **Config status** is **Inactive**.

Related commands

nat static enable

nat static inbound

nat static inbound net-to-net

nat static inbound object-group

nat static outbound

nat static outbound net-to-net

nat static outbound object-group

display nat statistics

Use **display nat statistics** to display NAT statistics.

Syntax

display nat statistics [**summary**] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

summary: Displays NAT statistics summary. If you do not specify this keyword, this command displays detailed NAT statistics.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays NAT statistics for all member devices.

Examples

Display detailed information about NAT statistics.

```
<Sysname> display nat statistics
Slot 1:
  Total session entries: 100
  Session creation rate: 0
  Total EIM entries: 1
  Total inbound NO-PAT entries: 0
  Total outbound NO-PAT entries: 0
  Total static port block entries: 10
  Total dynamic port block entries: 15
  Active static port block entries: 0
  Active dynamic port block entries: 0
```

Table 22 Command output

Field	Description
Total session entries	Number of NAT session entries.
Session creation rate	Number of NAT sessions created per second.
Total EIM entries	Total number of EIM entries.
Total inbound NO-PAT entries	Total number of inbound NO-PAT entries.
Total outbound NO-PAT entries	Total number of outbound NO-PAT entries.
Total static port block entries	Total number of static NAT444 mappings.
Total dynamic port block entries	Total number of dynamic port block mappings that can be created. It equals the number of port blocks for dynamic assignment, including the assigned and unassigned port blocks.
Active static port block entries	Number of static port block mappings that are in use.
Active dynamic port block entries	Number of dynamic port block mappings that have been created. It equals the number of dynamically assigned port blocks.

Display NAT statistics summary.

```
<Sysname> display nat statistics summary
EIM: Total EIM entries.
SPB: Total static port block entries.
DPB: Total dynamic port block entries.
ASPB: Active static port block entries.
ADPB: Active dynamic port block entries.
Slot Sessions  EIM       SPB       DPB       ASPB      ADPB
2    0         0         0         1572720   0         0
```

Table 23 Command output

Field	Description
Sessions	Number of NAT session entries.
EIM	Number of EIM entries.

Field	Description
SPB	Number of static NAT444 mappings.
DPB	Number of dynamic port block mappings that can be created. It equals the number of port blocks for dynamic assignment, including the assigned and unassigned port blocks.
ASPB	Number of static port block mappings in use.
ADPB	Number of dynamic port block mappings that have been created. It equals the number of dynamically assigned port blocks.

exclude-ip

Use **exclude-ip** to exclude IP addresses from being used in address translation.

Use **undo exclude-ip** to allow the IP addresses to be used in address translation.

Syntax

exclude-ip *start-address end-address*

undo exclude-ip *start-address end-address*

Default

All IP addresses in the NAT address group can be used as the NAT addresses.

Views

NAT address group view

Predefined user roles

network-admin

context-admin

Parameters

start-address end-address: Specifies the start and end IP addresses of the address range. The end address must not be lower than the start address. If they are the same, you specify only one IP address.

Usage guidelines

If some IP addresses in a NAT address group cannot be used for address translation, you can use this command to exclude them.

You can configure this command multiple times to specify a maximum of 100 IP address ranges excluded from address translation. No address ranges can overlap. The start IP address and the end IP address in an excluded range must be in the range configured in the **address** *start-address end-address* command. Each excluded IP address range can contain a maximum of 4096 IP addresses.

Examples

Exclude IP addresses 10.1.1.2, 10.1.1.3 to 10.1.1.5 in NAT address group from being used in address translation.

```
<Sysname> system-view
[Sysname] nat address-group 2
[Sysname-address-group-2] address 10.1.1.1 10.1.1.15
[Sysname-address-group-2] exclude-ip 10.1.1.2 10.1.1.2
[Sysname-address-group-2] exclude-ip 10.1.1.3 10.1.1.5
```

Related commands

address

global-ip-pool

Use **global-ip-pool** to add a public IP address range to a NAT port block group.

Use **undo global-ip-pool** to remove a public IP address range from a NAT port block group.

Syntax

global-ip-pool *start-address end-address*

undo global-ip-pool *start-address*

Default

No public IP address ranges exist.

Views

NAT port block group view

Predefined user roles

network-admin

context-admin

Parameters

start-address end-address: Specifies the start IP address and end IP address of a public IP address range. The end IP address cannot be lower than the start IP address. If the start and end IP addresses are the same, only one public IP address is specified.

Usage guidelines

A static port block mapping maps a public IP address to multiple private IP addresses and assigns a unique port block to each private IP address. The number of port blocks that a public IP address can assign is determined by dividing the number of ports in the port range by the port block size.

Every time you execute this command, an address range can contain a maximum of 256 public IP addresses. All public IP address ranges in one port block group cannot overlap.

Public IP address ranges in different port block groups can overlap. The port ranges for overlapped public IP address ranges cannot overlap.

Examples

Add a public IP address range to the port block group **1**. The public IP address range consists of IP addresses from 202.10.1.1 to 202.10.1.10.

```
<Sysname> system-view
[Sysname] nat port-block-group 1
[Sysname-port-block-group-1] global-ip-pool 202.10.1.1 202.10.1.10
```

Related commands

nat port-block-group

inside ip

Use **inside ip** to add a server to an internal server group.

Use **undo inside ip** to remove a server from an internal server group.

Syntax

inside ip *inside-ip* **port** *port-number* [**weight** *weight-value*]

undo inside ip *inside-ip* **port** *port-number*

Default

An internal server group has no server members.

Views

Internal server group view

Predefined user roles

network-admin

context-admin

Parameters

inside-ip: Specifies the IP address of an internal server.

port *port-number*: Specifies the port number of an internal server, in the range of 1 to 65535, excluding FTP port 20.

weight *weight-value*: Specifies the weight of the internal server. The value range is 1 to 1000, and the default value is 100.

Usage guidelines

An internal server with a larger weight receives a larger percentage of connections in the internal server group.

Examples

Add a server with IP address 10.1.1.2 and port number 30 to internal server group 1.

```
<Sysname> system-view
[Sysname] nat server-group 1
[Sysname-nat-server-group-1] inside ip 10.1.1.2 port 30
```

Related commands

nat server-group

local-ip-address

Use **local-ip-address** to add a private IP address range to a NAT port block group.

Use **undo local-ip-address** to remove a private IP address range from a NAT port block group.

Syntax

local-ip-address *start-address end-address* [**vpn-instance** *vpn-instance-name*]

undo local-ip-address *start-address end-address* [**vpn-instance** *vpn-instance-name*]

Default

No private IP address ranges exist in a NAT port block group.

Views

NAT port block group view

Predefined user roles

network-admin

context-admin

Parameters

start-address end-address: Specifies the start IP address and end IP address of a private IP address range. The end IP address cannot be lower than the start IP address. If the start and end IP addresses are the same, only one private IP address is specified.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the private IP address range belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the private IP address range does not belong to any VPN instance, do not specify this option.

Usage guidelines

A static port block mapping maps one public IP address to multiple private IP addresses and assigns a unique port block to each private IP address.

When you add multiple private IP address ranges to the same port block group, follow these restrictions:

- The private IP address ranges in the same VPN instance cannot overlap.
- The private IP address ranges that do not belong to any VPN instances cannot overlap.

In a NAT port block group, the number of private IP addresses cannot be larger than the number of assignable port blocks. Otherwise, some private IP addresses cannot obtain port blocks. The number of port blocks that a public IP address can assign is determined by dividing the number of ports in the port range by the port block size.

Examples

Add a private IP address range to port block group 1. The private IP address range consists of IP addresses from 172.16.1.1 to 172.16.1.255.

```
<Sysname> system-view
[Sysname] nat port-block-group 1
[Sysname-port-block-group-1] local-ip-address 172.16.1.1 172.16.1.255
```

Related commands

nat port-block-group

nat address-group

Use **nat address-group** to create a NAT address group and enter its view, or enter the view of an existing NAT address group.

Use **undo nat address-group** to delete a NAT address group.

Syntax

nat address-group *group-id* [**name** *group-name*]

undo nat address-group *group-id*

Default

No NAT address groups exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

group-id: Specifies the ID of a NAT address group. The value range for this argument is 0 to 65535.

name *group-name*: Assigns a name to the NAT address group. The *group-name* argument is a case-sensitive string of 1 to 63 characters.

Usage guidelines

A NAT address group is a set of address ranges. Use the **address** command to add an address range to a NAT address group. Dynamic NAT translates the source IP address of a packet into an IP address in the address group.

Examples

Create a NAT address group numbered 1 and named **abc**.

```
<Sysname> system-view
[Sysname] nat address-group 1 name abc
```

Related commands

address

display nat address-group

display nat all

nat inbound

nat outbound

nat alg

Use **nat alg** to enable NAT ALG for the specified or all supported protocols.

Use **undo nat alg** to disable NAT ALG for the specified or all supported protocols.

Syntax

nat alg { **all** | **dns** | **ftp** | **h323** | **icmp-error** | **ils** | **mgcp** | **nbt** | **pptp** | **rsh** | **rtsp** | **sccp** | **sctp** | | **sip** | **sqlnet** | **tftp** | **xdmcp** }

undo nat alg { **all** | **dns** | **ftp** | **h323** | **icmp-error** | **ils** | **mgcp** | **nbt** | **pptp** | **rsh** | **rtsp** | **sccp** | **sctp** | | **sip** | **sqlnet** | **tftp** | **xdmcp** }

Default

NAT ALG is enabled for DNS, FTP, ICMP error messages, PPTP, and RTSP, and is disabled for the other supported protocols.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

all: Enables NAT ALG for all supported protocols.

dns: Enables NAT ALG for DNS.

ftp: Enables NAT ALG for FTP.

h323: Enables NAT ALG for H.323.

icmp-error: Enables NAT ALG for ICMP error packets.

ils: Enables NAT ALG for ILS.

mgcp: Enables NAT ALG for MGCP.

nbt: Enables NAT ALG for NBT.

pptp: Enables NAT ALG for PPTP.

rsh: Enables NAT ALG for RSH.

rtsp: Enables NAT ALG for RTSP.

sccp: Enables NAT ALG for SCCP.

sctp: Enables NAT ALG for SCTP.

sip: Enables NAT ALG for SIP.

sqlnet: Enables NAT ALG for SQLNET.

tftp: Enables NAT ALG for TFTP.

xdmcp: Enables NAT ALG for XDMCP.

Usage guidelines

NAT ALG translates address or port information in the application layer payload to ensure connection establishment.

For example, an FTP application includes a data connection and a control connection. The IP address and port number for the data connection depend on the payload information of the control connection. This requires NAT ALG to translate the address and port information to establish the data connection.

Examples

Enable NAT ALG for FTP.

```
<Sysname> system-view
[Sysname] nat alg ftp
```

Related commands

display nat all

nat configuration-for-new-connection

Use **nat configuration-for-new-connection enable** to enable NAT configuration changes to take effect only on new connections.

Use **undo configuration-for-new-connection enable** to disable NAT configuration changes from taking effect only on new connections.

Syntax

nat configuration-for-new-connection enable

undo nat configuration-for-new-connection enable

Default

NAT configuration change taking effect only on new connections is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

Non-default vSystems do not support this command.

By default, NAT configuration changes (such as adding, deleting, editing, or moving NAT rules) might cause traffic on an established connection to match a new NAT rule. As a result, you must create a new connection.

Execute this command if you do not want the NAT configuration change to affect existing connections. After you execute this command on the device, it still performs address translation according to the NAT rules before the configuration change for traffic on existing connections. For traffic on new connections, the device matches the traffic according to the priority of NAT rules after the configuration change and performs address translation based on the matching NAT rules.

Examples

Enable NAT configuration change to take effect only on new connections.

```
<Sysname> system-view
[Sysname] nat configuration-for-new-connection enable
```

Related commands

display nat all

nat dns-map

Use **nat dns-map** to configure a NAT DNS mapping.

Use **undo nat dns-map** to remove a NAT DNS mapping.

Syntax

nat dns-map domain *domain-name* **protocol** *pro-type* { **interface** *interface-type interface-number* | **ip** *global-ip* } **port** *global-port*

undo nat dns-map domain *domain-name*

Default

No NAT DNS mappings exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

domain *domain-name*: Specifies the domain name of an internal server. A domain name is a dot-separated case-insensitive string that can include letters, digits, hyphens (-), underscores (_), and dots (.) (for example, aabbcc.com). The domain name can contain a maximum of 253 characters, and each separated string contains no more than 63 characters.

protocol *pro*-type: Specifies the type of the protocol used by the internal server, **tcp** or **udp**.

ip *global-ip*: Specifies the public IP address used by the internal server to provide services for the external network.

port *global-port*: Specifies the public port number used by the internal server to provide services for the external network. The port number format can be one of the following:

- A number in the range of 1 to 65535.
- A protocol name, a string of 1 to 15 characters. For example, **ftp** and **telnet**.

Usage guidelines

NAT DNS mapping must cooperate with the NAT Server feature.

- A NAT DNS mapping maps the domain name of an internal server to the public IP address, public port number, and protocol type of the internal server.
- A NAT server mapping maps the public IP and port to the private IP and port of the internal server.

The cooperation allows an internal host to access an internal server on the same private network by using the domain name of the internal server when the DNS server is on the public network. The DNS reply from the external DNS server contains only the domain name and public IP address of the internal server in the payload. The NAT interface might have multiple internal servers configured with the same public IP address but different private IP addresses. DNS ALG might find an incorrect internal server by using only the public IP address. If a DNS mapping is configured, DNS ALG can obtain the public IP address, public port number, and protocol type of the internal server by using the domain name. Then it can find the correct internal server by using the public IP address, public port number, and protocol type of the internal server.

You can configure multiple NAT DNS mappings.

Examples

Configure a NAT DNS mapping to map the domain name **www.server.com** to the public IP address **202.112.0.1**, public port number **12345**, and protocol type TCP.

```
<Sysname> system-view
[Sysname] nat dns-map domain www.server.com protocol tcp ip 202.112.0.1 port 12345
```

Related commands

display nat all

display nat dns-map

nat server

nat global-policy

Use **nat global-policy** to create the global NAT policy and enter its view, or enter the view of the existing global NAT policy.

Use **undo nat global-policy** to delete the global NAT policy and all the configuration in the global NAT policy.

Syntax

nat global-policy

undo nat global-policy

Default

No global NAT policy exists.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

The global NAT policy contains a set of NAT rules to identify and translate matching packets. The packet match criteria includes source IP address, destination IP address, service type, source security zone, and destination security zone. The global NAT policy supports translating the source IP address and destination IP address of the matching packets.

You do not need to apply the global NAT policy to any interface.

The global NAT policy has priority over interface-based NAT. If both are configured, the matching packets are translated as follows:

- If the global NAT policy contains only source address translation rules, the source address translation follows the NAT policy, and the destination address translation follows the interface-based rules.
- If the global NAT policy contains only destination address translation rules, the destination address translation follows the NAT policy, and the source address translation follows the interface-based rules.
- If the global NAT policy contains both source and destination address translation rules, both the source and destination address translations follow the NAT policy. The interface-based source and destination address translation rules do not take effect.

Examples

Create the global NAT policy and enter its view.

```
<Sysname> system-view
[Sysname] nat global-policy
[Sysname-nat-global-policy]
```

Related commands

display nat all

display nat global-policy

nat hairpin enable

Use **nat hairpin enable** to enable NAT hairpin.

Use **undo nat hairpin enable** to disable NAT hairpin.

Syntax

nat hairpin enable

undo nat hairpin enable

Default

NAT hairpin is disabled.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

NAT hairpin allows internal hosts to access each other or allows internal hosts to access internal servers. It must cooperate with NAT Server, outbound dynamic NAT, or outbound static NAT. The source and destination IP addresses of the packets are translated on the interface connected to the internal network.

When NAT hairpin works in conjunction with NAT Server, you must configure NAT server mappings in one of the following methods with a protocol type specified:

- Configuring common NAT server mappings
- Configuring load sharing NAT server mappings

Examples

Enable NAT hairpin on interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat hairpin enable
```

Related commands

display nat all

nat outbound

nat server

nat static outbound

nat icmp-error reply

Use **nat icmp-error reply** to enable sending ICMP error messages upon NAT failures.

Use **undo nat icmp-error reply** to restore the default.

Syntax

nat icmp-error reply

undo nat icmp-error reply

Default

No ICMP error messages are sent upon NAT failures.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

By default, sending ICMP error messages upon NAT failures is disabled on the NAT device. Applications using the ICMP protocol cannot be notified when an event occurs. With this feature enabled, the NAT device sends ICMP error messages upon NAT failures for the applications to locate and troubleshoot the failures.

Examples

Enable sending ICMP error messages upon NAT failures.

```
<Sysname> system-view
[Sysname] nat icmp-error reply
```

nat inbound

Use **nat inbound** to configure an inbound dynamic NAT rule.

Use **undo nat inbound** to delete an inbound dynamic NAT rule.

Syntax

nat inbound { *ipv4-acl-number* | **name** *ipv4-acl-name* } **address-group** { *group-id* | **name** *group-name* } [**vpn-instance** *vpn-instance-name*] [**no-pat** [**reversible**] [**add-route**]] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**counting**] [**description** *text*]

undo nat inbound { *ipv4-acl-number* | **name** *ipv4-acl-name* }

Default

No inbound dynamic NAT rules exist.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-acl-number: Specifies an ACL by its number in the range of 2000 to 3999.

name *ipv4-acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters. The ACL name must start with an English letter and to avoid confusion, it cannot be **all**.

address-group *group-id*: Specifies an address group for address translation.

group-id: Specifies the address group ID. The value range for this argument is 0 to 65535.

name *group-name*: Specifies the address group name, a case-insensitive string of 1 to 63 characters.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the addresses in the address group belong. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the addresses in the address group do not belong to any VPN instance, do not specify this option.

no-pat: Uses the NO-PAT mode. If you do not specify this keyword, PAT is used. PAT supports only TCP, UDP, and ICMP query packets. For an ICMP packet, the ICMP ID is used as its source port number.

reversible: Enables reverse address translation. Reverse address translation uses existing NO-PAT entries to translate the destination address for connections actively initiated from the internal network to the external network.

add-route: Automatically adds a route to the source address after translation. The output interface is the NAT interface and the next hop is the source address before translation.

rule *rule-name*: Specifies a name for the rule, a case-sensitive string of 1 to 63 characters. It cannot contain backward slashes (\), forward slashes (/), colons (:), asterisks (*), question marks (?), left angle brackets (<), right angle brackets (>), vertical bars (|), quotation marks ("), or at signs (@). If you do not specify this option, the rule does not have a name.

priority *priority*: Specifies a priority for the rule, in the range of 0 to 2147483647. The default value is 4294967295. A smaller value represents a higher priority. If you do not specify this option, the rule has the lowest priority among the same type of NAT rules.

disable: Disables the inbound dynamic NAT rule. If you do not specify this keyword, the rule is enabled.

counting: Enables NAT counting. The number of flows that use the address mapping is counted.

description *text*: Specifies a description for the inbound dynamic NAT rule. The *text* argument is a case-insensitive string of 1 to 63 characters.

Usage guidelines

Inbound dynamic NAT translates the source IP addresses of incoming packets permitted by the ACL into IP addresses in the address group.

Inbound dynamic NAT supports the following modes:

- **PAT**—Performs both IP address translation and port translation.
- **NO-PAT**—Performs only IP address translation.

The NO-PAT mode supports reverse address translation. Reverse address translation uses ACL reverse matching to identify packets to be translated. ACL reverse matching works as follows:

- Compares the source IP address/port of a packet with the destination IP addresses/ports in the ACL.
- Translates the destination IP address of the packet according to the matching NO-PAT entry, and then compares the translated destination IP address/port with the source IP addresses/ports in the ACL.

Inbound dynamic NAT typically cooperates with one of the following to implement bidirectional NAT:

- Outbound dynamic NAT (the **nat outbound** command).
- NAT Server (the **nat server** command).
- Outbound static NAT (the **nat static** command).

An address group cannot be used by both the **nat inbound** and **nat outbound** commands. It cannot be used by the **nat inbound** command in both PAT and NO-PAT modes.

Do not specify the **add-route** keyword if the subnets where the internal and external networks reside overlap. For other network scenarios:

- If you specify the **add-route** keyword, the device automatically adds a route to the source address after translation for a packet. The destination address is the NAT address in the NAT address group, the output interface is the interface where the command is executed, and the next hop is the source address before translation.
- If you do not specify the **add-route** keyword, you must manually add the route. As a best practice, add routes manually because automatic route adding is slow.

An ACL can be used by only one inbound dynamic NAT rule on an interface.

You can configure multiple inbound dynamic NAT rules on an interface.

The **vpn-instance** parameter is required if you deploy inbound dynamic NAT for VPNs. The specified VPN instance must be the VPN instance to which the NAT interface belongs.

Inbound dynamic NAT rules configured with the same priority value are matched by using their ACLs.

- NAT rules with named ACLs have higher priorities than NAT rules with unnamed ACLs.
- NAT rules with named ACLs are matched in alphabetical order of their ACL names.
- NAT rules with unnamed ACLs are matched in descending order of their ACL numbers.

Examples

Configure ACL 2001 to permit packets only from subnet 10.110.10.0/24 in VPN **vpn10** to pass through.

```
<Sysname> system-view
[Sysname] acl basic 2001
```

```
[Sysname-acl-ipv4-basic-2001] rule permit vpn-instance vpn10 source 10.110.10.0 0.0.0.255
[Sysname-acl-ipv4-basic-2001] rule deny
[Sysname-acl-ipv4-basic-2001] quit
```

Configure the MPLS L3VPN instance named **vpn10**.

```
[Sysname] ip vpn-instance vpn10
[Sysname-vpn-instance-vpn10] route-distinguisher 100:001
[Sysname-vpn-instance-vpn10] vpn-target 100:1 export-extcommunity
[Sysname-vpn-instance-vpn10] vpn-target 100:1 import-extcommunity
[Sysname-vpn-instance-vpn10] quit
```

Create address group 1 and add the address range of 202.110.10.10 to 202.110.10.12 to the group.

```
[Sysname] nat address-group 1
[Sysname-address-group-1] address 202.110.10.10 202.110.10.12
[Sysname-address-group-1] quit
```

Configure an inbound NO-PAT rule on interface GigabitEthernet 1/0/1. NAT translates the source addresses of incoming packets into the addresses in address group 1, and automatically adds routes for translated packets. Set the rule name to **abc**, and the priority to 0.

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat inbound 2001 address-group 1 vpn-instance vpn10 no-pat
add-route rule abc priority 0
```

Related commands

display nat all

display nat inbound

display nat no-pat

nat inbound rule move

Use **nat inbound rule move** to change the priority of an inbound dynamic NAT rule.

Syntax

nat inbound rule move *nat-rule-name1* { **after** | **before** } *nat-rule-name2*

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

nat-rule-name1: Specifies the name of the rule be moved.

after: Moves the rule *nat-rule-name1* to the line after the rule *nat-rule-name2* (called the reference rule). The priority value of the reference rule is not changed. The priority value of the moved rule equals the priority value of the reference rule plus one.

before: Moves the rule *nat-rule-name1* to the line before the rule *nat-rule-name2*. The priority value of the reference rule is not changed. The priority value of the moved rule equals the priority value of the reference rule minus one.

nat-rule-name2: Specifies the name of the NAT rule as a reference rule for the NAT rule to be moved.

Usage guidelines

This command is applicable only to named inbound dynamic NAT rules.

A NAT rule appearing earlier on the rule list has a higher priority for packet matching.

Examples

Move the inbound dynamic NAT rule **abc** to the line before the rule **def**.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat inbound rule move abc before def
```

Related commands

nat inbound

nat link-switch recreate-session

Use **nat link-switch recreate-session** to enable NAT session recreation after link switchover.

Use **undo nat link-switch recreate-session** to disable NAT session recreation after link switchover.

Syntax

nat link-switch recreate-session

undo nat link-switch recreate-session

Default

NAT session recreation is disabled after link switchover.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command is applicable to a WAN network where two interfaces of the NAT device are configured with outbound dynamic NAT rules using different address groups. When the link of one interface fails, traffic on this link is switched to the link of another interface and the NAT device operates as follows:

- If the two interfaces are in different security zones, the NAT device deletes old session entries after link switchover. When user traffic later arrives, it triggers the NAT session recreation. This mechanism ensures that internal users can access the external network.
- If the two interfaces are in the same security zone, the NAT device retains old session entries after link switchover. Internal users cannot access the external network because the device uses old session entries to match the user traffic. To avoid this issue, enable this feature to ensure availability of NAT services.

Examples

Enable NAT session recreation after link switchover.

```
<Sysname> system-view
[Sysname] nat link-switch recreate-session
```

Related commands

display nat all

nat log alarm

Use **nat log alarm** to enable NAT alarm logging.

Use **undo nat log alarm** to disable NAT alarm logging.

Syntax

nat log alarm

undo nat log alarm

Default

NAT alarm logging is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

Packets that need to be translated are dropped if the NAT resources are not enough. In NO-PAT, the NAT resources refer to the public IP addresses. In EIM PAT, the NAT resources refer to public IP addresses and ports. In NAT444, the NAT resources refer to public IP addresses, port blocks, or ports in port blocks. NAT alarm logging monitors the usage of NAT resources and outputs logs if the NAT resources are not enough.

For NAT444 dynamic port block mappings, an alarm log is generated upon the port block assignment failure or the failure that port resources cannot meet the user address translation requirement.

Before configuring alarm logging for NAT, you must configure the custom NAT log generation and outputting features. For more information about information center, see *Network Management and Monitoring Configuration Guide*.

This command take effect only after you use the **nat log enable** command to enable NAT logging.

Examples

Enable NAT alarm logging.

```
<Sysname> system-view
[Sysname] nat log alarm
```

Related commands

display nat all

display nat log

nat log enable

nat log enable

Use **nat log enable** to enable NAT logging.

Use **undo nat log enable** to disable NAT logging.

Syntax

nat log enable [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }]

undo nat log enable

Default

NAT logging is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

acl: Specifies an ACL.

ipv4-acl-number: Specifies an ACL by its number in the range of 2000 to 3999.

name *ipv4-acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters. The ACL name must start with an English letter and to avoid confusion, it cannot be **all**.

Usage guidelines

You must enable NAT logging before you enable NAT session logging, NAT444 user logging (including port block assignment and withdrawal logging), NAT alarm logging, or NAT NO-PAT logging.

The **acl** keyword takes effect only for NAT session logging. If an ACL is specified, flows matching the permit rule might trigger NAT session logs. If you do not specify an ACL, all flows processed by NAT might trigger NAT session logs.

Examples

Enable NAT logging.

```
<Sysname> system-view
[Sysname] nat log enable
```

Related commands

display nat all

display nat log

nat log alarm

nat log flow-active

nat log flow-begin

nat log flow-end

nat log no-pat ip-usage

- **nat log port-block-assign**
- **nat log port-block-withdraw**

nat log flow-active

Use **nat log flow-active** to enable logging for active NAT flows and set the logging interval.

Use **undo nat log flow-active** to disable logging for active NAT flows.

Syntax

nat log flow-active *time-value*

undo nat log flow-active

Default

Logging for active NAT flows is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

time-value: Specifies the interval for logging active NAT flows, in the range of 10 to 120 minutes.

Usage guidelines

Active NAT flows are NAT sessions that last for a long time. The logging feature helps track active NAT flows by periodically logging the active NAT flows.

Logging for active NAT flows takes effect only after you enable NAT logging.

Examples

Enable logging for active NAT flows and set the logging interval to 10 minutes.

```
<Sysname> system-view
[Sysname] nat log flow-active 10
```

Related commands

display nat all

display nat log

nat log enable

nat log flow-begin

Use **nat log flow-begin** to enable logging for NAT session establishment events.

Use **undo nat log flow-begin** to disable logging for NAT session establishment events.

Syntax

nat log flow-begin

undo nat log flow-begin

Default

Logging for NAT session establishment events is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

Logging for NAT session establishment events takes effect only after you enable NAT logging.

Examples

Enable logging for NAT session establishment events.

```
<Sysname> system-view
[Sysname] nat log flow-begin
```

Related commands

display nat all

display nat log

nat log enable

nat log flow-end

Use **nat log flow-end** to enable logging for NAT session removal events.

Use **undo nat log flow-end** to disable logging for NAT session removal events.

Syntax

nat log flow-end

undo nat log flow-end

Default

Logging for NAT session removal events is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

Logging for NAT session removal events takes effect only after you enable NAT logging.

Examples

Enable logging for NAT session removal events.

```
<Sysname> system-view
[Sysname] nat log flow-end
```

Related commands

display nat all

display nat log

nat log enable

nat log no-pat ip-usage

Use **nat log no-pat ip-usage** to enable logging for the IP usage of a NAT address group in NO-PAT mode and set a usage threshold.

undo nat log no-pat ip-usage disable logging for the IP usage of a NAT address group in NO-PAT mode.

Syntax

nat log no-pat ip-usage [**threshold** *value*]

undo nat log no-pat ip-usage

Default

Logging for the IP usage of a NAT address group is disabled.

Views

System view

Predefines user roles

network-admin

context-admin

Parameters

threshold *value*: Specifies the IP usage threshold of a NAT address group, in percentage. The value range is 40 to 100, and the default is 90%.

Usage guidelines

The system generates a log if the IP usage of a NAT address group exceeds the threshold.

This command takes effect only after you enable the NAT logging by using the **nat log enable** command.

Examples

Enable logging for the IP usage of a NAT address group in NO-PAT mode and set the threshold to 60%.

```
<Sysname> system-view
[Sysname] nat log no-pat ip-usage threshold 60
```

Related commands

display nat log

display nat no-pat ip-usage

nat log enable

nat log port-block usage threshold

Use **nat log port-block usage threshold** to set the port block usage threshold.

Use **undo nat log port-block port-usage threshold** to restore the default.

Syntax

nat log port-block usage threshold *threshold-value*

undo nat log port-block usage threshold

Default

The port block usage threshold is 90%.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

threshold-value: Specifies a threshold in the range of 40 to 100 in percentage.

Usage guidelines

A log is generated when the port block usage exceeds the threshold.

Examples

Set the port block usage threshold to 60%.

```
<Sysname> system-view
[Sysname] nat log port-block usage threshold 60
```

Related commands

display nat all

display nat log

nat log enable

nat log port-block-assign

Use **nat log port-block-assign** to enable NAT444 user logging for port block assignment.

Use **undo nat log port-block-assign** to disable NAT444 user logging for port block assignment.

Syntax

nat log port-block-assign

undo nat log port-block-assign

Default

NAT444 user logging is disabled for port block assignment.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

For static port block mappings, the NAT444 gateway generates a user log when it translates the first connection from a private IP address.

For dynamic port block mappings, the NAT444 gateway generates a user log when it assigns or extends a port block for a private IP address.

This command takes effect only after you use the **nat log enable** command to enable NAT logging.

Examples

Enable NAT444 user logging for port block assignment.

```
<Sysname> system-view
```

```
[Sysname] nat log port-block-assign
```

Related commands

display nat all

display nat log

nat log enable

nat log port-block-withdraw

Use **nat log port-block-withdraw** to enable NAT444 user logging for port block withdrawal.

Use **undo nat log port-block-withdraw** to disable NAT444 user logging for port block withdrawal.

Syntax

nat log port-block-withdraw

undo nat log port-block-withdraw

Default

NAT444 user logging is disabled for port block withdrawal.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

For static port block mappings, the NAT444 gateway generates a user log when all connections from a private IP address are disconnected.

For dynamic port block mappings, the NAT444 gateway generates a user log when all the following conditions are met:

- The port blocks (including the extended ones) assigned to the private IP address are withdrawn.
- The corresponding mapping entry is deleted.

This command takes effect only after you use the **nat log enable** command to enable NAT logging.

Examples

Enable NAT444 user logging for port block withdrawal.

```
<Sysname> system-view
[Sysname] nat log port-block-withdraw
```

Related commands

display nat all

display nat log

nat log enable

nat mapping-behavior endpoint-independent

Use **nat mapping-behavior endpoint-independent** to specify the Endpoint-Independent Mapping (EIM) mode for PAT.

Use **undo nat mapping-behavior** to restore the default.

Syntax

nat mapping-behavior endpoint-independent [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }]

undo nat mapping-behavior endpoint-independent

Default

Address and Port-Dependent Mapping applies.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

acl: Specifies an ACL to define the applicable scope of Endpoint-Independent Mapping.

ipv4-acl-number: Specifies an ACL by its number in the range of 2000 to 3999.

name *ipv4-acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters. The ACL name must start with an English letter and to avoid confusion, it cannot be **all**.

Usage guidelines

PAT supports the following NAT mapping modes:

- **Endpoint-Independent Mapping**—Uses the same IP and port mapping (EIM entry) for packets from the same source and port to any destination. EIM allows external hosts to access the internal hosts by using the NAT IP address and port. It allows internal hosts behind different NAT gateways to access each other.
- **Address and Port-Dependent Mapping**—Uses different IP and port mappings for packets with the same source IP and port to different destination IP addresses and ports. APDM allows an external host to access an internal host only under the condition that the internal host has previously accessed the external host. It is secure, but it does not allow internal hosts behind different NAT gateways to access each other.

This command takes effect only on outbound PAT. Address and Port-Dependent Mapping always applies to inbound PAT.

If you specify an ACL, Endpoint-Independent Mapping applies to packets that are permitted by the ACL. If you do not specify an ACL, Endpoint-Independent Mapping applies to all packets.

Examples

Apply the Endpoint-Independent Mapping mode to all packets for address translation.

```
<Sysname> system-view
[Sysname] nat mapping-behavior endpoint-independent
```

Apply the Endpoint-Independent Mapping mode to FTP and HTTP packets, and the Address and Port-Dependent Mapping mode to other packets for address translation.

```
<Sysname> system-view
[Sysname] acl advanced 3000
```

```
[Sysname-acl-ipv4-adv-3000] rule permit tcp destination-port eq 80
[Sysname-acl-ipv4-adv-3000] rule permit tcp destination-port eq 21
[Sysname-acl-ipv4-adv-3000] quit
[Sysname] nat mapping-behavior endpoint-independent acl 3000
```

Related commands

nat outbound

display nat eim

nat outbound

Use **nat outbound** to configure an outbound dynamic NAT rule.

Use **undo nat outbound** to delete an outbound dynamic NAT rule.

Syntax

NO-PAT:

nat outbound [*ipv4-acl-number* | **name** *ipv4-acl-name*] **address-group** { *group-id* | **name** *group-name* } [**vpn-instance** *vpn-instance-name*] **no-pat** [**reversible**] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**counting**] [**description** *text*]

undo nat outbound [*ipv4-acl-number* | **name** *ipv4-acl-name*]

PAT:

nat outbound [*ipv4-acl-number* | **name** *ipv4-acl-name*] [**address-group** { *group-id* | **name** *group-name* }] [**vpn-instance** *vpn-instance-name*] [**port-preserved**] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**counting**] [**description** *text*]

undo nat outbound [*ipv4-acl-number* | **name** *ipv4-acl-name*]

Default

No outbound dynamic NAT rules exist.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-acl-number: Specifies an ACL by its number in the range of 2000 to 3999.

name *ipv4-acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters. The ACL name must start with an English letter and to avoid confusion, it cannot be **all**.

address-group: Specifies an address group for NAT. If you do not specify an address group, the IP address of the interface is used as the NAT address. Easy IP is used.

group-id: Specifies the address group ID. The value range for this argument is 0 to 65535.

name *group-name*: Specifies the address group name, a case-insensitive string of 1 to 63 characters.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the addresses in the address group belong. The *vpn-instance-name* argument is a case-sensitive

string of 1 to 31 characters. If the addresses in the address group do not belong to any VPN instance, do not specify this option.

no-pat: Uses the NO-PAT mode. If you do not specify this keyword, PAT is used. PAT only supports TCP, UDP, and ICMP query packets. For an ICMP packet, the ICMP ID is used as its source port number.

reversible: Enables reverse address translation. Reverse address translation uses existing NO-PAT entries to translate the destination address for connections actively initiated from the external network to the internal network.

port-preserved: Tries to preserve port number for PAT. This keyword does not take effect on dynamic NAT port block mapping.

rule *rule-name*: Specifies a name for the rule, a case-sensitive string of 1 to 63 characters. It cannot contain backward slashes (\), forward slashes (/), colons (:), asterisks (*), question marks (?), left angle brackets (<), right angle brackets (>), vertical bars (|), quotation marks ("), or at signs (@). If you do not specify this option, the rule does not have a name.

priority *priority*: Specifies a priority for the rule, in the range of 0 to 2147483647. The default value is 4294967295. A smaller value represents a higher priority. If you do not specify this option, the rule has the lowest priority among the same type of NAT rules.

disable: Disables the outbound dynamic NAT rule. If you do not specify this keyword, the rule is enabled.

counting: Enables NAT counting. The number of flows that use the address mapping is counted.

description *text*: Specifies a description for the outbound dynamic NAT rule. The *text* argument is a case-insensitive string of 1 to 63 characters.

Usage guidelines

Outbound dynamic NAT is typically configured on the interface connected to the external network. You can configure multiple outbound dynamic NAT rules on an interface.

Outbound dynamic NAT supports the following modes:

- **PAT**—Performs both IP address translation and port translation. The PAT mode allows external hosts to actively access the internal hosts if the Endpoint-Independent Mapping behavior is used.
- **NO-PAT**—Performs only IP address translation. The NO-PAT mode allows external hosts to actively access the internal hosts if you specify the **reversible** keyword. If an ACL is specified, reverse address translation only applies to packets permitted by ACL reverse matching. ACL reverse matching works as follows:
  - Compares the source IP address/port of a packet with the destination IP addresses/ports in the ACL.
  - Translates the destination IP address of the packet according to the matching NO-PAT entry, and then compares the translated destination IP address/port with the source IP addresses/ports in the ACL.

  Dynamic NAT444 does not support the NO-PAT mode.

When you specify a NAT address group, follow these restrictions and guidelines:

- An address group cannot be used by both the **nat inbound** and **nat outbound** commands.
- An address group cannot be used by the **nat outbound** command in both PAT and NO-PAT modes.
- When port block parameters are specified in the NAT address group, this command configures a dynamic NAT port block mapping. Packets matching the ACL permit rule are processed by dynamic NAT444.

When you specify an ACL, follow these restrictions and guidelines:

- An ACL can be used by only one outbound dynamic NAT rule on an interface.

- If you configure multiple outbound dynamic NAT rules, only one outbound dynamic NAT rule can contain no ACL.
- If you specify an ACL, NAT translates the source IP addresses of outgoing packets permitted by the ACL into IP addresses in the address group. If you do not specify an ACL, NAT translates all packets.
- Outbound dynamic NAT rules with ACLs configured on an interface takes precedence over those without ACLs. If two ACL-based dynamic NAT rules are configured, the rule with the higher ACL number has higher priority.

The **vpn-instance** parameter is required if you deploy outbound dynamic NAT for VPNs. The specified VPN instance must be the VPN instance to which the NAT interface belongs.

Outbound dynamic NAT rules configured with the same priority value and an ACL are matched by using the ACLs in the rule.

- NAT rules with named ACLs have higher priorities than NAT rules with unnamed ACLs.
- NAT rules with named ACLs are matched in alphabetical order of their ACL names.
- NAT rules with unnamed ACLs are matched in descending order of their ACL numbers.

Examples

Configure ACL 2001 to permit packets only from subnet 10.110.10.0/24 to pass through.

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 10.110.10.0 0.0.0.255
[Sysname-acl-ipv4-basic-2001] rule deny
[Sysname-acl-ipv4-basic-2001] quit
```

Create address group 1 and add the address range of 202.110.10.10 to 202.110.10.12 to the group.

```
[Sysname] nat address-group 1
[Sysname-address-group-1] address 202.110.10.10 202.110.10.12
[Sysname-address-group-1] quit
```

Configure an outbound dynamic PAT rule on interface GigabitEthernet 1/0/1 to translate the source addresses of outgoing packets permitted by ACL 2001 into the addresses in address group 1.

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat outbound 2001 address-group 1
[Sysname-GigabitEthernet1/0/1] quit
```

Or

Configure an outbound NO-PAT rule on interface GigabitEthernet 1/0/1 to translate the source addresses of outgoing packets permitted by ACL 2001 into the addresses in address group 1.

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat outbound 2001 address-group 1 no-pat
[Sysname-GigabitEthernet1/0/1] quit
```

Or

Enable Easy IP to use the IP address of GigabitEthernet 1/0/1 as the NAT address.

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet 1/0/1] nat outbound 2001
[Sysname-GigabitEthernet 1/0/1] quit
```

Or

Configure an outbound NO-PAT rule on GigabitEthernet 1/0/1 to translate the source addresses of outgoing packets permitted by ACL 2001 into the addresses in address group 1. Enable reverse address translation.

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat outbound 2001 address-group 1 no-pat reversible
```

Related commands

display nat eim

display nat outbound

nat mapping-behavior

nat outbound ds-lite-b4

Use **nat outbound ds-lite-b4** to configure DS-Lite B4 address translation.

Use **undo nat outbound ds-lite-b4** to remove the DS-Lite B4 address translation configuration.

Syntax

nat outbound ds-lite-b4 { *ipv6-acl-number* | **name** *ipv6-acl-name* } **address-group** *group-id*

undo nat outbound ds-lite-b4 { *ipv6-acl-number* | **name** *ipv6-acl-name* }

Default

No DS-Lite B4 address translation configuration exists.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-acl-number: Specifies the number of an IPv6 ACL to match the IPv6 addresses of B4 elements. The value range for the argument is 2000 to 2999.

name *ipv6-acl-name*: Specifies the name of an IPv6 ACL to match the IPv6 addresses of B4 elements. The ACL name is a case-insensitive string of 1 to 63 characters. It must start with an English letter and to avoid confusion, it cannot be **all**.

address-group *group-id*: Specifies an address group by its ID. The value range for the *group-id* argument is 0 to 65535. Port block parameters are required in the address group for DS-Lite B4 address translation.

Usage guidelines

DS-Lite B4 address translation applies to the scenario where a DS-Lite tunnel connects an IPv6 network to an IPv4 network. DS-Lite port block mapping is configured on the AFTR's interface connected to the external IPv4 network and performs dynamic port block mapping based on the B4 element. The B4 element refers to a B4 router or a DS-Lite host.

DS-Lite B4 address translation dynamically maps a public IPv4 address and a port block to the IPv6 address of the B4 element. The DS-Lite host or hosts behind the B4 router use the mapped public IPv4 address and port block to access the public IPv4 network.

Examples

Configure IPv6 ACL 2100 to identify packets from subnet 2000::/64.

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2100
```

```
[Sysname-acl-ipv6-basic-2100] rule permit source 2000::/64
[Sysname-acl-ipv6-basic-2100] quit
```

Create address group 1 and add public addresses 202.110.10.10 through 202.110.10.12 to the group.

```
[Sysname] nat address-group 1
[Sysname-nat-address-group-1] address 202.110.10.10 202.110.10.12
```

Set the port block size to 256.

```
[Sysname-nat-address-group-1] port-block block-size 256
[Sysname-nat-address-group-1] quit
```

Configure DS-Lite port block mapping on GigabitEthernet 1/0/1 to use address group 1 to translate packets permitted by ACL 2100.

```
 [Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat outbound ds-lite-b4 2100 address-group 1
```

Related commands

display nat outbound

nat outbound port-block-group

Use **nat outbound port-block-group** to configure a static outbound port block mapping rule on an interface.

Use **undo nat outbound port-block-group** to delete a static port block mapping rule on an interface.

Syntax

nat outbound port-block-group *group-id* [**rule** *rule-name*] [**counting**]

undo nat outbound port-block-group *group-id*

Default

No static outbound port block mapping rule is configured on an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

group-id: Specifies a NAT port block group by its ID. The value range for this argument is 0 to 65535.

rule *rule-name*: Specifies a name for the rule, a case-sensitive string of 1 to 63 characters. It cannot contain backward slashes (\), forward slashes (/), colons (:), asterisks (*), question marks (?), left angle brackets (<), right angle brackets (>), vertical bars (|), quotation marks ("), or at signs (@). If you do not specify this option, the rule does not have a name.

counting: Enables NAT counting. The number of flows that use the address mapping is counted.

Usage guidelines

After you configure this command on an interface, the system automatically computes the mappings and creates entries for them. When a private IP address accesses the public network, the private IP

address is translated to the mapped public IP address, and the ports are translated to ports in the selected port block.

You can configure multiple port block mapping rules on an interface.

In an IRF fabric, you must execute the **ip fast-forwarding load-sharing** command. Otherwise, the port assignment conflict will occur.

Examples

Configure a static outbound port block mapping rule on GigabitEthernet 1/0/1, and specify the rule name as **abc**.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat outbound port-block-group 1 rule abc
```

Related commands

display nat all

display nat outbound port-block-group

display nat port-block

nat port-block-group

nat outbound rule move

Use **nat outbound rule move** to change the priority of an outbound dynamic NAT rule.

Syntax

nat outbound rule move *nat-rule-name1* { **after** | **before** } *nat-rule-name2*

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

nat-rule-name1: Specifies the name of the NAT rule to be moved.

after: Moves the rule *nat-rule-name1* to the line after the rule *nat-rule-name2* (called the reference rule). The priority value of the reference rule is not changed. The priority value of the moved rule equals the priority value of the reference rule plus one.

before: Moves the rule *nat-rule-name1* to the line before the rule *nat-rule-name2*. The priority value of the reference rule is not changed. The priority value of the moved rule equals the priority value of the reference rule minus one.

nat-rule-name2: Specifies the name of the NAT rule as a reference rule for the NAT rule to be moved.

Usage guidelines

This command is applicable only to named outbound dynamic NAT rules.

A NAT rule appearing earlier on the rule list has a higher priority for packet matching.

Examples

Move the outbound dynamic NAT rule **abc** to the line before the rule **def**.

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat outbound rule move abc before def
```

Related commands

nat outbound

nat periodic-statistics enable

Use **nat periodic-statistics enable** to enable periodic NAT statistics collection.

Use **undo nat periodic-statistics enable** to disable periodic NAT statistics collection.

Syntax

nat periodic-statistics enable

undo nat periodic-statistics enable

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280	No
NFNX5-HD6480, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	Yes

Default

Periodic NAT statistics collection is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This feature periodically counts sessions and port block assignment failures for address groups.

This feature might cause intensive CPU usage. You can disable this feature when CPU resources are insufficient.

Examples

Enable periodic NAT statistics collection.

```
<Sysname> system-view
[Sysname] nat periodic-statistics enable
```

Related commands

nat periodic-statistics interval

nat periodic-statistics interval

Use **nat periodic-statistics interval** to set the interval for periodic NAT statistics collection.

Use **undo nat periodic-statistics interval** to restore the default.

Syntax

nat periodic-statistics interval *interval*

undo nat periodic-statistics interval

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280	No
NFNX5-HD6480, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	Yes

Default

The interval for periodic NAT statistics collection is 300 seconds.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies the interval for collecting periodic NAT statistics. The value range is 180 to 604800 seconds.

Usage guidelines

A narrower interval indicates intensive CPU usage. As a best practice, use the default interval value.

Examples

Set the interval for periodic NAT statistics collection to 500 seconds.

```
<Sysname> system-view
[Sysname] nat periodic-statistics interval 500
```

Related commands

nat periodic-statistics enable

nat policy

Use **nat policy** to create a NAT policy and enter its view, or enter the view of an existing NAT policy.

Use **undo nat policy** to delete the NAT policy and all the configuration in the NAT policy.

Syntax

nat policy

undo nat policy

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	No

Default

No NAT policy exists.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

The NAT policy performs address translation for outgoing packets on the interfaces that the rules are applied. The NAT policy contains a set of NAT rules. The device identifies the packets based on the object groups in the NAT rules, and translates addresses according to the method in the matching rule.

The NAT policy supports only dynamic address translation, and the NAT policy has a higher priority than the dynamic address translation configuration on the interface.

Examples

Create a NAT policy and enter its view.

```
<Sysname> system
[Sysname] nat policy
[Sysname-nat-policy]
```

Related commands

`display nat all`

`display nat policy`

`rule name`

nat port-block global-share enable

Use **`nat port-block global-share enable`** to enable port block global sharing.

Use **`undo nat port-block global-share enable`** to disable port block global sharing.

Syntax

`nat port-block global-share enable`

`undo nat port-block global-share enable`

Default

Port block global sharing is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

When multiple interfaces have dynamic NAT port block mapping configured, the interfaces might create different port block mappings for packets from the same IP address. You can use this command to configure the interfaces to use the same port block mapping for translating packets from the same IP address.

Examples

Enable port block global sharing.

```
<Sysname> system-view
[Sysname] nat port-block global-share enable
```

Related commands

port-block

nat port-block synchronization enable

Use **nat port-block synchronization enable** to enable dynamic NAT port block mapping synchronization.

Use **undo nat port-block synchronization enable** to disable dynamic NAT port block mapping synchronization.

Syntax

nat port-block synchronization enable

undo nat port-block synchronization enable

Default

Dynamic NAT port block mapping synchronization is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

Dynamic NAT port block mapping synchronization enables the master and the backup to synchronize dynamic port block mappings, which ensures smooth switchover without service interruption.

Examples

Enable dynamic NAT port block mapping synchronization.

```
<Sysname> system-view
[Sysname] nat port-block synchronization enable
```

nat port-block-group

Use **nat port-block-group** to create a NAT port block group and enter its view, or enter the view of an existing NAT port block group.

Use **undo nat port-block-group** to delete a NAT port block group.

Syntax

nat port-block-group *group-id*

undo nat port-block-group *group-id*

Default

No NAT port block groups exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

group-id: Assigns an ID to the NAT port block group. The value range for this argument is 0 to 65535.

Usage guidelines

A NAT port block group is configured to implement static port block mapping for NAT444.

You must configure the following items for a NAT port block group:

- A minimum of one private IP address range (see the **local-ip-address** command).
- A minimum of one public IP address range (see the **global-ip-address** command).
- A port range (see the **port-range** command).
- A port block size (see the **block-size** command).

The system computes static port block mappings according to the port block group configuration, and creates entries for the mappings.

Examples

Create NAT port block group **1**.

```
<Sysname>system-view
[Sysname]nat port-block-group 1
[Sysname-port-block-group-1]
```

Related commands

block-size

display nat all

display nat port-block-group

global-ip-pool

local-ip-address

nat outbound port-block-group

port-range

nat port-load-balance enable

Use **nat port-load-balance enable** to enable NAT port halving.

Use **undo nat port-load-balance enable** to disable NAT port halving.

Syntax

nat port-load-balance enable slot *slot-number*

undo nat port-load-balance enable slot *slot-number*

Default

NAT port halving is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. This device will use the lower half portion of the port block.

Usage guidelines

After you enable NAT port halving in VRRP load balancing on an IRF fabric, each port block will be equally divided between the two devices. The two devices will use different ports to translate packets from the same IP address, avoiding port assignment conflicts.

Before enabling this feature, for successfully port allocation, make sure the address group meets the following requirements:

- For dynamic outbound NAT, the number of ports for the public IP addresses in the address group must not less than 2.
- For dynamic NAT444, the number of port blocks and ports for public IP addresses in the address group must not less than 2.

Do not use this feature in VRRP standard mode.

Examples

Enable NAT port halving.

```
<Sysname> system
[Sysname] nat port-load-balance enable slot 1
```

Related commands

nat port-block synchronization enable

port-block

port-range

nat redirect reply-route

Use **nat redirect reply-route enable** to enable NAT reply redirection.

Use **undo nat redirect reply-route enable** to disable NAT reply redirection.

Syntax

nat redirect reply-route enable

undo nat redirect reply-route enable

Default

NAT reply redirection is disabled.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

NAT reply redirection allows an interface to use the NAT session entry information to translate the destination IP addresses for NAT reply packets and find the output interfaces for the NATed reply packets.

Examples

Enable NAT reply redirection on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat redirect reply-route enable
```

nat remote-backup port-alloc

Use **nat remote-backup port-alloc** to specify NAT port ranges for the two devices in the hot backup system.

Use **undo nat remote-backup port-alloc** to restore the default.

Syntax

nat remote-backup port-alloc { **primary** | **secondary** }

undo nat remote-backup port-alloc

Default

The two devices in the hot backup system share NAT port resources.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

primary: Specifies the first half of the port range.

secondary: Specifies the second half of the port range.

Usage guidelines

For dual-active hot backup, different IP+port combinations on the two devices might be translated to the same NAT IP+port resources due to the following reasons:

- The two devices in the hot backup system share NAT addresses.
- The same NAT port range is assigned to each device.

To avoid this situation, execute this command on the primary device to equally divide the port resources for the two devices. Executing the command on the primary device also makes the remaining half of the port range be automatically assigned to the secondary device. For example, if you execute the **nat remote-backup port-alloc secondary** command on the primary device, the **nat remote-backup port-alloc primary** command is automatically executed on the secondary device. For more information about the hot backup system, see *High Availability Configuration Guide*.

You do not need to execute this command for active/standby hot backup. No port conflict exists in this mode because only one device processes NAT services.

Examples

Specify one device in the hot backup system to use the first half of the port range.

```
<Sysname> system-view
[Sysname] nat remote-backup port-alloc primary
```

nat server

Use **nat server** to create a NAT server mapping (also called NAT server rule). The mapping maps the private IP address and port of an internal server to a public address and port.

Use **undo nat server** to delete a NAT server mapping.

Syntax

Common NAT server mapping:

- A single public address with no or a single public port:

  nat server [**protocol** *pro-type*] **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* } [*global-port*] [**vpn-instance** *global-vpn-instance-name*] **inside** *local-address* [*local-port*] [**vpn-instance** *local-vpn-instance-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }] [**reversible**] [**vrrp** *virtual-router-id*] [**rule** *rule-name*] [**disable**] [**counting**] [**description** *text*]

  undo nat server [**protocol** *pro-type*] **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* } [*global-port*] [**vpn-instance** *global-vpn-instance-name*]

- A single public address with consecutive public ports:

  nat server protocol *pro-type* **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* } *global-port1 global-port2* [**vpn-instance** *global-vpn-instance-name*] **inside** { { *local-address* | *local-address1 local-address2* } *local-port* | *local-address local-port*1 *local-port*2 } [**vpn-instance** *local-vpn-instance-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }] [**vrrp** *virtual-router-id*] [**rule** *rule-name*] [**disable**] [**counting**] [**description** *text*]

  undo nat server protocol *pro-type* **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* } *global-port1 global-port2* [**vpn-instance** *global-vpn-instance-name*]

- Consecutive public addresses with no public port:

  nat server protocol *pro-type* **global** *global-address1 global-address2* [**vpn-instance** *global-vpn-instance-name*] **inside** { *local-address* |

local-address1 local-address2 } [*local-port*] [**vpn-instance** *local-vpn-instance-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }] [**vrrp** *virtual-router-id*] [**rule** *rule-name*] [**disable**] [**counting**] [**description** *text*]

undo nat server protocol *pro-type* **global** *global-address1 global-address2* [*global-port*] [**vpn-instance** *global-vpn-instance-name*]

- Consecutive public addresses with one single public port:

  nat server protocol *pro-type* **global** *global-address1 global-address2 global-port* [**vpn-instance** *global-vpn-instance-name*] **inside** { *local-address* [*local-port1 local-port2*] | [*local-address* | *local-address1 local-address2*] [*local-port*] } [**vpn-instance** *local-vpn-instance-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }] [**vrrp** *virtual-router-id*] [**rule** *rule-name*] [**disable**] [**counting**] [**description** *text*]

  undo nat server protocol *pro-type* **global** *global-address1 global-address2 global-port* [**vpn-instance** *global-vpn-instance-name*]

Load sharing NAT server mapping:

nat server protocol *pro-type* **global** { { *global-address* | **current-interface** | **interface** *interface-type interface-number* } { *global-port* | *global-port1 global-port2* } | *global-address1 global-address2 global-port* } [**vpn-instance** *global-vpn-instance-name*] **inside server-group** *group-id* [**vpn-instance** *local-vpn-instance-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }] [**vrrp** *virtual-router-id*] [**rule** *rule-name*] [**disable**] [**counting**] [**description** *text*]

undo nat server protocol *pro-type* **global** { { *global-address* | **current-interface** | **interface** *interface-type interface-number* } { *global-port* | *global-port1 global-port2* } | *global-address1 global-address2 global-port* } [**vpn-instance** *global-vpn-instance-name*]

ACL-based NAT server mapping:

nat server global { *ipv4-acl-number* | **name** *ipv4-acl-name* } **inside** *local-address* [*local-port*] [**vpn-instance** *local-vpn-instance-name*] [**vrrp** *virtual-router-id*] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**counting**] [**description** *text*]

undo nat server global { *ipv4-acl-number* | **name** *ipv4-acl-name* }

Default

No NAT server mappings exist.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

protocol *pro-type*: Specifies a protocol type. When the protocol is TCP or UDP, NAT Server can be configured with port information. If you do not specify a protocol type, the command applies to packets of all protocols. The protocol type format can be one of the following:

- A number in the range of 1 to 255.

- A protocol name of **icmp**, **tcp**, or **udp**.

global: Specifies the public network information about the internal server.

global-address: Specifies the public address of an internal server.

global-address1 global address2: Specifies a public IP address range, which can include a maximum of 10000 addresses. The *global-address1* argument specifies the start address, and the *global address2* argument specifies the end address that must be greater than the start address.

ipv4-acl-number: Specifies an ACL by its number in the range of 2000 to 3999.

name *ipv4-acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters. The ACL name must start with an English letter and to avoid confusion, it cannot be **all**.

current-interface: Enables Easy IP on the current interface. The primary IP address of the interface is used as the public address for the internal server.

interface *interface-type interface-number*: Enables Easy IP on the interface specified by its type and number. The primary IP address of the interface is used as the public address for the internal server. Only loopback interfaces are supported.

global-port1 global-port2: Specifies a public port number range, which can include a maximum of 10000 ports. The *global-port1* argument specifies the start port, and the *global-port2* argument specifies the end port that must be greater than the start port. The public port number format can be one of the following:

- A number in the range of 1 to 65535. Both the start port and the end port support this format.
- A protocol name, a string of 1 to 15 characters. For example, **http** and **telnet**. Only the start port supports this format.

inside: Specifies the private network information about the internal server.

local-address1 local-address2: Specifies a private IP address range. The *local-address1* argument specifies the start address, and the *local-address2* argument specifies the end address that must be greater than the start address. The number of addresses in the range must equal the number of ports in the public port number range.

local-port: Specifies the private port number. The private port number format can be one of the following:

- A number in the range of 1 to 65535, excluding FTP port 20.
- A protocol name, a string of 1 to 15 characters. For example, **http** and **telnet**.

global-port: Specifies the public port number. The default value and value range are the same as those for the *local-port* argument.

local-address: Specifies the private IP address.

vpn-instance *global-vpn-instance-name*: Specifies the MPLS L3VPN instance to which the advertised public IP addresses belong. The *global-vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the public IP addresses do not belong to any VPN instance, do not specify this option.

vpn-instance *local-vpn-instance-name*: Specifies the MPLS L3VPN instance to which the internal server belongs. The *local-vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the internal server does not belong to any VPN instance, do not specify this option.

server-group *group-id*: Specifies the internal server group to which the internal server belongs. With this parameter, the load sharing NAT Server feature is configured. The *group-id* argument specifies the internal server group ID. The value range for the *group-id* argument is 0 to 65535.

acl: Specifies an ACL. If you specify an ACL, only packets permitted by the ACL can be translated by using the mapping.

ipv4-acl-number: Specifies an ACL by its number in the range of 2000 to 3999.

name *ipv4-acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters. The ACL name must start with an English letter and to avoid confusion, it cannot be **all**.

reversible: Allows reverse address translation. Reverse address translation applies to connections actively initiated by internal servers to the external network. It translates the private IP addresses of the internal servers to their public IP addresses.

vrrp *virtual-router-id*: Specifies a VRRP group by its virtual router ID in the range of 1 to 255.

rule *rule-name*: Specifies a name for the mapping, a case-sensitive string of 1 to 63 characters. It cannot contain backward slashes (\), forward slashes (/), colons (:), asterisks (*), question marks (?), left angle brackets (<), right angle brackets (>), vertical bars (|), quotation marks ("), or at signs (@). If you do not specify this option, the mapping does not have a name.

priority *priority*: Specifies a priority for the mapping, in the range of 0 to 2147483647. The default value is 4294967295. A smaller value represents a higher priority. If you do not specify this option, the mapping has the lowest priority among the same type of NAT rules.

disable: Disables the NAT server mapping. If you do not specify this keyword, the mapping is enabled.

counting: Enables NAT counting. The number of flows that use the address mapping is counted.

description *text*: Specifies a description for the NAT server mapping. The *text* argument is a case-insensitive string of 1 to 63 characters.

Usage guidelines

You can configure the NAT server mapping to allow servers (such as Web, FTP, Telnet, POP3, and DNS servers) in the internal network or an MPLS VPN instance to provide services for external users.

NAT server mappings are usually configured on the interface connected to the external network on a NAT device. By using the *global-address* and *global-port* arguments, external users can access the internal server at *local-address* and *local-port*. When the protocol type is not **udp** (protocol number 17) or **tcp** (protocol number 6), you can configure only one-to-one IP address mappings. The following table describes the address-port mappings between an external network and an internal network for NAT Server.

Table 24 Address-port mappings for NAT Server

External network	Internal network
One public address	One private address
One public address and one public port number	One private address and one private port number
One public address and *N* consecutive public port numbers	• One private address and one private port number • *N* consecutive private addresses and one private port number • One private address and *N* consecutive private port numbers
N consecutive public addresses	• One private address • *N* consecutive private addresses

External network	Internal network
N consecutive public addresses and one public port number	• One private address and one private port number • *N* consecutive private addresses and one private port number • One private address and *N* consecutive private port numbers
One public address and one public port number	One internal server group
One public address and *N* consecutive public port numbers	
N consecutive public addresses and one public port number	
Public addresses matching an ACL	One private address
	One private address and one private port

The mapping of the protocol type, public address, and public port number must be unique for an internal server on an interface. This restriction also applies when Easy IP is used. The maximum number of NAT server mappings equals the number of public ports in the specified public port range.

The **vpn-instance** parameter is required if you configure NAT server mappings in VPN networks. The specified VPN instance must be the VPN instance to which the NAT interface belongs.

As a best practice, do not configure Easy IP for multiple NAT server mappings by using the same interface.

If the IP address of an interface used by Easy IP changes and conflicts with the IP address of a NAT server mapping not using Easy IP, the Easy IP configuration becomes invalid. If the conflicting IP address is modified to another IP address or the NAT server mapping without Easy IP is removed, the Easy IP configuration takes effect.

When you configure a load sharing NAT server mapping, you must make sure a user uses the same public address and public port to access the same service on an internal server. For this purpose, make sure value *N* in the following mappings is equal to or less than the number of servers in the internal server group:

- One public address and *N* consecutive public port numbers are mapped to one internal server group.
- *N* consecutive public addresses and a public port number are mapped to one internal server group.

ACL-based NAT server mappings that are configured with the same priority value are matched by using the ACLs in their rules:

- Mappings with named ACLs have higher priorities than mappings with unnamed ACLs.
- Mappings with named ACLs are matched in alphabetical order of their ACL names.
- Mappings with unnamed ACLs are matched in descending order of their ACL numbers.

In a hot backup system collaborating with VRRP, when you configure a NAT server mapping on the primary device in the hot backup system, specify a VRRP group facing the external network. If you do not perform the binding, the uplink Layer 3 device directly connected to the hot backup system might send downlink packets to the backup device, causing service anomalies.

An error message for a rollback failure when you perform a configuration rollback for an internal server in the following situation:

- In the running configuration, the name of a NAT server mapping is assigned automatically by the system.
- In the replacement configuration file, the name does not exist.

The system will compare the running configuration file and the replacement file, and display an error message about the mismatch. You can ignore the error message because the NAT server mapping configuration in the configuration file is installed successfully. For example, the NAT server mapping configuration is **nat server global 112.1.1.1 inside 192.168.20.1** in the running configuration, and the is **nat server global 112.1.1.1 inside 192.168.20.1 rule *ServerRule_num*** in the replacement configuration file. After the rollback operation, the new NAT server configuration is successfully installed.

Examples

Allow external users to access the internal Web server at 10.110.10.10 through http://202.110.10.10:8080.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat server protocol tcp global 202.110.10.10 8080 inside 10.110.10.10 http
[Sysname-GigabitEthernet1/0/1] quit
```

Allow external users to access the internal FTP server at 10.110.10.11 in the VPN instance **vrf10** through ftp://202.110.10.10.

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat server protocol tcp global 202.110.10.10 21 inside 10.110.10.11 vpn-instance vrf10
[Sysname-GigabitEthernet1/0/1] quit
```

Allow external hosts to ping the host at 10.110.10.12 in the VPN instance **vrf10** by using the **ping 202.110.10.11** command.

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat server protocol icmp global 202.110.10.11 inside 10.110.10.12 vpn-instance vrf10
[Sysname-GigabitEthernet1/0/1] quit
```

Allow external hosts to access the Telnet services of internal servers at 10.110.10.1 to 10.110.10.100 in the VPN instance **vrf10** through the public address 202.110.10.10 and port numbers from 1001 to 1100. As a result, a user can Telnet to 202.110.10.10:1001 to access 10.110.10.1, Telnet to 202.110.10.10:1002 to access 10.110.10.2, and so on.

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat server protocol tcp global 202.110.10.10 1001 1100 inside 10.110.10.1 10.110.10.100 telnet vpn-instance vrf10
```

Configure an ACL-based NAT server mapping to allow users to use IP addresses in subnet 192.168.0.0/24 to access the internal server at 10.0.0.172.

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule 5 permit ip destination 192.168.0.0 0.0.0.255
[Sysname-acl-ipv4-adv-3000] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat server global 3000 inside 10.0.0.172
```

Related commands

display nat all

display nat server

nat server-group

nat server rule

Use **nat server rule global destination-ip inside** to create an object group-based NAT server rule.

Use **undo nat server rule** to delete an object group-based NAT server mapping.

Syntax

nat server rule *rule-name* **global destination-ip** *object-group-name*&<1-5> [**service** *object-group-name*] **inside** *local-address* [*local-port*] [**vrrp** *virtual-router-id*] [**disable**] [**counting**] [**description** *text*]

undo nat server rule *rule-name*

nat server rule *rule-name* **global** { **destination-ip** *object-group-name*&<1-5> | **service** *object-group-name* }

undo nat server rule *rule-name* **global** { **destination-ip** *object-group-name*&<1-5> | **service** *object-group-name* }

Default

No object group-based NAT server mapping exists.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

rule-name: Specifies a rule name. The name is a case-insensitive string of 1 to 63 characters, excluding hyphens (-) and percent signs (%). You must use the escape character (\) if you use a backslash (\) or quotation marks (") in the name.

global: Specifies the external network information that the internal server uses to provide services to the external network.

destination-ip *object-group-name*&<1-5>: Specifies a space-separated list of up to five address object group items. The *object-group-name* argument specifies the name of an address object group, a case-insensitive string of 1 to 5 characters. If spaces are included in the object group name, enclose the name in quotation marks, for example, "a 1".

service *object-group-name*: Specifies a service object group by its name, a case-insensitive string of 1 to 31 characters.

inside: Specifies the internal information of the server.

local-address: Specifies the private IP address of the internal server.

local-port: Specifies the private port number of the server. The private port number format can be one of the following:

- A number in the range of 1 to 65535, excluding FTP port 20.
- A protocol name, a string of 1 to 15 characters. For example, **http** and **telnet**.

vrrp *virtual-router-id*: Specifies a VRRP group by its virtual router ID in the range of 1 to 255.

disable: Disables the object group-based NAT Server rule.

counting: Enables NAT counting. The number of flows that use the address mapping is counted.

description *text*: Specifies a description for the object group-based NAT Server rule. The *text* argument is a case-insensitive string of 1 to 63 characters.

Usage guidelines

When multiple object group-based NAT server rules are configured, the rule configured earlier has a higher priority. The match process of a packet stops when the packet matches a rule. Different object group-based NAT server rules can use the same address object group or service object group.

Before you use the **nat server rule** *rule-name* **global destination-ip** *object-group-name* or **nat server rule** *rule-name* **global service** *object-group-name* command, follow these restrictions and guidelines:

- Make sure the rule has been created.
- You cannot add duplicate address object groups to the same rule by using the **nat server rule** *rule-name* **global destination-ip** *object-group-name* command. If only one address object group is used by the rule, you cannot use the **undo nat server rule** *rule-name* **global destination-ip** *object-group-name* command to delete this address object group.
- Only one service object group can be used by one rule. If no service object group is specified when you create a rule, you can use the **nat server rule** *rule-name* **global service** *object-group-name* command to specify it. If a service object group has been specified when you create the rule, you cannot use this command to modify the service object group.

In a hot backup system collaborating with VRRP, when you configure an object group-based NAT server on the primary device in the hot backup system, specify a VRRP group facing the external network. If you do not perform the binding, the uplink Layer 3 device directly connected to the hot backup system might send downlink packets to the backup device, causing service anomalies.

Before you configure an object group-based NAT server rule, make sure the object groups to be used by the NAT server rule have been created.

Only IPv4 address object groups are supported, and the IPv4 address object groups cannot have excluded IPv4 addresses.

The private port number in the NAT server rule takes effect only when the protocol type is TCP or UDP for the service object group.

You can create a maximum of 4096 object group-based NAT server rules.

Examples

Configure the NAT Server on GigabitEthernet 1/0/1 and use address object groups **a1**, **a2**, and **a3** to match public IP addresses and use service object group **b1** to match public ports.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat server rule aaa global destination-ip a1 a2 a3 service b1 inside 1.1.1.1 80
```

Configure the NAT Server on GigabitEthernet 1/0/1 and use address object group **a1** to match public IP addresses, and then add address object groups **a2** and **a3** and service object group **b1** to the rule.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat server rule aaa global destination-ip a1 inside 1.1.1.1 80
[Sysname-GigabitEthernet1/0/1] nat server rule aaa global destination-ip a1 a2 service b1
```

Related commands

display nat all

display nat server

nat server rule move

Use **nat server rule move** to change the priority of an ACL-based NAT server rule.

Syntax

nat server rule move *nat-rule-name1* { **after** | **before** } *nat-rule-name2*

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

nat-rule-name1: Specifies the name of the NAT rule to be moved.

after: Moves the rule *nat-rule-name1* to the line after the rule *nat-rule-name2* (called the reference rule). The priority value of the reference rule is not changed. The priority value of the moved rule equals the priority value of the reference rule plus one.

before: Moves the rule *nat-rule-name1* to the line before the rule *nat-rule-name2*. The priority value of the reference rule is not changed. The priority value of the moved rule equals the priority value of the reference rule minus one.

nat-rule-name2: Specifies the name of the NAT rule as a reference rule for the NAT rule to be moved.

Usage guidelines

This command is applicable only to named ACL-based NAT server rules.

A NAT rule appearing earlier on the rule list has a higher priority for packet matching.

Examples

Move the ACL-based NAT server rule **abc** to the line before the ACL-based NAT server rule **def**.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat server rule move abc before def
```

Related commands

nat server

nat server-group

Use **nat server-group** to create an internal server group and enter its view, or enter the view of an existing internal server group.

Use **undo nat server-group** to delete an internal server group.

Syntax

nat server-group *group-id*

undo nat server-group *group-id*

Default

No internal server groups exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

group-id: Assigns an ID to the internal server group. The value range for this argument is 0 to 65535.

Usage guidelines

An internal server group can contain multiple members configured by the **inside ip** command.

Examples

Create internal server group 1.

```
<Sysname> system-view
[Sysname] nat server-group 1
```

Related commands

display nat all

display nat server-group

inside ip

nat server

nat session create-rate enable

Use **nat session create-rate enable** to enable statistics collection for NAT session creation rate.

Use **undo nat session create-rate enable** to disable statistics collection for NAT session creation rate.

Syntax

nat session create-rate enable

undo nat session create-rate enable

Default

Statistics collection for NAT session creation rate is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This feature collects information about NAT session creation rates. To view the statistics, use the **display nat statistics** command.

Examples

Enable statistics collection for NAT session creation rate.

```
<Sysname> system-view
[Sysname] nat session create-rate enable
```

Related commands

display nat statistics

nat static enable

Use **nat static enable** to enable static NAT on an interface.

Use **undo nat static enable** to disable static NAT on an interface.

Syntax

nat static enable

undo nat static enable

Default

Static NAT is disabled.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

Static NAT mappings take effect on an interface only after static NAT is enabled on the interface.

Examples

Configure an outbound static NAT mapping between private IP address 192.168.1.1 and public IP address 2.2.2.2, and enable static NAT on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] nat static outbound 192.168.1.1 2.2.2.2
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat static enable
```

Related commands

display nat all

display nat static

nat static

nat static net-to-net

nat static inbound

Use **nat static inbound** to configure a one-to-one mapping for inbound static NAT.

Use **undo nat static inbound** to delete a one-to-one mapping for inbound static NAT.

Syntax

nat static inbound *global-ip* [**vpn-instance** *global-vpn-instance-name*] *local-ip* [**vpn-instance** *local-vpn-instance-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } [**reversible**]] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**counting**] [**description** *text*]

undo nat static inbound *global-ip* [**vpn-instance** *global-vpn-instance-name*] *local-ip* [**vpn-instance** *local-vpn-instance-name*]

Default

No NAT mappings exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

global-ip: Specifies a public IP address.

vpn-instance *global-vpn-instance-name*: Specifies the MPLS L3VPN instance to which the public IP address belongs. The *global-vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the public IP address does not belong to any VPN instance, do not specify this option.

local-ip: Specifies a private IP address.

vpn-instance *local-vpn-instance-name*: Specifies the MPLS L3VPN instance to which the private IP address belongs. The *local-vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the private IP address does not belong to any VPN instance, do not specify this option.

acl: Specifies an ACL to identify the internal hosts that can access the external network.

ipv4-acl-number: Specifies an ACL by its number in the range of 2000 to 3999.

name *ipv4-acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters. The ACL name must start with an English letter and to avoid confusion, it cannot be **all**.

reversible: Enables reverse address translation for connections actively initiated from the internal network to the private IP address.

rule *rule-name*: Specifies a name for the mapping, a case-sensitive string of 1 to 63 characters. It cannot contain backward slashes (\), forward slashes (/), colons (:), asterisks (*), question marks (?), left angle brackets (<), right angle brackets (>), vertical bars (|), quotation marks ("), or at signs (@). If you do not specify this option, the mapping does not have a name.

priority *priority*: Specifies a priority for the mapping, in the range of 0 to 2147483647. The default value is 4294967295. A smaller value represents a higher priority. If you do not specify this option, the mapping has the lowest priority among the same type of NAT rules.

disable: Disables the one-to-one inbound static mapping. If you do not specify this keyword, the mapping is enabled.

counting: Enables NAT counting. The number of flows that use the address mapping is counted.

description *text*: Specifies a description for the one-to-one inbound static mapping. The *text* argument is a case-insensitive string of 1 to 63 characters.

Usage guidelines

When the source IP address of a packet from the external network to the internal network matches the *global-ip*, the source IP address is translated into the *local-ip*. When the destination IP address of a packet from the internal network to the external network matches the *local-ip*, the destination IP address is translated into the *global-ip*.

When you specify an ACL, follow these restrictions and guidelines:

- If you do not specify an ACL, the source address of all incoming packets and the destination address of all outgoing packets are translated.
- If you specify an ACL and do not specify the **reversible** keyword, the source address of incoming packets permitted by the ACL is translated. The destination address is not translated for connections actively initiated from the internal network to the private IP address.
- If you specify both an ACL and the **reversible** keyword, the source address of incoming packets permitted by the ACL is translated. If packets of connections actively initiated from the internal network to the private IP address are permitted by ACL reverse matching, the destination address is translated. ACL reverse matching works as follows:
  - Compares the source IP address/port of a packet with the destination IP addresses/ports in the ACL.
  - Translates the destination IP address of the packet according to the mapping, and then compares the translated destination IP address/port with the source IP addresses/ports in the ACL.

Static NAT takes precedence over dynamic NAT when both are configured on an interface.

You can configure multiple inbound static NAT mappings by using the **nat static inbound** command and the **nat static inbound net-to-net** command.

The **vpn-instance** parameter is required if you deploy inbound static NAT in VPN networks. The specified VPN instance must be the VPN instance to which the NAT interface belongs.

One-to-one mappings for inbound static NAT that are configured with the same priority value and an ACL are matched by using the ACLs in the mappings.

- Mappings with named ACLs have higher priorities than mappings with unnamed ACLs.
- Mappings with named ACLs are matched in alphabetical order of their ACL names.
- Mappings with unnamed ACLs are matched in descending order of their ACL numbers.

Examples

Configure an inbound static NAT mapping between public IP address 2.2.2.2 and private IP address 192.168.1.1.

```
<Sysname> system-view
[Sysname] nat static inbound 2.2.2.2 192.168.1.1
```

Related commands

display nat all

display nat static

nat static enable

nat static inbound net-to-net

Use **nat static inbound net-to-net** to configure a net-to-net mapping for inbound static NAT.

Use **undo nat static inbound net-to-net** to remove a net-to-net mapping for inbound static NAT.

Syntax

nat static inbound net-to-net *global-start-address global-end-address* [**vpn-instance** *global-vpn-instance-name*] **local** *local-network* { *mask-length* | *mask* } [**vpn-instance** *local-vpn-instance-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } [**reversible**]] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**counting**]

undo nat static inbound net-to-net *global-start-address global-end-address* [**vpn-instance** *global-vpn-instance-name*] **local** *local-network* { *mask-length* | *mask* } [**vpn-instance** *local-vpn-instance-name*]

Default

No NAT mappings exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

global-start-address global-end-address: Specifies a public address range which can contain a maximum of 256 addresses. The *global-end-address* must not be lower than *global-start-address*. If they are the same, only one public address is specified.

vpn-instance *global-vpn-instance-name*: Specifies the MPLS L3VPN instance to which the public IP addresses belong. The *global-vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the public IP addresses do not belong to any VPN instance, do not specify this option.

local-network: Specifies a private network address.

mask-length: Specifies the mask length of the private network address, in the range of 8 to 31.

mask: Specifies the mask of the private network address.

vpn-instance *local-vpn-instance-name*: Specifies the MPLS L3VPN instance to which the private network address belongs. The *local-vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the private network address does not belong to any VPN instance, do not specify this option.

acl: Specifies an ACL to identify the internal hosts that can access the external network.

ipv4-acl-number: Specifies an ACL by its number in the range of 2000 to 3999.

name *ipv4-acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters. The ACL name must start with an English letter and to avoid confusion, it cannot be **all**.

reversible: Enables reverse address translation for connections actively initiated from the internal network to the private IP addresses.

rule *rule-name*: Specifies a name for the mapping, a case-sensitive string of 1 to 63 characters. It cannot contain backward slashes (\), forward slashes (/), colons (:), asterisks (*), question marks (?), left angle brackets (<), right angle brackets (>), vertical bars (|), quotation marks ("), or at signs (@). If you do not specify this option, the mapping does not have a name.

priority *priority*: Specifies a priority for the mapping, in the range of 0 to 2147483647. The default value is 4294967295. A smaller value represents a higher priority. If you do not specify this option, the mapping has the lowest priority among the same type of NAT rules.

disable: Disables the net-to-net inbound static mapping. If you do not specify this keyword, the mapping is enabled.

counting: Enables NAT counting. The number of flows that use the address mapping is counted.

Usage guidelines

Specify a public network through a start address and an end address, and a private network through a private address and a mask.

When the source address of a packet from the external network matches the public address range, the source address is translated into a private address in the private address range. When the destination address of a packet from the internal network matches the private address range, the destination address is translated into a public address in the public address range.

The public end address cannot be greater than the greatest IP address in the subnet determined by the public start address and the private network mask. For example, if the private address is 2.2.2.0 with a mask 255.255.255.0 and the public start address is 1.1.1.100, the public end address cannot be greater than 1.1.1.255, the greatest IP address in the subnet 1.1.1.0/24.

When you specify an ACL, follow these restrictions and guidelines:

- If you do not specify an ACL, the source address of all incoming packets and the destination address of all outgoing packets are translated.
- If you specify an ACL and do not specify the **reversible** keyword, the source address of incoming packets permitted by the ACL is translated. The destination address is not translated for connections actively initiated from the internal network to the private IP addresses.
- If you specify both an ACL and the **reversible** keyword, the source address of incoming packets permitted by the ACL is translated. If packets of connections actively initiated from the internal network to the private IP addresses are permitted by ACL reverse matching, the destination address is translated. ACL reverse matching works as follows:
  - Compares the source IP address/port of a packet with the destination IP addresses/ports in the ACL.
  - Translates the destination IP address of the packet according to the mapping, and then compares the translated destination IP address/port with the source IP addresses/ports in the ACL.

Static NAT takes precedence over dynamic NAT when both are configured on an interface.

You can configure multiple inbound static NAT mappings by using the **nat static inbound** command and the **nat static inbound net-to-net** command.

The **vpn-instance** parameter is required if you deploy inbound static NAT in VPN networks. The specified VPN instance must be the VPN instance to which the NAT interface belongs.

Net-to-net mappings for inbound static NAT that are configured with the same priority value and an ACL are matched by using the ACLs in the mappings.

- Mappings with named ACLs have higher priorities than mappings with unnamed ACLs.
- Mappings with named ACLs are matched in alphabetical order of their ACL names.
- Mappings with unnamed ACLs are matched in descending order of their ACL numbers.

Examples

Configure an inbound static NAT between public network address 202.100.1.0/24 and private network address 192.168.1.0/24.

```
<Sysname> system-view
[Sysname] nat static inbound net-to-net 202.100.1.1 202.100.1.255 local 192.168.1.0 24
```

Related commands

display nat all

display nat static

nat static enable

nat static inbound net-to-net rule move

Use **nat static inbound net-to-net rule move** to change the priority of an inbound net-to-net static NAT rule.

Syntax

nat static inbound net-to-net rule move *nat-rule-name1* { **after** | **before** } *nat-rule-name2*

Default

An inbound net-to-net static NAT rule appearing earlier on the rule list has a higher priority for packet matching.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

nat-rule-name1: Specifies the name of the NAT rule to be moved.

after: Moves the rule *nat-rule-name1* to the line after the rule *nat-rule-name2* (called the reference rule). The priority value of the reference rule is not changed. The priority value of the moved rule equals the priority value of the reference rule plus one.

before: Moves the rule *nat-rule-name1* to the line before the rule *nat-rule-name2*. The priority value of the reference rule is not changed. The priority value of the moved rule equals the priority value of the reference rule minus one.

nat-rule-name2: Specifies the name of the NAT rule as a reference rule for the NAT rule to be moved.

Examples

Move the inbound net-to-net static NAT rule **abc** to the line before the inbound net-to-net static NAT rule **def**.

```
<Sysname> system-view
[Sysname] nat static inbound net-to-net rule move abc before def
```

Related commands

nat static inbound net-to-net

nat static inbound object-group

Use **nat static inbound object-group** to configure an object group-based inbound static NAT mapping.

Use **undo nat static inbound object-group** to remove an object group-based inbound static NAT mapping.

Syntax

nat static inbound object-group *global-object-group-name* [**vpn-instance** *global-vpn-instance-name*] **object-group** *local-object-group-name*

[**vpn-instance** *local-vpn-instance-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } [**reversible**]] [**disable**] [**counting**]

undo nat static inbound object-group *global-object-group-name* [**vpn-instance** *global-vpn-instance-name*]

Default

No NAT mappings exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

object-group *global-object-group-name*: Specifies an object group of public IPv4 addresses. The *global-object-group-name* argument is a case-insensitive string of 1 to 31 characters.

vpn-instance *global-vpn-instance-name*: Specifies the MPLS L3VPN instance to which the public IP addresses belong. The *global-vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the public IP addresses do not belong to any VPN instance, do not specify this option.

object-group *local-object-group-name*: Specifies an object group of private IPv4 addresses. The *local-object-group-name* argument is a case-insensitive string of 1 to 31 characters.

vpn-instance *local-vpn-instance-name*: Specifies the MPLS L3VPN instance to which the private IP addresses belong. The *local-vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the private IP addresses do not belong to any VPN instance, do not specify this option.

acl: Specifies an ACL to identify the packets that can use the mapping.

ipv4-acl-number: Specifies an ACL by its number in the range of 2000 to 3999.

name *ipv4-acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters. The ACL name must start with an English letter and to avoid confusion, it cannot be **all**.

reversible: Enables reverse address translation. Reverse address translation applies to connections actively initiated by internal hosts to the external hosts. It uses the mapping to translate destination addresses for packets of these connections if the packets are permitted by ACL reverse matching.

disable: Disables the object group based inbound static mapping. If you do not specify this keyword, the mapping is enabled.

counting: Enables NAT counting. The number of flows that use the address mapping is counted.

Usage guidelines

This command specifies public and private IP addresses through IPv4 address object groups.

When the source address of an income packet matches the public address object group, the source address is translated into a private address in the private address object group. When the destination address of an outgoing packet matches the private address object group, the destination address is translated into a public address in the public address object group.

When you specify object groups for an inbound static mapping, follow these restrictions and guidelines:

- The public or private IPv4 address object group can contain only one IPv4 address object.
- The quantity of IPv4 addresses in the private IPv4 address object group cannot be smaller than that in the public IPv4 address object group.
- The object in the private IPv4 address object group cannot be an address range.
- If the private IPv4 object group contains a host address, the host address cannot be on the same subnet as the interface configured with this mapping.
- One IPv4 address object group can only contain one host object or subnet object. Otherwise, the mapping does not take effect.
- A subnet object cannot have excluded addresses. Otherwise, the mapping does not take effect.

When you specify an ACL, follow these restrictions and guidelines:

- If you do not specify an ACL, the source addresses of all incoming packets and the destination addresses of all outgoing packets are translated.
- If you specify an ACL and do not specify the **reversible** keyword, the source addresses of incoming packets permitted by the ACL are translated. The destination addresses of packets are not translated for connections actively initiated by internal hosts to the external hosts.
- If you specify both an ACL and the **reversible** keyword, the source addresses of incoming packets permitted by the ACL are translated. If packets of connections actively initiated by internal hosts to the external hosts are permitted by ACL reverse matching, the destination addresses are translated. ACL reverse matching works as follows:
  - Compares the source IP address/port of a packet with the destination IP addresses/ports in the ACL.
  - Translates the destination IP address of the packet according to the mapping, and then compares the translated destination IP address/port with the source IP addresses/ports in the ACL.

Static NAT takes precedence over dynamic NAT when they are both configured on an interface.

You can configure multiple inbound static NAT mappings by using the **nat static inbound** , **nat static inbound net-to-net** , and **nat static inbound object-group** commands.

The **vpn-instance** parameter is required if you deploy inbound static NAT in VPN networks. The specified VPN instance must be the VPN instance to which the NAT interface belongs.

Examples

Configure an object group-based inbound static NAT mapping between public IP address 2.2.2.2 and private IP address 192.168.1.1.

```
<Sysname> system-view
[Sysname] object-group ip address global
[Sysname-obj-grp-ip-global] network host address 2.2.2.2
[Sysname-obj-grp-ip-global] quit
[Sysname] object-group ip address local
[Sysname-obj-grp-ip-local] network host address 192.168.1.1
[Sysname-obj-grp-ip-local] quit
[Sysname] nat static inbound object-group global object-group local
```

Related commands

display nat all

display nat static

nat static enable

nat static inbound rule move

Use **nat static inbound rule move** to change the priority of an inbound one-to-one static NAT rule.

Syntax

nat static inbound rule move *nat-rule-name1* { **after** | **before** } *nat-rule-name2*

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

nat-rule-name1: Specifies the name of the NAT rule to be moved.

after: Moves the rule *nat-rule-name1* to the line after the rule *nat-rule-name2* (called the reference rule). The priority value of the reference rule is not changed. The priority value of the moved rule equals the priority value of the reference rule plus one.

before: Moves the rule *nat-rule-name1* to the line before the rule *nat-rule-name2*. The priority value of the reference rule is not changed. The priority value of the moved rule equals the priority value of the reference rule minus one.

nat-rule-name2: Specifies the name of the NAT rule as a reference rule for the NAT rule to be moved.

Usage guidelines

This command is applicable only to named inbound one-to-one static NAT rules.

A NAT rule appearing earlier on the rule list has a higher priority for packet matching.

Examples

Move the inbound one-to-one static NAT rule **abc** to the line before the inbound one-to-one static NAT rule **def**.

```
<Sysname> system-view
[Sysname] nat static inbound rule move abc before def
```

Related commands

nat static inbound

nat static outbound

Use **nat static outbound** to configure a one-to-one mapping for outbound static NAT.

Use **undo nat static outbound** to remove a one-to-one mapping for outbound static NAT.

Syntax

nat static outbound *local-ip* [**vpn-instance** *local-vpn-instance-name*] *global-ip* [**vpn-instance** *global-vpn-instance-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } [**reversible**]] [**vrrp** *virtual-router-id*] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**counting**] [**description** *text*]

undo nat static outbound *local-ip* [**vpn-instance** *local-vpn-instance-name*] *global-ip* [**vpn-instance** *global-vpn-instance-name*]

Default

No NAT mappings exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

local-ip: Specifies a private IP address.

vpn-instance *local-vpn-instance-name*: Specifies the MPLS L3VPN instance to which the private IP address belongs. The *local-vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the private IP address does not belong to any VPN instance, do not specify this option.

global-ip: Specifies a public IP address.

vpn-instance *global-vpn-instance-name*: Specifies the MPLS L3VPN instance to which the public IP address belongs. The *global-vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the public IP address does not belong to any VPN instance, do not specify this option.

acl: Specifies an ACL to define the destination IP addresses that internal hosts can access.

ipv4-acl-number: Specifies an ACL by its number in the range of 3000 to 3999.

name *ipv4-acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters. The ACL name must start with an English letter and to avoid confusion, it cannot be **all**.

reversible: Enables reverse address translation for connections actively initiated from the external network to the public IP address.

vrrp *virtual-router-id*: Specifies a VRRP group by its virtual router ID in the range of 1 to 255.

rule *rule-name*: Specifies a name for the mapping, a case-sensitive string of 1 to 63 characters. It cannot contain backward slashes (\), forward slashes (/), colons (:), asterisks (*), question marks (?), left angle brackets (<), right angle brackets (>), vertical bars (|), quotation marks ("), or at signs (@). If you do not specify this option, the mapping does not have a name.

priority *priority*: Specifies a priority for the mapping, in the range of 0 to 2147483647. The default value is 4294967295. A smaller value represents a higher priority. If you do not specify this option, the mapping has the lowest priority among the same type of NAT rules.

disable: Disables the one-to-one outbound static mapping. If you do not specify this keyword, the mapping is enabled.

counting: Enables NAT counting. The number of flows that use the address mapping is counted.

description *text*: Specifies a description for the one-to-one outbound static mapping. The *text* argument is a case-insensitive string of 1 to 63 characters.

Usage guidelines

When the source IP address of an outgoing packet matches the *local-ip*, the IP address is translated into the *global-ip*. When the destination IP address of an incoming packet matches the *global-ip*, the destination IP address is translated into the *local-ip*.

When you specify an ACL, follow these restrictions and guidelines:

- If you do not specify an ACL, the source address of all outgoing packets and the destination address of all incoming packets are translated.
- If you specify an ACL and do not specify the **reversible** keyword, the source address of outgoing packets permitted by the ACL is translated. The destination address is not translated for connections actively initiated from the external network to the public IP address.
- If you specify both an ACL and the **reversible** keyword, the source address of outgoing packets permitted by the ACL is translated. If packets of connections actively initiated from the external network to the public IP address are permitted by ACL reverse matching, the destination address is translated. ACL reverse matching works as follows:
  - Compares the source IP address/port of a packet with the destination IP addresses/ports in the ACL.
  - Translates the destination IP address of the packet according to the mapping, and then compares the translated destination IP address/port with the source IP addresses/ports in the ACL.

Static NAT takes precedence over dynamic NAT when they are both configured on an interface.

You can configure multiple outbound static NAT mappings by using the **nat static outbound** command and the **nat static outbound net-to-net** command.

The **vpn-instance** parameter is required if you deploy outbound static NAT in VPN networks. The specified VPN instance must be the VPN instance to which the NAT interface belongs.

In a hot backup system collaborating with VRRP, when you configure a one-to-one mapping for outbound static NAT on the primary device in the hot backup system, specify a VRRP group facing the external network. If you do not perform the binding, the uplink Layer 3 device directly connected to the hot backup system might send downlink packets to the backup device, causing service anomalies.

One-to-one mappings for outbound static NAT that are configured with the same priority value and an ACL are matched by using the ACLs in the mappings.

- Mappings with named ACLs have higher priorities than mappings with unnamed ACLs.
- Mappings with named ACLs are matched in alphabetical order of their ACL names.
- Mappings with unnamed ACLs are matched in descending order of their ACL numbers.

Examples

Configure an outbound static NAT mapping between public IP address 2.2.2.2 and private IP address 192.168.1.1.

```
<Sysname> system-view
[Sysname] nat static outbound 192.168.1.1 2.2.2.2
```

Configure outbound static NAT, and allow the internal user 192.168.1.1 to access the external network 3.3.3.0/24 by using the public IP address 2.2.2.2.

```
<Sysname> system-view
[Sysname] acl advanced 3001
[Sysname-acl-ipv4-adv-3001] rule permit ip destination 3.3.3.0 0.0.0.255
[Sysname-acl-ipv4-adv-3001] quit
[Sysname] nat static outbound 192.168.1.1 2.2.2.2 acl 3001
```

Related commands

display nat all

display nat static

nat static enable

nat static outbound net-to-net

Use **nat static outbound net-to-net** to configure a net-to-net outbound static NAT mapping.

Use **undo nat static outbound net-to-net** to remove the specified net-to-net outbound static NAT mapping.

Syntax

nat static outbound net-to-net *local-start-address local-end-address* [**vpn-instance** *local-vpn-instance-name*] **global** *global-network* { *mask-length* | *mask* } [**vpn-instance** *global-vpn-instance-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } [**reversible**]] [**vrrp** *virtual-router-id*] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**counting**]

undo nat static outbound net-to-net *local-start-address local-end-address* [**vpn-instance** *local-vpn-instance-name*] **global** *global-network* { *mask-length* | *mask* } [**vpn-instance** *global-vpn-instance-name*]

Default

No NAT mappings exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

local-start-address local-end-address: Specifies a private address range which can contain a maximum of 256 addresses. The *local-end-address* must not be lower than *local-start-address*. If they are the same, only one private address is specified.

vpn-instance *local-vpn-instance-name*: Specifies the MPLS L3VPN instance to which the private IP addresses belong. The *local-vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the private IP addresses do not belong to any VPN instance, do not specify this option.

global-network: Specifies a public network address.

mask-length: Specifies the mask length of the public network address, in the range of 8 to 31.

mask: Specifies the mask of the public network address.

vpn-instance *global-vpn-instance-name*: Specifies the MPLS L3VPN instance to which the public network address belongs. The *global-vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the public network address does not belong to any VPN instance, do not specify this option.

acl: Specifies an ACL to define the destination IP addresses that internal hosts can access.

ipv4-acl-number: Specifies an ACL number in the range of 2000 to 3999.

name *ipv4-acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters. The ACL name must start with an English letter and to avoid confusion, it cannot be **all**.

reversible: Enables reverse address translation for connections actively initiated from the external network to the public IP addresses.

vrrp *virtual-router-id*: Specifies a VRRP group by its virtual router ID in the range of 1 to 255.

rule *rule-name*: Specifies a name for the mapping, a case-sensitive string of 1 to 63 characters. It cannot contain backward slashes (\), forward slashes (/), colons (:), asterisks (*), question marks (?), left angle brackets (<), right angle brackets (>), vertical bars (|), quotation marks ("), or at signs (@). If you do not specify this option, the mapping does not have a name.

priority *priority*: Specifies a priority for the mapping, in the range of 0 to 2147483647. The default value is 4294967295. A smaller value represents a higher priority. If you do not specify this option, the mapping has the lowest priority among the same type of NAT rules.

disable: Disables the net-to-net outbound static mapping. If you do not specify this keyword, the mapping is enabled.

counting: Enables NAT counting. The number of flows that use the address mapping is counted.

Usage guidelines

Specify a private network through a start address and an end address, and a public network through a public address and a mask.

When the source address of a packet from the internal network matches the private address range, the source address is translated into a public address in the public address range. When the destination address of a packet from the external network matches the public address range, the destination address is translated into a private address in the private address range.

The private end address cannot be greater than the greatest IP address in the subnet determined by the private start address and the public network mask. For example, the public address is 2.2.2.0 with a mask 255.255.255.0, and the private start address is 1.1.1.100. The private end address cannot be greater than 1.1.1.255, the greatest IP address in the subnet 1.1.1.0/24.

When you specify an ACL, follow these restrictions and guidelines:

- If you do not specify an ACL, the source address of all outgoing packets and the destination address of all incoming packets are translated.
- If you specify an ACL and do not specify the **reversible** keyword, the source address of outgoing packets permitted by the ACL is translated. The destination address is not translated for connections actively initiated from the external network to the public IP addresses.
- If you specify both an ACL and the **reversible** keyword, the source address of outgoing packets permitted by the ACL is translated. If packets of connections actively initiated from the external network to the public IP addresses are permitted by ACL reverse matching, the destination address is translated. ACL reverse matching works as follows:
  - Compares the source IP address/port of a packet with the destination IP addresses/ports in the ACL.
  - Translates the destination IP address of the packet according to the mapping, and then compares the translated destination IP address/port with the source IP addresses/ports in the ACL.

Static NAT takes precedence over dynamic NAT when they are both configured on an interface.

You can configure multiple outbound static NAT mappings by using the **nat static outbound** command and the **nat static outbound net-to-net** command.

The **vpn-instance** parameter is required if you deploy outbound static NAT in VPN networks. The specified VPN instance must be the VPN instance to which the NAT interface belongs.

In a hot backup system collaborating with VRRP, when you configure a net-to-net outbound static NAT mapping on the primary device in the hot backup system, specify a VRRP group facing the external network. If you do not perform the binding, the uplink Layer 3 device directly connected to the hot backup system might send downlink packets to the backup device, causing service anomalies.

Net-to-net mappings for outbound static NAT that are configured with the same priority value and an ACL are matched by using the ACLs in the mappings.

- Mappings with named ACLs have higher priorities than mappings with unnamed ACLs.
- Mappings with named ACLs are matched in alphabetical order of their ACL names.
- Mappings with unnamed ACLs are matched in descending order of their ACL numbers.

Examples

Configure an outbound static NAT mapping between private network address 192.168.1.0/24 and public network address 2.2.2.0/24.

```
<Sysname> system-view
[Sysname] nat static outbound net-to-net 192.168.1.1 192.168.1.255 global 2.2.2.0 24
```

Configure outbound static NAT. Allow internal users on subnet 192.168.1.0/24 to access the external subnet 3.3.3.0/24 by using public IP addresses on subnet 2.2.2.0/24.

```
<Sysname> system-view
[Sysname] acl advanced 3001
[Sysname-acl-ipv4-adv-3001] rule permit ip destination 3.3.3.0 0.0.0.255
[Sysname-acl-ipv4-adv-3001] quit
[Sysname] nat static outbound net-to-net 192.168.1.1 192.168.1.255 global 2.2.2.0 24 acl
3001
```

Related commands

display nat all

display nat static

nat static enable

nat static outbound net-to-net rule move

Use **nat static outbound net-to-net rule move** to change the priority of an outbound net-to-net static NAT rule.

Syntax

nat static outbound net-to-net rule move *nat-rule-name1* { **after** | **before** } *nat-rule-name2*

Default

An outbound net-to-net static NAT rule appearing earlier on the rule list has a higher priority for packet matching.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

nat-rule-name1: Specifies the name of the NAT rule to be moved.

after: Moves the rule *nat-rule-name1* to the line after the rule *nat-rule-name2* (called the reference rule). The priority value of the reference rule is not changed. The priority value of the moved rule equals the priority value of the reference rule plus one.

before: Moves the rule *nat-rule-name1* to the line before the rule *nat-rule-name2*. The priority value of the reference rule is not changed. The priority value of the moved rule equals the priority value of the reference rule minus one.

nat-rule-name2: Specifies the name of the NAT rule as a reference rule for the NAT rule to be moved.

Examples

Move the outbound net-to-net static NAT rule **abc** to the line before the outbound net-to-net static NAT rule **def**.

```
<Sysname> system-view
[Sysname] nat static outbound net-to-net rule move abc before def
```

Related commands

nat static outbound net-to-net

nat static outbound object-group

Use **nat static outbound object-group** to configure an object group-based outbound static NAT mapping.

Use **undo nat static outbound object-group** to remove an object group-based outbound static NAT mapping.

Syntax

nat static outbound object-group *local-object-group-name* [**vpn-instance** *local-vpn-instance-name*] **object-group** *global-object-group-name* [**vpn-instance** *global-vpn-instance-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } [**reversible**]] [**vrrp** *virtual-router-id*] [**disable**] [**counting**]

undo nat static outbound object-group *local-object-group-name* [**vpn-instance** *local-vpn-instance-name*]

Default

No NAT mappings exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

object-group *local-object-group-name*: Specifies an object group of private IPv4 addresses. The *local-object-group-name* argument is a case-insensitive string of 1 to 31 characters.

vpn-instance *local-vpn-instance-name*: Specifies the MPLS L3VPN instance to which the private IP addresses belong. The *local-vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the private IP addresses do not belong to any VPN instance, do not specify this option.

object-group *global-object-group-name*: Specifies an object group of public IPv4 addresses. The *global-object-group-name* argument is a case-insensitive string of 1 to 31 characters.

vpn-instance *global-vpn-instance-name*: Specifies the MPLS L3VPN instance to which the public IP addresses belong. The *global-vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the public IP addresses do not belong to any VPN instance, do not specify this option.

acl: Specifies an ACL to identify the packets that can use the mapping.

ipv4-acl-number: Specifies an ACL number in the range of 2000 to 3999.

name *ipv4-acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters. The ACL name must start with an English letter and to avoid confusion, it cannot be **all**.

reversible: Allows reverse address translation. Reverse address translation applies to connections actively initiated by external hosts to the internal hosts. It uses the mapping to translate destination addresses for packets of these connections if the packets are permitted by ACL reverse matching.

vrrp *virtual-router-id*: Specifies a VRRP group by its virtual router ID in the range of 1 to 255.

disable: Disables the object group based outbound static mapping. If you do not specify this keyword, the mapping is enabled.

counting: Enables NAT counting. The number of flows that use the address mapping is counted.

Usage guidelines

This command specifies public and private IP addresses through IPv4 address object groups.

When the source address of a packet from the private network matches the private address object group, the source address is translated into a public address in the public address object group. When the destination address of a packet from the public network matches the public address object group, the destination address is translated into a private address in the private address object group.

When you specify object groups for an outbound static mapping, follow these restrictions and guidelines:

- The public or private IPv4 address object group can contain only one IPv4 address object.
- The quantity of IPv4 addresses in the private IPv4 address object group cannot be larger than that in the public IPv4 address object group.
- The object in the public IPv4 address object group cannot be an address range.
- An IPv4 address object group can only contain a host object or a subnet object. Otherwise, the mapping does not take effect.
- A subnet object cannot have excluded IPv4 addresses. Otherwise, the mapping does not take effect.

When you specify an ACL, follow these restrictions and guidelines:

- If you do not specify an ACL, the source addresses of all outgoing packets and the destination addresses of all incoming packets are translated.
- If you specify an ACL and do not specify the **reversible** keyword, the source addresses of outgoing packets permitted by the ACL are translated. The destination addresses of packets are not translated for connections actively initiated by external hosts to the internal hosts.
- If you specify both an ACL and the **reversible** keyword, the source addresses of outgoing packets permitted by the ACL are translated. If packets of connections actively initiated by external hosts to the internal hosts are permitted by ACL reverse matching, the destination addresses are translated. ACL reverse matching works as follows:
    - Compares the source IP address/port of a packet with the destination IP addresses/ports in the ACL.

- Translates the destination IP address of the packet according to the mapping, and then compares the translated destination IP address/port with the source IP addresses/ports in the ACL.

Static NAT takes precedence over dynamic NAT when they are both configured on an interface.

You can configure multiple outbound static NAT mappings by using the **nat static outbound**, **nat static outbound net-to-net**, and **nat static outbound object-group** commands.

The **vpn-instance** parameter is required if you deploy outbound static NAT in VPN networks. The specified VPN instance must be the VPN instance to which the NAT interface belongs.

In a hot backup system collaborating with VRRP, when you configure an object group-based outbound static NAT mapping on the primary device in the hot backup system, specify a VRRP group facing the external network. If you do not perform the binding, the uplink Layer 3 device directly connected to the hot backup system might send downlink packets to the backup device, causing service anomalies.

Examples

Configure an object group-based outbound static NAT mapping between private IP address 192.168.1.1 and public IP address 2.2.2.2.

```
<Sysname> system-view
[Sysname] object-group ip address global
[Sysname-obj-grp-ip-global] network host address 2.2.2.2
[Sysname-obj-grp-ip-global] quit
[Sysname] object-group ip address local
[Sysname-obj-grp-ip-local] network host address 192.168.1.1
[Sysname-obj-grp-ip-local] quit
[Sysname] nat static outbound object-group local object-group global
```

Related commands

display nat all

display nat static

nat static outbound rule move

Use **nat static outbound rule move** to change the priority of an outbound one-to-one static NAT rule.

Syntax

nat static outbound rule move *nat-rule-name1* { **after** | **before** } *nat-rule-name2*

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

nat-rule-name1: Specifies the name of the NAT rule to be moved.

after: Moves the rule *nat-rule-name1* to the line after the rule *nat-rule-name2* (called the reference rule). The priority value of the reference rule is not changed. The priority value of the moved rule equals the priority value of the reference rule plus one.

before: Moves the rule *nat-rule-name1* to the line before the rule *nat-rule-name2*. The priority value of the reference rule is not changed. The priority value of the moved rule equals the priority value of the reference rule minus one.

nat-rule-name2: Specifies the name of the NAT rule as a reference rule for the NAT rule to be moved.

Usage guidelines

This command is applicable only to named outbound one-to-one static NAT rules..

A NAT rule appearing earlier on the rule list has a higher priority for packet matching.

Examples

Move the outbound one-to-one static NAT rule **abc** to the line before the outbound one-to-one static NAT rule **def**.

```
<Sysname> system-view
[Sysname] nat static outbound rule move abc before def
```

Related commands

nat static outbound

nat timestamp delete

Use **nat timestamp delete** to enable the deletion of timestamps in TCP SYN and SYN ACK packets.

Use **undo nat timestamp delete** to restore the default.

Syntax

nat timestamp delete [**vpn-instance** *vpn-instance-name*]

undo nat timestamp delete [**vpn-instance** *vpn-instance-name*]

Default

The TCP SYN and SYN ACK packets carry the timestamp.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN to which the TCP SYN and SYN ACK packets belong. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If you do not specify this option, this command applies to TCP SYN and SYN ACK packets on the public network.

Usage guidelines

With this feature configured, the system deletes the timestamps from the TCP SYN and SYN ACK packets after dynamic address translation.

If PAT mode is configured on an interface by using **nat inbound** or **nat outbound**, and the tcp_timestamp and tcp_tw_recycle function is configured on the TCP server, TCP connections might not be established. To solve the problem, you can shut down the tcp_tw_recycle function or configure the **nat timestamp delete** command.

You can enable this feature for multiple VPN instances by repeating the command with different VPN parameters.

Examples

Enable the deletion of the timestamp for TCP SYN and SYN ACK packets on the public network.

```
<Sysname> system-view
[Sysname] nat timestamp delete
```

Enable the deletion of the timestamp for TCP SYN and SYN ACK packets on the VPN instance **aa**.

```
<Sysname> system-view
[Sysname] nat timestamp delete vpn-instance aa
```

Related commands

nat outbound

nat inbound

outbound-interface

Use **outbound-interface** to apply the NAT rule to the outgoing traffic on an interface.

Use **undo outbound-interface** to restore the default.

Syntax

outbound-interface *interface-type interface-number*

undo outbound-interface

Default

A NAT rule is not applied to the outgoing traffic on an interface.

Views

NAT rule view

Predefined user roles

network-admin

context-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

After you execute the command, the NAT rule applies to the outgoing traffic passing through the specified interface.

Examples

Apply the NAT rule **aaa** to the outgoing traffic on GigabitEthernet 1/0/2.

```
<Sysname> system
[Sysname] nat policy
[Sysname-nat-policy] rule name aaa
[Sysname-nat-policy-rule-aaa] outbound-interface gigabitethernet 1/0/2
```

Related commands

display nat all

display nat policy

port-block

Use **port block** to configure port block parameters for a NAT address group.

Use **undo port block** to restore the default.

Syntax

port block block-size *block-size* [**extended-block-number** *extended-block-number*]

undo port block

Default

No port block parameters are configured for a NAT address group.

Views

NAT address group view

Predefined user roles

network-admin

context-admin

Parameters

block-size *block-size*: Specifies the port block size. The value range for the *block-size* argument is 1 to 65535. In a NAT address group, the port block size cannot be larger than the number of ports in the port range.

extended-block-number *extended-block-number*: Specifies the number of extended port blocks, in the range of 1 to 5. When a private IP address accesses the public network, but the ports in the selected port block are all occupied, the NAT444 gateway extends port blocks one by one for the private IP address.

Usage guidelines

To configure dynamic port block mappings, port block parameters are required in the NAT address group. When a private IP address initiates a connection to the public network, the NAT444 gateway assigns it a public IP address and a port block, and creates an entry for the mapping. For subsequent connections from the private IP address, the NAT444 gateway translates the private IP address to the mapped public IP address and the ports to ports in the selected port block.

Examples

Set the port block size to 256 and the number of extended port blocks to 1 in NAT address group 2.

```
<Sysname> system-view
[Sysname] nat address-group 2
[Sysname-address-group-2] port-block block-size 256 extended-block-number 1
```

Related commands

nat address-group

port-range

Use **port-range** to specify a port range for public IP addresses.

Use **undo port-range** to restore the default.

Syntax

port-range *start-port-number end-port-number*

undo port-range

Default

The port range for public IP addresses is 1 to 65535.

Views

NAT address group view

NAT port block group view

Predefined user roles

network-admin

context-admin

Parameters

start-port-number end-port-number: Specifies the start port number and end port number for the port range. The end port number cannot be smaller than the start port number. As a best practice, set the start port number to be equal to or larger than 1024 to avoid an application protocol identification error.

Usage guidelines

The port range must include all ports that public IP addresses use for address translation.

The number of ports in a port range cannot be smaller than the port block size.

Examples

Specify the port range as 1024 to 65535 for NAT address group 1.

```
<Sysname> system-view
[Sysname] nat address-group 1
[Sysname-address-group-1] port-range 1024 65535
```

Specify the port range as 30001 to 65535 for NAT port block group 1.

```
<Sysname> system-view
[Sysname] nat port-block-group 1
[Sysname-port-block-group-1] port-range 30001 65535
```

Related commands

nat address-group

nat port-block-group

probe

Use **probe** to specify a probe method for a NAT address group.

Use **undo probe** to cancel the probe method for a NAT address group.

Syntax

probe *template-name*

undo probe *template-name*

Default

No probe method is specified for a NAT address group.

Views

NAT address group view

Predefined user roles

network-admin

context-admin

Parameters

template-name: Specifies the name of an NQA template used for address probe. The name is a case-insensitive string of 1 to 32 characters.

Usage guidelines

The NAT address group probing uses an NQA template to detect the reachability of the addresses in the group.

The device periodically sends probe packets to the specified destination address in the NQA template. The source IP addresses in the probe packets are the IP addresses in the NAT address group.

- If the device receives a response packet for a probe, the probed source IP address can be used for address translation.
- If the device does not receive a response packet for a probe, the probed source IP address will be excluded from address translation temporarily. However, in the next NQA operation period, this excluded IP address is also probed. If a response is received in this round, the IP address can be used for address translation.

You can specify multiple NQA templates for one NAT address group. An IP address in the address group is identified as reachable as long as one probe for this IP address succeeds.

This command is applicable to NAT address groups used for outbound address translation. The manually configured excluded IP addresses are not probed.

When you configure NQA template for probing IP addresses in NAT address group, do not configure the source IP address in the template.

Examples

Create NQA ICMP template **4**, and specify it as the probe method for NAT address group **1**.

```
<Sysname> system-view
[Sysname] nqa template icmp t4
[Sysname-nqatplt-icmp-t4] quit
[Sysname] nat address-group 1
[Sysname-lb-lgroup-lg] probe t4
```

Related commands

display nat probe address-group

exclude-ip

nqa template (*Network Management and Monitoring Command Reference*)

reset nat count statistics

Use **reset nat count statistics** to clear NAT counting statistics.

Syntax

reset nat count statistics { **all** | **dynamic** | **global-policy** | **server** | **static** | **static-port-block** }

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

all: Clears all counting statistics for NAT mappings.

dynamic: Clears counting statistics for dynamic NAT mappings.

global-policy: Clears counting statistics for the global NAT policy.

server: Clears counting statistics for NAT server mappings.

static: Clears counting statistics for static NAT mappings.

static-port-block: Clears counting statistics for NAT444 mappings.

Examples

Clear all counting statistics for static NAT mappings.

```
<Sysname> reset nat count statistics all
```

Related commands

display nat inbound

display nat outbound

display nat outbound port-block-group

display nat port-block

display nat static

display nat server

reset nat periodic-statistics

Use **reset nat periodic-statistics** to clear periodic NAT statistics.

Syntax

reset nat periodic-statistics [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears periodic NAT statistics for all member devices.

Examples

Clear periodic NAT statistics of slot 1.

```
<Sysname> reset nat periodic-statistics slot 1
```

Related commands

display nat periodic-statistics

reset nat session

Use **reset nat session** to clear NAT sessions.

Syntax

reset nat session [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears NAT sessions for all member devices.

Examples

Clear NAT sessions for the specified slot.

```
<Sysname> reset nat session slot 1
```

Related commands

display nat session

rule move (interface-based NAT policy view)

Use **rule move** to rearrange NAT rules to change their priority.

Syntax

rule move *rule-name1* { **after** | **before** } [*rule-name2*]

Views

Interface-based NAT policy view

Predefined user roles

network-admin

context-admin

Parameters

rule-name1: Specifies the name of the NAT rule to be moved. The rule name is a case-insensitive string of 1 to 63 characters.

after: Places the rule *rule-name1* after the rule *rule-name2* (called the reference rule).

before: Places the rule *rule-name1* before the reference rule.

rule-name2: Specifies the NAT rule as a reference rule. The rule name is a case-insensitive string of 1 to 63 characters. If you do not specify this argument, the priority of *rule-name1* changes as follows:

- If **after** is specified, the rule *rule-name1* will have the lowest priority.
- If **before** is specified, the rule *rule-name1* will have the highest priority.

Usage guidelines

You can execute this command to rearrange only existing NAT rules to change their priority.

Examples

Place the NAT rule **aaa** before the NAT rule **bbb** in the interface-based NAT policy.

```
<Sysname> system
[Sysname] nat policy
[Sysname-nat-policy] rule move aaa before bbb
```

rule move (global NAT policy view)

Use **rule move** to rearrange NAT rules to change their priority.

Syntax

rule move *rule-name1* [**type** { **nat** | **nat64** | **nat66** }] { **after** | **before** } [*rule-name2* [**type** { **nat** | **nat64** | **nat66** }]]

Views

Global NAT policy view

Predefined user roles

network-admin

context-admin

Parameters

rule-name1: Specifies the name of the NAT rule to be moved. The rule name is a case-insensitive string of 1 to 63 characters.

type: Specifies a NAT rule type.

nat: Specifies the IPv4-to-IPv4 address translation rule.

nat64: Specifies the rule for translation between IPv4 and IPv6 addresses.

nat66: Specifies the IPv6-to-IPv6 address translation rule.

after: Places the rule *rule-name1* after the rule *rule-name2* (called the reference rule).

before: Places the rule *rule-name1* before the reference rule.

rule-name2: Specifies the NAT rule as a reference rule. The rule name is a case-insensitive string of 1 to 63 characters. If you do not specify this argument, the priority of *rule-name1* changes as follows:

- If **after** is specified, the rule *rule-name1* will have the lowest priority.
- If **before** is specified, *rule-name1* will have the highest priority.

Usage guidelines

You can execute this command to rearrange only existing NAT rules to change their priority.

The rule type is optional in this command. Specify an exact rule type if you specify the **type** keyword.

When you rearrange global NAT rules to change their priority, make sure all NAT rules containing destination address translation methods are before the NAT rules containing only source address translation methods.

- Do not place a NAT rule containing a destination address translation method after a NAT rule containing only a source address translation method.
- Do not place a NAT rule containing only a source address translation method before a NAT rule containing a destination address translation method.

Examples

Place the NAT rule **aaa** before the NAT rule **bbb** in the global NAT policy.

```
<Sysname> system
[Sysname] nat global-policy
[Sysname-nat-global-policy] rule move aaa before bbb
```

Related commands

display nat all

display nat policy

rule name

Use **rule name** to create a NAT rule and enter NAT rule view, or enter the view of an existing NAT rule.

Use **undo rule name** to delete the specified NAT rule.

Syntax

Interface-based NAT policy view:

rule name *rule-name*

undo rule name *rule-name*

Global NAT policy view:

rule name *rule-name* [**type** { **nat** | **nat64** | **nat66** }]

undo rule name *rule-name*

Default

No NAT rule exists.

Views

Interface-based NAT policy view

Global NAT policy view

Predefined user roles

network-admin

context-admin

Parameters

rule-name: Specifies the name of the NAT rule. The rule name is a case-insensitive string of 1 to 63 characters. Valid characters cannot include hyphens (-) and percent signs (%). If you want to use a backslash (\) or a quotation mark ("), you must enter the escape character (\) before the backslash or the quotation mark. If you want to include spaces in the string, you must enclose the name string in quotation marks ("), for example, "XXX XXX".

type: Specifies the type of NAT rules in the global NAT policy. If you do not specify this keyword, the NAT rule type is NAT.

nat: Specifies the NAT-type rules in the global NAT policy, which are used for translation between IPv4 addresses.

nat64: Specifies the NAT64-type rules in the global NAT policy, which are used for translation between IPv4 addresses and IPv6 addresses.

nat66: Specifies the NAT66-type rules in the global NAT policy, which are used for translation between IPv6 addresses or translation between IPv6 prefixes.

Usage guidelines

When you create, move, or modify the type of a NAT rule, follow these restrictions and guidelines:

- In a NAT policy, the priority of NAT rules are determined by the configuration order. A rule configured earlier has a higher priority. You can use the **rule move** command to rearrange the NAT rules. To view the priority order of the NAT rules in a policy, use the **display nat policy** command.
- You cannot repeatedly execute the **rule name** *rule-name* **type** command to modify the type of a NAT rule. To modify the type of a NAT rule, first use the **undo rule name** command to delete the NAT rule, and then execute the **rule name** *rule-name* **type** command to create a NAT rule.
- The interface-based NAT policy supports a maximum of 4096 NAT rules. The global NAT policy supports a maximum of 10000 NAT rules.

Examples

In the interface-based NAT policy, create a NAT rule named **aaa** and enter its view.

```
<Sysname> system
[Sysname] nat policy
[Sysname-nat-policy] rule name aaa
[Sysname-nat-policy-rule-aaa]
```

In the global NAT policy, create a NAT rule named **aaa** and enter its view.

```
<Sysname> system
[Sysname] nat global-policy
[Sysname-nat-global-policy] rule name aaa
[Sysname-nat-global-policy-rule-aaa]
```

Related commands

display nat all

display nat global-policy

display nat policy

rule move

service

Use **service** to specify a service object group for the NAT rule.

Use **undo service** to delete a service object group from a NAT rule.

Syntax

service *object-group-name*

undo service [*object-group-name*]

Default

No service object group is specified for a NAT rule.

Views

NAT rule view

Predefined user roles

network-admin

context-admin

Parameters

object-group-name: Specifies the name of a service object group. The name is a case-insensitive string of 1 to 31 characters, and it cannot be **any**. If spaces are included in the name, enclose the name in quotation marks ("), for example, "XXX XXX".

Usage guidelines

The NAT device uses the services specified in this command to identify matching packets. Only packets with the matching services are translated.

To translate source IP addresses of outgoing packets, use this command with the **action snat** command. To translate both the source IP address and destination IP address of incoming packets, use this command together with the **action snat** and **action dnat** commands.

The service object group must already exist.

If you do not specify a service object group in the **undo service** command, the command deletes all service object groups in the NAT rule.

A NAT rule can have a maximum of 256 service object groups.

Examples

In the interface-based policy, specify NAT rule **aaa** to use **service1**, **service2**, and **service3** as the service object groups.

```
<Sysname> system
[Sysname] nat policy
[Sysname-nat-policy] rule name aaa
[Sysname-nat-policy-rule-aaa] service service1
[Sysname-nat-policy-rule-aaa] service service2
[Sysname-nat-policy-rule-aaa] service service3
```

In the global NAT policy, specify NAT rule **aaa** to use **service1**, **service2**, and **service3** as the service object groups.

```
<Sysname> system
[Sysname] nat global-policy
[Sysname-nat-global-policy] rule name aaa
[Sysname-nat-global-policy-rule-aaa] service service1
[Sysname-nat-global-policy-rule-aaa] service service2
[Sysname-nat-global-policy-rule-aaa] service service3
```

Related commands

display nat all

display nat global-policy

display nat policy

object-group (*Security Command Reference*)

source-ip

Use **source-ip** to specify a source IP address match criterion for a NAT rule.

Use **undo source-ip** to delete a source IP address match criterion from a NAT rule.

Syntax

NAT-type rule view in the interface-based NAT policy:

source-ip *ipv4-object-group-name*

undo source-ip [*ipv4-object-group-name*]

NAT-type rule view in the global NAT policy:

source-ip { **host** *ip-address* | **subnet** *subnet-ip-address mask-length* }

undo source-ip { **host** [*ip-address*] | **subnet** [*subnet-ip-address mask-length*] }

NAT64-type rule view in the global NAT policy:

source-ip { *ipv4-object-group-name* | *ipv6-object-group-name* }

undo source-ip [*ipv4-object-group-name* | *ipv6-object-group-name*]

source-ip { **host** { *ipv4-address* | *ipv6-address* } | **subnet** { *subnet-ipv4-address mask-length* | *ipv6-prefix prefix-length* } }

undo source-ip { **host** [*ipv4-address* | *ipv6-address*] | **subnet** [*ipv4-address mask-length* | *ipv6-prefix prefix-length*] }

NAT66-type rule view in the global NAT policy:

source-ip *ipv6-object-group-name*

undo source-ip [*ipv6-object-group-name*]

source-ip { **host** *ipv6-address* | **subnet** *ipv6-prefix prefix-length* }

undo source-ip { **host** *ipv6-address* | **subnet** *ipv6-prefix prefix-length* }

Default

A NAT rule does not have any source IP address match criteria.

Views

NAT rule view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-object-group-name: Specifies the name of a source IPv4 address object group. The name is a case-insensitive string of 1 to 63 characters, and it cannot be **any**. If spaces are included in the name, enclose the name in quotation marks ("), for example, "XXX XXX".

ipv6-object-group-name: Specifies the name of a source IPv6 address object group. The name is a case-insensitive string of 1 to 63 characters, and it cannot be **any**. If spaces are included in the name, enclose the name in quotation marks ("), for example, "XXX XXX".

host *ipv4-address*: Specifies an IPv4 address to match source IPv4 address. The IPv4 address cannot be an all-zero address, all-one address, Class D address, Class E address, or loopback address.

host *ipv6-address*: Specifies an IPv6 address to match source IPv6 address.

subnet *subnet-ipv4-address mask-length*: Specifies a subnet to match source IPv4 addresses. The *subnet-ipv4-address* argument specifies the subnet address. The *mask-length* argument specifies the mask length, which can be 8, 16, or an integer in the range of 24 to 31.

subnet *ipv6-prefix prefix-length*: Specifies an IPv6 prefix for a NAT rule. The *ipv6-prefix* argument indicates an IPv6 prefix. The *prefix-length* argument indicates the prefix length in the range of 1 to 128.

Usage guidelines

The NAT device uses the source IP addresses specified in this command to identify matching packets. Only packets with the matching source IP addresses are translated.

When you reference an address object group, follow these restrictions and guidelines:

- The address object group must already exist.
- For an address object group to be successfully referenced by the source address translation method, make sure the objects in the referenced address object group are created through the following methods:
  - [*object-id*] **network host address** *ip-address*
  - [*object-id*] **network subnet** *ip-address* { *mask-length* | *mask* }
  - [*object-id*] **network range** *ip-address1 ip-address2*

  For more information about these commands, see object group commands in *Security Command Reference*.

If you do not specify any parameters in the **undo source-ip** command, the command deletes all source address match criteria in the NAT rule.

When you configure match criteria for a NAT rule, follow these restrictions and guidelines:

- A NAT rule can have a maximum of 256 source address object groups.
- If you configure multiple packet match criteria in a NAT64-type rule, the IP address type in the later configured packet match criteria must be the same as that in the earlier configured packet match criteria. For example, if you first execute the **source-ip host 192.168.1.1** command, the **source-ip host 100::1** command executed later does not take effect. Select an IP type as needed.
- If you execute the following commands in the same NAT rule, the most recent configuration takes effect:
  - **source-ip**
  - **source-ip host**
  - **source-ip subnet**

Examples

In the interface-based NAT policy, configure NAT rule **aaa** to use source address object groups **desIP1**, **desIP2**, and **desIP3** as the packet match criteria.

```
<Sysname> system
[Sysname] nat policy
[Sysname-nat-policy] rule name aaa
[Sysname-nat-policy-rule-aaa] source-ip srcip1
[Sysname-nat-policy-rule-aaa] source-ip srcip2
[Sysname-nat-policy-rule-aaa] source-ip srcip3
```

In the global NAT policy, configure NAT rule **aaa** to use source address object groups **desIP1**, **desIP2**, and **desIP3** as the packet match criteria.

```
<Sysname> system
```

```
[Sysname] nat global-policy
[Sysname-nat-global-policy] rule name aaa
[Sysname-nat-global-policy-rule-aaa] source-ip srcip1
[Sysname-nat-global-policy -rule-aaa] source-ip srcip2
[Sysname-nat-global-policy -rule-aaa] source-ip srcip3
```

Related commands

display nat all

display nat global-policy

display nat policy

object-group *(Security Command Reference)*

source-zone

Use **source-zone** to specify a source security zone in a NAT rule.

Use **undo source-zone** to delete a source security zone from a NAT rule.

Syntax

source-zone *source-zone-name*

undo source-zone [*source-zone-name*]

Default

No source security zones are specified in a NAT rule.

Views

NAT rule view

Predefined user roles

network-admin

context-admin

Parameters

source-zone-name: Specifies the name of a source security zone. The name is a case-insensitive string of 1 to 31 characters, and it cannot be **any**. You can specify a nonexistent security zone. This command takes effect after you use the **security-zone name** command to create the security zone. For more information about security zones, see *Security Configuration Guide*.

Usage guidelines

The NAT device uses the source security zones specified in this command to identify matching packets. Only packets with the matching source security zones are translated.

To translate source IP addresses of outgoing packets, use this command with the **action snat** command. To translate both the source IP address and destination IP address of incoming packets, use this command together with the **action snat** and **action dnat** commands.

This command does not support modifying source security zones. To modify the source security zone for a NAT rule, first execute the **undo destination-zone** command to delete the zone, and then execute the **destination-zone** command to specify a new one.

If you do not specify a source security zone in the **undo source-zone** command, the command deletes all source security zones in the NAT rule.

This command is available only in NAT rule view of the global NAT policy.

A NAT rule can have a maximum of 16 source security zones.

Examples

Specify source security zone **trust** for NAT rule **rule1**.

```
<Sysname> system-view
[Sysname] nat global-policy
[Sysname-nat-global-policy] rule name rule1
[Sysname-nat-global-policy-rule-rule1] source-zone trust
```

Related commands

security-zone name (*Security Command Reference*)

vrf

Use **vrf** to specify a VPN instance in a NAT rule.

Use **undo vrf** to delete a VPN instance from a NAT rule.

Syntax

vrf *vrf-name*

undo vrf *vrf-name*

Default

No VPN instances are specified in a NAT rule.

Views

NAT rule view

Predefined user roles

network-admin

context-admin

Parameters

vrf-name: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

If you use this command together with the **action snat** command, it works as follows:

1. The NAT device uses the VPN instance to which the packet belongs to identify matching packets. Only packets with the matching VPN instances are translated. The NAT device records the VPN information in the mapping entry.
2. When the server in the external network replies to the internal host, the NAT device translates addresses according to the mapping entry and forwards the packets after source address translation to the internal host.

If you use this command together with the **action dnat** command, it works as follows:

1. The NAT device uses the VPN instance to which the packet belongs to identify matching packets. Only packets with the matching VPN instances are translated. The NAT device records the VPN information in the mapping entry.
2. When the internal server replies to the host in the external network, the NAT device translates addresses according to the mapping entry and forwards the packets after destination address translation to the host.

This command is available only in NAT rule view of the global NAT policy.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify VPN instance **vpn1** for NAT rule **rule1**.

```
<sysname> system-view
[sysname] nat global-policy
[sysname-nat-global-policy] rule name rule1
[sysname-nat-global-policy-rule-rule1] vrf vpn1
```

Related commands

action dnat

action snat

vrrp vrid (interface-based NAT)

Use **vrrp vrid** to bind a VRRP group to a NAT address group or a NAT port block group.

Use **undo vrrp vrid** to restore the default.

Syntax

vrrp vrid *virtual-router-id*

undo vrrp vrid

Default

A NAT address group or a NAT port block group is not bound to any VRRP group.

Views

NAT address group view

NAT port block group view

Predefined user roles

network-admin

context-admin

Parameters

virtual-router-id: Specifies a VRRP group by its virtual router ID in the range of 1 to 255.

Usage guidelines

In a hot backup system collaborating with VRRP, source address translation that uses a NAT address group or port block group assigns the public IP address after translation to the address management module. Both the active and standby devices advertise the mappings between the public IP address and MAC addresses of their own physical interfaces to all nodes in the same LAN. As a result, the uplink Layer 3 device directly connected to the hot backup system might send downlink packets to the backup device, causing service anomalies.

To avoid such an issue, bind the NAT address group or port block group to a VRRP group. Then, only the master device responds to ARP requests with the virtual MAC address of the VRRP group. The uplink Layer 3 device directly connected to the hot backup system sends downlink packets only to the master device.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Bind VRRP group **1** to NAT address group **2**.

```
<Sysname> system-view
```

```
[Sysname] nat address-group 2
[Sysname-address-group-2] vrrp vrid 1
```

Related commands

display nat address-group

display nat port-block-group

nat address-group

nat port-block-group

vrrp vrid (*High Availability Command Reference*)

Contents

NAT66 commands

display nat66 all

Use **display nat66 all** to display all NAT66 configurations.

Syntax

display nat66 all

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display all NAT66 configurations.

```
<Sysname> display nat66 all
NAT66 source information:
  Totally 1 source rules.
  Interface(outbound): GigabitEthernet1/0/1
    Original prefix/prefix-length: 11::/64
    Translated prefix/prefix-length: 22::/64

NAT66 destination information:
  Totally 1 destination rules.
  Interface(inbound): GigabitEthernet1/0/2
    Original prefix/prefix-length: FD01:203:405::/48
    Translated prefix/prefix-length: 1::/48
```

Table 1 Command output

Field	Description
NAT66 source information	Configuration information about NAT66 source address translation.
NAT66 destination information	Configuration information about NAT66 destination address translation.
Totally *n* source rules	Total number of source address translation rules.
Totally *n* destination rules	Total number of destination address translation rules.
Interface(outbound)	Interface configured with NAT66 source address translation rules.
Interface(inbound)	Interface configured with NAT66 destination address translation rules.
Original prefix/prefix-length	Prefix and prefix length before NAT66 translation.
Translated prefix/prefix-length	Prefix and prefix length after NAT66 translation.

Related commands

nat66 prefix destination

nat66 prefix source

display nat66 session

Use **display nat66 session** to display NAT66 sessions.

Syntax

display nat66 session [**slot** *slot-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays NAT66 sessions for all member devices.

verbose: Displays detailed information about NAT66 sessions. If you do not specify this keyword, the command displays brief information about NAT66 sessions.

Usage guidelines

If you do not specify any parameters, this command displays brief information about all NAT66 sessions.

Examples

Display brief information about NAT66 sessions for the specified slot.

```
<Sysname> display nat66 session slot 1
Slot 1:
Initiator:
  Source      IP/port: FD01:203:405::1/4048
  Destination IP/port: 2001:DB8:1::100/21
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/2

Total sessions found: 1
```

Display detailed information about NAT66 sessions for the specified slot.

```
<Sysname> display nat session slot 1 verbose
Slot 1:
Initiator:
  Source      IP/port: FD01:203:405::1/4048
  Destination IP/port: 2001:DB8:1::100/21
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
```

```
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Trust
Responder:
  Source      IP/port: 2001:DB8:1::100/21
  Destination IP/port: 1:0:0:309::1/4048
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: Trust
State: TCP_ESTABLISHED
Application: FTP
Rule ID: -/-/-
Rule name:
Start time: 2018-12-10 09:19:28  TTL: 3585s
Initiator->Responder:            0 packets          0 bytes
Responder->Initiator:            0 packets          0 bytes

Total sessions found: 1
```

Table 2 Command output

Field	Description
Initiator	Session information about the initiator.
Responder	Session information about the responder.
Source IP/port	Source IPv6 address and port number.
Destination IP/port	Destination IPv6 address and port number.
VPN instance/VLAN ID/Inline ID	This field is not supported in the current software version. • **VPN instance**—MPLS L3VPN instance to which the session belongs. • **VLAN ID**—ID of the VLAN to which the session belongs for Layer 2 forwarding. • **Inline ID**—ID of the INLINE to which the session belongs for Layer 2 forwarding. If no settings are specified, this field displays slash-separated hyphens (***-/-/-***).
Protocol	Transport layer protocol type: **DCCP**, **ICMPv6**, **Raw IP**, **SCTP**, **TCP**, **UDP**, or **UDP-Lite**. The number after the protocol is the protocol number.
Inbound interface	Input interface.
Source security zone	Security zone to which the input interface belongs. If the input interface does not belong to any security zone, this field displays a hyphen (**-**).
State	NAT66 session state.
Application	Application layer protocol type, such as **FTP** and **DNS**. This field displays **OTHER** for the protocol types identified by non-well-known ports.
Rule ID	ID of the security policy rule.
Rule name	Name of the security policy rule.
Start time	Time when the session starts.
TTL	Remaining lifetime of the NAT66 session, in seconds.

Initiator->Responder	Number of packets and packet bytes from the initiator to the responder.
Responder->Initiator	Number of packets and packet bytes from the responder to the initiator.
Total sessions found	Total number of sessions.

Related commands

reset nat66 session

display nat66 statistics

Use **display nat66 statistics** to display NAT66 statistics.

Syntax

display nat66 statistics [**summary**] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

summary: Displays NAT66 statistics summary. If you do not specify this keyword, the command displays detailed NAT66 statistics.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays NAT66 statistics for all member devices.

Examples

Display detailed NAT66 statistics.

```
<Sysname> display nat66 statistics
Slot 1:
  Total session entries: 0
  Total outbound NO-PAT entries: 0
```

Table 3 Command output

Field	Description
Total session entries	Number of NAT66 session entries.
Total outbound NO-PAT entries	Number of NAT66 NO-PAT entries.

Display NAT66 statistics summary.

```
<Sysname> display nat66 statistics summary
Slot Sessions
1    100
```

Table 4 Command output

Field	Description
Sessions	Number of NAT66 session entries.

nat66 prefix destination

Use **nat66 prefix destination** to configure an IPv6 prefix mapping for IPv6 destination address translation.

Use **undo nat66 prefix destination** to remove an IPv6 prefix mapping for IPv6 destination address translation.

Syntax

nat66 prefix destination *original-ipv6-prefix prefix-length* [**protocol** *pro-type* [*global-port*]] *translated-ipv6-prefix prefix-length* [*local-port*]

undo nat66 prefix destination *original-ipv6-prefix prefix-length* [**protocol** *pro-type* [*global-port*]] *translated-ipv6-prefix prefix-length* [*local-port*]

Default

No IPv6 prefix mappings are configured for IPv6 destination address translation.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

original-ipv6-prefix: Specifies the original IPv6 prefix. For IPv6 destination address translation, specify the external prefix.

protocol *pro-type*: Specifies a protocol type. If you do not specify a protocol type, the command applies to packets of all protocols. The protocol type format can be one of the following:

- A number in the range of 1 to 255. The values 50 (ESP) and 51 (AH) are not supported.
- A protocol name of **ipv6-icmp**, **tcp**, or **udp**.

global-port: Specifies a public port number for the internal server, in the range of 1 to 65535. If you do not specify this argument, the translation will be performed no matter what the destination port number is. You can specify this argument only when the protocol type is TCP or UDP.

translated-ipv6-prefix: Specifies the translated IPv6 prefix. For IPv6 destination address translation, specify the internal prefix.

prefix-length: Specifies a prefix length, in the range of 1 to 128.

local-port: Specifies a private port number for the internal server, in the range of 1 to 65535. If you do not specify this argument, the value for this argument is the same as the value of the *global-port* argument. If you do not specify the *global-port* and *local-port* arguments, the port number is not translated. You can specify this argument only when the protocol type is TCP or UDP.

Usage guidelines

To allow external users to access internal servers (such as Web or FTP server), configure IPv6 destination prefix mappings on the interface connected to the external network.

When you configure IPv6 destination prefix mappings, follow these restrictions and guidelines:

- The prefix length before and after NAT66 must be the same.
- On one interface, the mapping between an external prefix and an internal prefix must be unique.
- On different interfaces, one external prefix cannot be mapped to different internal prefixes.
- The translated IPv6 prefix cannot be the same as the prefix of the public IPv6 address of the NAT66 device or the prefix of the IPv6 address of an external host.
- The command does not support modifying an existing IPv6 prefix mapping. To modify it, first execute the **undo nat66 prefix destination** command to remove the mapping, and then configure the new one.

This feature cannot perform translation on IPsec protected packets with encapsulated by ESP or AH.

Examples

On GigabitEthernet 1/0/1, configure an IPv6 destination prefix mapping to translate IPv6 prefix 2001::/64 to IPv6 prefix 2101::/64.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat66 prefix destination 2001:: 64 2101:: 64
```

On GigabitEthernet 1/0/1, configure an IPv6 destination prefix mapping to translate IPv6 prefix 2001::/64 and port 64 to IPv6 prefix 2101::/64 and port 200 for packets destined for the internal FTP server.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat66 prefix destination 2001:: 64 protocol tcp 100 2101:: 64 200
```

Related commands

display nat66 all

nat66 prefix source

Use **nat66 prefix source** to configure an IPv6 prefix mapping for IPv6 source address translation.

Use **undo nat66 prefix source** to remove an IPv6 prefix mapping for IPv6 source address translation.

Syntax

nat66 prefix source *original-ipv6-prefix prefix-length translated-ipv6-prefix prefix-length* [**pat**]

undo nat66 prefix source *original-ipv6-prefix prefix-length translated-ipv6-prefix prefix-length* [**pat**]

Default

No IPv6 prefix mappings are configured for IPv6 source address translation.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

original-ipv6-prefix: Specifies the original IPv6 prefix. For IPv6 source address translation, specify the internal prefix.

translated-ipv6-prefix: Specifies the translated IPv6 prefix. For IPv6 source address translation, specify the external prefix.

prefix-length: Specifies a prefix length, in the range of 1 to 128.

pat: Uses the PAT mode for address translation. In this mode, port information is translated. If you do not specify this keyword, the device does not translate port information.

Usage guidelines

NAT66 source address translation is applicable to the following scenarios:

- **Single internal and external network**—The NAT66 device is connected to an internal network and an external network. Hosts in the internal network uses locally routed IPv6 prefixes. When an internal host sends packets to access the external network, the NAT66 device translates the source IPv6 address prefix in the packets to a global unicast address prefix.
- **Redundancy and load sharing**—Multiple NAT66 devices are deployed between two IPv6 networks and they use ECMPs for load sharing. To allow any NAT66 device to process IPv6 traffic among different sites, configure the same source prefix mappings on these NAT66 devices.
- **Multihoming**—In a multihomed network, NAT66 devices are connected to an internal network and multiple external networks. One internal prefix is mapped to different external prefixes on the NAT66 devices, so that one internal address can be translated to multiple external addresses.

When you configure source prefix mappings, follow these restrictions and guidelines:

- Source prefix mappings are typically configured on the interface connected to the external network.
- The prefix length before and after NAT66 in a mapping must be the same if this mapping does not support port translation.
- On one interface, the mapping between an internal prefix and an external prefix must be unique.
- On different interfaces, different internal prefixes cannot be mapped to the same external prefix.
- The translated IPv6 prefix cannot be the same as the prefix of the public IPv6 address of the NAT66 device or the prefix of the destination public IPv6 address.
- The command does not support modifying an existing prefix mapping. To modify it, first execute the **undo nat66 prefix source** command to remove the mapping, and then configure the new one.

This feature cannot perform translation on IPsec protected packets with encapsulated by ESP or AH.

Examples

On GigabitEthernet 1/0/1, configure an IPv6 source prefix mapping to translate IPv6 prefix FD9C:58ED:7D73:2::/64 to 2101::/64.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat66 prefix source fd9C:58ed:7d73:2:: 64 2101:: 64
```

On GigabitEthernet 1/0/1, configure an IPv6 source prefix mapping in PAT mode to translate IPv6 prefix FD9C:58ED:7D73:2::/64 to 2101::/64.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat66 prefix source fd9C:58ed:7d73:2:: 64 2101:: 64 pat
```

Related commands

display nat66 all

reset nat66 session

Use **reset nat66 session** to delete NAT66 sessions.

Syntax

reset nat66 session [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command deletes NAT66 sessions for all member devices.

Examples

Delete NAT66 sessions for the specified slot.

```
<Sysname> reset nat66 session slot 1
```

Related commands

display nat66 session

Contents

AFT commands

address

Use **address** to add an address range to an AFT address group.

Use **address** to remove an address range from an AFT address group.

Syntax

address *start-address end-address*

undo address *start-address end-address*

Default

No address ranges exist.

Views

AFT address group view

Predefined user roles

network-admin

context-admin

Parameters

start-address end-address: Specifies the start and end IP addresses for an address range. The end address cannot be lower than the start address. If they are the same, the address range has only one IP address.

Usage guidelines

An AFT address group is a set of address ranges. Dynamic AFT translates an IPv6 address to an IPv4 address in one of the address ranges.

Each address range can contain a maximum of 256 addresses.

Make sure the address ranges do not overlap.

Examples

Add two address ranges to AFT address group 2.

```
<Sysname> system-view
[Sysname] aft address-group 2
[Sysname-aft-address-group-2] address 10.1.1.1 10.1.1.15
[Sysname-aft-address-group-2] address 10.1.1.20 10.1.1.30
```

Related commands

aft address-group

aft address-group

Use **aft address-group** to create an AFT address group and enter its view, or enter the view of an existing AFT address group.

Use **undo aft address-group** to delete an AFT address group.

Syntax

aft address-group *group-id*

undo aft address-group *group-id*

Default

No AFT address groups exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

group-id: Assigns an ID to the address group. The value range for this argument is 0 to 65535.

Usage guidelines

An AFT address group is a set of address ranges. Use the **address** command to add an address range.

The AFT address group is used in dynamic AFT. Dynamic AFT translates the source address of an IPv6 packet to an IPv4 address in the address group.

Examples

Create AFT address group 1 and enter its view.

```
<Sysname> system-view
[Sysname] aft address-group 1
[Sysname-aft-address-group-1]
```

Related commands

address

aft v6tov4 source

display aft address-group

display aft configuration

aft alg

Use **aft alg** to enable AFT ALG for the specified or all supported protocols.

Use **undo aft alg** to disable AFT ALG for the specified or all supported protocols.

Syntax

aft alg { **all** | **dns** | **ftp** | **http** | **icmp-error** }

undo aft alg { **all** | **dns** | **ftp** | **http** | **icmp-error** }

Default

AFT ALG is enabled for DNS, FTP, ICMP error messages, and HTTP.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

all: Enables AFT ALG for all supported protocols.

dns: Enables AFT ALG for DNS.

ftp: Enables AFT ALG for FTP.

http: Enables AFT ALG for HTTP.

icmp-error: Enables AFT ALG for ICMP error packets.

Usage guidelines

AFT ALG translates address or port information in the application layer payloads.

For example, an FTP application includes a data connection and a control connection. The IP address and port number for the data connection depend on the payload information of the control connection. This requires AFT ALG to translate the address and port information.

You can execute this command multiple times to enable AFT ALG for different protocols.

Examples

Enable AFT ALG for FTP.

```
<Sysname> system-view
[Sysname] aft alg ftp
```

Related commands

display aft configuration

aft enable

Use **aft enable** to enable AFT on an interface.

Use **undo aft enable** to disable AFT on an interface.

Syntax

aft enable

undo aft enable

Default

AFT is disabled on an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

You must enable AFT on interfaces connected to the IPv4 network and interfaces connected to the IPv6 network.

Examples

Enable AFT on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] aft enable
```

Related commands

display aft configuration

aft log enable

Use **aft log enable** to enable AFT logging.

Use **undo aft log enable** to disable AFT logging.

Syntax

aft log enable

undo aft log enable

Default

AFT logging is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

For security auditing, you can enable AFT logging to record AFT session information. An AFT session is a session whose source and destination IP addresses are translated by AFT.

AFT can log the following events:

- An AFT port block is created.
- An AFT port block is deleted.
- An AFT session is established.

  To log AFT session establishment events, you must also execute the **aft log flow-begin** command.
- An AFT session is removed.

  To log AFT session removal events, you must also execute the **aft log flow-end** command.

The logs are sent to the information center of the device. For the logs to be output correctly, you must also configure the information center on the device. For more information about information center configuration, see *Network Management and Monitoring Configuration Guide*.

Examples

Enable AFT logging.

```
<Sysname> system-view
[Sysname] aft log enable
```

Related commands

aft log flow-begin

aft log flow-end

display aft configuration

aft log flow-begin

Use **aft log flow-begin** to enable AFT session establishment logging.

Use **undo aft log flow-begin** to disable AFT session establishment logging.

Syntax

aft log flow-begin

undo aft log flow-begin

Default

AFT session establishment logging is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This feature enables the AFT module to generate a log entry for every AFT session establishment event.

AFT session establishment logging takes effect only after you enable AFT logging.

Examples

Enable AFT session establishment logging.

```
<Sysname> system-view
[Sysname] aft log flow-begin
```

Related commands

aft log enable

aft log flow-end

display aft configuration

aft log flow-end

Use **aft log flow-end** to enable AFT session removal logging.

Use **undo aft log flow-end** to disable AFT session removal logging.

Syntax

aft log flow-end

undo aft log flow-end

Default

AFT session removal logging is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This feature enables the AFT module to generate a log entry for every AFT session removal event.

AFT session removal logging takes effect only after you enable AFT logging.

Examples

Enable AFT session removal logging.

```
<Sysname> system-view
[Sysname] aft log flow-end
```

Related commands

aft log enable

aft log flow-begin

display aft configuration

aft port-load-balance enable

Use **aft port-load-balance enable** to enable AFT port halving.

Use **undo aft port-load-balance enable** to disable AFT port halving.

Syntax

aft port-load-balance enable slot *slot-number*

undo aft port-load-balance enable

Default

AFT port halving is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. This device will use the lower half of the port block.

Usage guidelines

AFT supports IRF hot backup in active/standby and dual-active mode. The AFT configuration for IRF hot backup depends on the deployment mode.

- In dual-active mode, if the two IRF member devices in an IRF fabric use the same AFT address group, the devices might map different IPv6 addresses and ports to the same IPv4 address and

port. To avoid this situation, enable AFT port halving on the devices. After you enable AFT port halving, each port block will be equally divided between the two devices. The two devices will use different ports to translate packets from different IP addresses, avoiding port assignment conflicts.

- You do not need to enable AFT port halving on the IRF member devices in active/standby mode.

This command is exclusive with the **aft remote-backup port-alloc** command.

Examples

Enable AFT port halving.

```
<Sysname> system-view
[Sysname] aft port-load-balance enable slot 1
```

Related commands

aft remote-backup port-alloc

aft prefix-general

Use **aft prefix-general** to configure a general prefix.

Use **undo aft prefix-general** to delete a general prefix.

Syntax

aft prefix-general *prefix-general prefix-length*

undo aft prefix-general *prefix-general prefix-length*

Default

No general prefixes exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

prefix-general: Specifies the general prefix.

prefix-length: Specifies the prefix length. The value for this argument can be 32, 40, 48, 56, 64, or 96.

Usage guidelines

A general prefix is an IPv6 address prefix of 32, 40, 48, 56, 64, or 96 bits. A general prefix can be used for source and destination address translation between IPv4 and IPv6.

When a general prefix is used alone, it provides IPv6-to-IPv4 source and destination address translation. If a source or destination IPv6 address matches the general prefix, AFT translates it to the embedded IPv4 address.

When a general prefix is used in the **aft v4tov6 source** or **aft v4tov6 destination** command, it provides IPv4-to-IPv6 source or destination address translation. If a source or destination IPv4 address matches the ACL, AFT constructs the IPv6 address by using the general prefix and the IPv4 address.

A general prefix cannot be on the same subnet as any interface on the device.

A general prefix must be different from a NAT64 prefix or an IVI prefix.

Examples

Specify **2000:db8e::** as a general prefix and set its prefix length to 32.

```
<Sysname> system-view
[Sysname] aft prefix-general 2000:db8e:: 32
```

Related commands

aft v4tov6 destination

aft v4tov6 source

display aft configuration

aft prefix-ivi

Use **aft prefix-ivi** to configure an IVI prefix.

Use **undo aft prefix-ivi** to delete an IVI prefix.

Syntax

aft prefix-ivi *prefix-ivi*

undo aft prefix-ivi *prefix-ivi*

Default

No IVI prefixes exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

prefix-ivi: Specifies an IVI prefix.

Usage guidelines

An IVI prefix is an IPv6 address prefix whose length is fixed at 32 bits. An IVI prefix can be used for IPv6-to-IPv4 source address translation and IPv4-to-IPv6 destination address translation.

When an IVI prefix is used alone, it provides IPv6-to-IPv4 source address translation. If a source IPv6 address matches the IVI prefix, AFT translates it to the embedded IPv4 address.

When an IVI prefix is used in the **aft v4tov6 destination** command, it provides IPv4-to-IPv6 destination address translation. If a destination IPv4 address matches the ACL, AFT constructs the IPv6 address by using the IVI prefix and the IPv4 address.

An IVI prefix must be different from a NAT64 prefix or a general prefix.

Examples

Specify **3000:db8e::** as an IVI prefix.

```
<Sysname> system-view
[Sysname] aft prefix-ivi 3000:db8e::
```

Related commands

aft v4tov6 destination

display aft configuration

aft prefix-nat64

Use **aft prefix-nat64** to configure a NAT64 prefix.

Use **undo aft prefix-nat64** to delete a NAT64 prefix.

Syntax

aft prefix-nat64 *prefix-nat64 prefix-length*

undo aft prefix-nat64 *prefix-nat64 prefix-length*

Default

No NAT64 prefixes exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

prefix-nat64: Specifies a NAT64 prefix.

prefix-length: Specifies the NAT64 prefix length. The value for this argument can be 32, 40, 48, 56, 64, or 96.

Usage guidelines

A NAT64 prefix is an IPv6 address prefix of 32, 40, 48, 56, 64, or 96 bits. A NAT64 prefix can be used for IPv4-to-IPv6 source address translation and IPv6-to-IPv4 destination address translation.

When a NAT64 prefix is used alone, it provides IPv6-to-IPv4 destination address translation. If a destination IPv6 address matches the NAT64 prefix, AFT translates it to the embedded IPv4 address.

When a NAT64 prefix is used alone or in the **aft v4tov6 source** command, it also provides IPv4-to-IPv6 source address translation. AFT constructs the IPv6 address by using the NAT64 prefix and the source IPv4 address. If the NAT64 prefix is used in the **aft v4tov6 source** command, AFT only translates packets permitted by the ACL.

To configure a 96-bit NAT64 prefix, make sure bits 64 through 71 are all 0. Otherwise, the configuration cannot be deployed.

A NAT64 prefix cannot be on the same subnet as any of the interfaces on the device.

A NAT64 prefix must be different from an IVI prefix or a general prefix.

Examples

Specify **2000:db8e::** as a NAT64 prefix and set its prefix length to 32.

```
<Sysname> system-view
[Sysname] aft prefix-nat64 2000:db8e:: 32
```

Related commands

aft v4tov6 source

display aft configuration

aft remote-backup port-alloc

Use **aft remote-backup port-alloc** to specify AFT port ranges for the two devices in the HA group.

Use **undo remote-backup port-alloc** to restore the default.

Syntax

aft remote-backup port-alloc { **primary** | **secondary** }

undo aft remote-backup port-alloc

Default

The two devices in the HA group share AFT port resources.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

primary: Specifies the lower half of the port block.

secondary: Specifies the higher half of the port block.

Usage guidelines

In the HA group in dual-active mode, different IP+port combinations on the two devices might be translated to the same AFT IP+port resources due to the following reasons:

- The two devices in the HA group share AFT addresses.
- The same AFT port range is assigned to each device.

To avoid this situation, execute this command on the primary device to equally divide the port resources for the two devices. Executing the command on the primary device also makes the remaining half of the port block be automatically assigned to the secondary device. For example, if you execute the **ft remote-backup port-alloc secondary** command on the primary device, the **aft remote-backup port-alloc primary** command is automatically executed on the secondary device. For more information about configuring the HA group, see *High Availability Configuration Guide*.

You do not need to execute this command for the HA group in active/standby mode. No port conflict exists in active/standby mode because only one device processes AFT services.

This command is exclusive with the **aft port-load-balance enable** command.

Examples

Specify the primary device in the HA group to use the lower half of the port block.

```
<Sysname> system-view
[Sysname] aft remote-backup port-alloc primary
```

Related commands

aft port-load-balance enable

aft turn-off tos

Use **aft turn-off tos** to set the ToS field to 0 for IPv4 packets translated from IPv6 packets.

Use **undo aft turn-off tos** to restore the default.

Syntax

aft turn-off tos

undo aft turn-off tos

Default

The ToS field value of translated IPv4 packets is the same as the Traffic Class field value of original IPv6 packets.

Views

System view

Predefined user roles

network-admin

context-admin

Examples

Set the ToS field to **0** for IPv4 packets translated from IPv6 packets.

```
<Sysname> system-view
[Sysname] aft turn-off tos
```

aft turn-off traffic-class

Use **aft turn-off traffic-class** to set the Traffic Class field to 0 for IPv6 packets translated from IPv4 packets.

Use **undo aft turn-off traffic-class** to restore the default.

Syntax

aft turn-off traffic-class

undo aft turn-off traffic-class

Default

The Traffic Class field value of translated IPv6 packets is the same as the ToS field value of original IPv4 packets.

Views

System view

Predefined user roles

network-admin

context-admin

Examples

Set the Traffic Class field to **0** for IPv6 packets translated from IPv4 packets.

```
<Sysname> system-view
[Sysname] aft turn-off traffic-class
```

aft v4server

Use **aft v4server** to configure an AFT mapping for an IPv4 internal server.

Use **undo aft v4server** to delete an AFT mapping for an IPv4 internal server.

Syntax

aft v4server protocol *protocol-type ipv6-destination-address ipv6-port-number* [**vpn-instance** *ipv6-vpn-instance-name*] *ipv4-destination-address ipv4-port-number* [**vpn-instance** *ipv4-vpn-instance-name*] [**vrrp** *virtual-router-id*]

undo aft v4server protocol { **tcp** | **udp** } *ipv6-destination-address ipv6-port-number* [**vpn-instance** *ipv6-vpn-instance-name*]

Default

No AFT mapping for an IPv4 internal server is configured.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

protocol *protocol-type*: Specifies a transport layer protocol by its type. The *protocol-type* argument can be **tcp** or **udp**.

ipv6-destination-address: Specifies an IPv6 address.

ipv6-port-number: Specifies an IPv6 port number in the range of 1 to 65535.

vpn-instance *ipv6-vpn-instance-name*: Specifies an IPv6 MPLS L3VPN instance to which the IPv6 address belongs. The *ipv6-vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the IPv6 address belongs to the public network, do not specify this option.

ipv4-destination-address: Specifies an IPv4 address.

ipv4-port-number: Specifies an IPv4 port number in the range of 1 to 65535.

vpn-instance *ipv4-vpn-instance-name*: Specifies an IPv4 MPLS L3VPN instance to which the IPv4 address belongs. The *ipv4-vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the IPv4 address belongs to the public network, do not specify this option.

vrrp *virtual-router-id*: Binds the IPv4 server to a VRRP group on the IPv6 network. The *virtual-router-id* parameter represents the virtual router ID of the VRRP group, in the range of 1 to 255.

Usage guidelines

This command maps the IPv4 address and port number of an IPv4 server to an IPv6 address and port number. IPv6 hosts can use the IPv6 address and port number to access the services provided by the IPv4 server.

In an HA hot backup network, execute this command on the primary device to bind an AFT IPv4 server to an HA-associated VRRP group on the IPv6 network. If you fail to do so, ARP might fail to resolve an IPv4-mapped IPv6 address into a correct MAC address.

An IPv4 server can be bound to only one VRRP group. You can execute this command multiple times to change the bound VRRP group for the IPv4 server.

The AFT mappings for different IPv4 internal servers cannot be the same.

Examples

Map IPv4 address **2.2.2.123** and port number **1720** of an IPv4 internal server to IPv6 address **3001::5** and port number **1720** for TCP packets.

```
<Sysname> system-view
[Sysname] aft v4server protocol tcp 3001::5 1720 2.2.2.123 1720
```

aft v4tov6 destination

Use **aft v4tov6 destination** to configure an IPv4-to-IPv6 destination address translation policy.

Use **undo aft v4tov6 destination** to delete an IPv4-to-IPv6 destination address translation policy.

Syntax

aft v4tov6 destination acl { **name** *ipv4-acl-name* **prefix-ivi** *prefix-ivi* [**vpn-instance** *ipv6-vpn-instance-name*] | **number** *ipv4-acl-number* { **prefix-general** *prefix-general prefix-length* | **prefix-ivi** *prefix-ivi* [**vpn-instance** *ipv6-vpn-instance-name*] } }

undo aft v4tov6 destination acl { **name** *ipv4-acl-name* | **number** *ipv4-acl-number* }

Default

No IPv4-to-IPv6 destination address translation policies exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

acl: Identifies IPv4 packets for address translation. AFT translates destination addresses for IPv4 packets permitted by the ACL.

name *ipv4-acl-name*: Specifies an IPv4 ACL by its name. The *ipv4-acl-name* argument is a case-insensitive string of 1 to 63 characters. It must start with an English letter and to avoid confusion, it cannot be **all**.

number *ipv4-acl-number*: Specifies an IPv4 ACL by its number in the range of 2000 to 3999.

prefix-general *prefix-general prefix-length*: Specifies a general prefix and its prefix length. The value for the *prefix-length* argument can be 32, 40, 48, 56, 64, or 96. AFT uses the general prefix to translate destination addresses for packets permitted by the ACL.

prefix-ivi *prefix-ivi*: Specifies an IVI prefix. AFT uses the IVI prefix to translate destination addresses for packets permitted by the ACL.

vpn-instance *ipv6-vpn-instance-name*: Specifies an IPv6 MPLS L3VPN instance to which translated IPv6 addresses belong. The *ipv6-vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the IPv6 addresses belong to the public network, do not specify this option.

Usage guidelines

You must specify different ACLs for different IPv4-to-IPv6 destination address translation policies.

You can specify a nonexistent IVI prefix or general prefix in a policy, but the policy takes effect only after you configure the prefix.

Examples

Configure the device to use IVI prefix **3000:db8e::** to translate IPv4 destination addresses to IPv6 addresses for IPv4 packets permitted by ACL 2000.

```
<Sysname> system-view
[Sysname] aft prefix-ivi 3000:db8e::
[Sysname] aft v4tov6 destination acl number 2000 prefix-ivi 3000:db8e::
```

Configure the device to use general prefix **2000:db8e::/32** to translate IPv4 destination addresses to IPv6 addresses for IPv4 packets permitted by ACL 2000.

```
<Sysname> system-view
[Sysname] aft v4tov6 destination acl number 2000 prefix-general 2000:db8e:: 32
```

Related commands

aft prefix-general

aft prefix-ivi

display aft configuration

aft v4tov6 source

Use **aft v4tov6 source** to configure an IPv4-to-IPv6 source address translation policy.

Use **undo aft v4tov6 source** to delete an IPv4-to-IPv6 source address translation policy.

Syntax

IPv4-to-IPv6 source address static mapping:

aft v4tov6 source *ipv4-address* [**vpn-instance** *ipv4-vpn-instance-name*] *ipv6-address* [**vpn-instance** *ipv6-vpn-instance-name*] [**vrrp** *virtual-router-id*]

undo aft v4tov6 source *ipv4-address* [**vpn-instance** *ipv4-vpn-instance-name*]

IPv4-to-IPv6 source address translation policy using a NAT64 prefix or general prefix:

aft v4tov6 source acl { **name** *ipv4-acl-name* **prefix-nat64** *prefix-nat64 prefix-length* [**vpn-instance** *ipv6-vpn-instance-name*] | **number** *ipv4-acl-number* { **prefix-general** *prefix-general prefix-length* | **prefix-nat64** *prefix-nat64 prefix-length* [**vpn-instance** *ipv6-vpn-instance-name*] } }

undo aft v4tov6 source acl { **name** *ipv4-acl-name* | **number** *ipv4-acl-number* }

Default

No IPv4-to-IPv6 source address translation policies exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-address: Specifies an IPv4 address.

vpn-instance *ipv4-vpn-instance-name*: Specifies an IPv4 MPLS L3VPN instance to which the IPv4 address belongs. The *ipv4-vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the IPv4 address belongs to the public network, do not specify this option.

ipv6-address: Specifies an IPv6 address. The IPv6 address in a static mapping cannot be on the same subnet as any interface on the device.

vpn-instance *ipv6-vpn-instance-name*: Specifies an IPv6 MPLS L3VPN instance to which the IPv6 address belongs. The *ipv6-vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the IPv6 address belongs to the public network, do not specify this option.

acl: Identifies IPv4 packets for address translation. AFT translates source addresses for packets permitted by the ACL.

name *ipv4-acl-name*: Specifies an IPv4 ACL by its name. The *ipv4-acl-name* argument is a case-insensitive string of 1 to 63 characters. It must start with an English letter and to avoid confusion, it cannot be **all**.

number *ipv4-acl-number*: Specifies an IPv4 ACL by its number in the range of 2000 to 3999.

prefix-general*prefix-general prefix-length*: Specifies a general prefix and its prefix length. The value for the *prefix-length* argument can be 32, 40, 48, 56, 64, or 96. AFT uses the general prefix to translate source IPv4 address for packets permitted by the ACL.

prefix-nat64 *prefix-nat64 prefix-length*: Specifies a NAT64 prefix and its prefix length. The value for the *prefix-length* argument can be 32, 40, 48, 56, 64, or 96. AFT uses the NAT64 prefix to translate source IPv4 address for packets permitted by the ACL.

vrrp *virtual-router-id*: Binds the IPv4-to-IPv6 source address translation policy to a VRRP group on the IPv6 network. The *virtual-router-id* parameter represents the virtual router ID of the VRRP group, in the range of 1 to 255.

Usage guidelines

In an HA hot backup network, execute this command on the primary device to bind an IPv4-to-IPv6 source address translation policy to an HA-associated VRRP group on the IPv6 network. If you do not do so, ARP might fail to resolve an IPv4-mapped IPv6 address into a correct MAC address.

An IPv4-to-IPv6 source address translation policy can be bound to only one VRRP group. You can execute this command multiple times to change the bound VRRP group for the policy.

The IPv4 or IPv6 addresses in different static mappings cannot be the same.

You must specify different ACLs for IPv4-to-IPv6 source address translation policies that use NAT64 prefixes or general prefixes.

You can specify a nonexistent NAT64 prefix or general prefix in a policy, but the policy takes effect only after you configure the prefix.

Examples

Map IPv4 source address **2.2.2.123** to IPv6 source address **3001::5**.

```
<Sysname> system-view
[Sysname] aft v4tov6 source 2.2.2.123 3001::5
```

Configure the device to use NAT64 prefix **2000::/32** to translate IPv4 source addresses to IPv6 addresses for IPv4 packets permitted by ACL 2000.

```
<Sysname> system-view
[Sysname] aft prefix-nat64 2000:: 32
```

```
[Sysname] aft v4tov6 source acl number 2000 prefix-nat64 2000:: 32
```

Configure the device to use general prefix **3000::/32** to translate IPv4 source addresses to IPv6 addresses for IPv4 packets permitted by ACL 2000.

```
<Sysname> system-view
[Sysname] aft v4tov6 source acl number 2000 prefix-general 3000:: 32
```

Related commands

aft prefix-general

aft prefix-nat64

display aft configuration

aft v6server

Use **aft v6server** to configure an AFT mapping for an IPv6 internal server.

Use **undo aft v6server** to delete an AFT mapping for an IPv6 internal server.

Syntax

aft v6server protocol *protocol-type ipv4-destination-address ipv4-port-number* [**vpn-instance** *ipv4-vpn-instance-name*] *ipv6-destination-address ipv6-port-number* [**vpn-instance** *ipv6-vpn-instance-name*] [**vrrp** *virtual-router-id*]

undo aft v6server protocol *protocol-type ipv4-destination-address ipv4-port-number* [**vpn-instance** *ipv4-vpn-instance-name*]

Default

The IPv6 internal server does not have an AFT mapping.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

protocol *protocol-type*: Specifies a transport layer protocol by its type. The *protocol-type* argument can be **tcp** or **udp**.

ipv4-destination-address: Specifies an IPv4 address.

ipv4-port-number: Specifies an IPv4 port number in the range of 1 to 65535.

vpn-instance *ipv4-vpn-instance-name*: Specifies an IPv4 MPLS L3VPN instance to which the IPv4 address belongs. The *ipv4-vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the IPv4 address belongs to the public network, do not specify this option.

ipv6-destination-address: Specifies an IPv6 address.

ipv6-port-number: Specifies an IPv6 port number in the range of 1 to 65535.

vpn-instance *ipv6-vpn-instance-name*: Specifies an IPv6 MPLS L3VPN instance to which the IPv6 address belongs. The *ipv6-vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the IPv6 address belongs to the public network, do not specify this option.

vrrp *virtual-router-id*: Binds the IPv6 server to a VRRP group on the IPv4 network. The *virtual-router-id* parameter represents the virtual router ID of the VRRP group, in the range of 1 to 255.

Usage guidelines

This command maps the IPv6 address and port number of an IPv6 server to an IPv4 address and port number.

In an HA hot backup network, execute this command on the primary device to bind an AFT IPv6 server to an HA-associated VRRP group on the IPv4 network. If you do not do so, ARP might fail to resolve an IPv6-mapped IPv4 address into a correct MAC address.

The AFT mappings for different IPv6 internal servers cannot be the same.

Examples

Map IPv6 address **3001::5** and port number **1720** of an IPv6 internal server to IPv4 address **2.2.2.123** and port number **1720** for TCP packets.

```
<Sysname> system-view
[Sysname] aft v6server protocol tcp 2.2.2.123 1720 3001::5 1720
```

Related commands

display aft configuration

aft v6tov4 source

Use **aft v6tov4 source** to configure an IPv6-to-IPv4 source address translation policy.

Use **undo aft v6tov4 source** to delete an IPv6-to-IPv4 source address translation policy.

Syntax

IPv6-to-IPv4 source address static mapping:

aft v6tov4 source *ipv6-address* [**vpn-instance** *ipv6-vpn-instance-name*] *ipv4-address* [**vpn-instance** *ipv4-vpn-instance-name*] [**vrrp** *virtual-router-id*]

undo aft v6tov4 source *ipv6-address* [**vpn-instance** *ipv6-vpn-instance-name*]

IPv6-to-IPv4 source address translation policy:

aft v6tov4 source { **acl ipv6** { **name** *ipv6-acl-name* | **number** *ipv6-acl-number* } | **prefix-nat64** *prefix-nat64 prefix-length* [**vpn-instance** *ipv6-vpn-instance-name*] } { **address-group** *group-id* [**no-pat** | **port-block-size** *blocksize*] | **interface** *interface-type interface-number* } [**vpn-instance** *ipv4-vpn-instance-name*]

undo aft v6tov4 source { **acl ipv6** { **name** *ipv6-acl-name* | **number** *ipv6-acl-number* } | **prefix-nat64** *prefix-nat64 prefix-length* [**vpn-instance** *ipv6-vpn-instance-name*] }

Default

No IPv6-to-IPv4 source address translation policies exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address: Specifies an IPv6 address.

vpn-instance *ipv6-vpn-instance-name*: Specifies an IPv6 MPLS L3VPN instance to which the IPv6 address belongs. The *ipv6-vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the IPv6 address belongs to the public network, do not specify this option.

ipv4-address: Specifies an IPv4 address.

vpn-instance *ipv4-vpn-instance-name*: Specifies an IPv4 MPLS L3VPN instance to which the IPv4 address belongs. The *ipv4-vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the IPv4 address belongs to the public network, do not specify this option.

vrrp *virtual-router-id*: Binds the IPv6-to-IPv4 source address translation policy to a VRRP group on the IPv4 network. The *virtual-router-id* parameter represents the virtual router ID of the VRRP group, in the range of 1 to 255.

acl ipv6: Identifies IPv6 packets for address translation. AFT translates source addresses for IPv6 packets permitted by the ACL.

name *ipv6-acl-name*: Specifies an IPv6 ACL by its name. The *ipv6-acl-name* argument is a case-insensitive string of 1 to 63 characters. It must start with an English letter and to avoid confusion, it cannot be **all**.

number *ipv6-acl-number*: Specifies an IPv6 ACL by its number in the range of 2000 to 3999.

prefix-nat64 *prefix-nat64 prefix-length*: Specifies a NAT64 prefix and its prefix length. The *prefix-length* argument represents a prefix length, which can be 32, 40, 48, 56, 64, or 96. AFT translates source IPv6 addresses for packets whose destination IPv6 addresses match the NAT64 prefix.

address-group *group-id*: Specifies an AFT address group by its ID in the range of 0 to 65535.

no-pat: Specifies the NO-PAT mode. If you do not specify the keyword, AFT uses the PAT mode.

port-block-size *blocksize*: Specifies the port block size in the range of 100 to 64512. If you do not specify the option, the port range will not be divided.

interface *interface-type interface-number*: Specifies an interface by its type and number. AFT translates source IPv6 addresses to the primary IPv4 address of the specified interface.

Usage guidelines

If you set a port block size, the port range (1024 to 65535) will be divided into port blocks by the port block size. For example, if you set the port block size to 1000, the port range is divided into port blocks 1024 to 2023, 2024 to 3023, and so on. The port blocks are used for PAT.

The IPv4 or IPv6 addresses in different static mappings cannot be the same.

You must specify different ACLs, NAT64 prefixes, and AFT address groups for different IPv6-to-IPv4 source address translation policies.

You can specify a nonexistent NAT64 prefix in a policy, but the policy takes effect only after you configure the prefix.

In an HA hot backup network, execute this command on the primary device to bind an IPv6-to-IPv4 source address translation policy to an HA-associated VRRP group on the IPv4 network. If you do not do so, ARP might fail to resolve an IPv6-mapped IPv4 address into a correct MAC address.

An IPv6-to-IPv4 source address translation policy can be bound to only one VRRP group. You can execute this command multiple times to change the bound VRRP group for the policy.

Examples

Map source IPv6 address **3001::5** to source IPv4 address **2.2.2.123**.

```
<Sysname> system-view
[Sysname] aft v6tov4 source 3001::5 2.2.2.123
```

Configure the device to use AFT address group 0 to translate source addresses for IPv6 packets permitted by ACL 2000.

```
<Sysname> system-view
[Sysname] aft v6tov4 source acl ipv6 number 2000 address-group 0 port-block-size 100
```

Related commands

display aft configuration

display aft port-block

display aft address-group

Use **display aft address-group** to display AFT address group information.

Syntax

display aft address-group [*group-id*]

View

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

group-id: Specifies an AFT address group ID in the range of 0 to 65535. If you do not specify this argument, the command displays information about all AFT address groups.

Examples

Display information about all AFT address groups.

```
<Sysname> display aft address-group
There are 3 AFT address groups.
Group ID   VRID   Start address         End address
1          ---    202.110.10.10         202.110.10.15
2          ---    202.110.10.20         202.110.10.25
                  202.110.10.30         202.110.10.35
6          ---    ---                   ---
```

Display information about AFT address group 1.

```
<Sysname> display aft address-group 1
Group ID   VRID   Start address         End address
1          ---    202.110.10.10         202.110.10.15
```

Table 1 Command output

Field	Description
There are *n* AFT address groups	Total number of existing AFT address groups.
Group ID	Address group ID.
VRID	Virtual router ID of a VRRP group. If no VRRP group is specified, this field displays three hyphens (---).
Start address	Start IP address of an address range. If you do not specify the start address, this field displays three hyphens (---).
End address	End IP address of an address range. If you do not specify the end address, this field displays three hyphens (---).

display aft address-mapping

Use **aft address-mapping** to display AFT mappings.

Syntax

display aft address-mapping [**slot** *slot-number*]

View

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays AFT mappings for all member devices.

Examples

Display AFT mappings.

```
<Sysname> display aft address-mapping
Slot 1:
IPv6: Source IP/port: 2000:0:FF01:101:100::8/1024
      Destination IP/port: 5000::1717:1714/1025
      VPN instance/VLAN ID/Inline ID: -/-/-
      Protocol: TCP(6)
IPv4: Source IP/port: 1.1.1.1/1031
      Destination IP/port: 23.23.23.20/1025
      VPN instance/VLAN ID/Inline ID: -/-/-
      Protocol: TCP(6)

Total address mappings found: 1
```

Table 2 Command output

Field	Description
IPv4	IPv4 address information.
IPv6	IPv6 address information.
Source IP/port	Source IP address and port number.
Destination IP/port	Destination IP address and port number.
VPN instance/VLAN ID/Inline ID	The fields identify the following information: • **VPN instance**—MPLS L3VPN instance to which the session belongs. • **VLAN ID**—VLAN to which the session belongs for Layer 2 forwarding. • **Inline ID**—Inline to which the session belongs for Layer 2 forwarding. If no VPN instance, VLAN ID, or Inline ID is specified, a hyphen (-) is displayed for the related field.
Protocol	Transport layer protocol type: **DCCP**, **ICMP**, **ICMPv6**, **Raw IP**, **SCTP**, **TCP**, **UDP**, or **UDP-Lite**.

display aft configuration

Use **`display aft configuration`** to display AFT configuration.

Syntax

`display aft configuration`

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Usage guidelines

To view AFT configurations by using the **`display aft configuration`** command, you must execute commands to configure the configurations first except the AFT ALG configuration.

Examples

Display AFT configuration.

```
<Sysname> display aft configuration
<Sysname> display aft configuration
aft address-group 1
  address 202.110.10.10 202.110.10.15
  address 101.1.1.100 101.1.1.200

aft prefix-ivi 3000:DB8E::
```

```
aft prefix-general 2000:DB8E:: 32

aft v6tov4 source acl ipv6 number 2000 address-group 0 port-block-size 100

aft v4tov6 source acl number 2000 prefix-nat64 2000:: 32

aft v4tov6 destination acl number 2000 prefix-ivi 3000:DB8E::

aft v6server protocol tcp 2.2.2.123 1720 3001::5 1720

aft turn-off tos

aft turn-off traffic-class

aft log enable

aft log flow-begin

aft log flow-end

interface GigabitEthernet1/0/1
  aft enable

AFT ALG:
  DNS        : Enabled
  FTP        : Enabled
  HTTP       : Enabled
  ICMP-ERROR : Enabled
```

Table 3 Command output

Field	Description
aft address-group XX	AFT address group ID.
VRID	Virtual router ID (VRRP group number).
address	Address ranges in the AFT address group.
aft port-load-balance enable XX	AFT port halving is enabled. The XX is in **slot** *number* format, which represents the member ID of an IRF member device.
aft remote-backup port-alloc XX	The XX indicates the AFT port ranges used by the primary and secondary devices in the HA group. **primary**—The primary device uses the lower half of the port block, and the secondary device uses the higher half of the port block. **secondary**—The primary device uses the higher half of the port block, and the secondary device uses the lower half of the port block.
aft prefix-nat64 X:X::X:X	NAT64 prefix address.
aft prefix-ivi X:X::X:X	IVI prefix.
aft prefix-general X:X::X:X	General prefix.
aft v6tov4 source XX	IPv6-to-IPv4 source address translation policy. For more information,

	see the **aft v6tov4 source** command.
aft v4tov6 source XX	IPv4-to-IPv6 source address translation policy. For more information, see the **aft v4tov6 source** command.
aft v4tov6 destination XX	IPv4-to-IPv6 destination address translation policy. For more information, see the **aft v4tov6 destination** command.
aft v6server protocol	AFT mapping for the IPv6 internal server.
aft v4server	AFT mapping for an IPv4 internal server.
aft turn-off tos	Value of the ToS field in IPv4 packets translated from IPv6 packets.
aft turn-off traffic-class	Value of the Traffic Class field in IPv6 packets translated from IPv4 packets.
aft log enable	AFT logging is enabled.
aft log flow-begin	AFT session establishment logging is enabled.
aft log flow-end	AFT session removal logging is enabled.
interface XXX	AFT-enabled interface.
aft enable	AFT is enabled.
AFT ALG	AFT ALG status: • Enabled. • Disabled.

display aft no-pat

Use **display aft no-pat** to display AFT NO-PAT entries.

Syntax

display aft no-pat [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays AFT NO-PAT entries for all member devices.

Usage guidelines

An AFT NO-PAT entry records a mapping between an IPv4 address and an IPv6 address without ports.

Examples

Display AFT NO-PAT entries.

```
<Sysname> display aft no-pat
Slot 1:
```

```
IPv6 address: 3006::0002
IPv4 address: 200.100.1.100
IPv4 VPN    : vpn2
IPv6 VPN    : vpn1

IPv6 address: 4016::1102
IPv4 address: 202.120.12.110
IPv4 VPN    : vpn2
IPv6 VPN    : vpn1

Total entries found: 2
```

Table 4 Command output

Field	Description
IPv6 address	Original IPv6 address.
IPv4 address	Translated IPv4 address.
IPv4 VPN	VPN instance to which the translated IPv4 address belongs. If the IPv4 address does not belong to a VPN instance, this field is not displayed.
IPv6 VPN	VPN instance to which the original IPv6 address belongs. If the IPv6 address does not belong to a VPN instance, this field is not displayed.
Total entries found	Total number of AFT NO-PAT entries.

display aft port-block

Use **display aft port-block** to display AFT port block mappings.

Syntax

display aft port-block [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays AFT port block mappings for all member devices.

Examples

Display AFT port block mappings.

```
<Sysname> display aft port-block
Slot 1:
IPv6 address: 3006::0002
IPv4 address: 200.100.1.100
```

```
Port block  : [1024 – 1123]
IPv4 VPN    : vpn2
IPv6 VPN    : vpn1

IPv6 address: 4016::1102
IPv4 address: 202.120.12.110
Port block  : [1024 – 1200]
IPv4 VPN    : vpn2
IPv6 VPN    : vpn1

Total entries found: 2
```

Table 5 Command output

Field	Description
IPv6 address	Original IPv6 address.
IPv4 address	Translated IPv4 address.
Port block	Port range for the translated IPv4 address.
IPv4 VPN	VPN instance to which the translated IPv4 address belongs. If the IPv4 address does not belong to a VPN instance, this field is not displayed.
IPv6 VPN	VPN instance to which the original IPv6 address belongs. If the IPv6 address does not belong to a VPN instance, this field is not displayed.
Total entries found	Total number of AFT port block mapping entries.

display aft session

Use **display aft session** to display AFT sessions.

Syntax

display aft session ipv4 [{ **source-ip** *source-ip-address* | **destination-ip** *destination-ip-address* } * [**vpn-instance** *ipv4-vpn-instance-name*]] [**slot** *slot-number*] [**verbose**]

display aft session ipv6 [{ **source-ip** *source-ipv6-address* | **destination-ip** *destination-ipv6-address* } * [**vpn-instance** *ipv6-vpn-instance-name*]] [**slot** *slot-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ipv4: Displays IPv4 AFT sessions.

source-ip *source-ip-address*: Specifies the source IPv4 address of the packets that initiate AFT sessions.

destination-ip *destination-ip-address*: Specifies the destination IPv4 address of the packets that initiate AFT sessions.

vpn-instance *ipv4-vpn-instance-name*: Specifies an IPv4 MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays AFT sessions for the public network.

ipv6: Displays IPv6 AFT sessions.

source-ip *source-ipv6-address*: Specifies the source IPv6 address of the packets that initiate AFT sessions.

destination-ip *destination-ipv6-address*: Specifies the destination IPv6 address of the packets that initiate AFT sessions.

vpn-instance *ipv6-vpn-instance-name*: Specifies an IPv6 MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays AFT sessions for the public network.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays AFT sessions for all member devices.

verbose: Display detailed information about AFT sessions. If you do not specify this keyword, this command displays brief information about AFT sessions.

Usage guidelines

If you do not specify any parameters, this command displays all AFT sessions.

Examples

Display detailed information about AFT sessions for the specified slot.

```
<Sysname> display aft session ipv4 slot 1 verbose
Slot 1:
Initiator:
  Source      IP/port: 10.1.1.1/217
  Destination IP/port: 20.1.1.1/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: Trust
Responder:
  Source      IP/port: 20.1.1.1/217
  Destination IP/port: 10.1.1.1/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Local
State: ICMP_REPLY
Application: ICMP
Rule ID: -/-/-
Rule name:
Start time: 2022-07-18 09:42:38  TTL: 28s
Initiator->Responder:            0 packets          0 bytes
```

```
Responder->Initiator:            0 packets          0 bytes
Total sessions found: 1
```

Table 6 Command output

Field	Description
Initiator	Session information about the initiator.
Source IP/port	Source IP address and port number.
Destination IP/port	Destination IP address and port number.
VPN instance/VLAN ID/Inline ID	The fields identify the following information: • **VPN instance**—MPLS L3VPN instance to which the session belongs. • **VLAN ID**—VLAN to which the session belongs for Layer 2 forwarding. • **Inline ID**—Inline to which the session belongs for Layer 2 forwarding. If no VPN instance, VLAN ID, or Inline ID is specified, a hyphen (-) is displayed for the related field.
Protocol	Transport layer protocol type: **DCCP**, **ICMP**, **ICMPv6**, **Raw IP**, **SCTP**, **TCP**, **UDP**, or **UDP-Lite**.
Inbound interface	Input interface.
Responder	Session information about the responder.
Source security zone	Security zone of the incoming interface.
State	AFT session state.
Application	Application layer protocol, such as **FTP** and **DNS**. This field displays **unknown** for the protocol types that are identified by non-well-known ports and are not user-defined.
Rule ID	ID of the security policy rule.
Rule name	Name of the security policy rule.
Start time	Time when the session starts.
TTL	Remaining lifetime of the session, in seconds.
Initiator->Responder	Number of packets and bytes from the initiator to the responder.
Responder->Initiator	Number of packets and bytes from the responder to the initiator.
Total sessions found	Total number of AFT sessions.

Related commands

`reset aft session`

display aft statistics

Use **`display aft statistics`** to display AFT statistics.

Syntax

`display aft statistics` [**`slot`** *`slot-number`*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays AFT statistics for all member devices.

Usage guidelines

If you do not specify any parameters, this command displays all AFT statistics.

Examples

Display all AFT statistics.

```
<Sysname> display aft statistics
Total NO-PAT entries found: 0
Total port-block entries found: 0
Total IPv4 sessions: 0
Total IPv6 sessions: 0
Dropped packets: 3006
  Configuration sequence changed: 0
  Failed to transfer payload: 0
  Failed to transfer packet header: 0
  Packet examination failed before packet sending: 0
  Failed to translate destination address: 0
  The translated destination address is invalid: 0
  Failed to translate source address: 0
  Failed to transfer FSBUF to MBUF: 0
  Session ext-info is null: 0
  Peer session is null: 0
  Failed to get translation information from session: 0
  Failed to create session: 0
  Failed to fragment the MBUF: 0
  Failed to create fast forwarding table: 0
  Failed to formalize session: 0
  Other reasons: 0
```

Table 7 Command output

Field	Description
Total NO-PAT entries found	Total number of AFT NO-PAT entries.
Total port-block entries found	Total number of AFT port block mappings.
Total IPv4 sessions	Total number of AFT IPv4 sessions.
Total IPv6 sessions	Total number of AFT IPv6 sessions.
Dropped packets	Number of packets dropped by AFT.
Configuration sequence changed	Number of packets dropped due to configuration sequence changes.

Field	Description
Failed to transfer payload	Number of packets dropped due to ALG failures.
Failed to transfer packet header	Number of packets dropped due to packet header transformation failures.
Packet examination failed before packet sending	Number of packets dropped due to packet examination failures before packet sending.
Failed to translate destination address	Number of packets dropped due to destination address translation failures.
The translated destination address is invalid	Number of packets dropped due to the invalidity of the translated destination address.
Failed to translate source address	Number of packets dropped due to source address translation failures.
Failed to transfer FSBUF to MBUF	Number of packets dropped due to FSBUF-to-MBUF transformation failures.
Session ext-info is null	Number of packets dropped due to session extended information acquisition failures.
Peer session is null	Number of packets dropped due to peer session lookup failures.
Failed to get translation information from session	Number of packets dropped due to translation information acquisition failures from sessions.
Failed to create session	Number of packets dropped due to session creation failures.
Failed to fragment the MBUF	Number of packets dropped due to fragmentation failures.
Failed to create fast forwarding table	Number of packets dropped due to fast forwarding table creation failures.
Failed to formalize session	Number of packets dropped due to session formalization failures.
Other reasons	Number of packets dropped due to other reasons.

Related commands

`reset aft statistics`

reset aft session

Use **`reset aft session`** to clear AFT sessions.

Syntax

`reset aft session` [**`slot`** *`slot-number`*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

`slot` *`slot-number`*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears AFT sessions for all member devices.

Usage guidelines

After you clear AFT sessions, the corresponding AFT NO-PAT entries and port block mappings are also cleared.

Examples

Clear all AFT sessions.

```
<Sysname> reset aft session
```

Related commands

display aft session

reset aft statistics

Use **reset aft** statistics to clear AFT statistics.

Syntax

reset aft statistics [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears AFT statistics for all member devices.

Usage guidelines

The AFT statistics include the number of dropped packets, the number of NO-PAT entries, and the number of port block entries. This command only resets the counter for dropped packets.

Examples

Clear all AFT statistics.

```
<Sysname> reset aft statistics
```

Related commands

display aft statistics

vrrp vrid

Use **vrrp vrid** to bind a VRRP group to an AFT address group.

Use **undo vrrp vrid** to restore the default.

Syntax

vrrp vrid *virtual-router-id*

undo vrrp vrid

Default

An AFT address group is not bound to any VRRP group.

Views

AFT address group view

Predefined user roles

network-admin

context-admin

Parameters

virtual-router-id: Specifies a VRRP group by its virtual router ID in the range of 1 to 255.

Usage guidelines

On an HA network, the virtual IP address of the VRRP group might be on the same subnet as the public IP addresses in the AFT address group. In this case, both of the HA group members might reply to ARP requests for MAC addresses corresponding to these public IP addresses. As a result, MAC addresses in ARP replies and ARP entries on the Layer 3 devices connected to the HA group might be incorrect. To avoid this situation, execute this command to force the master device to use the virtual MAC address of VRRP group in ARP replies. For more information about configuring the HA group, see *High Availability Configuration Guide*.

For active/standby HA, execute this command on the primary device in the HA group.

For dual-active HA, select one of the following methods for VRRP group binding according to the AFT resource allocation between the two devices in the HA group:

- If the two devices share the same AFT address group, execute the **vrrp vrid** command on the primary device. To prevent different master devices from using the same IP-port mapping for different hosts, specify the PAT translation mode and execute the **aft remote-backup port-alloc** command on the primary device.
- If the two devices use different AFT address groups, user traffic with different source IPv6 addresses is identified by ACLs in AFT rules. To enable different master devices to translate the forward user traffic, specify different gateway addresses for different internal users. To direct the reverse traffic to different master devices, bind AFT address groups to different VRRP groups on the primary device.

If you execute the **vrrp vrid** command multiple times, the most recent configuration takes effect.

Examples

Bind VRRP group **1** to AFT address group **2**.

```
<Sysname> system-view
[Sysname] aft address-group 2
[Sysname-aft-address-group-2] vrrp vrid 1
```

Related commands

display aft address-group

NSFOCUS Firewall Series

NF VPN Command Reference

NSFOCUS Technologies, Inc.

Document version: 6W600-20230221

Preface

This command reference describes the commands for configuring VPN features, including:SSL VPN, IPsec, tunneling, GRE, L2TP, and ADVPN.

This preface includes the following topics about the documentation:

- Audience.
- Conventions.

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators.

Conventions

The following information describes the conventions used in the documentation.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select a minimum of one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
CAUTION:	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Contents

SSL VPN commands

aaa domain

Use **aaa domain** to specify an ISP domain for authentication, authorization, and accounting of SSL VPN users in an SSL VPN context.

Use **undo aaa domain** to restore the default.

Syntax

aaa domain *domain-name*

undo aaa domain

Default

The default ISP domain is used for authentication, authorization, and accounting of SSL VPN users in an SSL VPN context.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

domain-name: Specifies the ISP domain name, a case-insensitive string of 1 to 255 characters. The name must meet the following requirements:

- The name cannot contain a forward slash (/), backslash (\), vertical bar (|), quotation marks ("), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or at sign (@).
- The name cannot be **d**, **de**, **def**, **defa**, **defau**, **defaul**, **default**, **i**, **if**, **if-**, **if-u**, **if-un**, **if-unk**, **if-unkn**, **if-unkno, if-unknow**, or **if-unknown**.

Usage guidelines

An SSL VPN username cannot carry ISP domain information. After this command is executed, an SSL VPN gateway uses the specified ISP domain for authentication, authorization, and accounting of SSL VPN users in the context.

Examples

Specify ISP domain **myserver** for authentication, authorization, and accounting of SSL VPN users in SSL VPN context **ctx1**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] aaa domain myserver
```

authentication server-type

Use **authentication server-type** to specify the authentication server type.

Use **undo authentication server-type** to restore the default.

Syntax

authentication server-type { **aaa** | **custom** }

undo authentication server-type

Default

The SSL VPN authentication server is an AAA authentication server.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

aaa: Specifies the AAA authentication server.

custom: Specifies the custom authentication server.

Usage guidelines

If you use a custom authentication server, you must also configure custom authentication settings, such as the URL of the custom authentication server and custom authentication HTTP request and response settings.

If you use an AAA authentication server, you must configure the AAA server. For more information about AAA server configuration, see *Security Configuration Guide*.

Examples

Specify the authentication server type as custom authentication server in SSL VPN context **ctx1**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] authentication server-type custom
```

Related commands

custom-authentication request-header-field

custom-authentication request-method

custom-authentication request-template

custom-authentication response-custom-template

custom-authentication response-field

custom-authentication response-format

custom-authentication response-success-value

custom-authentication timeout

custom-authentication url

authentication use

Use **authentication use** to specify the authentication methods required for user login.

Use **undo authentication use** to restore the default.

Syntax

authentication use { **all** | **any-one** }

undo authentication use

Default

To log in to an SSL VPN context, a user must pass all the authentication methods enabled for the context.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

all: Uses all enabled authentication methods.

any-one: Uses any enabled authentication method.

Usage guidelines

You can enable username/password authentication, certificate authentication, or both for an SSL VPN context. The authentication methods required for logging in to the SSL VPN context depend on the configuration of this command:

- If the **authentication use all** command is configured, a user must pass all the enabled authentication methods for login.
- If the **authentication use any-one** command is configured, a user can log in after passing any enabled authentication method.

Examples

Configure SSL VPN context **ctx** to allow users to log in after passing any enabled authentication method.

```
<Sysname> system-view
[Sysname] sslvpn context ctx
[Sysname-sslvpn-context-ctx] authentication use any-one
```

Related commands

certificate-authentication enable

display sslvpn context

password-authentication enable

bandwidth

Use **bandwidth** to set the expected bandwidth for an interface.

Use **undo bandwidth** to restore the default.

Syntax

bandwidth *bandwidth-value*

undo bandwidth

Default

The expected bandwidth is 64 kbps for an interface.

Views

SSL VPN AC interface view

Predefined user roles

network-admin

context-admin

Parameters

bandwidth-value: Specifies the expected bandwidth in the range of 1 to 400000000 kbps.

Usage guidelines

The expected bandwidth for an interface affects CBQ bandwidth and link costs in OSPF, OSPFv3, and IS-IS. For more information about CBQ bandwidth, see QoS configuration in *ACL and QoS Configuration Guide*. For more information about link costs, see *Layer 3—IP Routing Configuration Guide*.

Examples

Set the expected bandwidth to 10000 kbps for SSL VPN AC 1000.

```
<Sysname> system-view
[Sysname] interface sslvpn-ac 1000
[Sysname-SSLVPN-AC1000] bandwidth 10000
```

certificate username-attribute

Use **certificate username-attribute** to specify the certificate attribute as the SSL VPN username.

Use **undo certificate username-attribute** to restore the default.

Syntax

certificate username-attribute { **cn** | **email-prefix** | **oid** *extern-id* }

undo certificate username-attribute

Default

The device uses the value of the CN attribute in the subject of the user certificate as the SSL VPN username.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

cn: Specifies the CN attribute value in the subject of the user certificate as the SSL VPN username.

email-prefix: Specifies the string before the at sign (@) of the email address in the subject of the user certificate as the SSL VPN username.

oid *extern-id*: Specifies a user certificate attribute by its OID. The value of the attribute will be used as the SSL VPN username. The *extern-id* argument represents the OID, which is an object identifier in dotted decimal notation.

Usage guidelines

The SSL VPN username specified by this command takes effect only after you execute the **certificate-authentication enable** command.

Examples

Use the value of the attribute whose OID is 1.1.1.1 in the user certificate as the SSL VPN username.

```
<Sysname> system-view
[Sysname] sslvpn context ctx
[Sysname-sslvpn-context-ctx] certificate username-attribute oid 1.1.1.1
```

Related commands

certificate-authentication enable

certificate-authentication enable

Use **certificate-authentication enable** to enable certificate authentication.

Use **undo certificate-authentication enable** to disable certificate authentication.

Syntax

certificate-authentication enable

undo certificate-authentication enable

Default

Certificate authentication is disabled.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Usage guidelines

After you enable certificate authentication, you must also execute the **client-verify** command in SSL server policy view. The SSL VPN gateway uses the digital certificate sent by an SSL VPN client to authenticate the client's identity. If the client's username and the username in the digital certificate are not the same, the client cannot log in to the SSL VPN gateway.

Examples

Enable certificate authentication.

```
<Sysname> system-view
[Sysname] sslvpn context ctx
[Sysname-sslvpn-context-ctx] certificate-authentication enable
```

Related commands

client-verify enable

client-verify optional

content-type

Use **content-type** to configure a file policy to rewrite a file in an HTTP response to a specific type of file.

Use **undo content-type** to restore the default.

Syntax

content-type { **css** | **html** | **javascript** | **other** }

undo content-type

Default

A file policy rewrites a file carried in an HTTP response to a file of the type indicated by the content-type field in the HTTP response.

Views

File policy view

Predefined user roles

network-admin

context-admin

Parameters

css: Changes the file type to CSS.

html: Changes the file type to HTML.

javascript: Changes the file type to JavaScript.

other: Does not change the file type.

Usage guidelines

A file policy rewrites a file carried in an HTTP response to a file of the type specified by this command. If the specified file type is different from that indicated by the content-type field in the HTTP response, users might not be able to read the file correctly.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure file policy **fp** to rewrite files to HTML files.

```
<Sysname> system-view
[Sysname] sslvpn context ctx
[Sysname-sslvpn-context-ctx] file-policy fp
[Sysname-sslvpn-context-ctx-file-policy-fp] content-type html
```

country code

Use **country-code** to specify the mobile country code.

Use **undo country-code** to restore the default.

Syntax

country-code *country-code*

undo country-code

Default

The country code is 86.

Views

SMS gateway authentication view

Predefined user roles

network-admin

context-admin

Parameters

country-code: Specifies the country code, a string of 1 to 7 characters. Only digits are supported.

Examples

Set the country code to 86 in SMS gateway authentication view.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] sms-auth sms-gw
[Sysname-sslvpn-context-ctx1-sms-auth-sms-gw] country-code 86
```

custom-authentication request-header-field

Use **custom-authentication request-header-field** to configure an HTTP request header field for custom authentication.

Use **undo custom-authentication request-header-field** to remove the configuration of an HTTP request header field for custom authentication.

Syntax

custom-authentication request-header-field *field-name* **value** *value*

undo custom-authentication request-header-field *field-name*

Default

A custom authentication request header includes the following fields:

- **Content-type:application/x-www-form-urlencoded**.
- **User-Agent:nodejs 4.1**.
- **Accept:text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q**.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

field-name: Specifies a request header field name, a case-insensitive string of 1 to 63 characters. The name cannot include the following characters:

- ()<>@,;:\"/[]?={}
- Spaces.
- Horizontal tabs.

- ASCII characters with codes ≤ 31 or ≥ 127.

value *value*: Specifies the value of the request header field, a string of 1 to 255 characters, which cannot contain question mark (?) metacharacters.

Usage guidelines

Use this command to configure HTTP request header fields sent to the custom authentication server. Perform this configuration after the custom authentication server is specified by using the **authentication server-type custom** command. To have the configuration take effect, you must also configure other custom authentication request settings, such as the HTTP request method and the request template.

Execute this command multiple times to configure multiple HTTP request header fields. For the same field, the most recent configuration takes effect.

Examples

Specify the **host** field as 192.168.56.2:8080 in the HTTP request header for custom authentication in SSL VPN context **ctx1**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] custom-authentication request-header-field host value
192.168.56.2:8080
```

Related commands

authentication server-type

custom-authentication request-method

custom-authentication request-template

custom-authentication url

custom-authentication request-method

Use **custom-authentication request-method** to configure the HTTP request method for custom authentication.

Use **undo custom-authentication request-method** to restore the default.

Syntax

custom-authentication request-method { **get** | **post** }

undo custom-authentication request-method

Default

The HTTP request method is GET.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

get: Specifies the GET method.

post: Specifies the POST method.

Usage guidelines

Use this command to configure the HTTP request method for authentication requests sent to the custom authentication server. Perform this configuration after the custom authentication server is specified by using the **authentication server-type custom** command. To have the configuration take effect, you must also configure other custom authentication request settings, such as the HTTP request header fields and the request template.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the POST request method for custom authentication in SSL VPN context **ctx1**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] custom-authentication request-method post
```

Related commands

authentication server-type

custom-authentication request-template

custom-authentication url

custom-authentication request-template

Use **custom-authentication request-template** to configure the request template for custom authentication.

Use **undo custom-authentication request-template** to restore the default.

Syntax

custom-authentication request-template *template*

undo custom-authentication request-template

Default

No request template is configured for custom authentication.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

template: Specifies the request template through which the SSL VPN gateway sends username and password information to the custom authentication server. The template is a case-insensitive string of 1 to 255 characters.

Usage guidelines

Use this command to configure the HTTP request template through which the SSL VPN gateway sends the username and password to the custom authentication server. Perform this configuration after the custom authentication server is specified by the **authentication server-type custom** command. To have the configuration take effect, you must also configure other custom authentication request settings, such as the HTTP request header fields and the request method.

If you execute this command multiple times, the most recent configuration takes effect.

This command supports the following request template formats:

- Form format for the POST and GET methods: username=$$USERNAME$$&password=$$PASSWORD_MD5$$&resid=1234.
- JSON type for the POST method: {“name”:”$$USERNAME$$”,“password”:”,$$PASSWORD$$”,“resid”:”1234”}.
- XML type for the GET method: <uname>$$USERNAME$$</uname><psw>$$PASSWORD$$</psw>.

The **USERNAME**, **PASSWORD**, and **PASSWORD_MD5** between $$ pairs in the request templates are variables. The **PASSWORD_MD5** represents a password encrypted by MD5. When a user logs in to the SSL VPN gateway, the gateway replaces these variables with the login username and password. Then, the SSL VPN gateway sends the authentication request to the custom authentication server.

Examples

Configure the custom authentication HTTP request template as **username=$$USERNAME$$&password=$$PASSWORD_MD5$$&resid=1952252223973828** in SSL VPN context **ctx1**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] custom-authentication request-template
username=$$USERNAME$$&password=$$PASSWORD_MD5$$&resid=1952252223973828
```

Related commands

authentication server-type

custom-authentication request-template

custom-authentication url

custom-authentication response-custom-template

Use **custom-authentication response-custom-template** to configure response templates for the fields in the HTTP response for custom authentication.

Use **undo custom-authentication response-custom-template** to restore the default.

Syntax

custom-authentication response-custom-template { **group** | **message** | **result** } *template*

undo custom-authentication response-custom-template { **group** | **message** | **result** }

Default

No response templates are configured for custom authentication.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

group: Specifies the group field in the authentication response.

message: Specifies the message field in the authentication response.

result: Specifies the result field in the authentication response.

template: Specifies the content of the response template for the specified field. The template is a case-insensitive string of 1 to 63 characters.

Usage guidelines

Use this command to configure the response templates for the device to identify the fields in a custom-format authentication response. Perform this configuration after the custom authentication server is specified by using the **authentication server-type custom** command. This configuration is applicable when the HTTP response format is **custom**. When you configure response templates, the response template for the result field is required.

When you configure a response template for a field, follow these restrictions and guidelines:

- A response template for a field must contain **$$value$$**.
  - The **value** keyword represents the field value in the response.
  - The pairs of dollar signs ($$) are used to identify the start and end of the field in a response. The device considers the content before the first $$ the start identifier and that after the second $$ the end identifier for parsing the field of the response.
- Make sure the contents before and after **$$value$$** in the response template are consistent with those before and after the field value in the response from the authentication server.

Here is an example. Assume that the result field information in the response from the authentication server is **auth-result=true,**. You must configure the response template for the result field as **auth-result=$$value$$,**. The contents before and after **$$value$$** are **auth-result=** and a comma (,), which are the same as those before and after **true**, respectively. Then, the device can use the **auth-result=$$value$$,** template to correctly identify and parse the result field in the authentication response.

Examples

Configure the response templates in SSL VPN context **ctx1** as **result=$$value$$,company=$$value$$,message=$$value$$**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] custom-authentication response-custom-template result
result=$$value$$,
[Sysname-sslvpn-context-ctx1] custom-authentication response-custom-template group
company=$$value$$,
[Sysname-sslvpn-context-ctx1] custom-authentication response-custom-template message
message=$$value$$
```

Related commands

authentication server-type

custom-authentication response-format

custom-authentication response-success-value

custom-authentication response-field

Use **custom-authentication response-field** to configure a field name in the HTTP response for custom authentication.

Use **undo custom-authentication response-field** to restore the default.

Syntax

custom-authentication response-field { **group** *group* | **message** *message* | **result** *result* }

undo custom-authentication response-field { **group** | **message** | **result** }

Default

No HTTP response field names are configured.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

group *group*: Specifies the name of the policy group field in the HTTP response, a case-insensitive string of 1 to 31 characters. In the authentication response, the value following the *group* argument represents the policy groups authorized to the user.

message *message*: Specifies the name of the message field in the HTTP response, a case-insensitive string of 1 to 31 characters. In the authentication response, the value following the *message* argument represents the authentication prompt.

result *result*: Specifies the name of the result field in the HTTP response, a case-insensitive string of 1 to 31 characters. In the authentication response, the value following the *message* argument represents the authentication result.

Usage guidelines

Use this command to configure the names of the fields in the HTTP response. Perform this configuration after the custom authentication server is specified by using the **authentication server-type custom** command. This configuration is applicable when the HTTP response format is JSON or XML. When you configure HTTP response field names, the result field name is required.

The device uses the configured field names to parse the HTTP response returned from the custom authentication server, as follows:

- If you specify the policy field name, the SSL VPN gateway uses the specified name to identify the policy group field in the response. For example, if the policy group field name is specified as **company**, the device uses the value following **company** in the response as the server-authorized policy group.

  The policy group finally assigned to the user is determined as follows:

  - If the SSL VPN context has the server-authorized policy group configured, the gateway assigns the authorized policy group to the user.
  - If the SSL VPN context has no policy groups, or the server does not authorize a policy group, the gateway assigned the default policy to the user.
- If you specify the message field name, the SSL VPN gateway uses the specified name to identify the authentication result message in the response. The message indicates the authentication result, such as authentication success or failure.
- If you specify the result field name, the SSL VPN gateway uses the specified name to identify the authentication result value in the response. The gateway then determines the authentication result based on the configured authentication success value (see the **custom-authentication response-success-value** command).

If you execute this command multiple times for a field, the most recent configuration takes effect.

Examples

Specify the group field name as **company** and the message field name as **resultDescription** in the custom authentication response for SSL VPN context **ctx1**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] custom-authentication response-field group company
[Sysname-sslvpn-context-ctx1] custom-authentication response-field message
resultDescription
```

Related commands

authentication server-type

custom-authentication response-format

Use **custom-authentication response-format** to specify the HTTP response format for custom authentication.

Use **undo custom-authentication response-format** to restore the default.

Syntax

custom-authentication response-format { **custom** | **json** | **xml** }

undo custom-authentication response-format

Default

The HTTP response format for custom authentication is JSON.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

custom: Specifies the XML format.

json: Specifies the JSON format.

xml: Specifies the custom response format.

Usage guidelines

Use this command to configure the HTTP response format for custom authentication after the custom authentication server is specified by using the **authentication server-type custom** command. After you specify the HTTP response format, you must also configure corresponding HTTP response settings (such as the HTTP response templates and field names) for the specified format.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the HTTP response format as **JSON** in SSL VPN context **ctx1**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] custom-authentication response-format json
```

Related commands

authentication server-type

custom-authentication response-custom-template

custom-authentication response-success-value

Use **custom-authentication response-success-value** to configure the authentication success value in the HTTP response for custom authentication.

Use **undo custom-authentication response-success-value** to restore the default.

Syntax

custom-authentication response-success-value *success-value*

undo custom-authentication response-success-value

Default

No authentication success value is configured for custom authentication.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

success-value: Specifies the value that represents the authentication success result, a case-insensitive string of 1 to 31 characters.

Usage guidelines

Use this command to configure the authentication success value in the HTTP response. Perform this configuration after the custom authentication server is specified by using the **authentication server-type custom** command. To have the configuration take effect, you must also configure other custom authentication settings, such as specifying the result field name in the HTTP response.

The SSL VPN gateway considers the user authentication successful only when the value of the result field in the custom authentication response is the value specified by this command.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the authentication success value as **true** in the custom authentication response for SSL VPN context **ctx1**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] custom-authentication response-success-value true
```

Related commands

authentication server-type

custom-authentication response-field

custom-authentication timeout

Use **custom-authentication timeout** to specify the custom authentication timeout.

Use **undo custom-authentication timeout** to restore the default.

Syntax

custom-authentication timeout *seconds*

undo custom-authentication timeout

Default

The custom authentication timeout is 15 seconds.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies the custom authentication timeout, in the range of 5 to 50 seconds.

Usage guidelines

After sending an HTTP request to the custom authentication server, the SSL VPN gateway waits for responses from the server. If the gateway receives no response within the authentication timeout, it returns an authentication failure message to the SSL VPN client.

Examples

Specify the custom authentication timeout as 20 seconds in SSL VPN context **ctx1**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] custom-authentication timeout 20
```

Related commands

authentication server-type

custom-authentication url

Use **custom-authentication url** to configure the URL of the custom authentication server.

Use **undo custom-authentication url** to restore the default.

Syntax

custom-authentication url *url*

undo custom-authentication url

Default

No URL is configured for the custom authentication server.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

url: Specifies the URL of the authentication server in an HTTP request sent by the SSL VPN gateway to the custom authentication server. The URL is a case-insensitive string of 1 to 255 characters, and it cannot contain question mark (?) metacharacters.

Usage guidelines

Use this command to configure the URL of the custom authentication server after the custom authentication server is specified by the **authentication server-type custom** command. To have the configuration take effect, you must also configure other custom authentication settings, such as the HTTP request header fields, request method, and request template.

A URL consists of the protocol type, host name or address, port number, and resource path. The complete URL format is *protocol type*://*host name or address*:*port number/resource path*. The protocol type currently supports only HTTP and HTTPS. If not specified, the protocol type is HTTP by default. If the URL contains an IPv6 address, enclose the IPv6 address in brackets, for example, http://[1234::5678]:8080.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure the URL of the custom authentication server in SSL VPN context **ctx1**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] custom-authentication url
http://192.168.56.2:8080/register/user/checkUserAndPwd
```

Related commands

authentication server-type

custom-authentication request-method

custom-authentication request-template

default

Use **default** to restore the default settings for an SSL VPN AC interface.

Syntax

default

Views

SSL VPN AC interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

CAUTION:

The **default** command might interrupt ongoing network services. Make sure you are fully aware of the impact of this command when you use it on a live network.

This command might fail to restore the default settings for some commands for reasons such as command dependencies or system restrictions. Use the **display this** command in interface view to identify these commands. Use their **undo** forms or follow the command reference to restore their

default settings. If your restoration attempt still fails, follow the error message instructions to resolve the problem.

Examples

Restore the default settings of **sslvpn-ac 1000**.

```
<Sysname> system-view
[Sysname] interface sslvpn-ac 1000
[Sysname-SSLVPN-AC1000] default
This command will restore the default settings. Continue? [Y/N]:y
```

default-policy-group

Use **default-policy-group** to specify a policy group as the default policy group.

Use **undo default-policy-group** to restore the default.

Syntax

default-policy-group *group-name*

undo default-policy-group

Default

No policy group is specified as the default policy group.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a policy group by its name, a case-insensitive string of 1 to 31 characters. The specified policy group must have been created.

Usage guidelines

You can configure multiple policy groups for an SSL VPN context. When a remote user accesses the SSL VPN context, the AAA server issues the authorized policy group to the associated SSL VPN gateway. The user can access only the resources allowed by the authorized policy group. If the AAA server does not issue an authorized policy group to the user, the user can access only the resources allowed by the default policy group.

Examples

Specify policy group **pg1** as the default policy group.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] policy-group pg1
[Sysname-sslvpn-context-ctx1-policy-group-pg1] quit
[Sysname-sslvpn-context-ctx1] default-policy-group pg1
```

Related commands

display sslvpn context

policy-group

description (shortcut view)

Use **description** to configure a description for a shortcut.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

No description is configured for a shortcut.

Views

Shortcut view

Predefined user roles

network-admin

context-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 63 characters.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure a description for shortcut **shortcut1**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] shortcut shortcut1
[Sysname-sslvpn-context-ctx1-shortcut-shortcut1] description shortcut1
```

description (SSL VPN AC interface view)

Use **description** to configure the description of an interface.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

The description of an interface is *interface name* **Interface**, for example, **SSLVPN-AC1000 Interface**.

Views

SSL VPN AC interface view

Predefined user roles

network-admin

context-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 255 characters.

Usage guidelines

Configure descriptions for interfaces for identification and management purposes.

You can use the **display interface** command to display the configured interface descriptions.

Examples

Configure a description of **SSL VPN A** for SSL VPN AC 1000.

```
<Sysname> system-view
[Sysname] interface sslvpn-ac 1000
[Sysname-SSLVPN-AC1000] description SSL VPN A
```

display interface sslvpn-ac

Use **display interface sslvpn-ac** to display SSL VPN AC interface information.

Syntax

display interface [**sslvpn-ac** [*interface-number*]] [**brief** [**description** | **down**]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

sslvpn-ac [*interface-number*]: Specifies an SSL VPN AC interface by its number in the range of 0 to 4095. If you do not specify the **sslvpn-ac** keyword, this command displays information about all interfaces except virtual access (VA) interfaces. If you specify the **sslvpn-ac** keyword without the *interface-number* argument, this command displays information about all SSL VPN AC interfaces. For more information about VA interfaces, see PPP configuration in *Layer 2—WAN Access Configuration Guide*.

brief: Displays brief interface information. If you do not specify this keyword, the command displays detailed interface information.

description: Displays complete interface descriptions. If you do not specify this keyword, the command displays only the first 27 characters of interface descriptions.

down: Displays information about interfaces in the physical state of DOWN and the causes. If you do not specify this keyword, the command displays information about interfaces in all states.

Examples

Display detailed information about SSL VPN AC 1000.

```
<Sysname> display interface sslvpn-ac 1000
SSLVPN-AC1000
Current state: UP
Line protocol state: DOWN
```

```
Description: SSLVPN-AC1000 Interface
Bandwidth: 64kbps
Maximum transmission unit: 1500
Internet protocol processing: Disabled
Link layer protocol is SSLVPN
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

Table 1 Command output

Field	Description
SSLVPN-AC1000	Information about interface SSL VPN AC 1000.
Current state	Physical link state of the interface: • **Administratively DOWN**—The interface has been shut down by using the **shutdown** command. • **DOWN**—The interface is administratively up, but its physical state is down (possibly because no physical link exists or the link has failed). • **UP**—The interface is both administratively and physically up.
Line protocol state	Data link layer state of the interface. The state is determined through automatic parameter negotiation at the data link layer. • **UP**—The data link layer protocol is up. • **UP (spoofing)**—The data link layer protocol is up, but the link is an on-demand link or does not exist. This attribute is typical of null interfaces and loopback interfaces. • **DOWN**—The data link layer protocol is down.
Description	Description of the interface.
Bandwidth	Expected bandwidth of the interface.
Maximum transmission unit	MTU of the interface.
Internet protocol processing: Disabled	The interface is not assigned an IP address and cannot process IP packets.
Internet address: *ip-address*/*mask-length* (*Type*)	IP address of the interface and type of the address in parentheses. Possible IP address types include: **Primary**—Manually configured primary IP address.
Last clearing of counters	Most recent time the counters were cleared by using the **reset counters interface** command. If the **reset counters interface** command has never been executed since the device starts up, this field displays **Never**.
Last 300 seconds input rate	Average input rate in the last 300 seconds.
Last 300 seconds output rate	Average output rate in the last 300 seconds.

Display brief information about all SSL VPN AC interfaces.

```
<Sysname> display interface sslvpn-ac brief
Brief information of interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
```

```
Interface            Link Protocol Primary IP         Description
SSLVPN-AC1000        UP   DOWN     --
```

Display brief information about SSL VPN AC 1000, including the complete interface description.

```
<Sysname> display interface sslvpn-ac 1000 brief description
Brief information of interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP         Description
SSLVPN-AC1000        UP    UP      1.1.1.1            SSLVPN-AC1000 Interface
```

Display information about interfaces in DOWN state and the causes.

```
<Sysname> display interface sslvpn-ac brief down
Brief information of interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Interface            Link Cause
SSLVPN-AC1000        ADM
SSLVPN-AC1001        ADM
```

Table 2 Command output

Field	Description
Brief information of interfaces in route mode:	Brief information about Layer 3 interfaces.
Interface	Abbreviated interface name.
Link	Physical link state of the interface: • **UP**—The interface is physically up. • **DOWN**—The interface is physically down. • **ADM**—The interface has been shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command. • **Stby**—The interface is a backup interface in standby state.
Protocol	Data link layer protocol state of the interface: • **UP**—The data link layer protocol of the interface is up. • **UP(s)**—The data link layer protocol of the interface is up, but the link is an on-demand link or does not exist. The **(s)** attribute represents the spoofing flag. This value is typical of null interfaces and loopback interfaces. • **DOWN**—The data link layer protocol of the interface is down.
Primary IP	Primary IP address of the interface.
Description	Description of the interface.
Cause	Cause for the physical link state of an interface to be **DOWN**: • **Administratively**—The interface has been manually shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command. • **Not connected**—No physical connection exists (possibly because the network cable is disconnected or faulty).

Related commands

reset counters interface

display sslvpn context

Use **display sslvpn context** to display SSL VPN context information.

Syntax

display sslvpn context [**brief** | **name** *context-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

brief: Displays brief SSL VPN context information. If you do not specify this keyword, the command displays detailed SSL VPN context information.

name *context-name*: Specifies an SSL VPN context by its name. An SSL VPN context name is a case-insensitive string of 1 to 31 characters, and can contain only letters, digits, and underscores (_). If you do not specify an SSL VPN context, this command displays information about all SSL VPN contexts.

Examples

Display detailed information about all SSL VPN contexts.

```
<Sysname> display sslvpn context
Context name: ctx1
  Operation state: Up
  AAA domain: domain1
  Certificate authentication: Enabled
  Certificate username-attribute: CN
  Password authentication: Enabled
  Authentication use: All
  SMS auth type: iMC
  Code verification: Disabled
  Default policy group: Not configured
  Associated SSL VPN gateway: gw1
    Domain name: 1
  Associated SSL VPN gateway: gw2
    Virtual host: abc.com
  Associated SSL VPN gateway: gw3
  SSL client policy configured: ssl1
  SSL client policy in use: ssl
  Maximum users allowed: 200
  VPN instance:vpn1
  Idle timeout: 30 min
  Idle-cut traffic threshold: 100 Kilobytes
  Authentication server-type: aaa
  Password changing: Disabled
```

```
Context name: ctx2
  Operation state: Down
  Down reason: Administratively down
  AAA domain not specified
  Certificate authentication: Enabled
  Certificate username-attribute: OID(2.5.4.10)
  Password authentication: Disabled
  Authentication use: Any-one
  SMS auth type: sms-gw
  Code verification: Disabled
  Default group policy: gp
  Associated SSL VPN gateway: -
  SSL client policy configured: ssl1
  SSL client policy in use: ssl
  Maximum users allowed: 200
  VPN instance not configured
  Idle timeout: 50 min
  Idle-cut traffic threshold: 100 Kilobytes
  Address pool: Conflicted with an IP address on the device
  Authentication server-type: custom
  Password changing: Disabled
```

Table 3 Command output

Field	Description
Context name	Name of the SSL VPN context.
Operation state	Operation state of the SSL VPN context: • **Up**—The context is running. • **Down**—The context is not running.
Down reason	Causes for the **Down** operations status: • **Administratively down**—The context is disabled. To enable the context, use the **`service enable`** command. • **No gateway associated**—The context is not associated with an SSL VPN gateway.
AAA domain	ISP domain for the SSL VPN context.
Certificate authentication	Whether certificate authentication is enabled for the SSL VPN context.
Password authentication	Whether username/password authentication is enabled for the SSL VPN context.
Authentication use	Authentication methods required for user login: • **All**—A user must pass all the enabled authentication methods to log in to the SSL VPN context. • **Any-one**—A user can log in to the SSL VPN context after passing any enabled authentication method.

Field	Description
Certificate username-attribute	Certificate attribute whose value is used as the SSL VPN username: • **CN**—CN attribute in the subject of the user certificate. • **Email-prefix**—String before the at sign (@) of the email address in the subject of the user certificate. • **OID(x.x.x.x)**—Object identifier of a user certificate attribute in dotted decimal notation. This field is displayed only when certificate authentication is enabled.
SMS auth type	SMS authentication types: • **iMC**—SMS authentication by an IMC server. • **sms-gw**—SMS authentication by an SMS gateway.
Code verification	Whether code verification is enabled for the SSL VPN context.
Default policy group	Default policy group used by the SSL VPN context.
Associated SSL VPN gateway	SSL VPN gateway associated with the SSL VPN context.
Domain name	Domain name specified for the SSL VPN context.
Virtual host	Virtual host name specified for the SSL VPN context.
SSL client policy configured	SSL client policy configured for the SSL VPN context. A newly configured SSL client policy takes effect only after the SSL VPN context is restarted.
SSL client policy in use	SSL client policy being used by the SSL VPN context.
Maximum users allowed	Maximum number of sessions allowed in the SSL VPN context.
VPN instance	VPN instance associated with the SSL VPN context.
Idle timeout	Maximum idle time of an SSL VPN session, in minutes.
Idle-cut traffic threshold	SSL VPN idle session disconnection traffic threshold.
Address pool: Conflicted with an IP address on the device	An IP address conflict was detected in the SSL VPN context.
Authentication server-type	Authentication server types: • **aaa**—AAA server. • **custom**—Custom authentication server.
Password changing	Status of the SSL VPN login password modification feature: • **Enabled**. • **Disabled**.

Display brief information about all SSL VPN contexts.

```
<Sysname> display sslvpn context brief
Context name   Admin   Operation   VPN instance   Gateway   Domain/VHost
ctx1           Up      Up          -              gw1       -/1
                                                  gw2       abc.com/-
                                                  gw3       -/-
ctx2           Down    Down        -              -         -/-
```

Table 4 Command output

Field	Description
Context name	Name of the SSL VPN context.

Field	Description
Admin	Administrative status of the SSL VPN context: • **Up**—The context has been enabled by using the **service enable** command. • **Down**—The context is disabled.
Operation	Operation state of the SSL VPN context: • **Up**—The context is running. • **Down**—The context is not running.
VPN instance	VPN instance associated with the SSL VPN context.
Gateway	SSL VPN gateway associated with the SSL VPN context.
Domain/VHost	Domain name or virtual host name specified for the SSL VPN context.

display sslvpn gateway

Use **display sslvpn gateway** to display SSL VPN gateway information.

Syntax

display sslvpn gateway [**brief** | **name** *gateway-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

brief: Displays brief SSL VPN gateway information. If you do not specify this keyword, the command displays detailed SSL VPN gateway information.

name *gateway-name*: Specifies an SSL VPN context by its name. An SSL VPN context name is a case-insensitive string of 1 to 31 characters, and can contain only letters, digits, and underscores (_). If you do not specify an SSL VPN context, this command displays information about all SSL VPN gateways.

Examples

Display detailed information about all SSL VPN gateways.

```
<Sysname> display sslvpn gateway
Gateway name: gw1
  Operation state: Up
  IP: 192.168.10.75  Port: 443
  HTTP redirect port: 80
  SSL server policy configured: ssl1
  SSL server policy in use: ssl
  Front VPN instance: vpn1
Gateway name: gw2
  Operation state: Down
```

```
  Down reason: Administratively down
  IP: 0.0.0.0  Port: 443
  SSL server policy configured: ssl1
  SSL server policy in use: ssl
  Front VPN instance: Not configured
Gateway name: gw3
  Operation state: Up
  IPv6: 3000::2  Port: 443
  SSL server policy configured: ssl1
  SSL server policy in use: ssl
  Front VPN instance: Not configured
```

Table 5 Command output

Field	Description
Gateway name	Name of the SSL VPN gateway.
Operation state	Operation state of the SSL VPN gateway: • **Up**—The gateway is running. • **Down**—The gateway is not running.
Down reason	Causes for the **Down** operation status: • **Administratively down**—The SSL VPN gateway is disabled. To enable the gateway, use the **service enable** command. • **VPN instance not exist**—The VPN instance to which the SSL VPN gateway belongs does not exist. • **Applying SSL server-policy failed**—Failed to apply the SSL server policy to the SSL VPN gateway.
IP	IPv4 address of the SSL VPN gateway.
IPv6	IPv6 address of the SSL VPN gateway.
Port	Port number of the SSL VPN gateway.
HTTP redirect port	HTTP redirection port number of the SSL VPN gateway.
SSL server policy configured	SSL server policy configured for the SSL VPN gateway. A newly configured SSL server policy takes effect only after the SSL VPN gateway is restarted.
SSL server policy in use	SSL server policy being used by the SSL VPN gateway.
Front VPN instance	Front VPN instance to which the SSL VPN gateway belongs.

Display brief information about all SSL VPN gateways.

```
<Sysname> display sslvpn gateway brief
Gateway name                    Admin  Operation
gw1                             Up     Up
gw2                             Down   Down (Administratively down)
gw3                             Up     Up
```

Table 6 Command output

Field	Description
Gateway name	Name of the SSL VPN gateway.

Field	Description
Admin	Administrative status of the SSL VPN gateway: • **Up**—The gateway has been enabled by using the **service enable** command. • **Down**—The gateway is disabled.
Operation	Operation state of the SSL VPN gateway: • **Up**—The gateway is running. • **Down (Administratively down)**—The gateway is disabled. To enable the gateway, use the **service enable** command. • **Down (VPN instance not exist)**—The gateway is down because the VPN instance to which the gateway belongs does not exist. • **Down (Applying SSL server-policy failed)**—The gateway is down because the SSL server policy failed to be applied to the gateway.

display sslvpn ip-tunnel statistics

Use **display sslvpn ip-tunnel statistics** to display packet statistics for IP access users.

Syntax

display sslvpn ip-tunnel statistics [**context** *context-name*] [**user** *user-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

context *context-name*: Specifies an SSL VPN context by its name. An SSL VPN context name is a case-insensitive string of 1 to 31 characters, and can contain only letters, digits, and underscores (_).

user *user-name*: Specifies an IP access user by username, a case-insensitive string of 1 to 63 characters.

Usage guidelines

If you do not specify any parameters, this command displays IP access packets statistics for all SSL VPN contexts.

If you only specify an SSL VPN context, this command displays IP access packet statistics for the specified context and for each SSL VPN user in the context.

If you only specify an SSL VPN user, this command displays IP access packet statistics for the specified user in all SSL VPN contexts.

If you specify both an SSL VPN context and user, this command displays IP access packet statistics for the specified user in the specified context.

Examples

Display IP access packet statistics for all SSL VPN contexts.

```
<Sysname> display sslvpn ip-tunnel statistics
IP-tunnel statistics in SSL VPN context ctx1:
  Client:
    In bytes  : 125574              Out bytes  : 1717349
  Server:
    In bytes  : 1717349             Out bytes  : 116186

IP-tunnel statistics in SSL VPN context ctx2:
  Client:
    In bytes  : 521                 Out bytes  : 1011
  Server:
    In bytes  : 1011                Out bytes  : 498
```

Display IP access packet statistics for SSL VPN context **ctx1** and for each user in the context.

```
<Sysname> display sslvpn ip-tunnel statistics context ctx1
IP-tunnel statistics in SSL VPN context ctx1:
  Client:
    In bytes  : 125574              Out bytes  : 1717349
  Server:
    In bytes  : 1717349             Out bytes  : 116186


SSL VPN session IP-tunnel statistics:
Context                       : ctx1
User                          : user1
Session ID                    : 1
User IPv4 address             : 192.168.56.1
Received requests             : 81
Sent requests                 : 0
Dropped requests              : 81
Received replies              : 0
Sent replies                  : 0
Dropped replies               : 0
Received keepalives           : 1
Sent keepalive replies        : 1
Received configuration updates: 0
Sent configuration updates    : 0

Context                       : ctx1
User                          : user2
Session ID                    : 2
User IPv6 address             : 1234::5001
Received requests             : 81
Sent requests                 : 0
Dropped requests              : 81
Received replies              : 0
Sent replies                  : 0
Dropped replies               : 0
Received keepalives           : 1
Sent keepalive replies        : 1
```

```
Received configuration updates: 0
Sent configuration updates    : 0
```

Display IP access packet statistics for user **user1** in all SSL VPN contexts.

```
<Sysname> display sslvpn ip-tunnel statistics user user1
SSL VPN session IP-tunnel statistics:
Context                       : ctx1
User                          : user1
Session ID                    : 1
User IPv4 address             : 192.168.56.1
Received requests             : 81
Sent requests                 : 0
Dropped requests              : 81
Received replies              : 0
Sent replies                  : 0
Dropped replies               : 0
Received keepalives           : 1
Sent keepalive replies        : 1
Received configuration updates: 0
Sent configuration updates    : 0

Context                       : ctx2
User                          : user1
Session ID                    : 2
User IPv6 address             : 1234::5001
Received requests             : 81
Sent requests                 : 0
Dropped requests              : 81
Received replies              : 0
Sent replies                  : 0
Dropped replies               : 0
Received keepalives           : 1
Sent keepalives replies       : 1
Received configuration updates: 0
Sent configuration updates    : 0
```

Display IP access packet statistics for user **user1** in SSL VPN context **ctx1**.

```
<Sysname> display sslvpn ip-tunnel statistics context ctx1 user user1
SSL VPN session IP-tunnel statistics:
Context                       : ctx1
User                          : user1
Session ID                    : 1
User IPv4 address             : 192.168.56.1
Received requests             : 81
Sent requests                 : 0
Dropped requests              : 81
Received replies              : 0
Sent replies                  : 0
```

```
Dropped replies               : 0
Received keepalives           : 1
Sent keepalive replies        : 1
Received configuration updates: 0
Sent configuration updates    : 0

Context                       : ctx1
User                          : user1
Session ID                    : 2
User IPv6 address             : 1234::5001
Received requests             : 81
Sent requests                 : 0
Dropped requests              : 81
Received replies              : 0
Sent replies                  : 0
Dropped replies               : 0
Received keepalives           : 1
Sent keepalives replies       : 1
Received configuration updates: 0
Sent configuration updates    : 0
```

Table 7 Command output

Field	Description
Context	SSL VPN context to which the SSL VPN user belongs.
User	Login username used by the SSL VPN user.
User IPv4 address	IPv4 address of the SSL VPN user.
User IPv6 address	IPv6 address of the SSL VPN user.
Received requests	Number of IP access requests received by the SSL VPN gateway from the user.
Sent requests	Number of IP access requests forwarded by the SSL VPN gateway to internal servers.
Dropped requests	Number of IP access requests dropped by the SSL VPN gateway.
Received replies	Number of IP access replies received by the SSL VPN gateway from internal servers.
Sent replies	Number of IP access replies forwarded by the SSL VPN gateway to the user.
Dropped replies	Number of IP access replies dropped by the SSL VPN gateway.
Received keepalives	Number of keepalive messages received by the SSL VPN gateway from the user.
Sent keepalives replies	Number of keepalive replies sent by the SSL VPN gateway to the user.
Received configuration updates	Number of configuration update messages received by the SSL VPN gateway from the user.
Sent configuration updates	Number of configuration update messages sent by the SSL VPN gateway to the user.

Field	Description
Client	Statistics of the traffic transmitted between the SSL VPN gateway and the IP access client: • **In bytes**—Number of bytes received by the SSL VPN gateway from the client. • **Out bytes**—Number of bytes sent by the SSL VPN gateway to the client.
Server	Statistics of the traffic transmitted between the SSL VPN gateway and the server: • **In bytes**—Number of bytes received by the SSL VPN gateway from the server. • **Out bytes**—Number of bytes sent by the SSL VPN gateway to the client.

display sslvpn policy-group

Use **display sslvpn policy-group** to display SSL VPN policy group information.

Syntax

display sslvpn policy-group *group-name* [**context** *context-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

group-name: Specifies a policy group by its name, a case-insensitive string of 1 to 31 characters.

context *context-name*: Specifies an SSL VPN context by its name. An SSL VPN context name is a case-insensitive string of 1 to 31 characters, and can contain only letters, digits, and underscores (_). If you do not specify an SSL VPN context, this command displays information about policy groups with the specified group name in all SSL VPN contexts.

Examples

Display information about policy groups named **pg1** in all SSL VPN contexts.

```
<Sysname> display sslvpn policy-group pg1
Group policy: pg1
  Context: context1
   Idle timeout: 35 min
   Redirect resource type: url-item
   Redirect resource name: url1

  Context: context2
   Idle timeout: 40 min
   Redirect resource: Not configured
```

Table 8 Command output

Field	Description
Idle timeout	Maximum idle time of an SSL VPN session, in minutes.
Redirect resource	Redirect resource in the policy group assigned to the SSL VPN context.

display sslvpn port-forward connection

Use **display sslvpn port-forward connection** to display TCP port forwarding connection information.

Syntax

display sslvpn port-forward connection [**context** *context-name*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

context *context-name*: Specifies an SSL VPN context by its name. An SSL VPN context name is a case-insensitive string of 1 to 31 characters, and can contain only letters, digits, and underscores (_). If you do not specify an SSL VPN context, this command displays TCP port forwarding connection information for all SSL VPN contexts.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays TCP port forwarding connection information for all member devices.

Examples

Display TCP port forwarding connection information for all SSL VPN contexts.

```
<Sysname> display sslvpn port-forward connection
SSL VPN context  : ctx1
  Client address : 192.0.2.1
  Client port    : 1025
  Server address : 192.168.0.39
  Server port    : 80
  Slot           : 1
  Status         : Connected
SSL VPN context  : ctx2
  Client address : 3000::983F:7A36:BD06:342D
  Client port    : 56190
  Server address : 300::1
  Server port    : 23
  Slot           : 1
  Status         : Connecting
```

Table 9 Command output

Field	Description
Client address	IP address of the SSL VPN client.
Client port	Port number of the SSL VPN client.
Server address	IP address of the internal server.
Server port	Port number of the internal server.
Slot	IRF member ID of the device.
Status	Connection status, **Connected** or **Connecting**.

display sslvpn prevent-cracking frozen-ip

Use **display sslvpn prevent-cracking frozen-ip** to display information about IP addresses frozen for cracking prevention.

Syntax

display sslvpn prevent-cracking frozen-ip { **statistics** | **table** } [**context** *context-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

statistics: Displays frozen IP address statistics.

table: Displays information about frozen IP address entries.

context *context-name*: Specifies an SSL VPN context by its name. An SSL VPN context name is a case-insensitive string of 1 to 31 characters, and can contain only letters, digits, and underscores (_). If you do not specify an SSL VPN context, this command displays frozen IP address information for all SSL VPN contexts.

Examples

Display frozen IP address statistics in all SSL VPN contexts.

```
<Sysname> display sslvpn prevent-cracking frozen-ip statistics
SSL VPN context: ctx1
Total number of frozen IP addresses: 1
Total number of username/password authentication failures: 1
Total number of code verification failures: 1
Total number of SMS authentication failures: 1
Total number of custom authentication failures: 1
SSL VPN context: ctx2
Total number of frozen IP addresses: 1
```

```
Total number of username/password authentication failures: 1
Total number of code verification failures: 1
Total number of SMS authentication failures: 1
Total number of custom authentication failures: 1
```

Display frozen IP address entries in all SSL VPN contexts.

```
<Sysname> display sslvpn prevent-cracking frozen-ip table
SSL VPN context: ctx1
IP address   Authentication method             Frozen at            Unfrozen at
8.1.1.80     code verification                2019-10-08 08:30:01  2019-10-08 08:35:04
3.3.3.30     Username/password authentication 2019-10-08 08:35:01  2019-10-08 08:39:04
SSL VPN context: ctx2
IP address   Authentication method             Frozen at            Unfrozen at
121.5.5.32   Username/password authentication  2019-10-08 08:31:01  2019-10-08 08:45:04
123.3.3.3    code verification                2019-10-08 08:35:01  2019-10-08 08:55:04
```

Table 10 Command output

Field	Description
SSL VPN context	Name of the SSL VPN context.
IP address	Frozen IP address.
Authentication method	Authentication methods required for logging in to the SSL VPN context. Options include: • **Username/password authentication**. • **Code verification**. • **SMS authentication**. • **Custom authentication**. The use of authentication methods must meet the following requirements: • You can enable one or multiple authentication methods. • Username/password authentication must be enabled in an SSL VPN context. • Custom authentication and SMS authentication cannot both be enabled at the same time. All authentication methods can be used independently except for code verification.
Frozen at	Time when the IP address was frozen.
Unfrozen at	Time when the frozen IP address is to be unfrozen. **N/A** means that the IP address will never be unfrozen.

display sslvpn session

Use **display sslvpn session** to display SSL VPN session information.

Syntax

display sslvpn session [**context** *context-name*] [**user** *user-name* | **verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

context *context-name*: Specifies an SSL VPN context by its name. An SSL VPN context name is a case-insensitive string of 1 to 31 characters, and can contain only letters, digits, and underscores (_). If you do not specify an SSL VPN context, this command displays SSL VPN session information for all SSL VPN contexts.

user *user-name*: Specifies an SSL VPN user by the username, a case-insensitive string of 1 to 63 characters. If you specify a user, this command displays detailed SSL VPN session information for the user. If you do not specify a user, this command displays brief SSL VPN session information for all users.

verbose: Displays detailed SSL VPN session information for all SSL VPN users. If you do not specify this keyword, the command displays brief SSL VPN session information for the specified or all SSL VPN users.

Examples

Display brief SSL VPN session information for all users in all SSL VPN contexts.

```
<Sysname> display sslvpn session
Total users: 4

SSL VPN context: ctx1
Users: 2
Username        Connections  Idle time   Created       User IP
user1           5            0/00:00:23  0/04:47:16    192.0.2.1
user2           5            0/00:00:46  0/04:48:36    192.0.2.2

SSL VPN context: ctx2
Users: 2
Username        Connections  Idle time   Created       User IP
user3           5            0/00:00:30  0/04:50:06    192.168.2.1
user4           5            0/00:00:50  0/04:51:16    192.168.2.2
```

Table 11 Command output

Field	Description
Total users	Total number of users in all SSL VPN contexts.
SSL VPN context	Name of the SSL VPN context.
Users	Number of users in the SSL VPN context.
Username	Login name for the SSL VPN session.
Connections	Number of connections in the SSL VPN session.
Idle time	Duration that the SSL VPN session has been idle, in the format of days/hh:mm:ss.
Created	Time elapsed since the SSL VPN session was created, in the format of days/hh:mm:ss.
User IP	IP address used by the SSL VPN session.

Display SSL VPN session information for SSL VPN user **user1**.

```
<Sysname> display sslvpn session user user1
User                    : user1
Authentication method   : Username/password authentication
Context                 : context1
Policy group            : pgroup
Idle timeout            : 30 min
Created at              : 13:49:27 UTC Wed 05/14/2014
Lastest                 : 17:50:58 UTC Wed 05/14/2014
User IPv4 address       : 192.0.2.1
Session ID              : 1
Web browser/OS          : Internet Explorer
Send rate               : 0.00 B/s
Receive rate            : 0.00 B/s
Sent bytes              : 0.00 B
Received bytes          : 0.00 B

User                    : user1
Authentication method   : Username/password authentication
Context                 : context2
Policy group            : Default
Idle timeout            : 2100 sec
Created at              : 14:15:12 UTC Wed 05/14/2014
Lastest                 : 18:56:58 UTC Wed 05/14/2014
User IPv6 address       : 0:30::983F:7A36:BD06:342D
Session ID              : 5
Web browser/OS          : Internet Explorer
Send rate               : 0.00 B/s
Receive rate            : 0.00 B/s
Sent bytes              : 0.00 B
Received bytes          : 0.00 B
```

Display detailed SSL VPN session information for all users in all SSL VPN contexts.

```
<Sysname> display sslvpn session verbose
User                    : user1
Authentication method   : Username/password authentication
Context                 : context1
Policy group            : pgroup
Idle timeout            : 30 min
Created at              : 13:49:27 UTC Wed 05/14/2014
Lastest                 : 17:50:58 UTC Wed 05/14/2014
User IPv4 address       : 192.0.2.1
Session ID              : 1
Web browser/OS          : Internet Explorer
Send rate               : 0.00 B/s
Receive rate            : 0.00 B/s
Sent bytes              : 0.00 B
Received bytes          : 0.00 B

User                    : user1
```

```
Authentication method  : Username/password authentication
Context                : context2
Policy group           : Default
Idle timeout           : 2100 sec
Created at             : 14:15:12 UTC Wed 05/14/2014
Lastest                : 18:56:58 UTC Wed 05/14/2014
User IPv6 address      : 0:30::983F:7A36:BD06:342D
Session ID             : 5
Web browser/OS         : Internet Explorer
Send rate              : 0.00 B/s
Receive rate           : 0.00 B/s
Sent bytes             : 0.00 B
Received bytes         : 0.00 B
```

Table 12 Command output

Field	Description
User	SSL VPN username.
Authentication method	Authentication methods required for logging in to the SSL VPN context. Options include: • **Username/password authentication**. • **Certificate authentication**. • **Code verification**. • **SMS authentication**. • **Custom authentication**. The use of authentication methods must meet the following requirements: • You can enable one or multiple authentication methods. • Username/password authentication, certificate authentication, or both must be enabled in an SSL VPN context. • Custom authentication and SMS authentication cannot both be enabled at the same time. • All authentication methods can be used independently except for code verification.
Context	Context to which the user belongs.
Policy group	Policy group used by the user.
Idle timeout	Idle timeout time of the SSL VPN session, in seconds.
Created at	Time at which the SSL VPN session was created.
Lastest	Most recent time when the SSL VPN user accessed resources through the SSL VPN session.
Allocated IP	IP address allocated to the iNode client of the SSL VPN user. This field is displayed only for iNode users.
User IPv4 address	IPv4 address used by the SSL VPN session.
User IPv6 address	IPv6 address used by the SSL VPN session.
Web browser/OS	Web browser or operating system used by the SSL VPN user.
Send rate	Sending rate of the SSL VPN session in one of the following units: • **B/s**—Bytes per second.

Field	Description
	• **KB/s**—Kilobytes per second. • **MB/s**—Megabytes per second. • **GB/s**—Gigabytes per second. • **TB/s**—Terabytes per second. • **PB/s**—Petabytes per second.
Receive rate	Receiving rate of the SSL VPN session in one of the following units: • **B/s**—Bytes per second. • **KB/s**—Kilobytes per second. • **MB/s**—Megabytes per second. • **GB/s**—Gigabytes per second. • **TB/s**—Terabytes per second. • **PB/s**—Petabytes per second.
Sent bytes	Traffic sent by the SSL VPN session in one of the following units: • **B**—Bytes. • **KB**—Kilobytes. • **MB**—Megabytes. • **GB**—Gigabytes. • **TB**—Terabytes. • **PB**—Petabytes.
Received bytes	Traffic received by the SSL VPN session in one of the following units: • **B**—Bytes. • **KB**—Kilobytes. • **MB**—Megabytes. • **GB**—Gigabytes. • **TB**—Terabytes. • **PB**—Petabytes.

display sslvpn webpage-customize template

Use **display sslvpn webpage-customize template** to display SSL VPN webpage template information.

Syntax

display sslvpn webpage-customize template

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display information about all webpage templates.

```
<Sysname> display sslvpn webpage-customize template
Template name            Type             Status
```

```
default                 Pre-defined       Normal
system                  Predefined        Normal
User1                   User-defined      File login.html missing
User2                   User-defined      File home.html missing
```

Table 13 Command output

Field	Description
Template name	Name of the SSL VPN webpage template.
Type	Type of the SSL VPN webpage template: • **Pre-defined**. • **User-defined**.
Status	State of the SSL VPN webpage template: • **Normal**—The template is complete and can be used. • **File login.html missing**—The login.html file is missing in the template. • **File home.html missing**—The home.html file is missing in the template. • **Version incompatible**—The version of the template is inconsistent with the version of the predefined template.

Related commands

sslvpn webpage-customize

webpage-customize

emo-server

Use **emo-server** to specify an Endpoint Mobile Office (EMO) server for mobile clients.

Use **undo emo-server** to restore the default.

Syntax

emo-server address { *host-name* | *ipv4-address* } **port** *port-number*

undo emo-server

Default

No EMO server is specified for mobile clients.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

address: Specifies the host name or IPv4 address of the EMO server.

host-name: Specifies the host name of the EMO server, a case-insensitive string of 1 to 127 characters. Valid characters are letters, digits, underscores (_), hyphens (-), and dots (.).

ipv4-address: Specifies the IPv4 address of the EMO server, in dotted decimal notation. The IP address cannot be a multicast, broadcast, or loopback address.

port *port-number*: Specifies the port number of the EMO server, in the range of 1025 to 65535.

Usage guidelines

An EMO server provides services for mobile clients. The SSL VPN gateway issues the EMO server information to the clients, and the clients can access available service resources through the EMO server.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the IP address of the EMO server as 10.10.1.1 and the port number as 9058 for context **ctx1**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] emo-server address 10.10.1.1 port 9058
```

exclude

Use **exclude** to add an excluded route to a route list.

Use **undo exclude** to delete an excluded route from a route list.

Syntax

exclude *ip-address* { *mask* | *mask-length* }

undo exclude *ip-address* { *mask* | *mask-length* }

Default

No excluded routes exist in a route list.

Views

Route list view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the destination IP address of the route. It cannot be a multicast, broadcast, or loopback address.

mask: Specifies the subnet mask of the destination IP address.

mask-length: Specifies the mask length of the destination IP address, an integer in the range of 0 to 32.

Usage guidelines

To deny user access to specific network nodes or segments behind an SSL VPN gateway, configure excluded routes for those nodes or segments.

When a client accesses the SSL VPN gateway in IP access mode, the SSL VPN gateway issues excluded routes to the client. The client adds the excluded routes to the local routing table. Traffic that matches the excluded routes are not sent to the SSL VPN gateway.

You can add multiple excluded routes to a route list.

If you execute the **include** and **exclude** commands to add the same route to a route list, the most recent configuration takes effect.

Examples

Add excluded route 192.168.0.0/16 to route list **rtlist**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] ip-route-list rtlist
[Sysname-sslvpn-context-ctx1-route-list-rtlist] exclude 192.168.0.0 16
```

Related commands

include

execution (port forwarding item view)

Use **execution** to configure a resource link for a port forwarding item.

Use **undo execution** to restore the default.

Syntax

execution *script*

undo execution

Default

No resource link is configured for a port forwarding item.

Views

Port forwarding item view

Predefined user roles

network-admin

context-admin

Parameters

script: Specifies the script for the resource link, a case-insensitive string of 1 to 255 characters.

Usage guidelines

You can configure a resource link in one of the following methods:

- Enter a URL resource in the format of **url(**'*url-value*'**)**. The *url-value* argument specifies the URL link. The complete format for *url-value* is *protocol*://*hostname or address*:*port number*/*resource path*.
- Enter an executable JavaScript for a resource to provide access to the resource.

After you configure a resource link for a port forwarding item, you can click the port forwarding name on the SSL VPN Web page to access the resource.

If you execute this command for a port forwarding item multiple times, the most recent configuration takes effect.

Examples

Configure the **url('http://127.0.0.1')** resource for port forwarding item **pfitem1**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] port-forward-item pfitem1
[Sysname-sslvpn-context-ctx1-forward-item-pfitem1] execution url('http://127.0.0.1')
```

execution (shortcut view)

Use **execution** to configure a resource link for a shortcut.

Use **undo execution** to restore the default.

Syntax

execution *script*

undo execution

Default

No resource link is configured for a shortcut.

Views

Shortcut view

Predefined user roles

network-admin

context-admin

Parameters

script: Specifies the script for the resource, a case-insensitive string of 1 to 255 characters.

Usage guidelines

You can configure a resource link in either of the following methods:

- Enter the resource link in the format of **url(**'*url-value*'**)**. The *url-value* argument specifies the corresponding resource. The complete format for *url-value* is *protocol*://*hostname or address*:*port number*/*resource path*.
- Enter an application resource in the format of **app**('*app-value*'). The *app-value* argument specifies the application path. For example, the *app-value* argument can be **c:\windows\system32\notepad++.exe,** which is used for opening the notepad++.exe application.
- Enter an executable JavaScript for a resource to provide access to the resource.

After you configure a resource link for a shortcut, you can click the shortcut name on the SSL VPN Web page to access the resource.

If you execute this command for a shortcut multiple times, the most recent configuration takes effect.

Examples

Configure the **url('http://10.0.0.1')** resource for shortcut **shortcut1**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] shortcut shortcut1
[Sysname-sslvpn-context-ctx1-shortcut-shortcut1] execution url('http://10.0.0.1')
```

Configure the **app('c:\windows\system32\notepad++.exe')** resource for shortcut **shortcut2**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] shortcut shortcut2
[Sysname-sslvpn-context-ctx1-shortcut-shortcut2] execution
app('c:\windows\system32\notepad++.exe')
```

file-policy

Use **file-policy** to create a file policy and enter its view, or enter the view of an existing file policy.

Use **undo file-policy** to delete a file policy.

Syntax

file-policy *policy-name*

undo file-policy *policy-name*

Default

No file policies exist.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies a file policy name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

The SSL VPN gateway uses a file policy to rewrite the content of Web page files before forwarding them to requesting Web access users.

You can configure multiple file policies in an SSL VPN context.

Examples

Create a file policy named **fp** and enter its view.

```
<Sysname> system-view
[Sysname] sslvpn context ctx
[Sysname-sslvpn-context-ctx] file-policy fp
[Sysname-sslvpn-context-ctx-file-policy-fp]
```

Related commands

sslvpn context

filter ip-tunnel acl

Use **filter ip-tunnel acl** to specify an advanced ACL for IP access filtering.

Use **undo filter ip-tunnel acl** to remove the advanced ACL configuration for IP access filtering.

Syntax

filter ip-tunnel [**ipv6**] **acl** *advanced-acl-number*

undo filter ip-tunnel [**ipv6**] **acl**

Default

All IP accesses are permitted.

Views

SSL VPN policy group view

Predefined user roles

network-admin

context-admin

Parameters

ipv6: Specifies an IPv6 ACL. Do not configure this keyword if you want to specify an IPv4 ACL.

acl *advanced-acl-number*: Specifies an advanced ACL by its number in the range of 3000 to 3999. If a rule in the specified ACL contains VPN settings, the rule does not take effect.

Usage guidelines

You can specify both an advanced ACL and a URI ACL for IP access filtering.

The SSL VPN gateway uses the following procedure to determine whether to forward an IP access request:

1. Matches the request against rules in the URI ACL:
   - If the request matches a permit rule, the gateway forwards the request.
   - If the request matches a deny rule, the gateway drops the request.
   - If the request does not match any rules in the URI ACL or if no URI ACL is available, the gateway proceeds to step 2.
2. Matches the request against rules in the advanced ACL:
   - If the request matches a permit rule, the gateway forwards the request.
   - If the request matches a deny rule, the gateway drops the request.
   - If the request does not match any rules in the advanced ACL or if no advanced ACL is available, the gateway drops the request.

If no URI ACL or advanced ACL is specified for IP access filtering, the SSL VPN gateway permits all IP accesses by default.

You can specify an IPv4 ACL, IPv6 ACL, or both by using this command, but you cannot specify multiple IPv4 ACLs or IPv6 ACLs. If you specify IPv4 or IPv6 ACLs multiple times, the most recent IPv4 or IPv6 ACL configuration takes effect.

Examples

Configure policy group **pg1** to use IPv4 ACL 3000 and IPv6 ACL 3500 for IP access filtering.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] policy-group pg1
[Sysname-sslvpn-context-ctx1-policy-group-pg1] filter ip-tunnel acl 3000
[Sysname-sslvpn-context-ctx1-policy-group-pg1] filter ip-tunnel ipv6 acl 3500
```

Related commands

filter ip-tunnel uri-acl

filter ip-tunnel uri-acl

Use **filter ip-tunnel uri-acl** to specify a URI ACL for IP access filtering.

Use **undo filter ip-tunnel uri-acl** to remove the URI ACL configuration for IP access filtering.

Syntax

filter ip-tunnel uri-acl *uri-acl-name*

undo filter ip-tunnel uri-acl

Default

All IP accesses are permitted.

Views

SSL VPN policy group view

Predefined user roles

network-admin

context-admin

Parameters

uri-acl-name: Specifies a URI ACL by its name, a case-insensitive string of 1 to 31 characters. The specified URI ACL must already exist.

Usage guidelines

You can specify both an advanced ACL and a URI ACL for IP access filtering.

The SSL VPN gateway uses the following procedure to determine whether to forward an IP access request:

1. Matches the request against rules in the URI ACL:
   - If the request matches a permit rule, the gateway forwards the request.
   - If the request matches a deny rule, the gateway drops the request.
   - If the request does not match any rules in the URI ACL or if no URI ACL is available, the gateway proceeds to step 2.
2. Matches the request against rules in the advanced ACL:
   - If the request matches a permit rule, the gateway forwards the request.
   - If the request matches a deny rule, the gateway drops the request.
   - If the request does not match any rules in the advanced ACL or if no advanced ACL is available, the gateway drops the request.

If no URI ACL or advanced ACL is specified for IP access filtering, the SSL VPN gateway permits all IP accesses by default.

If a rule in the URI ACL specified for IP access filtering contains HTTP or HTTPS settings, the rule does not take effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure policy group **abcpg** to use URI ACL **abcuriacl** for IP access filtering.

```
<Sysname> system-view
[Sysname] sslvpn context abc
[Sysname-sslvpn-context-abc] policy-group abcpg
[Sysname-sslvpn-context-abc-policy-group-abcpg] filter ip-tunnel uri-acl abcuriacl
```

filter tcp-access acl

Use **filter tcp-access acl** to specify an advanced ACL for TCP access filtering.

Use **undo filter tcp-access acl** to remove the advanced ACL configuration for TCP access filtering.

Syntax

filter tcp-access [**ipv6**] **acl** *advanced-acl-number*

undo filter tcp-access [**ipv6**] **acl**

Default

A user can access only the TCP resources in the TCP port forwarding list authorized to the user.

Views

SSL VPN policy group view

Predefined user roles

network-admin

context-admin

Parameters

ipv6: Specifies an IPv6 ACL. Do not configure this keyword if you want to specify an IPv4 ACL.

acl *advanced-acl-number*: Specifies an advanced ACL by its number in the range of 3000 to 3999. If a rule in the specified ACL contains VPN settings, the rule does not take effect.

Usage guidelines

You can specify both an advanced ACL and a URI ACL for TCP access filtering.

For mobile client users, the SSL VPN gateway uses the following procedure to determine whether to forward a TCP access request:

1. Matches the request against the authorized port forwarding list.
   - If the request matches a port forwarding item in the list, the gateway forwards the request.
   - If the request does not match any port forwarding items in the list, the gateway proceeds to step 2.
2. Matches the request against the rules in the URI ACL:
   - If the request matches a permit rule, the gateway forwards the request.
   - If the request matches a deny rule, the gateway drops the request.
   - If the request does not match any rules in the URI ACL or if no URI ACL is available, the gateway proceeds to step 3.
3. Matches the request against the rules in the advanced ACL:
   - If the request matches a permit rule, the gateway forwards the request.
   - If the request matches a deny rule, the gateway drops the request.
   - If the request does not match any rules in the advanced ACL or if no advanced ACL is available, the gateway drops the request.

For PC users, the ACLs configured for TCP access filtering do not take effect. They can access only the TCP resources authorized to them through the TCP port forwarding list.

You can specify an IPv4 ACL, IPv6 ACL, or both by using this command, but you cannot specify multiple IPv4 ACLs or IPv6 ACLs. If you specify IPv4 or IPv6 ACLs multiple times, the most recent IPv4 or IPv6 ACL configuration takes effect.

Examples

Configure policy group **pg1** to use IPv4 ACL 3000 and IPv6 ACL 3500 for TCP access filtering.

```
<Sysname> system-view
[Sysname]sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] policy-group pg1
[Sysname-sslvpn-context-ctx1-policy-group pg1] filter tcp-access acl 3000
[Sysname-sslvpn-context-ctx1-policy-group pg1] filter tcp-access ipv6 acl 3500
```

Related commands

filter tcp-access uri-acl

filter tcp-access uri-acl

Use **filter tcp-access uri-acl** to specify a URI ACL for TCP access filtering.

Use **undo filter tcp-access uri-acl** to remove the URI ACL configuration for TCP access filtering.

Syntax

filter tcp-access uri-acl *uri-acl-name*

undo filter tcp-access uri-acl

Default

A user can access only the TCP resources in the TCP port forwarding list authorized to the user.

Views

SSL VPN policy group view

Predefined user roles

network-admin

context-admin

Parameters

uri-acl-name: Specifies a URI ACL by its name, a case-insensitive string of 1 to 31 characters. The specified URI ACL must already exist.

Usage guidelines

You can specify both an advanced ACL and a URI ACL for TCP access filtering.

For mobile client users, the SSL VPN gateway uses the following procedure to determine whether to forward a TCP access request:

1. Matches the request against the authorized port forwarding list.
   - If the request matches a port forwarding items in the list, the gateway forwards the request.
   - If the request does not match any port forwarding items in the list, the gateway proceeds to step 2.
2. Matches the request against the rules in the URI ACL:
   - If the request matches a permit rule, the gateway forwards the request.
   - If the request matches a deny rule, the gateway drops the request.
   - If the request does not match any rules in the URI ACL or if no URI ACL is available, the gateway proceeds to step 3.
3. Matches the request against the rules in the advanced ACL:
   - If the request matches a permit rule, the gateway forwards the request.
   - If the request matches a deny rule, the gateway drops the request.
   - If the request does not match any rules in the advanced ACL or if no advanced ACL is available, the gateway drops the request.

For PC users, the ACLs configured for TCP access filtering do not take effect. They can access only the TCP resources authorized to them through the TCP port forwarding list.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure policy group **abcpg** to use URI ACL **abcuriacl2** for TCP access filtering.

```
<Sysname> system-view
[Sysname] sslvpn context abc
```

```
[Sysname-sslvpn-context-abc] policy-group abcpg
[Sysname-sslvpn-context-abc-policy-group-abcpg] filter tcp-access uri-acl abcuriacl2
```

Related commands

filter tcp-access acl

filter web-access acl

Use **filter web-access acl** to specify an advanced ACL for Web access filtering.

Use **undo filter web-access acl** to remove the advanced ACL configuration for Web access filtering.

Syntax

filter web-access [**ipv6**] **acl** *advanced-acl-number*

undo filter web-access [**ipv6**] **acl**

Default

A user can access only the Web resources in the URL list authorized to the user.

Views

SSL VPN policy group view

Predefined user roles

network-admin

context-admin

Parameters

ipv6: Specifies an IPv6 ACL. Do not configure this keyword if you want to specify an IPv4 ACL.

acl *advanced-acl-number*: Specifies an advanced ACL by its number in the range of 3000 to 3999. If a rule in the specified ACL contains VPN settings, the rule does not take effect.

Usage guidelines

You can specify both an advanced ACL and a URI ACL for Web access filtering.

The SSL VPN gateway uses the following procedure to determine whether to forward a Web access request:

1. Matches the request against the authorized URL list.
   - If the request matches a URL item in the list, the gateway forwards the request.
   - If the request does not match any URL entries in the list, the gateway proceeds to step 2.
2. Matches the request against rules in the URI ACL:
   - If the request matches a permit rule, the gateway forwards the request.
   - If the request matches a deny rule, the gateway drops the request.
   - If the request does not match any rules in the URI ACL or if no URI ACL is available, the gateway proceeds to step 3.
3. Matches the request against rules in the advanced ACL:
   - If the request matches a permit rule, the gateway forwards the request.
   - If the request matches a deny rule, the gateway drops the request.
   - If the request does not match any rules in the advanced ACL or if no advanced ACL is available, the gateway drops the request.

You can specify an IPv4 ACL, IPv6 ACL, or both by using this command, but you cannot specify multiple IPv4 ACLs or IPv6 ACLs. If you specify IPv4 or IPv6 ACLs multiple times, the most recent IPv4 or IPv6 ACL configuration takes effect.

Examples

Configure policy group **pg1** to use IPv4 ACL 3000 and IPv6 ACL 3500 for Web access filtering.

```
<Sysname> system-view
[Sysname]sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] policy-group pg1
[Sysname-sslvpn-context-ctx1-policy-group pg1] filter web-access acl 3000
[Sysname-sslvpn-context-ctx1-policy-group pg1] filter web-access ipv6 acl 3500
```

Related commands

filter web-access uri-acl

filter web-access uri-acl

Use **filter web-access uri-acl** to specify a URI ACL for Web access filtering.

Use **undo filter web-access uri-acl** to remove the URI ACL configuration for Web access filtering.

Syntax

filter web-access uri-acl *uri-acl-name*

undo filter web-access uri-acl

Default

Users can access only the Web resources authorized to them through the URL list.

Views

SSL VPN policy group view

Predefined user roles

network-admin

context-admin

Parameters

uri-acl-name: Specifies a URI ACL by its name, a case-insensitive string of 1 to 31 characters. The specified URI ACL must already exist.

Usage guidelines

The SSL VPN gateway uses the following procedure to determine whether to forward a Web access request:

1. Matches the request against the authorized URL list.
   - If the request matches a URL item in the list, the gateway forwards the request.
   - If the request does not match any URL entries in the list, the gateway proceeds to step 2.
2. Matches the request against rules in the URI ACL:
   - If the request matches a permit rule, the gateway forwards the request.
   - If the request matches a deny rule, the gateway drops the request.
   - If the request does not match any rules in the URI ACL or if no URI ACL is available, the gateway proceeds to step 3.
3. Matches the request against rules in the advanced ACL:

- If the request matches a permit rule, the gateway forwards the request.
- If the request matches a deny rule, the gateway drops the request.
- If the request does not match any rules in the advanced ACL or if no advanced ACL is available, the gateway drops the request.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure policy group **abcpg** to use URI ACL **abcuriacl1** for Web access filtering.

```
<Sysname> system-view
[Sysname] sslvpn context abc
[Sysname-sslvpn-context-abc] policy-group abcpg
[Sysname-sslvpn-context-abc-policy-group-abcpg] filter web-access uri-acl abcuriacl1
```

Related commands

filter web-access acl

force-logout

Use **force-logout** to force online users to log out.

Syntax

force-logout [**all** | **session** *session-id* | **user** *user-name*]

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

all: Logs out all users.

session *session-id*: Logs out all users in a session. The *session-id* argument specifies the session ID in the range of 1 to 4294967295.

user *user-name*: Logs out a user. The *user-name* argument specifies the username, a case-sensitive string of 1 to 63 characters.

Examples

Log out all users in session 1.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] force-logout session 1
```

force-logout max-onlines enable

force-logout max-onlines enable to enable the force logout feature.

undo force-logout max-onlines enable to disable the force logout feature.

Syntax

force-logout max-onlines enable

undo force-logout max-onlines enable

Default

The force logout feature is disabled.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Usage guidelines

By default, a user cannot log in if the number of logins using the account reaches the limit.

When a login is attempted but logins using the account reach the maximum, this feature logs out the user with the longest idle time to allow the new login.

Examples

Enable the force logout feature.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] force-logout max-onlines enable
```

gateway (SMS gateway authentication view)

Use **gateway** to specify an SMS gateway for SMS authentication.

Use **undo gateway** to restore the default.

Syntax

gateway *sms-gateway-name*

undo gateway

Default

No SMS gateway is specified for SMS authentication.

Views

SMS gateway authentication view

Predefined user roles

network-admin

context-admin

Parameters

sms-gateway-name: Specifies an SMS gateway by its name, a case-insensitive string of 1 to 31 characters. Valid characters are letters, digits, and underscores (_).

Examples

Specify SMS gateway **gw1** in SMS gateway authentication view.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] sms-auth sms-gw
[Sysname-sslvpn-context-ctx1-sms-auth-sms-gw] gateway gw1
```

gateway (SSL VPN context view)

Use **gateway** to associate an SSL VPN context with an SSL VPN gateway.

Use **undo gateway** to remove associated SSL VPN gateways.

Syntax

gateway *gateway-name* [**domain** *domain-name* | **virtual-host** *virtual-host-name*]

undo gateway [*gateway-name*]

Default

An SSL VPN context is not associated with an SSL VPN gateway.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

gateway-name: Specifies an SSL VPN gateway by its name, a case-insensitive string of 1 to 31 characters. Valid characters are letters, digits, and underscores (_).

domain *domain-name*: Specifies a domain name for the SSL VPN context, a case-insensitive string of 1 to 127 characters.

virtual-host *virtual-host-name*: Specifies a virtual host name for the SSL VPN context, a case-insensitive string of 1 to 127 characters. Valid characters are letters, digits, underscores (_), hyphens (-), and dots (.).

Usage guidelines

When you associate an SSL VPN context with an SSL VPN gateway, follow these guidelines:

- Make sure the context has a domain name or virtual host name different than any existing contexts associated with the SSL VPN gateway.

  The SSL VPN gateway uses the domain name or virtual host name that a remote user entered to determine the SSL VPN context to which the user belongs.
- If you do not specify a domain name or virtual host name for the context, you cannot associate other SSL VPN contexts with the SSL VPN gateway.

You can associate an SSL VPN context with a maximum of 10 SSL VPN gateways.

Examples

Associate SSL VPN context **ctx1** with SSL VPN gateway **gw1**, and specify the domain name as **domain1** for the context.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] gateway gw1 domain domain1
```

Related commands

display sslvpn context

heading

Use **heading** to configure a heading for a URL list.

Use **undo heading** to restore the default.

Syntax

heading *string*

undo heading

Default

The heading of a URL list is **Web**.

Views

URL list view

Predefined user roles

network-admin

context-admin

Parameters

string: Specifies a URL list heading, a case-sensitive string of 1 to 31 characters.

Examples

Specify **urlhead** as the heading of URL list **url**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] url-list url
[Sysname-sslvpn-context-ctx1-url-list-url] heading urlhead
```

Related commands

sslvpn context

url-list

http-redirect

Use **http-redirect** to enable HTTP redirection.

Use **undo http-redirect** to disable HTTP redirection.

Syntax

http-redirect [**port** *port-number*]

undo http-redirect

Default

HTTP redirection is disabled. An SSL VPN gateway does not process HTTP traffic.

Views

SSL VPN gateway view

Predefined user roles

network-admin

context-admin

Parameters

port-number: Specifies the HTTP port number to listen to, a value of 80 (the default) or in the range of 1025 to 65535.

Usage guidelines

This command enables an SSL VPN gateway to perform the following operations:

1. Listen to an HTTP port.
2. Redirect HTTP requests with the port number to the port used by HTTPS.
3. Send redirection packets to clients.

Examples

Enable HTTP redirection for HTTP port 1025.

```
<Sysname> system-view
[Sysname] sslvpn gateway gateway1
[Sysname-sslvpn-gateway-gateway1] http-redirect port 1025
```

idle-cut traffic-threshold

Use **idle-cut traffic-threshold** to set the SSL VPN session idle-cut traffic threshold.

Use **undo idle-cut traffic-threshold** to restore the default.

Syntax

idle-cut traffic-threshold *kilobytes*

undo idle-cut traffic-threshold

Default

The SSL VPN session idle-cut traffic threshold is 0 Kilobytes. An SSL VPN session will be disconnected if no traffic is transmitted within the session idle timeout.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

kilobytes: Specifies the session idle-cut traffic threshold in Kilobytes. The value range is 1 to 4294967295.

Usage guidelines

The SSL VPN session idle-cut traffic threshold refers to the minimum traffic required in the session idle timeout interval for a session not to be disconnected as an idle session.

After the idle-cut traffic threshold is set, the system counts the traffic transmitted in each SSL VPN session at intervals specified by the **timeout idle** command. If the traffic is less than the idle-cut traffic threshold, the system determines the session to be idle and disconnects the session.

If you change the setting of the **idle-cut traffic-threshold** or **timeout idle** command in an SSL VPN context, all session idle-cut traffic counters in the SSL VPN context will be cleared.

Examples

Set the SSL VPN session idle-cut traffic threshold to 1000 Kilobytes in SSL VPN context **ctx1**.

```
<Sysname> system-view
```

```
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] idle-cut traffic-threshold 1000
```

Related commands

timeout idle

include

Use **include** to add an included route to a route list.

Use **undo include** to delete an included route from a route list.

Syntax

include *ip-address* { *mask* | *mask-length* }

undo include *ip-address* { *mask* | *mask-length* }

Default

No included routes exist.

Views

Route list view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the destination IP address of the route. It cannot be a multicast, broadcast, or loopback address. The specified IP address must be the address of the network segment where the internal servers reside.

mask: Specifies the subnet mask.

mask-length: Specifies the mask length of the route, an integer in the range of 0 to 32.

Usage guidelines

To permit user access to specific network nodes or segments behind an SSL VPN gateway, configure included routes for those nodes or segments.

When a client accesses an SSL VPN gateway in IP access mode, the SSL VPN gateway issues the included routes to the client. The client adds the included routes to the local routing table, using the VNIC as the output interface. Traffic that matches the included routes are sent to the SSL VPN gateway through the VNIC.

You can add multiple included routes to a route list.

If you execute the **include** and **exclude** commands to add the same route to a route list, the most recent configuration takes effect.

Examples

Add included route 10.0.0.0/8 to route list **rtlist**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] ip-route-list rtlist
[Sysname-sslvpn-context-ctx1-route-list-rtlist] include 10.0.0.0 8
```

Related commands

exclude

interface sslvpn-ac

Use **interface sslvpn-ac** to create an SSL VPN AC interface and enter its view, or enter the view of an existing SSL VPN AC interface.

Use **undo interface sslvpn-ac** to delete an SSL VPN AC interface.

Syntax

interface sslvpn-ac *interface-number*

undo interface sslvpn-ac *interface-number*

Default

No SSL VPN AC interfaces exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interface-number: Specifies an SSL VPN AC interface number in the range of 0 to 4095.

Examples

Create SSL VPN AC 1000 and enter its view.

```
<Sysname>system-view
[Sysname]interface SSLVPN-AC 1000
[Sysname-SSLVPN-AC1000]
```

ip address

Use **ip address** to configure an IPv4 address and a port number for an SSL VPN gateway.

Use **undo ip address** to restore the default.

Syntax

ip address *ip-address* [**port** *port-number*]

undo ip address

Default

An SSL VPN gateway uses IPv4 address 0.0.0.0 and port number 443.

Views

SSL VPN gateway view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies an IP address for the SSL VPN gateway, in dotted decimal notation.

port *port-number*: Specifies a port number for the SSL VPN gateway. The port number is 443 (the default value) or in the range of 1025 to 65535.

Usage guidelines

A remote user uses the IPv4 address and port number configured by this command to access an SSL VPN gateway.

The specified IPv4 address must be the IP address of an interface on the gateway device and is reachable from clients and internal servers.

If the gateway uses the default address (0.0.0.0), make sure its port number is different from the port number of the HTTPS server on the device.

The IPv4 address and port number of an SSL VPN gateway cannot both be the same as those of the HTTPS server on the device. Otherwise, you can access only the SSL VPN Web interface but cannot access the device management Web interface by using those IPv4 address and port number.

If you execute this command multiple times, the most recent configuration takes effect.

An SSL VPN gateway can use an IPv4 address, an IPv6 address, but not both. If you configure both IPv4 and IPv6 addresses, the most recent configuration takes effect. (The IPv6 address is configured by using the **ipv6 address** command.)

Examples

Configure the IPv4 address of SSL VPN gateway **gw1** as 10.10.1.1 and the port number as 8000.

```
<Sysname> system-view
[Sysname] sslvpn gateway gw1
[Sysname-sslvpn-gateway-gw1] ip address 10.10.1.1 port 8000
```

Related commands

display sslvpn gateway

ipv6 address

ip-route-list

Use **ip-route-list** to create a route list for an SSL VPN context and enter its view, or enter the view of an existing route list.

Use **undo ip-route-list** to delete a route list.

Syntax

ip-route-list *list-name*

undo ip-route-list *list-name*

Default

No route lists exist.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

list-name: Specifies a name for the route list, a case-insensitive string of 1 to 31 characters.

Usage guidelines

You can add routes to a route list. The routes can be issued to IP access clients for them to access internal servers behind the SSL VPN gateway.

You cannot delete a route list that is used by a policy group. To delete the route list, execute the **undo ip-tunnel access-route** command to remove the configuration and then execute the **undo ip-route-list** command.

Examples

In SSL VPN context **ctx1**, create a route list named **rtlist** and enter its view.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] ip-route-list rtlist
[Sysname-sslvpn-context-ctx1-route-list-rtlist]
```

Related commands

ip-tunnel access-route

ip-tunnel access-route

Use **ip-tunnel access-route** to specify the routes to be issued to clients.

Use **undo ip-tunnel access-route** to restore the default.

Syntax

ip-tunnel access-route { *ip-address* { *mask-length* | *mask* } | **force-all** | **ip-route-list** *list-name* }

undo ip-tunnel access-route

Default

No routes to be issued to clients are specified.

Views

SSL VPN policy group view

Predefined user roles

network-admin

context-admin

Parameters

ip-address { *mask-length* | *mask* }: Configures a route to be issued to a client. The *ip-address* argument specifies the destination address of the route. It cannot be a multicast, broadcast, or loopback address. The *mask-length* argument specifies the mask length of the route, in the range of 0 to 32.

force-all: Forces all traffic to be sent to the SSL VPN gateway.

ip-route-list *list-name*: Issues routes in the specified route list to clients. The *list-name* argument specifies the route list name, a case-insensitive string of 1 to 31 characters. The specified route list must have been created by using the **ip-route-list** command.

Usage guidelines

When a client accesses an SSL VPN gateway in IP access mode, the SSL VPN gateway issues the configured route or the specified routes to the client. The client adds the routes, using the VNIC as the output interface. Packets from the client to the internal servers match the routes, and therefore are sent to the SSL VPN gateway through the VNIC.

To issue multiple routes to a client, execute the **ip-tunnel access-route ip-route-list** *list-name* command. To issue a route to a client, execute the **ip-tunnel access-route** *ip-address* { *mask-length* | *mask* } command.

After you execute the **ip-tunnel access-route force-all** command, the SSL VPN gateway issues a default route to the SSL VPN client. The default route uses the VNIC as the output interface and has the highest priority among all default routes on the client. Packets for destinations not in the routing table are sent to the SSL VPN gateway through the VNIC. The SSL VPN gateway monitors the SSL VPN client in real time. It does not allow the client to delete the default route or add a default route with a higher priority.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

In the view of policy group **pg1**, configure the SSL VPN gateway to issue routes in route list **rtlist** to a client.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] ip-route-list rtlist
[Sysname-sslvpn-context-ctx1-route-list-rtlist] include 10.0.0.0 8
[Sysname-sslvpn-context-ctx1-route-list-rtlist] include 20.0.0.0 8
[Sysname-sslvpn-context-ctx1-route-list-rtlist] quit
[Sysname-sslvpn-context-ctx1] policy-group pg1
[Sysname-sslvpn-context-ctx1-policy-group-pg1] ip-tunnel access-route ip-route-list
rtlist
```

Related commands

ip-route-list

ip-tunnel address-pool (SSL VPN context view)

Use **ip-tunnel address-pool** to specify an address pool for IP access in an SSL VPN context.

Use **undo ip-tunnel address-pool** to restore the default.

Syntax

ip-tunnel address-pool *pool-name* **mask** { *mask-length* | *mask* }

undo ip-tunnel address-pool

Default

No address pool is specified for IP access in an SSL VPN context.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

pool-name: Specifies an address pool by its name, a case-insensitive string of 1 to 31 characters.

mask { *mask-length* | *mask* }: Specifies the mask length or mask of the address pool. The value range for the mask length is 1 to 30.

Usage guidelines

When a client accesses an SSL VPN gateway in IP access mode, the SSL VPN gateway allocates an IP address to the client from either of the following address pools:

- Address pool specified for the policy group authorized to the client.
- Address pool specified for the SSL VPN context. This address pool is used only if no address pool is specified for the policy group authorized to the client.

If no free address is available in the address pool or the address pool does not exist, address allocation to the client will fail and the client's IP access request will be rejected.

If you specify a nonexistent address pool, the pool is effective for address allocation after it is created.

You can specify only one address pool for an SSL VPN context. If you execute this command multiple times, the most recent configuration takes effect.

For IP access users to access the SSL VPN gateway correctly, make sure the IP addresses in the address pool do not conflict with the IP addresses used on the device.

Examples

Specify address pool **pool1** for IP access.

```
<Sysname> system-view
[Sysname] sslvpn context ctx
[Sysname-sslvpn-context-ctx] ip-tunnel address-pool pool1 mask 24
```

Related commands

sslvpn ip address-pool

ip-tunnel address-pool (SSL VPN policy group view)

Use **ip-tunnel address-pool** to specify an address pool for IP access in an SSL VPN policy group.

Use **undo ip-tunnel address-pool** to restore the default.

Syntax

ip-tunnel address-pool *pool-name* **mask** { *mask-length* | *mask* }

undo ip-tunnel address-pool

Default

No address pool is specified for IP access in an SSL VPN policy group.

Views

SSL VPN policy group view

Predefined user roles

network-admin

context-admin

Parameters

pool-name: Specifies an address pool by its name, a case-insensitive string of 1 to 31 characters.

mask { *mask-length* | *mask* }: Specifies the mask length or mask of the address pool. The value range for the mask length is 1 to 30.

Usage guidelines

When a client accesses an SSL VPN gateway in IP access mode, the SSL VPN gateway allocates an IP address to the client from either of the following address pools:

- Address pool specified for the policy group authorized to the client.
- Address pool specified for the SSL VPN context. This address pool is used only if no address pool is specified for the policy group authorized to the client.

If no free address is available in the address pool or the address pool does not exist, address allocation to the client will fail and the client's IP access request will be rejected.

If you specify a nonexistent address pool, the pool is effective for address allocation after it is created.

You can specify only one address pool for an SSL VPN policy group. If you execute this command for an SSL VPN policy group multiple times, the most recent configuration takes effect.

For IP access users to access the SSL VPN gateway correctly, make sure the IP addresses in the address pool do not conflict with the IP addresses used on the device.

Examples

Specify address pool **pool1** for IP access in SSL VPN policy group **pg1**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] policy-group pg1
[Sysname-sslvpn-context-ctx1-policy-group-pg1] ip-tunnel address-pool pool1 mask 24
```

Related commands

sslvpn ip address-pool

ip-tunnel bind address

Use **ip-tunnel bind address** to bind IP addresses to an SSL VPN user.

Use **undo ip-tunnel bind address** to restore the default.

Syntax

ip-tunnel bind address { *ip-address-list* | **auto-allocate** *number* }

undo ip-tunnel bind address

Default

An SSL VPN user is not bound to IP addresses.

Views

SSL VPN user view

Predefined user roles

network-admin

context-admin

Parameters

ip-address-list: Specifies an IP address list, a string of 1 to 255 characters, which can contain digits, dots (.), commas (,), and hyphens (-). The IP address list specifies comma-separated IP address items. Each item specifies an IP address or specifies a range of IP addresses in the form of

start IP address-end IP address. For example, 10.1.1.5,10.1.1.10-10.1.1.20. The IP address list can contain a maximum of 10000 addresses excluding multicast addresses, broadcast addresses, and loopback addresses.

auto-allocate *number*: Enables the SSL VPN gateway to automatically bind the specified number of free IP addresses to the user. The value range for the *number* argument is 1 to 10.

Usage guidelines

When an SSL VPN user accesses the SSL VPN gateway in IP access mode, the SSL VPN gateway must assign an IP address to the user. This command allows you to specify the IP addresses that can be assigned to a user.

You can bind IP addresses to an SSL VPN user as follows:

- Use the *ip-address-list* argument to bind a list of IP addresses to the user.

  When the user accesses the SSL VPN gateway in IP access mode, the SSL VPN gateway assigns a bound IP address to the user.

  If an IP address has been assigned to another user, the SSL VPN gateway terminates the connection for that user and releases the IP address.
- Use the **auto-allocate** *number* option to enable the SSL VPN gateway to automatically bind the specified number of free addresses in the IP access address pool to the user.

The IP addresses to be bound to an SSL VPN user must meet the following requirements:

- If an IP access address pool is specified for the SSL VPN policy group authorized to the user, the IP addresses must exist in the address pool.
- If no address pool is specified for the SSL VPN policy group, the IP addresses must exist in the address pool specified for the SSL VPN context of the user.

You can bind the same IP address to different SSL VPN users only when the SSL VPN contexts of the users are associated with different VPN instances.

If you configure this command multiple times, the most recent configuration takes effect.

Examples

Bind IP addresses 10.1.1.5, 10.1.1.10 through 10.1.1.20, and 10.1.1.30 to SSL VPN user **user1**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx
[Sysname-sslvpn-context-ctx] user user1
[Sysname-sslvpn-context-ctx-user-user1] ip-tunnel bind address
10.1.1.5,10.1.1.10-10.1.1.20,10.1.1.30
```

Related commands

user

ip-tunnel dns-server

Use **ip-tunnel dns-server** to specify a DNS server for IP access.

Use **undo ip-tunnel dns-server** to restore the default.

Syntax

ip-tunnel dns-server { **primary** | **secondary** } *ip-address*

undo ip-tunnel dns-server { **primary** | **secondary** }

Default

No DNS servers are specified for IP access.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

primary: Specifies the primary DNS server.

secondary: Specifies the secondary DNS server.

ip-address: Specifies the IP address of the DNS server. It cannot be a multicast, broadcast, or loopback address.

Examples

Specify the primary DNS server 1.1.1.1 for IP access.

```
<Sysname> system-view
[Sysname] sslvpn context ctx
[Sysname-sslvpn-context-ctx] ip-tunnel dns-server primary 1.1.1.1
```

ip-tunnel interface

Use **ip-tunnel interface** to specify an SSL VPN AC interface for IP access in an SSL VPN context.

Use **undo ip-tunnel interface** to restore the default.

Syntax

ip-tunnel interface sslvpn-ac *interface-number*

undo ip-tunnel interface

Default

No SSL VPN AC interface is specified for IP access in an SSL VPN context.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

sslvpn-ac *interface-number*: Specifies the number of an SSL VPN AC interface. The interface must have been created.

Usage guidelines

The SSL VPN gateway uses the specified SSL VPN AC interface to communicate with SSL VPN users in IP access mode. It uses the SSL VPN AC interface to forward packets sent by the user to remote servers and to forward the servers' replies back to the user.

Examples

Specify SSL VPN AC 100 for IP access.

```
<Sysname> system-view
[Sysname] sslvpn context ctx
```

```
[Sysname-sslvpn-context-ctx] ip-tunnel interface sslvpn-ac 100
```

Related commands

interface sslvpn-ac

ip-tunnel keepalive

Use **ip-tunnel keepalive** to set the keepalive interval for IP access.

Use **undo ip-tunnel keepalive** to restore the default.

Syntax

ip-tunnel keepalive *seconds*

undo ip-tunnel keepalive

Default

The keepalive interval is 30 seconds for IP access.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies the keepalive interval in the range of 0 to 600 seconds. If the interval is set to 0 seconds, a client does not send keepalive messages to the SSL VPN gateway.

Usage guidelines

A client sends keepalive messages to the SSL VPN gateway to maintain sessions between them.

If an SSL VPN gateway does not receive any data or keepalive messages from a client during the session idle timeout time, it terminates the session with the client.

Set the keepalive interval to be shorter than the session idle timeout timer configured by the **timeout idle** command.

Examples

Set the keepalive interval to 50 seconds for SSL VPN context **ctx**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx
[Sysname-sslvpn-context-ctx] ip-tunnel keepalive 50
```

ip-tunnel log

Use **ip-tunnel log** to enable logging for IP address allocations and releases, IP access connection close events, or IP access packet drop events.

Use **undo ip-tunnel log** to disable logging for IP address allocations and releases, IP access connection close events, or IP access packet drop events.

Syntax

ip-tunnel log { **address-alloc-release** | **connection-close** | **packet-drop** }

undo ip-tunnel log { **address-alloc-release** | **connection-close** | **packet-drop** }

Default

Logging is disabled for IP access connection close events or IP access packet drop events.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

address-alloc-release: Enables logging for IP address allocations and releases for the VNIC of the IP access client.

connection-close: Enables logging for IP access connection close events.

packet-drop: Enables logging for IP access packet drop events.

Usage guidelines

If logging is enabled for IP address allocations and releases for the VNIC of the IP access client, the SSL VPN gateway generates logs when the VNIC's IP address is allocated or released.

If logging for IP access connection close events is enabled, the SSL VPN gateway generates logs when the connections established for SSL VPN IP access users are closed.

If logging for IP access packet drop events is enabled, the SSL VPN gateway generates logs when packets for SSL VPN IP access users are dropped.

The logs are sent to the information center of the device. For the logs to be output correctly, you must also configure the information center on the device. For more information about the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Enable logging for IP access connection close events.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] ip-tunnel log connection-close
```

Related commands

sslvpn context

ip-tunnel rate-limit

Use **ip-tunnel rate-limit** to set a rate limit for IP access upstream or downstream traffic.

Use **undo ip-tunnel rate-limit** to remove the rate limit set for IP access upstream or downstream traffic.

Syntax

ip-tunnel rate-limit { **downstream** | **upstream** } { **kbps** | **pps** } *value*

undo ip-tunnel rate-limit { **downstream** | **upstream** }

Default

No rate limit is set for IP access upstream or downstream traffic.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

downstream: Specifies the IP access downstream traffic, which is sent by internal servers to IP access users.

upstream: Specifies the IP access upstream traffic, which is sent by IP access users to internal servers.

kbps: Sets the unit of measurement for the rate limit to kilobits per second.

pps: Sets the unit of measurement for the rate limit to packets per second.

value: Sets the rate limit value, in the range of 1000 to 100000000.

Usage guidelines

You can set a rate limit for IP access upstream and downstream traffic, respectively. If you set the rate limit for the same traffic direction multiple times, the most recent configuration takes effect.

If the IP access upstream or downstream traffic exceeds the rate limit, subsequent upstream or downstream traffic will be discarded.

Examples

In SSL VPN context **ctx1**, set the rate limit to 10000 pps for IP access upstream traffic.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] ip-tunnel rate-limit upstream pps 10000
```

ip-tunnel web-resource auto-push

Use **ip-tunnel web-resource auto-push** to enable automatic pushing of accessible resources to IP access users through the Web page.

Use **undo ip-tunnel web-resource auto-push** to disable automatic pushing of accessible resources to IP access users through the Web page.

Syntax

ip-tunnel web-resource auto-push

undo ip-tunnel web-resource auto-push

Default

Automatic pushing of accessible resources to IP access users through the Web page is disabled.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Usage guidelines

This feature enables automatic pushing of accessible resources to a user through the Web page after the user logs in to the SSL VPN gateway through the IP access client (iNode client).

This feature is supported only when the iNode client is installed in the Windows system. You can install the iNode client in one of the following methods:

- Log in to the SSL VPN gateway through the browser, and then download and install the iNode client that comes with the device.
- Install the iNode client downloaded from the official website. In this way, you must select the iNode installation package for VPN gateway generation when customizing the iNode client. Otherwise, the user will be automatically logged out because the pushed webpage cannot detect whether the iNode client is logged in.

Examples

Enable automatic pushing of accessible resources to IP access users through the Web page in SSL VPN context **ctx1**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] ip-tunnel web-resource auto-push
```

ip-tunnel wins-server

Use **ip-tunnel wins-server** to specify a WINS server for IP access.

Use **undo ip-tunnel wins-server** to restore the default.

Syntax

ip-tunnel wins-server { **primary** | **secondary** } *ip-address*

undo ip-tunnel wins-server { **primary** | **secondary** }

Default

No WINS servers are specified for IP access.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

primary: Specifies the primary WINS server.

secondary: Specifies the secondary WINS server.

ip-address: Specifies the IPv4 address of the WINS server. It cannot be a multicast, broadcast, or loopback address.

Examples

Specify the primary WINS server 1.1.1.1 for IP access.

```
<Sysname> system-view
[Sysname] sslvpn context ctx
[Sysname-sslvpn-context-ctx] ip-tunnel wins-server primary 1.1.1.1
```

ipv6 address

Use **ipv6 address** to configure an IPv6 address and a port number for an SSL VPN gateway.

Use **undo ipv6 address** to restore the default.

Syntax

ipv6 address *ipv6-address* [**port** *port-number*]

undo ipv6 address

Default

No IPv6 address is configured for an SSL VPN gateway.

Views

SSL VPN gateway view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address: Specifies an IPv6 address for the SSL VPN gateway, a 16-byte hexadecimal string separated by colons.

port *port-number*: Specifies a port number for the SSL VPN gateway. The port number is 443 (the default value) or in the range of 1025 to 65535.

Usage guidelines

A remote user uses the IPv6 address and port number configured by this command to access an SSL VPN gateway.

The specified IPv6 address must be the address of an interface on the gateway device and is reachable from clients and internal servers.

Do not use the management address of the device as the IPv6 address of the SSL VPN gateway.

The IPv6 address and port number of an SSL VPN gateway cannot both be the same as those of the HTTPS server on the device. Otherwise, you can access only the SSL VPN Web interface but cannot access the device management Web interface by using those IPv6 address and port number.

If you execute this command multiple times, the most recent configuration takes effect.

An SSL VPN gateway can use an IPv4 address, an IPv6 address, but not both. If you configure both IPv4 and IPv6 addresses, the most recent configuration takes effect. (The IPv4 address is configured by using the **ip address** command.)

Examples

Configure the IPv6 address of SSL VPN gateway **gw1** as 200::1 and the port number as 8000.

```
<Sysname> system-view
[Sysname] sslvpn gateway gw1
[Sysname-sslvpn-gateway-gw1] ipv6 address 200::1 port 8000
```

Related commands

display sslvpn gateway

ip address

local-port

Use **local-port** to configure a port forwarding instance for a port forwarding item.

Use **undo local-port** to remove the configuration.

Syntax

local-port *local-port-number* **local-name** *local-name* **remote-server** *remote-server* **remote-port** *remote-port-number* [**description** *text*]

undo local-port

Default

A port forwarding item does not contain a port forwarding instance.

Views

Port forwarding item view

Predefined user roles

network-admin

context-admin

Parameters

local-port-number: Specifies a local port number in the range of 1 to 65535. The specified port number must be different from the port numbers of any existing services on the SSL VPN client.

local-name *local-name*: Specifies a local address or a local host name, a case-insensitive string of 1 to 253 characters. Valid characters are letters, digits, underscores (_), hyphens (-), and dots (.). To specify an IPv4 address, use an address in the network segment 127.0.0.0/8. To specify an IPv6 address, enclose the IPv6 address in brackets. For example, **local-name** [1234::5678].

remote-server *remote-server*: Specifies the IP address or domain name of a TCP service on an internal server. The *remote-server* argument is a case-insensitive string of 1 to 253 characters. Valid characters are letters, digits, underscores (_), hyphens (-), and dots (.). To specify an IPv6 address, enclose the IPv6 address in brackets. For example, **remote-server** [1234::5678].

remote-port *remote-port-number*: Specifies the port number of the TCP service on the internal server, in the range of 1 to 65535.

description *text*: Specifies a description, a case-sensitive string of 1 to 63 characters.

Usage guidelines

A port forwarding instance maps a TCP service on an internal server to a local address and port number on an SSL VPN client.

For example, for an SSL VPN client to use local address 127.0.0.1 and port 80 to access the internal HTTP server 192.168.0.213, perform the following tasks:

1. Create a port forwarding item (**tcp1** in this example).
2. Configure a port forwarding instance for the port forwarding item.

   ```
   local-port 80 local-name 127.0.0.1 remote-server 192.168.0.213 remote-port 80
   ```

   The port forwarding instance will be displayed together with the port forwarding item name on the SSL VPN Web page. In this example, **tcp1 (127.0.0.1:80 -> 192.168.0.213)** will be displayed.

If you map a TCP service to a local host name, the TCP access client software will add the IP address corresponding to the host name to the host file **hosts**. When the client logs out, the software restores the original host file. The host file **hosts** is in the directory **C:\Windows\System32\drivers\etc** of the client host.

You can configure only one port forwarding instance for a port forwarding item. If you execute this command for a port forwarding item multiple times, the most recent configuration takes effect.

Examples

Configure a port forwarding instance for port forwarding item **pfitem1**. The port forwarding instance maps IP address 192.168.0.213 and port 80 of the internal HTTP server to local address 127.0.0.1 and port 80.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] port-forward-item pfitem1
[Sysname-sslvpn-context-ctx1-port-forward-item-pfitem1] local-port 80 local-name
127.0.0.1 remote-server 192.168.0.213 remote-port 80 description http
```

Related commands

port-forward-item

log resource-access enable

Use **log resource-access enable** to enable resource access logging.

Use **undo log resource-access enable** to disable resource access logging.

Syntax

log resource-access enable [**brief** | **filtering**] *

undo log resource-access enable

Default

Resource access logging is disabled.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

brief: Records brief resource access information. If you specify this keyword, only the address and port number of the accessed resource will be recorded. If you do not specify this keyword, a large amount of information including webpage formatting information will be recorded.

filtering: Enables resource access log filtering. With this keyword specified, the device generates only one log for accesses of the same user to the same resource in a minute. If this keyword is not specified, the device generates a log for each resource access.

Usage guidelines

This feature logs resource accesses of SSL VPN users. The logs are sent to the information center of the device.

With the information center, you can set log message filtering and output rules, including output destinations.

The information center can output SSL VPN resource access logs to any destinations except the console and the monitor terminal. If you configure the console or monitor terminal as an output destination, the output destination setting will not take effect.

To view SSL VPN resource access logs stored on the device, use the **display logbuffer** command. Make sure you do not disable log output to the log buffer, which is enabled by default.

For more information about configuring the information center, see *Network Management and Monitoring Configuration Guide*.

If you execute the **log resource-access enable** command multiple times, the most recent configuration takes effect.

Examples

Enable resource access logging.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] log resource-access enable
```

log user-login enable

Use **log user-login enable** to enable logging for user login and logoff events.

Use **undo log user-login enable** to disable logging for user login and logoff events.

Syntax

log user-login enable

undo log user-login enable

Default

Logging for user login and logoff events is disabled.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Usage guidelines

This feature logs user login and logoff events. The logs are sent to the information center of the device. For the logs to be output correctly, you must also configure the information center on the device. For more information about the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Enable logging for user logins and logouts.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] log user-login enable
```

login-message

Use **login-message** to configure the welcome message to be displayed on the SSL VPN login page.

Use **undo log login-message** to restore the default.

Syntax

login-message { **chinese** *chinese-message* | **english** *english-message* }

undo login-message { **chinese** | **english** }

Default

The login welcome message is **Welcome to SSL VPN**.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

chinese *chinese-message*: Configures a login welcome message for the Chinese Web interface, a case-sensitive string of 1 to 255 characters.

english *english-message*: Configures a login welcome message for the English Web interface, a case-sensitive string of 1 to 255 characters.

Examples

Configure the login welcome message as **hello**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] login-message english hello
```

logo

Use **logo** to specify a logo to be displayed on SSL VPN webpages.

Use **undo logo** to restore the default.

Syntax

logo { **file** *file-name* | **none** }

undo logo

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

file *file-name*: Specifies a logo file by its name, a case-insensitive string of 1 to 255 characters. The file must be a .gif, .jpg, or .png file, and its size cannot exceed 100 KB. As a best practice, use a file whose image resolution is 110*30 pixels.

none: Specifies that no logo is displayed.

Usage guidelines

The specified logo file must exist on the local device.

After you specify a logo file, the logo is displayed on SSL VPN webpages even if the file is deleted.

Examples

Specify the logo in file **flash:/mylogo.gif** as the logo displayed on SSL VPN webpages.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] logo file flash:/mylogo.gif
```

max-onlines

Use **max-onlines** to set the maximum number of concurrent logins for each account.

Use **undo max-onlines** to restore the default.

Syntax

max-onlines *number*

undo max-onlines

Default

The maximum number of concurrent logins for each account is 32.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

number: Specifies the maximum number, in the range of 0 to 1048575. Value 0 indicates that the number of concurrent logins for each account is not limited.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the maximum number of concurrent logins for each account to 50.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] max-onlines 50
```

max-users

Use **max-users** to set the maximum number of sessions for an SSL VPN context.

Use **undo max-users** to restore the default.

Syntax

max-users *max-number*

undo max-users

Default

An SSL VPN context supports a maximum of 1048575 sessions.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

max-number: Specifies the maximum number of sessions, in the range of 1 to 1048575

Usage guidelines

If the limit is reached, new users cannot access the SSL VPN gateway.

Examples

Set the maximum number of sessions to 500 for SSL VPN context **ctx1**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] max-users 500
```

Related commands

display sslvpn context

message-server

Use **message-server** to specify a message server for mobile clients.

Use **undo message-server** to restore the default.

Syntax

message-server address { *host-name* | *ipv4-address* } **port** *port-number*

undo message-server

Default

No message server is specified for mobile clients.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

address: Specifies the host name or IPv4 address of the message server.

host-name: Specifies the host name of the message server, a case-insensitive string of 1 to 127 characters. Valid characters are letters, digits, underscores (_), hyphens (-), and dots (.).

ipv4-address: Specifies the IPv4 address of the message server, in dotted decimal notation. The IP address cannot be a multicast, broadcast, or loopback address.

port *port-number*: Specifies the port number of the message server, in the range of 1025 to 65535.

Usage guidelines

A message server provides services for mobile clients. The SSL VPN gateway issues the message server information to the clients, and the clients can access the message server.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the IP address of the message server as 10.10.1.1 and the port number as 8000 for context **ctx1**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx
[Sysname-sslvpn-context-ctx] message-server address 10.10.1.1 port 8000
```

Related commands

sslvpn context

mobile-num

Use **mobile-num** to specify the mobile number for receiving SMS messages.

Use **undo mobile-num** to restore the default.

Syntax

mobile-num *number*

undo mobile-num

Default

No mobile number is specified for receiving SMS messages.

Views

SSL VPN user view

Predefined user roles

network-admin

context-admin

Parameters

number: Specifies the mobile number, a string of 1 to 31 digits.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the mobile number as 111111 for user **user1** to receive SMS messages.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] user user1
[Sysname-sslvpn-context-ctx1-user-user1] mobile-num 111111
```

mobile-num-binding enable

Use **mobile-num-binding enable** to enable mobile number binding.

Use **undo mobile-num-binding enable** to disable mobile number binding.

Syntax

mobile-num-binding enable

undo mobile-num-binding enable

Default

Mobile number binding is disabled.

Views

SMS gateway authentication view

Predefined user roles

network-admin

context-admin

Usage guidelines

After SMS gateway authentication is enabled, a user must complete authentication through SMS messages to log in to the SSL VPN gateway.

- If the mobile number binding feature is enabled, the SSL VPN gateway displays **Please enter mobile number** for the user at the first login of the user. The user will use the entered mobile number to receive SMS messages for authentication. The SSL VPN gateway will bind the mobile number to the user and will not ask the user for the mobile number in subsequent logins.
- If the mobile number binding feature is disabled, the SSL VPN gateway will use the mobile number specified in SSL VPN user view for authentication of the user. If no mobile number is specified in SSL VPN user view, the login will fail.

If a mobile number is specified in SSL VPN user view, the mobile number binding feature does not take effect for the user. The SMS gateway always sends SMS messages to the specified mobile number for authentication of the user.

Examples

Enable mobile number binding in SMS gateway authentication view.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] sms-auth sms-gw
[Sysname-sslvpn-context-ctx-sms-auth-sms-gw] mobile-num-binding enable
```

Related commands

mobile-num

mtu

Use **mtu** to set the MTU of an SSL VPN AC interface.

Use **undo mtu** to restore the default.

Syntax

mtu *size*

undo mtu

Default

The default MTU is 1500 bytes.

Views

SSL VPN AC interface view

Predefined user roles

network-admin

context-admin

Parameters

size: Specifies an MTU value in the range of 100 to 64000 bytes.

Examples

Set the MTU of interface SSL VPN AC 1000 to 1430 bytes.

```
<Sysname> system-view
[Sysname] interface sslvpn-ac 1000
[Sysname-SSLVPN-AC1000] mtu 1430
```

new-content

Use **new-content** to specify the new content used to replace the old content.

Use **undo new-content** to restore the default.

Syntax

new-content *string*

undo new-content

Default

The new content used to replace the old content is not specified.

Views

Rewrite rule view

Predefined user roles

network-admin

context-admin

Parameters

string: Specifies the new content, a case-sensitive string of 1 to 256 characters.

Usage guidelines

During file content rewriting, the new content will replace the old content specified by using the **old-content** command.

If the new content contains spaces, enclose the content in double quotation marks.

Examples

Specify the new content in rewrite rule **rule1** of file policy **fp**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx
[Sysname-sslvpn-context-ctx] file-policy fp
[Sysname-sslvpn-context-ctx-file-policy-fp] rewrite-rule rule1
[Sysname-sslvpn-context-ctx-file-policy-fp-rewrite-rule-rule1] new-content
sslvpn_rewrite_htmlcode(d)
```

Related commands

old-content

notify-message

Use **notify-message** to configure a notification message to be displayed on a webpage.

Use **undo notify-message** to restore the default.

Syntax

notify-message { **login-page** | **resource-page** } { **chinese** *chinese-message* | **english** *english-message* }

undo notify-message { **login-page** | **resource-page** } { **chinese** | **english** }

Default

No notification message is configured.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

login-page: Specifies the SSL VPN gateway login page.

resource-page: Specifies the SSL VPN gateway resource page.

chinese *chinese-message*: Specifies the notification message to be displayed on the Chinese Web interface, a case-sensitive string of 1 to 255 characters.

english *english-message*: Specifies the notification message to be displayed on the English Web interface, a case-sensitive string of 1 to 255 characters.

Usage guidelines

Execute this command to configure a notification message displayed on the SSL VPN login page or resource page. The message is generally used to notify users to change their passwords.

In an SSL VPN context, if you execute this command multiple times for the same page of the same language, the most recent configuration takes effect.

Examples

In SSL VPN context **ctx1**, specify the notification message on the SSL VPN gateway login page as **Please change the password after login**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] notify-message login-page english Please change the
password after login
```

old-content

Use **old-content** to specify the old file content to be rewritten.

Use **undo old-content** to restore the default.

Syntax

old-content *string*

undo old-content

Default

The old file content to be rewritten is not specified.

Views

Rewrite rule view

Predefined user roles

network-admin

context-admin

Parameters

string: Specifies the old content, a case-sensitive string of 1 to 256 characters.

Usage guidelines

During file content rewriting, the old file content will be replaced by the new content specified by using the **new-content** command.

If the old content contains spaces, enclose the content in double quotation marks.

In the same file policy, the old content specified in different rewrite rules must be unique.

Examples

Specify the content to be rewritten in rewrite rule **rule1** of file policy **fp**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx
[Sysname-sslvpn-context-ctx] file-policy fp
[Sysname-sslvpn-context-ctx-file-policy-fp] rewrite rule rule1
[Sysname-sslvpn-context-ctx-file-policy-fp-rewrite-rule-rule1] old-content
"a.b.c.innerHTML = d;"
```

Related commands

new-content

password-authentication enable

Use **password-authentication enable** to enable username/password authentication.

Use **undo password-authentication enable** to disable username/password authentication.

Syntax

password-authentication enable

undo password-authentication enable

Default

Username/password authentication is enabled for an SSL VPN context.

Views

SSL VPN context

Predefined user roles

network-admin

context-admin

Examples

Disable username/password authentication for SSL VPN context **ctx**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx
[Sysname-sslvpn-context-ctx] undo password-authentication enable
```

Related commands

`certificate-authentication enable`

`display sslvpn context`

password-box hide

Use **`password-box hide`** to hide the password input box on the SSL VPN Web login page.

Use **`undo password-box hide`** to display the password input box on the SSL VPN Web login page.

Syntax

`password-box hide`

`undo password-box hide`

Default

The password input box is displayed on the SSL VPN Web login page.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Usage guidelines

If you want users to log in to the SSL VPN webpage by using authentication methods other than the username/password method, hide the password input box and configure the intended authentication methods.

After the password input box is hidden on the SSL VPN Web login page, only SSL VPN users with empty passwords can log in through the username/password authentication method.

Examples

Hide the password input box on the SSL VPN Web login page.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] password-box hide
```

password-changing enable (SSL VPN context view)

Use **`password-changing enable`** to enable SSL VPN users to modify passwords.

Use **`undo password-changing enable`** to disable SSL VPN users from modifying passwords.

Syntax

`password-changing enable`

`undo password-changing enable`

Default

SSL VPN users are allowed to modify passwords.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Usage guidelines

The password modification feature allows you to determine whether SSL VPN users in the SSL VPN context can modify their login passwords.

If you enable this feature, SSL VPN users that log in to the SSL VPN Web interface can modify the login password on the personal settings page. If you disable this feature, the modify password function will be hidden on the SSL VPN Web interface, so users cannot modify their passwords.

An SSL VPN user is able to modify the password only when password modification is enabled in both SSL VPN user view and SSL VPN context view.

Examples

Enable password modification for SSL VPN users in SSL VPN context **ctx1**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] password-changing enable
```

Related commands

display sslvpn context

password-changing enable (SSL VPN user view)

password-changing enable (SSL VPN user view)

Use **password-changing enable** to enable an SSL VPN user to modify the password.

Use **undo password-changing enable** to disable an SSL VPN user from modifying the password.

Syntax

password-changing enable

undo password-changing enable

Default

An SSL VPN user is allowed to modify the password.

Views

SSL VPN user view

Predefined user roles

network-admin

context-admin

Usage guidelines

The password modification feature allows you to determine whether the specified SSL VPN user can modify the login password.

If you enable this feature, a user that logs in to the SSL VPN Web interface can modify the login password on the personal settings page. If you disable this feature, the modify password function will be hidden on the SSL VPN Web interface, so a user cannot modify the password.

Examples

Enable password modification for SSL VPN user **user1**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] user user1
[Sysname-sslvpn-context-ctx1-user-user1] password-changing enable
```

Related commands

password-changing enable (SSL VPN context view)

password-complexity-message

Use **password-complexity-message** to configure a password complexity message.

Use **undo password-complexity-message** to restore the default.

Syntax

password-complexity-message { **chinese** *chinese-message* | **english** *english-message* }

undo password-complexity-message { **chinese** | **english** }

Default

No password complexity message is configured.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

chinese *chinese-message*: Specifies the password complexity message to be displayed on the Chinese Web interface, a case-sensitive string of 1 to 255 characters.

english *english-message*: Specifies the password complexity message to be displayed on the English Web interface, a case-sensitive string of 1 to 255 characters.

Usage guidelines

The password complexity message will be displayed on the SSL VPN password modification page to notify users of password complexity requirements.

In an SSL VPN context, if you execute this command multiple times for the same language, the most recent configuration takes effect.

Examples

In SSL VPN context **ctx1**, specify the password complexity message as **The password must contain uppercase and lowercase letters**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] password-complexity-message english The password must
contain uppercase and lowercase letters
```

policy-group

Use **policy-group** to create an SSL VPN policy group and enter its view, or enter the view of an existing SSL VPN policy group.

Use **undo policy-group** to delete a policy group.

Syntax

policy-group *group-name*

undo policy-group *group-name*

Default

No SSL VPN policy groups exist.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a name for the policy group, a case-insensitive string of 1 to 31 characters.

Usage guidelines

An SSL VPN policy group contains a set of rules for resource access authorization.

You can configure multiple SSL VPN policy groups for an SSL VPN context. When a remote user accesses the SSL VPN context, the AAA server issues the authorized policy group to the associated SSL VPN gateway. The user can access only the resources allowed by the authorized policy group. If the AAA server does not authorize the user to use a policy group, the user can access only the resources allowed by the default policy group.

Examples

Create a policy group named **pg1** and enter its view.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] policy-group pg1
[Sysname-sslvpn-context-ctx1-policy-group-pg1]
```

Related commands

default-policy-group

port-forward

Use **port-forward** to create a port forwarding list for an SSL VPN context and enter its view, or enter the view of an existing port forwarding list.

Use **undo port-forward** to delete a port forwarding list.

Syntax

port-forward *port-forward-name*

undo port-forward *port-forward-name*

Default

No port forwarding lists exist.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

port-forward-name: Specifies a name for the port forwarding list, a case-insensitive string of 1 to 31 characters. The name cannot start with **item-**.

Usage guidelines

Port forwarding lists provide TCP access services for SSL VPN users.

In port forwarding list view, you can use the **port-forward-item** command to create port forwarding items. Each port forwarding item defines an accessible TCP service provided on an internal server.

You can assign a port forwarding list to a policy group by using the **resources port-forward** command. After the AAA server authorizes a user to use a policy group, the SSL VPN Web page provides the user the port forwarding list assigned to the group. The user can access the TCP services provided by the port forwarding list.

Examples

Create port forwarding list **pflist1** and enter its view.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] port-forward pflist1
[Sysname-sslvpn-context-ctx1-port-forward-pflist1]
```

Related commands

local-port

resources port-forward

port-forward-item

Use **port-forward-item** to create a port forwarding item and enter its view, or enter the view of an existing port forwarding item.

Use **undo port-forward-item** to delete a port forwarding item.

Syntax

port-forward-item *item-name*

undo port-forward-item *item-name*

Default

No port forwarding items exist.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

item-name: Specifies a name for the port forwarding item, a case-insensitive string of 1 to 31 characters.

Usage guidelines

A port forwarding item defines an accessible TCP service provided on an internal server. It contains the following settings:

- A port forwarding instance.

  A port forwarding instance is configured by using the **local-port** command. It makes an internal TCP service accessible through a local address and port number on the SSL VPN client.

- (Optional.) A resource link.

  A resource link is configured by using the **execution** command.

  After you configure a resource link for a port forwarding item, the port forwarding item name will be displayed on the SSL VPN Web page as a link. You can click the link to access the resource directly.

  Make sure the resource link matches the TCP service specified by the port forwarding instance.

After you create a port forwarding item, you can assign it to a port forwarding list by using the **resources port-forward-item** command.

Examples

Create a port forwarding item named **pfitem1** and enter its view.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] port-forward-item pfitem1
[Sysname-sslvpn-context-ctx1-port-forward-item-pfitem1]
```

Related commands

execution

local-port

resources port-forward-item

prevent-cracking freeze-ip

Use **prevent-cracking freeze-ip** to configure IP address freezing parameters for cracking prevention.

Use **undo prevent-cracking freeze-ip** to restore the default.

Syntax

prevent-cracking freeze-ip login-failures *login-failures* **freeze-time** *freeze-time*

undo prevent-cracking freeze-ip

Default

The maximum number of consecutive login failures allowed for an IP address is 64, and the period of time to freeze an IP address is 30 seconds.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

login-failures *login-failures*: Specifies the maximum number of consecutive login failures allowed for an IP address before freezing it to prevent cracking.

freeze-time *freeze-time*: Specifies the period of time to freeze an IP address, in the range of 30 to 1800 seconds.

Usage guidelines

The cracking prevention feature reduces the risk of brute-force cracking of user login information by limiting the number of login attempts from the same IP address.

If the number of consecutive login failures of the same IP address reaches the maximum number specified by this command, the IP address will be frozen for the specified period. During the freeze period, the IP address is prohibited from logging in to the SSL VPN context. When the freeze period expires, the frozen IP address will be unfrozen automatically.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

In SSL VPN context **ctx1**, configure the device to freeze an IP address if it consecutively fails login for 100 times and set the freeze period of time to 60 seconds.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] prevent-cracking freeze-ip login-failures 100 freeze-time
60
```

Related commands

display sslvpn prevent-cracking frozen-ip

prevent-cracking freeze-ip enable

Use **prevent-cracking freeze-ip enable** to enable IP address freezing for cracking prevention.

Use **undo prevent-cracking freeze-ip enable** to disable IP address freezing for cracking prevention.

Syntax

prevent-cracking freeze-ip enable

undo prevent-cracking freeze-ip enable

Default

IP address freezing for cracking prevention is disabled.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Examples

In SSL VPN context **ctx1**, enable IP address freezing for cracking prevention.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] prevent-cracking freeze-ip enable
```

Related commands

display sslvpn prevent-cracking frozen-ip

pevent-cracking unfreeze-ip

Use **prevent-cracking unfreeze-ip** to unfreeze IP addresses frozen for cracking prevention.

Syntax

prevent-cracking unfreeze-ip { **all** | { **ipv4** | **ipv6** } *ip-address* }

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

all: Specifies all frozen IP addresses.

ipv4: Specifies a frozen IPv4 address.

Ipv6: Specifies a frozen IPv6 address.

ip-address: IP address to be unfrozen.

Usage guidelines

Unfrozen IP addresses are allowed to log in to the SSL VPN context again.

Examples

In SSL VPN context **ctx1**, unfreeze all frozen IP addresses.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] prevent-cracking unfreeze-ip all
```

Related commands

display sslvpn prevent-cracking frozen-ip

pevent-cracking verify-code

Use **prevent-cracking verify-code** to configure code verification parameters for cracking prevention.

Use **undo prevent-cracking verify-code** to restore the default.

Syntax

prevent-cracking verify-code login-failures *login-failures*

undo prevent-cracking verify-code

Default

A maximum of five consecutive login failures are allowed for an IP address.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

login-failures *login-failures*: Specifies the maximum number of consecutive login failures allowed for an IP address, in the range of 1 to 63.

Usage guidelines

The cracking prevention feature reduces the risk of brute-force cracking of user login information by limiting the number of login attempts from the same IP address.

If the number of consecutive login failures of an IP address exceeds the maximum number specified by this command, code verification is performed to prevent cracking. An SSL VPN user using the IP address must enter a correct verification code to log in to the SSL VPN context.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

In SSL VPN context **ctx1**, configure the device to perform code verification if an IP address consecutively fails login for more than 10 times.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] prevent-cracking verify-code login-failures-times 10
```

pevent-cracking verify-code enable

Use **prevent-cracking verify-code enable** to enable code verification for cracking prevention.

Use **undo prevent-cracking verify-code enable** to disable code verification for cracking prevention.

Syntax

prevent-cracking verify-code enable

undo prevent-cracking verify-code enable

Default

Code verification for cracking prevention is disabled.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Examples

In SSL VPN context **ctx1**, enable code verification for cracking prevention.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] prevent-cracking verify-code enable
```

rate-limit

Use **rate-limit** to set a rate limit for SSL VPN session upstream or downstream traffic.

Use **undo rate-limit** to remove the rate limit set for SSL VPN session upstream or downstream traffic.

Syntax

rate-limit { **downstream** | **upstream** } *value*

undo rate-limit { **downstream** | **upstream** }

Default

No rate limit is set for SSL VPN session upstream or downstream traffic.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

downstream: Specifies the SSL VPN downstream traffic, which is sent by internal servers to SSL VPN users.

upstream: Specifies the SSL VPN upstream traffic, which is sent by SSL VPN users to internal servers.

value: Sets the rate limit for the specified traffic, in the range of 1000 to 100000000 kbps.

Usage guidelines

You can set a rate limit for SSL VPN session upstream and downstream traffic, respectively. If you set the rate limit for the same traffic direction multiple times, the most recent configuration takes effect.

If the SSL VPN session upstream or downstream traffic exceeds the rate limit, subsequent upstream or downstream traffic will be discarded.

Examples

In SSL VPN context **ctx1**, set the rate limit to 10000 kbps for SSL VPN session upstream traffic.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] rate-limit upstream 10000
```

redirect-resource

Use **redirect-resource** to specify the Web resource to which SSL VPN users are redirected after login.

Use **undo redirect-resource** to restore the default.

Syntax

redirect-resource { **shortcut** | **url-item** } *resource-name*

undo redirect-resource

Default

After logging in to the SSL VPN gateway, a user directly enters the SSL VPN resource list page, and no webpage redirection is performed.

Views

SSL VPN policy group view

Predefined user roles

network-admin

context-admin

Parameters

shortcut: Specifies a shortcut resource.

url-item: Specifies a URL item resource.

resource-name: Specifies the resource name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

By default, a user directly enters the SSL VPN resource list page after logging in to the SSL VPN gateway. You can use this command to redirect a user to a specific webpage after the user logs in to the SSL VPN gateway.

If a policy group authorized to a user contains a redirect resource, the SSL VPN gateway first opens the SSL VPN resource list page for the user. After a while, it redirects the user to the webpage specified in the redirect resource. The user can press the back button on the Web browser to return to the SSL VPN resource list page.

If multiple policy groups are authorized to a user, the device searches the policy groups for a redirect resource in authorization time order (first authorized first searched). If a redirect resource is found, the device stops searching and redirects the user to the redirect resource. If no redirect resource is found, no redirection will be performed.

In an SSL VPN policy group view, if you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify URL item **url1** as the redirect resource of SSL VPN policy group **pg1**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] policy-group pg1
[Sysname-sslvpn-context-ctx1-policy-group-pg1] redirect-resource url-item url1
```

Related commands

display sslvpn policy-group

reset counters interface sslvpn-ac

Use **reset counters interface sslvpn-ac** to clear SSL VPN AC interface statistics.

Syntax

reset counters interface [**sslvpn-ac** [*interface-number*]]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

sslvpn-ac [*interface-number*]: Specifies an SSL VPN AC interface by its number in the range of 0 to 4095. If you do not specify this option, the command clears statistics for all interfaces. If you specify the **sslvpn-ac** keyword without the *interface-number* argument, this command clears statistics for all existing SSL VPN AC interfaces.

Usage guidelines

Use this command to clear old statistics so you can observe new traffic statistics on an SSL VPN AC interface.

Examples

Clear statistics for SSL VPN AC 1000.

```
<Sysname> reset counters interface sslvpn-ac 1000
```

Related commands

display interface sslvpn-ac

reset sslvpn ip-tunnel statistics

Use **reset sslvpn ip-tunnel statistics** to clear packet statistics for IP access users.

Syntax

reset sslvpn ip-tunnel statistics [**context** *context-name* [**session** *session-id*]]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

context *context-name*: Specifies an SSL VPN context by its name. An SSL VPN context name is a case-insensitive string of 1 to 31 characters, and can contain only letters, digits, and underscores (_). If you do not specify an SSL VPN context, this command clear packet statistics for IP access users in all SSL VPN contexts.

session *session-id*: Specifies a session by its ID in the range of 1 to 4294967295. If you do not specify a session, this command clears packet statistics for all IP access users in the specified SSL VPN context.

Usage guidelines

To view the SSL VPN sessions in different SSL VPN contexts, execute the **display sslvpn session** command.

If you do not specify any parameters, this command clear packets statistics for all IP access users in all SSL VPN contexts.

Examples

Clear the IP access packet statistics in all SSL VPN contexts.

```
<Sysname> reset sslvpn ip-tunnel statistics
```

Clear the IP access packet statistics in SSL VPN context **ctx1**.

```
<Sysname> reset sslvpn ip-tunnel statistics context ctx1
```

Clear the IP access packet statistics of session 1 in SSL VPN context **ctx**.

```
<Sysname> reset sslvpn ip-tunnel statistics context ctx1 session 1
```

Related commands

display sslvpn ip-tunnel statistics

display sslvpn session

resources port-forward

Use **resources port-forward** to assign a port forwarding list to an SSL VPN policy group.

Use **undo resources port-forward** to remove the configuration.

Syntax

resources port-forward *port-forward-name*

undo resources port-forward

Default

An SSL VPN policy group does not contain a port forwarding list.

Views

SSL VPN policy group view

Predefined user roles

network-admin

context-admin

Parameters

port-forward-name: Specifies the name of an existing port forwarding list. A port forwarding list name is a case-insensitive string of 1 to 31 characters.

Usage guidelines

After the AAA server authorizes a user to use a policy group, the SSL VPN Web page provides the user the port forwarding list assigned to the group. The user can access the TCP services provided by the port forwarding list.

Examples

Assign port forwarding list **pflist1** to SSL VPN policy group **pg1**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] policy-group pg1
[Sysname-sslvpn-context-ctx1-policy-group-pg1] resources port-forward pflist1
```

Related commands

local-port

port-forward

resources port-forward-item

Use **resources port-forward-item** to assign a port forwarding item to a port forwarding list.

Use **undo resources port-forward-item** to remove a port forwarding item from a port forwarding list.

Syntax

resources port-forward-item *item-name*

undo resources port-forward-item *item-name*

Default

A port forwarding list does not contain any port forwarding items.

Views

Port forwarding list view

Predefined user roles

network-admin

context-admin

Parameters

item-name: Specifies a port forwarding item by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

Before you assign a port forwarding item to a port forwarding list, make sure the port forwarding item has been created by using the **port-forward-item** command.

You can assign multiple port forwarding items to a port forwarding list.

Examples

Create a port forwarding item named **pfitem1**, and then assign it to port forwarding list **pflist1**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] port-forward-item pfitem1
[Sysname-sslvpn-context-ctx1-port-forward-item-pfitem1] quit
[Sysname-sslvpn-context-ctx1] port-forward pflist1
[Sysname-sslvpn-context-ctx1-port-forward-pflist1] resources port-forward-item pfitem1
```

Related commands

port-forward-item

resources shortcut

Use **resources shortcut** to assign a shortcut to a shortcut list.

Use **undo resources shortcut** to remove a shortcut from a shortcut list.

Syntax

resources shortcut *shortcut-name*

undo resources shortcut *shortcut-name*

Default

A shortcut list does not contain any shortcuts.

Views

Shortcut list view

Predefined user roles

network-admin

context-admin

Parameters

shortcut-name: Specifies a shortcut by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

You can assign multiple shortcuts to a shortcut list.

Examples

Assign shortcut **list1** to shortcut list **shortcut1**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] shortcut shortcut1
[Sysname-sslvpn-context-ctx1-shortcut-shortcut1] quit
[Sysname-sslvpn-context-ctx1] shortcut-list list1
[Sysname-sslvpn-context-ctx1-shortcut-list-list1] resources shortcut shortcut1
```

resources shortcut-list

Use **resources shortcut-list** to assign a shortcut list to an SSL VPN policy group.

Use **undo resources shortcut-list** to restore the default.

Syntax

resources shortcut-list *list-name*

undo resources shortcut-list

Default

An SSL VPN policy group does not contain a shortcut list.

Views

SSL VPN policy group view

Predefined user roles

network-admin

context-admin

Parameters

list-name: Specifies a shortcut list by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

You can assign only one shortcut list to an SSL VPN policy group. After the AAA server authorizes a user to use a policy group, the SSL VPN Web page provides the user the shortcut list assigned to the group. The user can click a shortcut to access the associated resource.

If you execute this command for an SSL VPN policy group multiple times, the most recent configuration takes effect.

Examples

Assign shortcut list **list1** to SSL VPN policy group **pg1**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] shortcut-list list1
[Sysname-sslvpn-context-ctx1-shortcut-list-list1] quit
[Sysname-sslvpn-context-ctx1] policy-group pg1
[Sysname-sslvpn-context-ctx1-policy-group-pg1] resources shortcut-list list1
```

resources uri-acl

Use **resources uri-acl** to specify a URI ACL for URL resource filtering in a URL item.

Use **undo resources uri-acl** to remove the URI ACL configuration from a URL item.

Syntax

resources uri-acl *uri-acl-name*

undo resources uri-acl

Default

No URI ACL is specified for URL resource filtering in a URL item.

Views

URL item view

Predefined user roles

network-admin

context-admin

Parameters

uri-acl-name: Specifies a URI ACL by its name, a case-insensitive string of 1 to 31 characters. The specified URI ACL must already exist.

Usage guidelines

The specified URI ACL will be used to filter the accessible resources under the URL specified in the URL item.

Examples

Specify URI ACL **abc** in URL item **serverA**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] url-item serverA
[Sysname-sslvpn-context-ctx1-url-item-serverA] resources uri-acl abc
```

Related commands

uri-acl

resources url-item

Use **resources url-item** to assign a URL item to a URL list.

Use **undo resources url-item** to remove a URL item from a URL list.

Syntax

resources url-item *url-item-name*

undo resources url-item *url-item-name*

Default

A URL list does not contain any URL items.

Views

URL list view

Predefined user roles

network-admin

context-admin

Parameters

url-item-name: Specifies a URL item by its name, a case-insensitive string of 1 to 31 characters. The specified URL item must already exist.

Usage guidelines

You can assign multiple URL items to a URL list.

Examples

Assign URL item **serverA** to URL list **list1**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] url-list list1
[Sysname-sslvpn-context-ctx1-url-list-list1] resources url-item serverA
```

Related commands

url-item

resources url-list

Use **resources url-list** to assign a URL list to an SSL VPN policy group.

Use **undo resources url-list** to remove the configuration.

Syntax

resources url-list *url-list-name*

undo resources url-list *url-list-name*

Default

An SSL VPN policy group does not contain a URL list.

Views

SSL VPN policy group view

Predefined user roles

network-admin

context-admin

Parameters

url-list-name: Specifies an existing URL list by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

In Web access mode, a remote user can use a Web browser to access URL resources in the URL list assigned to the authorized SSL VPN policy group.

Examples

Assign URL list **url1** to SSL VPN policy group **pg1**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] policy-group pg1
[Sysname-sslvpn-context-ctx1-policy-group-pg1] resources url-list url1
```

Related commands

policy-group

sslvpn context

url-list

resources-file

Use **resources-file** to specify a file for SSL VPN users to download on the SSL VPN resource page.

Use **undo resources-file** to restore the default.

Syntax

resources-file { **chinese** *chinese-filename* | **english** *english-filename* }

undo resources-file { **chinese** | **english** }

Default

No file is provided for SSL VPN users to download.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

chinese *chinese-filename*: Specifies the name of the file to be provided on the Chinese Web interface, a case-sensitive string of 1 to 31 characters.

english *english-filename*: Specifies the name of the file to be provided on the English Web interface, a case-sensitive string of 1 to 31 characters.

Usage guidelines

Before executing this command, you must upload the file for users to download to the file system on the device in advance. The specified file name must be the absolute path of the file.

In an SSL VPN context, if you execute this command multiple times for the same language, the most recent configuration takes effect.

Examples

In SSL VPN context **ctx1**, specify the file for users to download on the SSL VPN resource page as **flash:/sslvpnhelp.pdf**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] resources-file english flash:/sslvpnhelp.pdf
```

rewrite server-response-message

Use **rewrite server-response-message** to rewrite a server reply message.

Use **undo rewrite server-response-message** to restore the default.

Syntax

rewrite server-response-message *server-response-message* { **chinese** *chinese-message* | **english** *english-message* }

undo rewrite server-response-message *server-response-message* { **chinese** | **english** }

Default

No server reply message is rewritten.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

server-response-message: Specifies the original server reply message to be rewritten, a case-sensitive string of 1 to 127 characters. If this message contains spaces, enclose the message in double quotation marks.

chinese *chinese-message*: Specifies the new server reply message to be displayed on the Chinese Web interface, a case-sensitive string of 1 to 127 characters.

english *english-message*: Specifies the new server reply message to be displayed on the English Web interface, a case-sensitive string of 1 to 127 characters.

Usage guidelines

If a server reply message (for example, an authentication, authorization, or accounting reply message) is hard to understand, execute this command to rewrite the server reply message. You can obtain server reply messages from the server to determine which messages should be rewritten.

If you execute this command multiple times to rewrite the same original server reply message in the same language, the most recent configuration takes effect.

Examples

In SSL VPN context **ctx1**, rewrite the server reply message **Success** to **User identity authentication succeeded**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] rewrite server-response-message Success english User
identity authentication succeeded
```

rewrite-rule

Use **rewrite-rule** to create a rewrite rule and enter its view, or enter the view of an existing rewrite rule.

Use **undo rewrite-rule** to delete a rewrite rule.

Syntax

rewrite-rule *rule-name*

undo rewrite-rule *rule-name*

Default

No rewrite rules exist.

Views

File policy view

Predefined user roles

network-admin

context-admin

Parameters

rule-name: Specifies a rule name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

You can configure multiple rewrite rules in a file policy.

Examples

Create a rewrite rule named **rule1** and enter its view.

```
<Sysname> system-view
[Sysname] sslvpn context ctx
[Sysname-sslvpn-context-ctx] file-policy fp
[Sysname-sslvpn-context-ctx-file-policy-fp] rewrite-rule rule1
[Sysname-sslvpn-context-ctx-file-policy-fp-rewrite-rule-rule1]
```

rule

Use **rule** to create a rule for a URI ACL.

Use **undo rule** to remove a rule from a URI ACL.

Syntax

rule [*rule-id*] { **deny** | **permit** } **uri** *uri-pattern-string*

undo rule *rule-id*

Default

No URL ACL rules exist in a URI ACL

Views

URI ACL view

Predefined user roles

network-admin

context-admin

Parameters

deny: Denies matching packets to pass.

permit: Allows matching packets to pass.

rule-id: Specifies a rule ID in the range of 0 to 65534. If you do not specify a rule ID when creating an ACL rule, the system automatically assigns it a rule ID. The numbering step is 5 for automatic numbering of rule IDs. An automatically assigned rule ID takes the nearest multiple of 5 higher than the current highest rule ID. For example, if the current highest rule ID is 28, the rule is numbered 30.

uri *uri-pattern-string*: Specifies a URI pattern. The URI pattern can contain a maximum of 256 characters in the format of *protocol*://*host:port/path*, where *protocol* and *host* are required. See Table 14 for descriptions of the fields in a URI pattern.

Table 14 URI field descriptions

Field	Description
protocol	Protocol name. Options are: • http. • https. • tcp. • udp. • icmp. • ip.

host	Domain name or address of a host.
	• Valid host address formats:
	  ○ IPv4 or IPv6 address. For example, 192.168.1.1.
	  ○ IPv4 or IPv6 address range in the format of *start address-end address*. For example, 3.3.3.1-3.3.3.200.
	  ○ IPv4 address with a mask length or IPv6 address with a prefix length. For example 2.2.2.2/24.
	  ○ A combination of the preceding host address formats separated by comma (,). For example, 192.168.1.1,3.3.3.1-3.3.3.200,2.2.2.2/24.
	• Valid domain name formats:
	  ○ Fully qualified domain name. For example, www.domain.com
	  ○ Domain name with the following wildcard characters:
	Asterisk (*)—Matches zero or more characters. For example, *.com.
	Question mark (?)—Matches one character. For example, www.do?main.com.
	Percent sign (%)—Matches one or more characters in a field of the domain name. For example, www.%.com.

port	Port number. If no port number is specified, the default port number of the protocol is used. Valid formats for this field: • Single port number. For example, 1002. • Port number range in the format of *start port-end port*. For example, 8080-8088. • A combination of the preceding formats separate by comma (,). For example, 1002,90,8080-8088.
path	String that identifies a directory or file on the host. The path is a sequence of fields separated by forward or backward slashes. The following wildcard characters are supported: • **Asterisk (*)**—Matches zero or more characters. For example, /path1/*. • **Question mark (?)**—Matches one character. For example, /path?/. • **Percent sign (%)**—Matches one or more characters in a field of the path. For example, /path1/%/.

Usage guidelines

You can add multiple rules to a URI ACL. The device matches a packet against the rules in ascending order of rule ID. The match process stops once a matching rule is found.

Examples

Add a rule to URI ACL **uriacla**.

```
<Sysname> system-view
[Sysname] sslvpn context abc
[Sysname-sslvpn-context-abc] uri-acl uriacla
[Sysname-sslvpn-context-abc-uri-acl-uriacla] rule 1 permit uri
http://*.abc.com:80,443,2000-5000/path/
```

self-service imc address

Use **self-service imc address** to specify an IMC server for password modification.

Use **undo self-service imc address** to restore the default.

Syntax

self-service imc address *ip-address* **port** *port-number* [**vpn-instance** *vpn-instance-name*]

undo self-service imc address

Default

No IMC server is specified for password modification.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the IP address of the IMC server, in dotted decimal notation.

port *port-number*: Specifies the port number of the IMC server, in the range of 1 to 65535.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the IMC server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. Do not specify this option if the IMC server is on the public network.

Usage guidelines

Password modification allows users to modify login passwords by themselves, and it is supported for local users and users authenticated by an IMC server.

Execute this command only when IMC authentication users need to modify the SSL VPN login passwords. After a user passes the identity authentication, the user can modify the password on the SSL VPN Web page. The new password is sent to the IMC server specified by this command for verification. If the verification succeeds, the user will use the new password for next logins.

Examples

Specify the IMC server at IP address 192.168.10.1 and port 443 in VPN instance **vpn1** for password modification of users in SSL VPN context **ctx1**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] self-service imc address 192.168.10.1 port 443 vpn-instance
vpn1
```

server-address

Use **server-address** to specify an IMC server for SMS authentication.

Use **undo server-address** to restore the default.

Syntax

server-address *ip-address* **port** *port-number* [**vpn-instance** *vpn-instance-name*]

undo server-address

Default

No IMC server is specified for SMS authentication.

Views

IMC SMS authentication view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the IP address of the IMC server, in dotted decimal notation.

port *port-number*: Specifies the port number of the IMC server, in the range of 1 to 65535.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the IMC server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. Do not specify this option if the IMC server is on the public network.

Examples

In IMC SMS authentication view, specify an IMC server (with IP address 192.168.151.1 and port 2000) in VPN instance **vpn1** for SMS authentication of users.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] sms-auth imc
[Sysname-sslvpn-context-ctx1-sms-auth-imc] server-address 192.168.151.1 port 2000
vpn-instance vpn1
```

service enable (SSL VPN context view)

Use **service enable** to enable an SSL VPN context.

Use **undo service enable** to disable an SSL VPN context.

Syntax

service enable

undo service enable

Default

An SSL VPN context is disabled.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Examples

Enable SSL VPN context **ctx1**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] service enable
```

Related commands

display sslvpn context

service enable (SSL VPN gateway view)

Use **service enable** to enable an SSL VPN gateway.

Use **undo service enable** to disable an SSL VPN gateway.

Syntax

service enable

undo service enable

Default

An SSL VPN gateway is disabled.

Views

SSL VPN gateway view

Predefined user roles

network-admin

context-admin

Examples

Enable SSL VPN gateway **gw1**.

```
<Sysname> system-view
[Sysname] sslvpn gateway gw1
[Sysname-sslvpn-gateway-gw1] service enable
```

Related commands

display sslvpn gateway

session-connections

Use **session-connections** to set the maximum number of connections allowed per session.

Use **undo session-connections** to restore the default.

Syntax

session-connections *number*

undo session-connections

Default

A maximum of 64 connections are allowed per session.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

number: Set the maximum number of connections allowed per session. The value can be 0 or in the range of 10 to 1000. Value 0 indicates that the number of connections per session is not limited.

Usage guidelines

If the number of connections in a session has reached the maximum, new connection requests for the session will be rejected with a **503 Service Unavailable** message.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the maximum number of connections allowed per session to 10.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] session-connections 10
```

shortcut

Use **shortcut** to create a shortcut and enter its view, or enter the view of an existing shortcut.

Use **undo shortcut** to delete a shortcut.

Syntax

shortcut *shortcut-name*

undo shortcut *shortcut-name*

Default

No shortcuts exist.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

shortcut-name: Specifies a shortcut name, a case-insensitive string of 1 to 31 characters. The shartcut name cannot start with **list-**.

Usage guidelines

After you create a shortcut, use the **execution** command to configure a resource link for it. Users can then click the shortcut name on the SSL VPN Web page to access the associated resource.

Examples

Create a shortcut named **shortcut1** and enter its view.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] shortcut shortcut1
[Sysname-sslvpn-context-ctx1-shortcut-shortcut1]
```

shortcut-list

Use **shortcut-list** to create a shortcut list and enter its view, or enter the view of an existing shortcut list.

Use **undo shortcut-list** to delete a shortcut list.

Syntax

shortcut-list *list-name*

undo shortcut-list *list-name*

Default

No shortcut lists exist.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

list-name: Specifies a name for the shortcut list, a case-insensitive string of 1 to 31 characters.

Examples

Create a shortcut list named **list1** and enter its view.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] shortcut-list list1
[Sysname-sslvpn-context-ctx1-shortcut-list-list1]
```

shutdown

Use **shutdown** to shut down an SSL VPN AC interface.

Use **undo shutdown** to bring up an SSL VPN AC interface.

Syntax

shutdown

undo shutdown

Default

An SSL VPN AC interface is up.

Views

SSL VPN AC interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

CAUTION:

The **shutdown** command interrupts ongoing network services. Make sure you are fully aware of the impact of this command when you use it on a live network.

Examples

Shut down SSL VPN AC 1000.

```
<Sysname> system-view
[Sysname] interface sslvpn-ac 1000
[Sysname-SSLVPN-AC1000] shutdown
```

sms-auth

Use **sms-auth** to create an SMS authentication view and enter its view, or enter the view of an existing SMS authentication view.

Use **undo sms-auth** to delete an SMS authentication view.

Syntax

sms-auth { **imc** | **sms-gw** }

undo sms-auth { **imc** | **sms-gw** }

Default

No SMS authentication views exist.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

imc: Specifies the IMC SMS authentication view.

sms-gw: Specifies the SMS gateway authentication view.

Examples

Create and enter SMS gateway authentication view in SSL VPN context **ctx1**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] sms-auth sms-gw
```

```
[Sysname-sslvpn-context-ctx1-sms-auth-sms-gw]
```

Related commands

sms-auth type

sms-auth type

Use **sms-auth type** to specify an SMS authentication type and enable SMS authentication.

Use **undo sms-auth type** to restore the default.

Syntax

sms-auth type { **imc** | **sms-gw** }

undo sms-auth type

Default

SMS authentication is disabled.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

imc: Specifies IMC SMS authentication.

sms-gw: Specifies SMS gateway authentication.

Usage guidelines

After you enable SMS authentication, the device uses SMS verification codes to authenticate SSL VPN users. A user is allowed to log in to the SSL VPN gateway only when the user passes the SMS authentication.

The device supports the following types of SMS authentication:

- IMC SMS authentication.

  SMS authentication for SSL VPN users is performed by an IMC server. You must configure the IP address and port number for the IMC server in IMC SMS authentication view.

- SMS gateway authentication.

  SMS gateway authentication for SSL VPN users is performed by an SMS gateway. You must specify the SMS gateway, the verification code resend interval, and the verification code validity period in SMS gateway authentication view.

Examples

Specify the SMS authentication type as SMS gateway authentication in SSL VPN context **ctx1**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] sms-auth type sms-gw
```

Related commands

display sslvpn context

sms-auth

sms-content

Use **sms-content** to configure the SMS content template.

Use **undo sms-content** to restore the default.

Syntax

sms-content *string*

undo sms-content

Default

The SMS content template is **Hello, $$USER$$, the verification code is $$VERIFYCODE$$, and its validity period is $$VALIDTIME$$ minutes.**

Views

SMS gateway authentication view

Predefined user roles

network-admin

context-admin

Parameters

string: Specifies the SMS content template, a case-sensitive string of 1 to 127 characters.

Usage guidelines

Use this command to configure the SMS content template that the SMS gateway uses to send SMS messages.

An SMS content template must contain the following variables:

- **$$USERNAME$$**—User name variable.
- **$$VERIFYCODE$$**—Verification code variable.
- **$$VALIDTIME$$**—Verification code validity period variable.

Examples

In SMS gateway authentication view, configure the SMS content template as **Hello, $$USER$$, the verification code is $$VERIFYCODE$$, and its validity period is $$VALIDTIME$$ in minutes.**

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] sms-auth sms-gw
[Sysname-sslvpn-context-ctx1-sms-auth-sms-gw] sms-content Hello, $$USER$$, the
verification code is $$VERIFYCODE$$, and its validity period is $$VALIDTIME$$ in minutes.
```

ssl client-policy

Use **ssl client-policy** to apply an SSL client policy to an SSL VPN context.

Use **undo ssl client-policy** to restore the default.

Syntax

ssl client-policy *policy-name*

undo ssl client-policy

Default

The default SSL client policy for SSL VPN is used. This policy supports the **dhe_rsa_aes_128_cbc_sha**, **dhe_rsa_aes_256_cbc_sha**, **rsa_3des_ede_cbc_sha**, **rsa_aes_128_cbc_sha**, and **rsa_aes_256_cbc_sha** cipher suites.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies an SSL client policy by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

You can apply only one SSL client policy to an SSL VPN context. For the applied SSL client policy to take effect, you must enable the SSL VPN context by using the **service enable** command. The SSL VPN gateway will use the parameters defined by the policy to establish SSL connections to HTTPS servers.

If you execute this command multiple times, the new configuration overwrites the previous configuration, but does not take effect. For the new configuration to take effect, disable the SSL VPN context and then re-enable it.

For information about configuring SSL client policies, see *Security Configuration Guide*.

Examples

Apply SSL client policy **abc** to SSL VPN context **ctx1**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] ssl client-policy abc
```

ssl server-policy

Use **ssl server-policy** to apply an SSL server policy to an SSL VPN gateway.

Use **undo ssl server-policy** to remove the application.

Syntax

ssl server-policy *policy-name*

undo ssl server-policy

Default

An SSL VPN gateway uses the SSL server policy of its self-signed certificate.

Views

SSL VPN gateway view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies the name of an SSL server policy, a case-insensitive string of 1 to 31 characters.

Usage guidelines

You can apply only one SSL server policy to an SSL VPN gateway. For the applied SSL server policy to take effect, you must enable the SSL VPN gateway by using the **service enable** command. The SSL VPN gateway will use the parameters defined by the policy to establish SSL connections to remote users.

If you execute this command multiple times, the new configuration overwrites the previous configuration but does not take effect. For the new configuration to take effect, disable the SSL VPN gateway and then enable the SSL VPN gateway. To disable and enable an SSL VPN gateway, use the **undo service enable** and **service enable** commands.

After you modify the content of the SSL server policy applied to an SSL VPN gateway, you must disable and then re-enable the gateway to validate the policy. To disable and enable an SSL VPN gateway, use the **undo service enable** and **service enable** commands.

Examples

Apply SSL server policy **CA_CERT** to SSL VPN gateway **gw1**.

```
<Sysname> system-view
[Sysname] sslvpn gateway gw1
[Sysname-sslvpn-gateway-gw1] ssl server-policy CA_CERT
```

Related commands

display sslvpn gateway

sslvpn context

Use **sslvpn context** to create an SSL VPN context and enter its view, or enter the view of an existing SSL VPN context.

Use **undo sslvpn context** to delete an SSL VPN context.

Syntax

sslvpn context *context-name*

undo sslvpn context *context-name*

Default

No SSL VPN contexts exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

context-name: Specifies an SSL VPN context name, a case-insensitive string of 1 to 31 characters. Valid characters are letters, digits, and underscores (_).

Usage guidelines

SSL VPN contexts contain different user sessions, accessible resources, and user authentication methods.

An SSL VPN gateway can be associated with multiple SSL VPN contexts. After a remote user logs in to an SSL VPN gateway, the user can access only the resources in the SSL VPN context to which the user belongs.

Examples

Create an SSL VPN context named **ctx1** and enter its view.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1]
```

Related commands

display sslvpn context

sslvpn gateway

Use **sslvpn gateway** to create an SSL VPN gateway and enter its view, or enter the view of an existing SSL VPN gateway.

Use **undo sslvpn gateway** to delete an SSL VPN gateway.

Syntax

sslvpn gateway *gateway-name*

undo sslvpn gateway *gateway-name*

Default

No SSL VPN gateways exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

gateway-name: Specifies an SSL VPN gateway name, a case-insensitive string of 1 to 31 characters. Valid characters are letters, digits, and underscores (_).

Usage guidelines

An SSL VPN gateway resides between remote users and the enterprise network to ensure secure access of remote users to the enterprise internal network. The SSL VPN gateway establishes an SSL connection to a remote user, and then authenticates the user before allowing the user to access an internal server.

You must perform the following tasks in the view of an SSL VPN gateway:

- Execute the **ip address** command to configure an IP address and a port number for the SSL VPN gateway.
- Execute the **ssl server-policy** command to apply an SSL server policy to the SSL VPN gateway.
- Execute the **service enable** command to enable the SSL VPN gateway.

You cannot delete an SSL VPN gateway that has been associated with an SSL VPN context. To delete the SSL VPN gateway, execute the **undo gateway** command to remove the association and then execute the **undo sslvpn gateway** command.

Examples

Create an SSL VPN context named **gw1** and enter its view.

```
<Sysname> system-view
[Sysname] sslvpn gateway gw1
[Sysname-sslvpn-gateway-gw1]
```

Related commands

display sslvpn gateway

sslvpn ip address-pool

Use **sslvpn ip address-pool** to create an address pool.

Use **undo sslvpn ip address-pool** to delete an address pool.

Syntax

sslvpn ip address-pool *pool-name start-ip-address end-ip-address*

undo sslvpn ip address-pool *pool-name*

Default

No address pools exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

pool-name: Specifies a name for the address pool, a case-insensitive string of 1 to 31 characters.

start-ip-address end-ip-address: Specifies the start IP address and end IP address for the pool. The end IP address must be greater than the start IP address. The start IP address and end IP address cannot be a multicast, broadcast, or loopback address.

Usage guidelines

The created address pools are used for address allocation to SSL VPN IP access clients. You can specify an address pool for an SSL VPN context or an SSL VPN policy group. An SSL VPN gateway uses the specified address pools to assign IP addresses to IP access clients.

Examples

Create an address pool named **pool1** and specify the address range as 10.1.1.1 to 10.1.1.254.

```
<Sysname> system-view
[Sysname] sslvpn ip address-pool pool1 10.1.1.1 10.1.1.254
```

Related commands

ip-tunnel address-pool (SSL VPN context view)

ip-tunnel address-pool (SSL VPN policy group view)

sslvpn log enable

Use **sslvpn log enable** to enable the SSL VPN global logging feature.

Use **undo sslvpn log enable** to disable the SSL VPN global logging feature.

Syntax

sslvpn log enable

undo sslvpn log enable

Default

The SSL VPN global logging feature is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This feature logs the following global events:

- SSL VPN access failures because of not associating SSL VPN contexts with gateways.
- SSL VPN access failures because of not enabling SSL VPN contexts.

The logs are sent to the information center of the device. For the logs to be output correctly, you must also configure the information center on the device. For more information about the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Enable the SSL VPN global logging feature.

```
<Sysname> system-view
[Sysname] sslvpn log enable
```

sslvpn webpage-customize

Use **sslvpn webpage-customize** to specify a webpage template for SSL VPN webpage customization.

Use **undo sslvpn webpage-customize** to restore the default.

Syntax

sslvpn webpage-customize *template-name*

undo sslvpn webpage-customize

Default

SSL VPN uses the system default webpages.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

template-name: Specifies a webpage template by its name, a string of 1 to 31 characters. The name cannot contain any of the following characters: forward slash (/), backslash (\), vertical bar (|),

colon (:), asterisk (*), quotation mark ("), question mark (?), left angle bracket (<), and right angle bracket (>).

Usage guidelines

This command allows you to set the global SSL VPN webpage template. Both predefined and user-defined webpage templates are available.

You can upload and download webpage templates through the SSL VPN Web interface.

To view all webpage templates in the system, use the **display sslvpn webpage-customize template** command.

In an SSL VPN context, the webpage template specified for the SSL VPN context takes precedence over the global SSL VPN webpage template. To specify a webpage template for an SSL VPN context, use the **webpage-customize** command in SSL VPN context view.

Examples

Use webpage template **template1** to customize SSL VPN webpages.

```
<Sysname> system-view
[Sysname] sslvpn webpage-customize template1
```

Related commands

display sslvpn webpage-customize template

webpage-customize

sso auto-build code

Use **sso auto-build code** to specify a character encoding method for SSO login requests that are built automtically.

Use **undo sso auto-build code** to restore the default.

Syntax

sso auto-build code { **gb18030** | **utf-8** }

undo sso auto-build code

Default

UTF-8 encoding is used for automatically built SSO login requests.

Views

URL item view

Predefined user roles

network-admin

context-admin

Parameters

gb18030: Specifies GB18030 encoding.

utf-8: Specifies UTF-8 encoding.

Usage guidelines

Encoding a login request is to convert the login request into a binary string for transmission. The SSL VPN gateway supports GB18030 and UTF-8 encoding methods. Specify an encoding method according to the decoding method used by the internal server.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

In URL item **servera**, set the encoding method to **GB18030** for automatically built SSO login requests.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] url-item servera
[Sysname-sslvpn-context-ctx1-url-item-servera] sso auto-build code gb18030
```

Related commands

sso auto-build custom-login-parameter

sso auto-build login-parameter-field

sso auto-build request-method

sso method

sso auto-build custom-login-parameter

Use **sso auto-build custom-login-parameter** to configure a custom login parameter for automatic building of SSO login requests.

Use **undo sso auto-build custom-login-parameter** to restore the default.

Syntax

sso auto-build custom-login-parameter name *parameter-name* **value** *value* [**encrypt**]

undo sso auto-build custom-login-parameter name *parameter-name*

Default

No custom parameter is configured for automatic building of SSO login requests.

Views

URL item view

Predefined user roles

network-admin

context-admin

Parameters

name *parameter-name*: Specifies the parameter name, a case-sensitive string of 1 to 63 characters.

value *value*: Specifies the attribute value, a case-sensitive string of 1 to 255 characters.

encrypt: Enables attribute value encryption through an encryption file. The encryption file is specified by the **sso auto-build encrypt-file** command.

Usage guidelines

Use this command to configure a custom login parameter (attribute name and value) if the auto-build SSO method is enabled.

The SSL VPN gateway will use the custom login parameter and other auto-build login parameters (configured by using the **sso auto-build login-parameter** command) to build login requests automatically.

Examples

In URL item **servera**, configure a custom login parameter for auto-build SSO. Configure the parameter's name as **commit** and the value as **login**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] url-item servera
[Sysname-sslvpn-context-ctx1-url-item-servera] sso auto-build custom-login-parameter
name commit value login
```

Related commands

sso auto-build code

sso auto-build encrypt-file

sso auto-build login-parameter

sso auto-build request-method

sso method

sso auto-build encrypt-file

Use **sso auto-build encrypt-file** to specify an encryption file to encrypt login parameters in automatically built SSO login requests.

Use **undo timeout idle** to restore the default.

Syntax

sso auto-build encrypt-file *filename*

undo sso auto-build encrypt-file

Default

No encryption file is specified for SSO login in the auto-build method.

Views

URL item view

Predefined user roles

network-admin

context-admin

Parameters

filename: Specifies an encryption file by its name, a case-insensitive string of 1 to 255 characters.

Usage guidelines

Use this command to specify an encryption file to encrypt the values of the parameters in automatically built SSO login requests. Encryption files are files that contain encryption functions written in JavaScript, and these files must be uploaded to the file management system of the device in advance.

If the encryption file to be used is the root directory of the device, you do not need to specify the file path when you execute this command. If the encryption file to be used is in a non-root directory of the device, you must specify the absolute path of the file when you execute this command.

You must write encryption functions in the following template:

```
function sslvpn_sso_encrypt(code)
{
```

```
//Encryption code
}
```

If you execute this command multiple times, the most recent configuration takes effect.

Examples

In URL item **servera**, specify encryption file **test.js** to encrypt the values of the parameters in automatically built SSO login requests.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] url-item servera
[Sysname-sslvpn-context-ctx1-url-item-servera] sso auto-build encrypt-file test.js
```

Related commands

sso auto-build custom-login-parameter

sso auto-build login-parameter-field

sso method

sso auto-build login-parameter

Use **sso auto-build login-parameter** to configure a login parameter for automatic building of SSO login requests.

Use **undo sso auto-build login-parameter** to restore the default.

Syntax

sso auto-build login-parameter { **cert-fingerprint** | **cert-serial** | **cert-title** | **custom-password** | **custom-username** | **login-name** | **login-password** | **mobile-num** | **user-group** } **name** *parameter-name* [**encrypt**]

undo sso auto-build login-parameter { **cert-fingerprint** | **cert-serial** | **cert-title** | **custom-password** | **custom-username** | **login-name** | **login-password** | **mobile-num** | **user-group** }

Default

No login parameters are configured for automatic building of SSO login requests.

Views

URL item view

Predefined user roles

network-admin

context-admin

Parameters

login-name: Uses the SSL VPN login username as the value of the SSO login parameter.

login-password: Uses the SSL VPN login password as the value of the SSO login parameter.

cert-title: Uses the certificate title as the value of the SSO login parameter.

cert-serial: Uses the certificate serial number as the value of the SSO login parameter.

cert-fingerprint: Uses the certificate fingerprint as the value of the SSO login parameter.

mobile-num: Uses the mobile phone number as the value of the SSO login parameter.

user-group: Uses the user group name as the value of the SSO login parameter.

custom-username: Uses the customized username as the value of the SSO login parameter.

custom-password: Uses the customized password as the value of the SSO login parameter.

name *parameter-name*: Specifies an attribute name for the SSO login parameter, a case-sensitive string of 1 to 63 characters.

encrypt: Enables attribute value encryption through an encryption file. The encryption file is specified by the **sso auto-build encrypt-file** command.

Usage guidelines

Use this command to configure a login parameter (attribute name and value) if the auto-build SSO method is enabled by using the **sso method auto-build** command. The attribute name is the parameter name used by the SSL VPN gateway to log in to the internal server. The parameter value used to log in to the internal server is the actual value abstracted according to the parameter value keyword specified in the command. For example, if you specify the **login-name** keyword for a parameter, the parameter value carried in the login request is the actual SSL VPN login username.

You can configure different values for the same attribute name, and configure different attribute names with the same value.

The SSL VPN gateway will use the login parameters configured by this command and custom login parameters (configured by the **sso auto-build custom-login-parameter** command) to build login requests automatically.

Upon receiving a login request, the internal server searches for the parameter values according to the parameter names to determine whether the login user is legitimate.

Examples

In URL item **servera**, configure a login parameter for auto-build SSO. Configure the parameter's value keyword as **cert-title** and attribute name as **login**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] url-item servera
[Sysname-sslvpn-context-ctx1-url-item-servera] sso auto-build login-parameter
cert-title name login encrypt
```

Related commands

sso auto-build code

sso auto-build custom-login-parameter

sso auto-build encrypt-file

sso auto-build request-method

sso method

sso auto-build request-method

Use **sso auto-build request-method** to specify the HTTP request method for automatically built SSO login requests.

Use **undo sso auto-build request-method** to restore the default.

Syntax

sso auto-build request-method { **get** | **post** }

undo sso auto-build request-method

Default

The GET request method is used for automatically built SSO login requests.

Views

URL item view

Predefined user roles

network-admin

context-admin

Parameters

get: Specifies the GET request method.

post: Specifies the POST request method.

Usage guidelines

This command specifies the HTTP request method used by the SSL VPN gateway to send HTTP requests to the internal server for SSO login. Specify the HTTP request method according to the internal server settings.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

In URL item **servera**, set the HTTP request method to **POST** for auto-build SSO login.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] url-item servera
[Sysname-sslvpn-context-ctx1-url-item-servera] sso auto-build request-method post
```

Related commands

sso auto-build code

sso auto-build custom-login-parameter

sso auto-build login-parameter-field

sso method

sso basic custom-username-password enable

Use **sso basic custom-username-password enable** to enable using a custom username and password for SSO login through basic authentication.

Use **undo sso basic custom-username-password enable** to restore the default.

Syntax

sso basic custom-username-password enable

undo sso basic custom-username-password enable

Default

SSL VPN login username and password are used for SSO login through basic authentication.

Views

URL item view

Predefined user roles

network-admin

context-admin

Usage guidelines

Execute this command if you specify basic authentication for SSO login. The custom username and password are configured in the SSL VPN Web interface.

Examples

In URL item **servera**, enable using the custom username and password for SSO login through basic authentication.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] url-item servera
[Sysname-sslvpn-context-ctx1-url-item-servera] sso basic custom-username-password
enable
```

Related commands

sso method

sso method

Use **sso method** to enable SSO and specify the SSO method.

Use **undo sso method** to restore the default.

Syntax

sso method { **auto-build** | **basic** }

undo sso method

Default

SSL VPN SSO login is disabled.

Views

URL item view

Predefined user roles

network-admin

context-admin

Parameters

auto-build: Automatically builds login requests to implement SSO.

basic: Performs basic authentication automatically to implement SSO.

Usage guidelines

SSO allows a user to use one set of login credentials (such as username and password) to access multiple trusted systems. With SSO, after users log in to the SSL VPN gateway in Web access mode, they can gain access to internal servers without entering the login credentials for the internal servers. The device supports the following methods for SSO login:

- Auto-build method

  Use a packet capture tool to obtain internal server login requests, and then configure SSO login settings based on the login requests to automatically build login requests to the internal servers. SSO login settings include the HTTP request method, login request encoding method, login parameters, and login data encryption file.

- Basic authentication

Basic authentication is a simple HTTP authentication scheme, which requires a Web client to enter a username and password to access the server. The server authenticates the client based on the username and password.

To implement SSO in the basic authentication method, the SSL VPN gateway acts as a Web client and automatically enters a username and password to perform HTTP basic authentication. The entered username and password can be SSL VPN username and password or a custom username and password.

The basic authentication SSO method is applicable only for logging in to the internal servers that support basic authentication.

Examples

In URL item **servera**, specify the SSO method as basic authentication.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] url-item servera
[Sysname-sslvpn-context-ctx1-url-item-servera] sso method basic
```

Related commands

sso auto-build code

sso auto-build custom-login-parameter

sso auto-build login-parameter

sso auto-build request-method

sso basic custom-username-password enable

sso encrypt file

timeout idle

Use **timeout idle** to set the idle timeout timer for SSL VPN sessions.

Use **undo timeout idle** to restore the default.

Syntax

timeout idle *minutes*

undo timeout idle

Default

The idle timeout timer is 30 minutes for SSL VPN sessions.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies the idle timeout timer in the range of 1 to 1440 minutes.

Usage guidelines

If the idle time of an SSL VPN session exceeds the specified idle timeout time, the session is terminated.

Examples

Set the idle timeout timer to 50 minutes for SSL VPN sessions.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] timeout idle 50
```

Related commands

display sslvpn policy-group

title

Use **title** to configure a title to be displayed on SSL VPN webpages.

Use **undo title** to restore the default.

Syntax

title { **chinese** *chinese-title* | **english** *english-title* }

undo title { **chinese** | **english** }

Default

The title is **SSL VPN**.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

chinese *chinese-title*: Configures a title in Chinese, a case-sensitive string of 1 to 255 characters.

english *english-title*: Configures a title in English, a case-sensitive string of 1 to 255 characters.

Examples

Configure the title as **SSL VPN service for company A**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] title english SSL VPN service for company A
```

uri-acl

Use **uri-acl** to create a URI ACL and enter its view, or enter the view of an existing URI ACL.

Use **undo uri-acl** to delete a URI ACL.

Syntax

uri-acl *uri-acl-name*

undo uri-acl *uri-acl-name*

Default

No URI ACLs exist.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

uri-acl-name: Specifies a name for the URI ACL, a case-insensitive string of 1 to 31 characters.

Usage guidelines

A URI ACL is a set of rules that permit or deny access to resources. You can use URI ACLs for IP, TCP, and Web access filtering of SSL VPN users.

You can create multiple URI ACLs in an SSL VPN context.

Examples

Create a URI ACL named **uriacla** and enter its view.

```
<Sysname> system-view
[Sysname] sslvpn context abc
[Sysname-sslvpn-context-abc] uri-acl uriacla
[Sysname-sslvpn-context-abc-uri-acl-uriacla]
```

url (file policy view)

Use **url** to specify the URL of the Web page file to be rewritten in a file policy.

Use **undo url** to restore the default.

Syntax

url *url*

undo url

Default

No file URL is specified in a file policy.

Views

File policy view

Predefined user roles

network-admin

context-admin

Parameters

url: Specifies the complete file path, a case-insensitive string of 1 to 256 characters.

Usage guidelines

A file policy can be used to modify only the Web page file whose URL is the same as the URL configured in the policy.

A file URL is in the format of *scheme://user:password@host:port/path*. Table 15 describes the fields in the file URL.

Table 15 URL field descriptions

Field	Description
scheme	Protocol type. Options include http and https.
user:password	Username and password used to access the file.
host	Host name or IP address of the server where the file resides. To specify an IPv6 address, enclose the IPv6 address in brackets. For example, http://[1234::5678]:8080/a.html.
port	Port number on which the server listens for resource access requests. If you do not specify a port number, the default port number of the protocol is used, which is 80 for HTTP and 443 for HTTPS.
path	Local path of the file on the server.

You can specify only one file URL in a file policy. In the same SSL VPN context, the URL specified for each file policy must be unique.

Examples

Specify a file URL for file policy **fp**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx
[Sysname-sslvpn-context-ctx] file-policy fp
[Sysname-sslvpn-context-ctx-file-policy-fp] url http://192.168.1.1:8080/js/test.js
```

url (URL item view)

Use **url** to specify a URL in a URL item.

Use **undo url** to remove the URL from a URL item.

Syntax

url *url*

undo url

Default

No URL is specified in a URL item.

Views

URL item view

Predefined user roles

network-admin

context-admin

Parameters

url: Specifies a URL, a case-insensitive string of 1 to 253 characters in the format of *protocol://host:port/path*.

Usage guidelines

Table 16 describes the fields in a URL.

Table 16 URL field descriptions

Field	Description
protocol	Protocol name. Options are: • http. • https. If you do not specify a protocol name, the default protocol (HTTP) is used.
host	Domain name or IP address of a host. To specify an IPv6 address, enclose the IPv6 address in brackets. For example. http://[1234::5678]:8080.
port	Port number. If you do not specify a port number, the default port number of the protocol is used, which is 80 for HTTP and 443 for HTTPS.
path	Path to the resource on the host.

You can specify only one URL in a URL item. If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify **www.abc.com** as the URL in URL item **serverA**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] url-item serverA
[Sysname-sslvpn-context-ctx1-url-item-serverA] url www.abc.com
```

url-item

Use **url-item** to create a URL item and enter its view, or enter the view of an existing URL item.

Use **undo url-item** to delete a URL item.

Syntax

url-item *url-item-name*

undo url-item *url-item-name*

Default

No URL items exist in an SSL VPN context.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

url-item-name: Specifies a name for the URL item, a case-insensitive string of 1 to 31 characters.

Usage guidelines

You can create multiple URL items in an SSL VPN context. Each URL item contains an accessible resource URL and can be assigned to a URL list in the SSL VPN context.

A URL item that has been assigned to a URL list cannot be deleted.

Examples

Create a URL item named **serverA** and enter URL item view.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] url-item serverA
[Sysname-sslvpn-context-ctx1-url-item-serverA]
```

url-list

Use **url-list** to create a URL list and enter its view, or enter the view of an existing URL list.

Use **undo url-list** to delete a URL list.

Syntax

url-list *name*

undo url-list *name*

Default

No URL lists exist.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

name: Specifies a name for the URL list, a case-insensitive string of 1 to 31 characters.

Examples

Create a URL list named **url1** and enter URL list view.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] url-list url1
[Sysname-sslvpn-context-ctx1-url-list-url1]
```

Related commands

sslvpn context

url-mapping

Use **url-mapping** to configure URL mapping in a URL item.

Use **undo url-mapping** to restore the default.

Syntax

url-mapping { **domain-mapping** *domain-name* | **port-mapping gateway** *gateway-name* [**virtual-host** *virtual-host-name*] } [**rewrite-enable**]

undo url-mapping

Default

The normal rewriting method is used.

Views

URL item view

Predefined user roles

network-admin

context-admin

Parameters

domain-mapping *domain-name*: Specifies the domain name mapping method. This method maps the URL to a domain name, a case-insensitive string of 1 to 127 characters which can contain letters, digits, underscores (_), hyphens (-), and dots (.). The specified domain cannot be the same as the domain name of the SSL VPN gateway.

port-mapping gateway *gateway-name*: Specifies the port mapping method. This method maps the URL to a gateway name and an optional virtual host name. The *gateway-name* argument specifies the gateway name, a case-insensitive string of 1 to 31 characters which can contain letters, digits, and underscores (_). The specified SSL VPN gateway name must be the name of an existing SSL VPN gateway.

virtual-host *virtual-host-name*: Specifies the virtual host name, a case-insensitive string of 1 to 127 characters which can contain letters, digits, underscores (_), hyphens (-), and dots (.). Do not specify a virtual host name if you want to use the SSL VPN gateway exclusively for the URL item.

rewrite-enable: Enables the SSL VPN gateway to rewrite the absolute URLs in the resource access response returned from the internal server. These absolute URLs are generally the URLs linked to other servers from the internal server. If you do not specify this keyword, these absolute URLs are not accessible. Enable this rewriting feature as a best practice to improve user experience.

Usage guidelines

The SSL VPN gateway rewrites the resource URLs in resource access responses that contain HTML, XML, CSS, or JavaScript files before sending the URLs to the requesting users. By default, the normal rewriting method is used for the URL rewriting. You can also configure the SSL VPN gateway to use the domain mapping or port mapping method.

Normal rewriting might cause problems such as missed URL rewriting and rewriting errors, resulting in SSL VPN clients not being able to access the internal resources. Use domain mapping or port mapping as a best practice. For more information about these mapping methods, see SSL VPN configuration in *Security Configuration Guide*.

When configuring the domain mapping method, make sure the SSL VPN client can resolve the mapped domain name (through DNS or the Hosts file) into the IP address of the SSL VPN gateway.

When configuring the port mapping method, you can specify an SSL VPN gateway exclusively for a URL item by specifying the gateway name without a virtual host name. To share an SSL VPN gateway with other URL items or SSL VPN contexts, specify the SSL VPN gateway name together with a virtual host name.

If you execute this command for a URL item multiple times, the most recent configuration takes effect.

Examples

Create URL item **serverA** and specify **www.server.com** as the resource URL. Map the resource URL to domain name **www.domain.com** and enable URL rewriting.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] url-item serverA
```

```
[Sysname-sslvpn-context-ctx1-url-item-serverA] url www.server.com
[Sysname-sslvpn-context-ctx1-url-item-serverA] url-mapping domain-mapping
www.domain.com rewrite-enable
```

Create URL item **serverB** and specify **www.server.com** as the resource URL. Map the resource URL to gateway **gw1** with virtual host name **host1** and enable URL rewriting.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] url-item serverB
[Sysname-sslvpn-context-ctx1-url-item-serverB] url www.server.com
[Sysname-sslvpn-context-ctx1-url-item-serverB] url-mapping port-mapping gateway gw1
virtual-host host1 rewrite-enable
```

Related commands

`url-item`

`url`

url-masking enable

Use **`url-masking enable`** to enable URL masking.

Use **`undo url-masking enable`** to disable URL masking.

Syntax

`url-masking enable`

`undo url-masking enable`

Default

URL masking is disabled.

Views

SSL VPN context view

URL item view

Predefined user roles

network-admin

context-admin

Usage guidelines

The URL masking feature hides the real Web access resource URLs configured in an SSL VPN context by converting the URLs into coded strings.

If URL masking is enabled in an SSL VPN context, all the Web resources in the context are enabled with URL masking. In this case, if you want to disable URL masking, you must use the **undo `url-masking enable`** command in the SSL VPN context view for all the Web resources.

You can enable or disable URL masking for a single URL in URL item view only when URL masking is disabled in SSL VPN context view.

Examples

Enable URL masking for the Web resource URL in a URL item.

```
<Sysname> system-view
[Sysname] sslvpn context ctx
[Sysname-sslvpn-context-ctx] url-item urlitem
```

```
[Sysname-sslvpn-context-ctx-url-item-urlitem] url-masking enable
```

Enable URL masking for all Web resource URLs in an SSL VPN context.

```
<Sysname> system-view
[Sysname] sslvpn context ctx
[Sysname-sslvpn-context-ctx] url-masking enable
```

user

Use **user** to create an SSL VPN user and enter SSL VPN user view, or enter the view of an existing SSL VPN user.

Use **undo user** to delete an SSL VPN user.

Syntax

user *username*

undo user *username*

Default

No SSL VPN users exist.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

username: Specifies the SSL VPN username, a case-sensitive string of 1 to 63 characters. The username cannot contain any of the following characters: forward slash (/), backslash (\), vertical bar (|), colon (:), asterisk (*), question mark (?), left angle bracket (<), and right angle bracket (>).

Usage guidelines

You can create multiple SSL VPN users in an SSL VPN context.

Examples

Create SSL VPN user **user1** and enter SSL VPN user view.

```
<Sysname> system-view
[Sysname] sslvpn context ctx
[Sysname-sslvpn-context-ctx] user user1
[Sysname-sslvpn-context-ctx-user-user1]
```

verification-code send-interval

Use **verification-code send-interval** to set the SMS verification code resend interval.

Use **undo verification-code send-interval** to restore the default.

Syntax

verification-code send-interval *seconds*

undo verification-code send-interval

Default

The SMS verification code resend interval is 60 seconds.

Views

SMS gateway authentication view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies the verification code resend interval, in the range of 0 to 3600 seconds.

Usage guidelines

This interval is the minimum amount of time that a user must wait before the user can re-obtain the SMS verification code.

Examples

In SMS gateway authentication view, set the verification code resend interval to 80 seconds.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] sms-auth sms-gw
[Sysname-sslvpn-context-ctx1-sms-auth-sms-gw] verification-code send-interval 80
```

verification-code validity

Use **verification-code validity** to set the SMS verification code validity period.

Use **undo verification-code validity** to restore the default.

Syntax

verification-code validity *minutes*

undo verification-code validity

Default

The SMS verification code validity period is one minute.

Views

SMS gateway authentication view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies the verification code validity period, in the range of 1 to 1440 minutes.

Examples

In SMS gateway authentication view, set the verification code validity period to 30 minutes.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] sms-auth sms-gw
[Sysname-sslvpn-context-ctx1-sms-auth-sms-gw] verification-code validity 30
```

verify-code

Use **verify-code enable** to enable code verification.

Use **undo verify-code enable** to disable code verification.

Syntax

verify-code enable

undo verify-code enable

Default

Code verification is disabled.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Usage guidelines

After code verification is enabled, a user must enter a correct verification code to log in to the SSL VPN webpage.

Examples

Enable code verification.

```
<Sysname> system-view
[Sysname] sslvpn context ctx
[Sysname-sslvpn-context-ctx] verify-code enable
```

vpn-instance (SSL VPN context view)

Use **vpn-instance** to associate an SSL VPN context with a VPN instance.

Use **undo vpn-instance** to restore the default.

Syntax

vpn-instance *vpn-instance-name*

undo vpn-instance

Default

An SSL VPN context is associated with the public network.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance-name: Specifies the name of a VPN instance, a case-sensitive string of 1 to 31 characters.

Usage guidelines

After you associate an SSL VPN context with a VPN instance, the resources managed by the context belong to the VPN instance.

An SSL VPN context can be associated with only one VPN instance.

You can associate an SSL VPN context with a nonexistent VPN instance. The context does not take effect until the associated VPN instance is created.

If you change the VPN instance associated with an SSL VPN context, all user-to-IP address bindings configured for SSL VPN users in the SSL VPN context will be removed.

Examples

Associate SSL VPN context **context1** with VPN instance **vpn1**.

```
<Sysname> System-view
[Sysname] sslvpn context context1
[Sysname-sslvpn-context-context1] vpn-instance vpn1
```

vpn-instance (SSL VPN gateway view)

Use **vpn-instance** to specify a VPN instance for an SSL VPN gateway.

Use **undo vpn-instance** to restore the default.

Syntax

vpn-instance *vpn-instance-name*

undo vpn-instance

Default

An SSL VPN gateway belongs to the public network.

Views

SSL VPN gateway view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance-name: Specifies the name of a VPN instance, a case-sensitive string of 1 to 31 characters.

Usage guidelines

The VPN instance specified for an SSL VPN gateway is called a front VPN instance.

You can specify only one VPN instance for an SSL VPN gateway.

You can specify a nonexistent VPN instance for an SSL VPN gateway. The SSL VPN gateway does not take effect until the VPN instance is created.

Examples

Specify VPN instance **vpn1** for SSL VPN gateway **gateway1**.

```
<Sysname> system-view
[Sysname] sslvpn gateway gateway1
[Sysname-sslvpn-gateway-gateway1] vpn-instance vpn1
```

web-access ip-client auto-activate

Use **web-access ip-client auto-activate** to enable automatic startup of the IP access client after Web login.

Use **undo web-access ip-client auto-activate** to disable automatic startup of the IP access client after Web login.

Syntax

web-access ip-client auto-activate

undo web-access ip-client auto-activate

Default

Automatic startup of the IP access client after Web login is disabled.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Usage guidelines

With this feature enabled, after a user logs in to the SSL VPN gateway through a Web browser, the IP access client on the user host will automatically connect to the gateway. If the IP access client software is not installed, the user will be prompted to install the software first.

For the IP access client to connect to the SSL VPN gateway correctly, make sure the IP access service and resources are configured on the SSL VPN gateway.

If an SSL VPN user has already logged in through an IP access client when this feature is enabled, the user cannot access the SSL VPN gateway directly through the Web browser. To access the SSL VPN gateway through the Web browser, the user must click **Open Resource List** in the IP access client.

Examples

Enable automatic startup of the IP access client after Web login in SSL VPN context **ctx1**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] web-access ip-client auto-activate
```

webpage-customize

Use **webpage-customize** to specify a webpage template for SSL VPN webpage customization.

Use **undo webpage-customize** to restore the default.

Syntax

webpage-customize *template-name*

undo webpage-customize

Default

The global SSL VPN webpage template is used.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

template-name: Specifies a webpage template by its name, a string of 1 to 31 characters. The name cannot contain any of the following characters: forward slash (/), backslash (\), vertical bar (|), colon (:), asterisk (*), quotation mark ("), question mark (?), left angle bracket (<), and right angle bracket (>).

Usage guidelines

This command allows you to set the webpage template for an SSL VPN context. Both predefined and user-defined webpage templates are available.

You can upload and download webpage templates through the SSL VPN Web interface.

To view all webpage templates in the system, use the **display sslvpn webpage-customize template** command.

In an SSL VPN context, the webpage template specified for the SSL VPN context takes precedence over the global SSL VPN webpage template. To set the global SSL VPN webpage template, use the **sslvpn webpage-customize** command in system view.

If a user-defined webpage template is specified in an SSL VPN context, all other webpage customization settings are invalid for the SSL VPN context.

Examples

Use webpage template **template1** to customize SSL VPN webpages in SSL VPN context **ctx**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx
[Sysname-sslvpn-context-ctx] webpage-customize template1
```

Related commands

display sslvpn webpage-customize template

sslvpn webpage-customize

wechat-work-authentication app-secret

Use **wechat-work-authentication app-secret** to specify the app secret key for WeChat Work (or WeCom) authentication.

Use **undo wechat-work-authentication app-secret** to restore the default.

Syntax

wechat-work-authentication app-secret *app-secret*

undo wechat-work-authentication app-secret

Default

No app secret key is specified for WeChat Work authentication.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

template-name: Specifies the app secret key, a case-insensitive string of 1 to 127 characters.

Usage guidelines

Each app has an independent secret key to ensure data security. Make sure the app secret key is not leaked.

The app secret key and the company ID are used together to generate important credentials for the SSL VPN gateway to obtain user information from the WeChat Work API server.

To view this secret key on the WeChat Work management platform, select the target app on the **App Management** page.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the app secret key as **hpLRFnu7OxedV5bNd9OD0Xi** in SSL VPN context **ctx**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx
[Sysname-sslvpn-context-ctx] wechat-work-authentication app-secret
hpLRFnu7OxedV5bNd9OD0Xi
```

Related commands

wechat-work-authentication corp-id

wechat-work-authentication authorize-field

Use **wechat-work-authentication authorize-field** to specify the name of the authorization policy group field.

Use **undo wechat-work-authentication authorize-field** to restore the default.

Syntax

wechat-work-authentication authorize-field *authorize-field*

undo wechat-work-authentication authorize-field

Default

No authorization policy group field name is specified for WeChat Work authentication.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

authorize-field: Specifies the name of the authorization policy group field, a case-insensitive string of 1 to 31 characters. Chinese characters are supported.

Usage guidelines

The SSL VPN gateway uses the specified field name to obtain the authorization policy group name (the organization information of users) from the response of the WeChat Work API server.

Assume that the name of the authorization policy group field is **group**. If the response of the WeChat Work API server contains the field **group:ziliao**, the SSL VPN gateway obtains the user's

authorization policy group name, **ziliao**. Then, the gateway will check whether a local policy group named **ziliao** exists:

- If yes, the user is authorized to access the corresponding internal resources in this policy group.
- If no, the user is authorized to access internal resources in the default policy group.

For the SSL VPN gateway to successfully resolve the authorization policy group name from the response, make sure you specify the correct authorization policy group field name in this command. You can obtain the authorization policy group field name from WeChat Work before executing this command.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the name of the authorization policy group field as **group** in SSL VPN context **ctx**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx
[Sysname-sslvpn-context-ctx] wechat-work-authentication authorize-field group
```

wechat-work-authentication corp-id

Use **wechat-work-authentication corp-id** to specify the company ID for WeChat Work authentication.

Use **undo wechat-work-authentication corp-id** to restore the default.

Syntax

wechat-work-authentication corp-id *corp-id*

undo wechat-work-authentication corp-id

Default

No company ID is specified for WeChat Work authentication.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

corp-id: Specifies the company ID, a case-insensitive string of 1 to 63 characters.

Usage guidelines

A company ID uniquely identifies a company on WeChat Work. The company ID and the secret key are used together to generate important credentials for the SSL VPN gateway to obtain user information from the WeChat Work API server.

To view the company ID on the WeChat Work management platform, go to **My Company** > **Company Information**.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the company ID as **wxdd725338566d6ffe** in SSL VPN context **ctx**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx
```

```
[Sysname-sslvpn-context-ctx] wechat-work-authentication corp-id wxdd725338566d6ffe
```

Related commands

wechat-work-authentication app-secret

wechat-work-authentication enable

Use **wechat-work-authentication enable** to enable WeChat Work authentication.

Use **undo wechat-work-authentication enable** to disable WeChat Work authentication.

Syntax

wechat-work-authentication enable

undo wechat-work-authentication enable

Default

WeChat Work authentication is disabled.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Usage guidelines

After WeChat Work authentication is enabled, the device obtains user information of a company from WeChat Work and uses the user information for authentication and authorization. If the authentication and authorization succeed, the users can access the internal resources. This feature is transparent to the users in the company.

Examples

Enable WeChat Work authentication in SSL VPN context **ctx**.

```
<Sysname> system-view
[Sysname] sslvpnc ontext ctx
[Sysname-sslvpn-context-ctx] wechat-work-authentication enable
```

wechat-work-authentication open-platform-url

Use **wechat-work-authentication open-platform-url** to specify the WeChat open platform URL.

Use **undo wechat-work-authentication open-platform-url** to restore the default.

Syntax

wechat-work-authentication open-platform-url { pre-defined | user-defined *user-defined-url* **}**

undo wechat-work-authentication open-platform-url

Default

No WeChat open platform URL is specified.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

pre-defined: Specifies the predefined WeChat open platform URL, **https://open.weixin.qq.com**.

user-defined *user-defined-url*: Specifies the WeChat open platform URL as needed, a case-insensitive string of 1 to 63 characters.

Usage guidelines

In general, after receiving a response from the internal server, the SSL VPN gateway will check whether the HTTP header contains the **Location** field. If the **Location** field exists, the SSL VPN gateway will rewrite the URL in the **Location** field and forward the response to the SSL VPN client. The subsequent requests of the SSL VPN client must access the redirected URL.

In particular cases, the response from the internal server to the SSL VPN gateway might require the user to send an authentication request to WeChat Work again. In this case, the SSL VPN gateway must not rewrite the WeChat Work server URL in the **Location** field so that the client can access the WeChat Work server to complete authentication and authorization. If the SSL VPN gateway rewrites the WeChat Work server URL, the WeChat Work server cannot receive the request from the client and WeChat Work authentication fails.

This command specifies the URL in the **Location** field that will not be rewritten by the SSL VPN gateway. For WeChat Work authentication to operate correctly, set the URL as the WeChat open platform URL.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the predefined URL **https://open.weixin.qq.com** as the WeChat open platform URL in SSL VPN context **ctx**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx
[Sysname-sslvpn-context-ctx] wechat-work-authentication open-platform url pre-defined
```

wechat-work-authentication timeout

Use **wechat-work-authentication timeout** to specify the WeChat Work authentication timeout.

Use **undo wechat-work-authentication timeout** to restore the default.

Syntax

wechat-work-authentication timeout *seconds*

undo wechat-work-authentication timeout

Default

The WeChat Work authentication timeout is 15 seconds.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies the WeChat Work authentication timeout, in the range of 5 to 50 seconds.

Usage guidelines

A WeChat Work authentication fails if the SSL VPN gateway does not receive the response from the WeChat Work API server within the timeout time after sending an HTTP request.

If the network delay is large, increase the timeout as a best practice to avoid misidentification of timeouts. If the network delay is small, reduce the timeout as a best practice for better identification of timeouts.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the WeChat Work authentication timeout as 20 seconds in SSL VPN context **ctx**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx
[Sysname-sslvpn-context-ctx] wechat-work-authentication timeout 20
```

wechat-work-authentication url

Use **wechat-work-authentication url** to specify the URL of the WeChat Work API server.

Use **undo wechat-work-authentication url** to restore the default.

Syntax

wechat-work-authentication url *url*

undo wechat-work-authentication url

Default

No WeChat Work API server URL is specified.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

url: Specifies the URL of the WeChat Work API server, a case-insensitive string of 1 to 255 characters.

Usage guidelines

To use WeChat Work authentication, you must execute this command to specify the actual URL of the WeChat Work API server. The SSL VPN gateway interacts with the specified WeChat Work API server to obtain user information upon receiving a packet redirected from the WeChat Work server. Then, the SSL VPN gateway uses the obtained information for user authentication and authorization.

The SSL VPN gateway requires domain name resolution to resolve the specified URL into the IP address of the WeChat Work API server. For more information about domain name resolution, see DNS configuration in *Layer 3—IP Services Configuration Guide*.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the URL of the WeChat Work API server as **https://qyapi.weixin.qq.com** in SSL VPN context **ctx**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx
[Sysname-sslvpn-context-ctx] wechat-work-authentication url https://qyapi.weixin.qq.com
```

wechat-work-authentication userid-field

Use **wechat-work-authentication userid-field** to specify the user ID field name used by the SSL VPN gateway to access the internal server.

Use **undo wechat-work-authentication userid-field** to restore the default.

Syntax

wechat-work-authentication userid-field *userid-field*

undo wechat-work-authentication userid-field

Default

No user ID field name is configured for the SSL VPN gateway to access the internal server.

Views

SSL VPN context view

Predefined user roles

network-admin

context-admin

Parameters

url: Specifies the user ID field name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

A user ID (user account) on WeChat Work uniquely identifies a user within a company. The SSL VPN gateway interacts with the WeChat Work API server to obtain user information, which contains the user ID of a user.

The SSL VPN gateway uses the specified user ID field name and the obtained user ID to construct the parameter to be carried in an access request sent to an internal server. For example, if you configure the user ID field name as **login** and the obtained user ID is **zhangsan**, the SSL VPN gateway will construct the parameter as **login=zhangsan**. When receiving the request from the SSL VPN gateway, the internal server abstracts the **login** field's value **zhangsan** as the user ID. To make sure the SSL VPN gateway can accurately encapsulate the parameter, you must obtain the user ID field name from the internal server in advance.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the user ID field name as **login** in SSL VPN context **ctx**.

```
<Sysname> system-view
[Sysname] sslvpn context ctx
[Sysname-sslvpn-context-ctx] wechat-work-authentication url https://qyapi.weixin.qq.com
```

Contents

IPsec commands

The SM1 algorithm is supported only on devices installed with a GM network data encryption module.

activate link

Use **activate link** to manually activate a link.

Syntax

activate link *link-id*

Views

IPsec smart link policy view

Predefined user roles

network-admin

context-admin

Parameters

link-id: Specifies the ID of an existing link in the IPsec smart link policy. The value range for this argument is 1 to 10.

Usage guidelines

To establish an IPsec tunnel over a specific link, use this command to activate the link.

If smart link selection is enabled, traffic will be switched to another link in turn if the packet loss ratio or delay over the link exceeds the link switchover thresholds. The first cyclic link switchover starts from the manually activated link and ends with the link that has the lowest priority. For example, after you activate the third link of four links, the first link switchover cycle is 3 > 4, and the subsequent link switchover cycles each are 1 > 2 > 3 > 4.

If smart link selection is disabled in the IPsec smart link policy, the manually activated link is always used and no link switchover will occur.

Examples

Manually activate link 2 in IPsec smart policy **smlkpolicy1**.

```
<Sysname> system-view
[Sysname] ipsec smart-link policy smlkpolicy1
[Sysname-ipsec-smart-link-policy-smlkpolicy1] activate link 2
```

Related commands

display ipsec smart-link policy

ah authentication-algorithm

Use **ah authentication-algorithm** to specify authentication algorithms for the AH protocol.

Use **undo ah authentication-algorithm** to restore the default.

Syntax

ah authentication-algorithm { **aes-xcbc-mac** | **md5** | **sha1** | **sha256** | **sha384** | **sha512** | **sm3** } *

undo ah authentication-algorithm

Default

AH does not use any authentication algorithms.

Views

IPsec transform set view

Predefined user roles

network-admin

context-admin

Parameters

aes-xcbc-mac: Specifies the HMAC-AES-XCBC-96 algorithm, which uses a 128-bit key. This keyword is available only for IKEv2.

md5: Specifies the HMAC-MD5-96 algorithm, which uses a 128-bit key.

sha1: Specifies the HMAC-SHA1-96 algorithm, which uses a 160-bit key.

sha256: Specifies the HMAC-SHA256 algorithm, which uses a 256-bit key.

sha384: Specifies the HMAC-SHA384 algorithm, which uses a 384-bit key.

sha512: Specifies the HMAC-SHA512 algorithm, which uses a 512-bit key.

sm3: Specifies the HMAC-SM3-96 algorithm, which uses a 256-bit key. This keyword is available only for IKEv1.

Usage guidelines

You can specify multiple AH authentication algorithms for one IPsec transform set, and the algorithm specified earlier has a higher priority.

For a manual or IKEv1-based IPsec policy, the first specified AH authentication algorithm takes effect. To make sure an IPsec tunnel can be established successfully, the IPsec transform sets specified at both ends of the tunnel must have the same first AH authentication algorithm.

Examples

Specify HMAC-SHA1 as the AH authentication algorithm for IPsec transform set **tran1**.

```
<Sysname> system-view
[Sysname] ipsec transform-set tran1
[Sysname-ipsec-transform-set-tran1] ah authentication-algorithm sha1
```

description

Use **description** to configure a description for an IPsec policy, IPsec profile, or IPsec policy template.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

No description is configured for an IPsec policy, IPsec profile, or IPsec policy template.

Views

IPsec policy view

IPsec policy template view

IPsec profile view

Predefined user roles

network-admin

context-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 80 characters.

Usage guidelines

You can configure different descriptions for IPsec policies, IPsec profiles, or IPsec policy templates to distinguish them.

Examples

Configure the description for IPsec policy **policy1** as **CenterToA**.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 1 isakmp
[Sysname-ipsec-policy-isakmp-policy1-1] description CenterToA
```

display ipsec { ipv6-policy | policy }

Use **display ipsec** { **ipv6-policy** | **policy** } to display information about IPsec policies.

Syntax

display ipsec { **ipv6-policy** | **policy** } [*policy-name* [*seq-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ipv6-policy: Displays information about IPv6 IPsec policies.

policy: Displays information about IPv4 IPsec policies.

policy-name: Specifies an IPsec policy by its name, a case-insensitive string of 1 to 63 characters.

seq-number: Specifies an IPsec policy entry by its sequence number in the range of 1 to 65535.

Usage guidelines

If you do not specify any parameters, this command displays information about all IPsec policies.

If you specify an IPsec policy name and a sequence number, this command displays information about the specified IPsec policy entry. If you specify an IPsec policy name without any sequence number, this command displays information about all IPsec policy entries with the specified name.

Examples

Display information about all IPv4 IPsec policies.

```
<Sysname> display ipsec policy
-----------------------------------------
IPsec Policy: mypolicy
-----------------------------------------

  ----------------------------
  Sequence number: 1
  Mode: Manual
  ----------------------------
  The policy configuration is incomplete:
           ACL not specified
           Incomplete transform-set configuration
  Description: This is my first IPv4 manual policy
  Security data flow:
  Remote address: 2.5.2.1
  Transform set: transform

  Inbound AH setting:
    AH SPI: 1200 (0x000004b0)
    AH string-key: ******
    AH authentication hex key:

  Inbound ESP setting:
    ESP SPI: 1400 (0x00000578)
    ESP string-key:
    ESP encryption hex key:
    ESP authentication hex key:

  Outbound AH setting:
    AH SPI: 1300 (0x00000514)
    AH string-key: ******
    AH authentication hex key:

  Outbound ESP setting:
    ESP SPI: 1500 (0x000005dc)
    ESP string-key: ******
    ESP encryption hex key:
    ESP authentication hex key:

  ----------------------------
  Sequence number: 2
  Mode: ISAKMP
  ----------------------------
  The policy configuration is incomplete:
           Remote-address not set
           ACL not specified
```

```
          Transform-set not set
  Description: This is my first IPv4 Isakmp policy
  Traffic Flow Confidentiality: Enabled
  Security data flow:
  Selector mode: standard
  Local address:
  Remote address: 5.3.6.9
  Remote address: test
  Transform set:
  IKE profile:
  IKEv2 profile:
  smart-link policy:
  SA trigger mode: Auto
  SA duration(time based): 3600 seconds
  SA duration(traffic based): 1843200 kilobytes
  SA soft-duration buffer(time based): 1000 seconds
  SA soft-duration buffer(traffic based): 43200 kilobytes
  SA idle time: 100 seconds
------------------------------------------
IPsec Policy: mycompletepolicy
Interface: LoopBack2
------------------------------------------

  ----------------------------
  Sequence number: 1
  Mode: Manual
  ----------------------------
  Description: This is my complete policy
  Security data flow: 3100
  Remote address: 2.2.2.2
  Transform set: completetransform

  Inbound AH setting:
    AH SPI: 5000 (0x00001388)
    AH string-key: ******
    AH authentication hex key:

  Inbound ESP setting:
    ESP SPI: 7000 (0x00001b58)
    ESP string-key: ******
    ESP encryption hex key:
    ESP authentication hex key:

  Outbound AH setting:
    AH SPI: 6000 (0x00001770)
    AH string-key: ******
    AH authentication hex key:
```

```
  Outbound ESP setting:
    ESP SPI: 8000 (0x00001f40)
    ESP string-key: ******
    ESP encryption hex key:
    ESP authentication hex key:

  ----------------------------
  Sequence number: 2
  Mode: ISAKMP
  ----------------------------
  Description: This is my complete policy
  Traffic Flow Confidentiality: Enabled
  Security data flow: 3200
  Selector mode: standard
  Local address:
  Remote address: 5.3.6.9
  Transform set:  completetransform
  IKE profile:
  IKEv2 profile:
  smart-link policy:
  SA trigger mode: Auto
  SA duration(time based): 3600 seconds
  SA duration(traffic based): 1843200 kilobytes
  SA soft-duration buffer(time based): 1000 seconds
  SA soft-duration buffer(traffic based): 43200 kilobytes
  SA idle time: 100 seconds
```

Display information about all IPv6 IPsec policies.

```
<Sysname> display ipsec ipv6-policy
-----------------------------------------
IPsec Policy: mypolicy
-----------------------------------------

  ----------------------------
  Sequence number: 1
  Mode: Manual
  ----------------------------
  Description: This is my first IPv6 policy
  Security data flow: 3600
  Remote address: 1000::2
  Transform set: mytransform

  Inbound AH setting:
    AH SPI: 1235 (0x000004d3)
    AH string-key: ******
    AH authentication hex key:

  Inbound ESP setting:
    ESP SPI: 1236 (0x000004d4)
```

```
  ESP string-key: ******
  ESP encryption hex key:
  ESP authentication hex key:

Outbound AH setting:
  AH SPI: 1237 (0x000004d5)
  AH string-key: ******
  AH authentication hex key:

Outbound ESP setting:
  ESP SPI: 1238 (0x000004d6)
  ESP string-key: ******
  ESP encryption hex key:
  ESP authentication hex key:

-----------------------------
Sequence number: 2
Mode: ISAKMP
-----------------------------
Description: This is my complete policy
Traffic Flow Confidentiality: Enabled
Security data flow: 3200
Selector mode: standard
Local address:
Remote address: 1000::2
Transform set:  completetransform
IKE profile:
IKEv2 profile:
smart-link policy:
SA trigger mode: Auto
SA duration(time based): 3600 seconds
SA duration(traffic based): 1843200 kilobytes
SA soft-duration buffer(time based): 1000 seconds
SA soft-duration buffer(traffic based): 43200 kilobytes
SA idle time: 100 seconds
```

Table 1 Command output

Field	Description
IPsec Policy	IPsec policy name.
Interface	Interface applied with the IPsec policy.
Sequence number	Sequence number of the IPsec policy entry.
Mode	Negotiation mode of the IPsec policy: • **Manual**—Manual mode. • **ISAKMP**—IKE negotiation mode. • **Template**—IPsec policy template mode.
The policy configuration is incomplete	IPsec policy configuration incomplete. Possible causes include: • The ACL is not configured.

Field	Description
	• The IPsec transform set is not configured. • The ACL does not have any **permit** statements. • The IPsec transform set configuration is not complete. • The peer IP address of the IPsec tunnel is not specified. • The SPI and key of the IPsec SA do not match those in the IPsec policy.
Description	Description of the IPsec policy.
Traffic Flow Confidentiality	Whether Traffic Flow Confidentiality (TFC) padding is enabled.
Security data flow	ACL used by the IPsec policy.
Selector mode	Data flow protection mode of the IPsec policy: **standard**, **aggregation**, or **per-host**.
Local address	Local end IP address of the IPsec tunnel (available only for the IKE-based IPsec policy).
Remote address	Remote end IP address or host name of the IPsec tunnel. The IP addresses and host name each are displayed in a separate line. The primary IP address is displayed in the first line. The other IP addresses and the host name are displayed in subsequent lines in the order that they were configured in the IPsec policy.
Transform set	Transform set used by the IPsec policy.
IKE profile	IKE profile used by the IPsec policy.
IKEv2 profile	IKEv2 profile used by the IPsec policy.
smart-link policy	Smart link policy used by the IPsec policy.
SA trigger mode	IPsec SA negotiation triggering mode: • **Auto**—Triggers SA negotiation when required IPsec configuration is complete. • **Traffic-based**—Triggers SA negotiation when traffic requires IPsec protection.
SA duration(time based)	Time-based IPsec SA lifetime, in seconds.
SA duration(traffic based)	Traffic-based IPsec SA lifetime, in Kilobytes.
SA soft-duration buffer(time based)	Time-based IPsec SA soft lifetime buffer, in seconds. If the time-based IPsec SA soft lifetime buffer is not configured, this field displays two consecutive hyphens (--).
SA soft-duration buffer(traffic based)	Traffic-based IPsec SA soft lifetime buffer, in Kilobytes. If the traffic-based IPsec SA soft lifetime buffer is not configured, this field displays two consecutive hyphens (--).
SA idle time	Idle timeout of the IPsec SA, in seconds. If the IPsec SA idle timeout is not configured, this field displays two consecutive hyphens (--).
AH string-key	AH string key. This field displays ****** if the key is configured and it is empty if the key is not configured.
AH authentication hex key	AH authentication hexadecimal key. This field displays ****** if the key is configured and it is empty if the key is not configured.
ESP string-key	ESP string key. This field displays ****** if the key is configured and it is empty if the key is not configured.
ESP encryption hex key	ESP encryption hexadecimal key. This field displays ****** if the

Field	Description
	key is configured and it is empty if the key is not configured.
ESP authentication hex key	ESP authentication hexadecimal key. This field displays ****** if the key is configured and it is empty if the key is not configured.

Related commands

ipsec { ipv6-policy | policy }

display ipsec { ipv6-policy-template | policy-template }

Use **display ipsec** { **ipv6-policy-template** | **policy-template** } to display information about IPsec policy templates

Syntax

display ipsec { **ipv6-policy-template** | **policy-template** } [*template-name* [*seq-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ipv6-policy-template: Displays information about IPv6 IPsec policy templates.

policy-template: Displays information about IPv4 IPsec policy templates.

template-name: Specifies an IPsec policy template by its name, a case-insensitive string of 1 to 63 characters.

seq-number: Specifies an IPsec policy template entry by its sequence number in the range of 1 to 65535.

Usage guidelines

If you do not specify any parameters, this command displays information about all IPsec policy templates.

If you specify an IPsec policy template name and a sequence number, this command displays information about the specified IPsec policy template entry. If you specify an IPsec policy template name without any sequence number, this command displays information about all IPsec policy template entries with the specified name.

Examples

Display information about all IPv4 IPsec policy templates.

```
<Sysname> display ipsec policy-template
-----------------------------------------------
IPsec Policy Template: template
-----------------------------------------------

  --------------------------------
```

```
  Sequence number: 1
  --------------------------------
Description: This is policy template
Traffic Flow Confidentiality: Disabled
Security data flow :
Selector mode: standard
Local address:
IKE profile:
IKEv2 profile:
Remote address: 162.105.10.2
Transform set:  testprop
IPsec SA local duration(time based): 3600 seconds
IPsec SA local duration(traffic based): 1843200 kilobytes
SA idle time: 100 seconds
```

Display information about all IPv6 IPsec policy templates.

```
<Sysname> display ipsec ipv6-policy-template
-----------------------------------------------
IPsec Policy Template: template6
-----------------------------------------------

  --------------------------------
  Sequence number: 1
  --------------------------------
Description: This is policy template
Traffic Flow Confidentiality: Disabled
Security data flow :
Selector mode: standard
Local address:
IKE profile:
IKEv2 profile:
Remote address: 200::1
Transform set: testprop
IPsec SA local duration(time based): 3600 seconds
IPsec SA local duration(traffic based): 1843200 kilobytes
SA idle time: 100 seconds
```

Table 2 Command output

Field	Description
IPsec Policy Template	IPsec policy template name.
Sequence number	Sequence number of the IPsec policy template entry.
Description	Description of the IPsec policy template.
Traffic Flow Confidentiality	Whether Traffic Flow Confidentiality (TFC) padding is enabled.
Security data flow	ACL used by the IPsec policy template.
Selector mode	Data flow protection mode of the IPsec policy template: **standard**, **aggregation**, or **per-host**.
Local address	Local end IP address of the IPsec tunnel.

Field	Description
IKE profile	IKE profile used by the IPsec policy template.
IKEv2 profile	IKEv2 profile used by the IPsec policy template.
Remote address	Remote end IP address of the IPsec tunnel.
Transform set	Transform set used by the IPsec policy template.
IPsec SA local duration(time based)	Time-based IPsec SA lifetime, in seconds.
IPsec SA local duration(traffic based)	Traffic-based IPsec SA lifetime, in Kilobytes.
SA idle time	Idle timeout of the IPsec SA, in seconds. If the IPsec SA idle timeout is not configured, this field displays two consecutive hyphens (--).

Related commands

ipsec { **ipv6-policy** | **policy** } **isakmp template**

display ipsec profile

Use **display ipsec profile** to display information about IPsec profiles.

Syntax

display ipsec profile [*profile-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

profile-name: Specifies an IPsec profile by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

If you do not specify any parameters, this command displays information about all IPsec profiles.

Examples

Display information about all IPsec profiles.

```
<Sysname> display ipsec profile
-------------------------------------------
IPsec profile: myprofile
Mode: isakmp
-------------------------------------------
  Transform set:  tran1
  IKE profile: profile
  SA duration(time based): 3600 seconds
```

```
  SA duration(traffic based): 1843200 kilobytes
  SA soft-duration buffer(time based): 1000 seconds
  SA soft-duration buffer(traffic based): 43200 kilobytes
  SA idle time: 100 seconds
-----------------------------------------------
IPsec profile: profile
Mode: manual
-----------------------------------------------
  Transform set: prop1
  Inbound AH setting:
    AH SPI: 12345 (0x00003039)
    AH string-key:
    AH authentication hex key: ******
  Inbound ESP setting:
    ESP SPI: 23456 (0x00005ba0)
    ESP string-key:
    ESP encryption hex-key: ******
    ESP authentication hex-key: ******
  Outbound AH setting:
    AH SPI: 12345 (0x00003039)
    AH string-key:
    AH authentication hex key: ******
  Outbound ESP setting:
    ESP SPI: 23456 (0x00005ba0)
    ESP string-key:
    ESP encryption hex key: ******
    ESP authentication hex key: ******
```

Table 3 Command output

Field	Description
IPsec profile	IPsec profile name.
Mode	Negotiation mode used by the IPsec profile.
Description	Description of the IPsec profile.
Transform set	IPsec transform set used by the IPsec profile.
IKE profile	IKE profile used by the IPsec profile.
SA duration(time based)	Time-based IPsec SA lifetime, in seconds.
SA duration(traffic based)	Traffic-based IPsec SA lifetime, in Kilobytes.
SA soft-duration buffer(time based)	Time-based IPsec SA soft lifetime buffer, in seconds. If the time-based IPsec SA soft lifetime buffer is not configured, this field displays two consecutive hyphens (--).
SA soft-duration buffer(traffic based)	Traffic-based IPsec SA soft lifetime buffer, in Kilobytes. If the traffic-based IPsec SA soft lifetime buffer is not configured, this field displays two consecutive hyphens (--).
SA idle time	IPsec SA idle timeout, in seconds. If the IPsec SA idle timeout is not configured, this field displays two consecutive hyphens (--).

Related commands

ipsec profile

display ipsec sa

Use **display ipsec sa** to display information about IPsec SAs.

Syntax

display ipsec sa [**brief** | **count** | **interface** *interface-type interface-number* | { **ipv6-policy** | **policy** } *policy-name* [*seq-number*] | **profile** *profile-name* | **remote** [**ipv6**] *ip-address*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

brief: Displays brief information about all IPsec SAs.

count: Displays the number of IPsec SAs.

interface *interface-type interface-number*: Specifies an interface by its type and number.

ipv6-policy: Displays detailed information about IPsec SAs created by using a specified IPv6 IPsec policy.

policy: Displays detailed information about IPsec SAs created by using a specified IPv4 IPsec policy.

policy-name: Specifies an IPsec policy by its name, a case-insensitive string of 1 to 63 characters.

seq-number: Specifies an IPsec policy entry by its sequence number. The value range is 1 to 65535.

profile: Displays detailed information about IPsec SAs created by using a specified IPsec profile.

profile-name: Specifies an IPsec profile by its name, a case-insensitive string of 1 to 63 characters.

remote *ip-address*: Specifies an IPsec SA by its remote end IP address.

ipv6: Specifies an IPsec SA by its remote end IPv6 address. If this keyword is not specified, the specified remote end IP address is an IPv4 address.

Usage guidelines

If you do not specify any parameters, this command displays detailed information about all IPsec SAs.

Examples

Display brief information about IPsec SAs.

```
<Sysname> display ipsec sa brief
```

```
------------------------------------------------------------------------
Interface/Global   Dst Address      SPI         Protocol  Status
------------------------------------------------------------------------
GE1/0/1            10.1.1.1         400         ESP       Active
GE1/0/1            255.255.255.255  4294967295  ESP       Active
GE1/0/1            100::1/64        500         AH        Active
Global             --               600         ESP       Active
```

Table 4 Command output

Field	Description
Interface/Global	Interface where the IPsec SA belongs to or global IPsec SA (created by using an IPsec profile).
Dst Address	Remote end IP address of the IPsec tunnel. For the IPsec SAs created by using IPsec profiles, this field displays two hyphens (**--**).
SPI	IPsec SA SPI.
Protocol	Security protocol used by IPsec.
Status	Status of the IPsec SA, which can only be **Active**.

Display the number of IPsec SAs.

```
<Sysname> display ipsec sa count
Total IPsec SAs count: 4
```

Display detailed information about all IPsec SAs.

```
<Sysname> display ipsec sa
-------------------------------
Interface: GigabitEthernet1/0/1
-------------------------------

  ----------------------------
  IPsec policy: r2
  Sequence number: 1
  Mode: ISAKMP
  ----------------------------
    Tunnel id: 3
    Encapsulation mode: tunnel
    Perfect Forward Secrecy:
    Inside VPN: vp1
    Extended Sequence Numbers enable: Y
    Traffic Flow Confidentiality enable: N
    Transmitting entity: Initiator
    Path MTU: 1443
    Tunnel:
        local  address: 2.2.2.2
        remote address: 1.1.1.2
    Flow:
        sour addr: 192.168.2.0/255.255.255.0  port: 0  protocol: ip
        dest addr: 192.168.1.0/255.255.255.0  port: 0  protocol: ip
```

```
    [Inbound ESP SAs]
      SPI: 3564837569 (0xd47b1ac1)
      Connection ID: 90194313219
      Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
      SA duration (kilobytes/sec): 4294967295/604800
      SA remaining duration (kilobytes/sec): 1843200/2686
      Max received sequence-number: 5
      Anti-replay check enable: Y
      Anti-replay window size: 32
      UDP encapsulation used for NAT traversal: N
      Status: Active

    [Outbound ESP SAs]
      SPI: 801701189 (0x2fc8fd45)
      Connection ID: 64424509441
      Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
      SA duration (kilobytes/sec): 4294967295/604800
      SA remaining duration (kilobytes/sec): 1843200/2686
      Max sent sequence-number: 6
      UDP encapsulation used for NAT traversal: N
      Status: Active
------------------------------
Global IPsec SA
------------------------------

  ----------------------------
  IPsec profile: profile
  Mode: Manual
  ----------------------------
    Encapsulation mode: transport
    [Inbound AH SA]
      SPI: 1234563 (0x0012d683)
      Connection ID: 64426789452
      Transform set: AH-SHA1
      No duration limit for this SA
    [Outbound AH SA]
      SPI: 1234563 (0x002d683)
      Connection ID: 64428999468
      Transform set: AH-SHA1
      No duration limit for this SA
```

Table 5 Command output

Field	Description
Interface	Interface where the IPsec SA belongs.
IPsec policy	Name of the IPsec policy.
IPsec profile	Name of the IPsec profile.

Field	Description
Sequence number	Sequence number of the IPsec policy entry.
Mode	Negotiation mode used by the IPsec policy: • **Manual**—Manual mode. • **ISAKMP**—IKE negotiation mode. • **Template**—IPsec policy template mode.
Tunnel id	IPsec tunnel ID.
Encapsulation mode	Encapsulation mode, transport or tunnel.
Perfect Forward Secrecy	Perfect Forward Secrecy (PFS) used by the IPsec policy for negotiation: • 768-bit Diffie-Hellman group (**dh-group1**). • 1024-bit Diffie-Hellman group (**dh-group2**). • 1536-bit Diffie-Hellman group (**dh-group5**). • 2048-bit Diffie-Hellman group (**dh-group14**). • 2048-bit and 256_bit subgroup Diffie-Hellman group (**dh-group24**). • 256-bit ECP Diffie-Hellman group (**dh-group19**). • 384-bit ECP Diffie-Hellman group (**dh-group20**).
Extended Sequence Numbers enable	Whether Extended Sequence Number (ESN) is enabled.
Traffic Flow Confidentiality enable	Whether Traffic Flow Confidentiality (TFC) padding is enabled.
Inside VPN	VPN instance to which the protected data flow belongs.
Transmitting entity	Role of the IKE negotiation entity: **Initiator** or **Responder**.
Path MTU	Path MTU of the IPsec SA.
Tunnel	Local and remote addresses of the IPsec tunnel.
local address	Local end IP address of the IPsec tunnel.
remote address	Remote end IP address of the IPsec tunnel.
Flow	Information about the data flow protected by the IPsec tunnel.
sour addr	Source IP address of the data flow.
dest addr	Destination IP address of the data flow.
port	Port number.
protocol	Protocol type of the protected flow.
SPI	SPI of the IPsec SA.
Connection ID	Identifier of the IPsec SA.
Transform set	Security protocol and algorithms used by the IPsec transform set.
SA duration (kilobytes/sec)	IPsec SA lifetime, in Kilobytes or seconds.
SA remaining duration (kilobytes/sec)	Remaining IPsec SA lifetime, in Kilobytes or seconds.

Field	Description
Max received sequence-number	Max sequence number in the received packets.
Max sent sequence-number	Max sequence number in the sent packets.
Anti-replay check enable	Whether anti-replay checking is enabled.
UDP encapsulation used for NAT traversal	Whether NAT traversal is used by the IPsec SA.
Status	Status of the IPsec SA, which can only be **Active**.
No duration limit for this SA	The manual IPsec SAs do not have lifetime.

Related commands

ipsec sa global-duration

reset ipsec sa

display ipsec smart-link policy

Use **display ipsec smart-link policy** to display information about IPsec smart link policies.

Syntax

display ipsec smart-link policy [**brief** | **name** *policy-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

brief: Displays brief information about all IPsec smart link policies.

name *policy-name*: Displays detailed information about a specific IPsec smart link policy. The *policy-name* argument specifies the policy name.

Usage guidelines

If you do not specify any parameters, this command displays detailed information about all IPsec smart link policies.

Examples

Display detailed information about IPsec smart link **smlkpolicy1**.

```
<Sysname> display ipsec smart-link policy name smlkpolicy1
-------------------------------------------------------------------------
Policy name                 :smlkpolicy1
State                       :Enabled
```

```
Probe count                  :10
Probe interval               :1 sec
Probe source IP address      :1.1.1.1
Probe destination IP address :3.3.3.3
Max link switch cycles       :3
IPsec policy name            :ipsecpolicy1
Interface                    :GigabitEthernet1/0/1
IPsec policy sequence number :1
Link ID   Local address   Remote address   Loss(%)   Delay(ms)   State
1         1.1.1.1         3.3.3.3          2         10          Active
2         2.2.2.2         4.4.4.4          0         0           Inactive
------------------------------------------------------------------------------
```

Table 6 Command output

Field	Description
Policy name	Name of the IPsec smart link policy.
State	State of the IPsec smart link selection feature in the policy: **Enabled** or **Disabled**.
Probe count	Number of link quality probe packets sent in each probe cycle.
Probe interval	Probe packet sending interval, in seconds.
Probe source IP address	Source IP address of the probe packets.
Probe destination IP address	Destination IP address of the probe packets.
Max link switch cycles	Maximum number of link switchover cycles.
IPsec policy name	Name of the IPsec policy to which the IPsec smart link policy is applied.
IPsec policy sequence number	Sequence number of the IPsec policy entry.
Link ID	ID of a link configured in the IPsec smart link policy.
Local address	Local IP address of the link.
Remote address	Remote IP address of the link.
Loss(%)	Packet loss ratio calculated during the last link quality probe cycle. If no link quality probe operation has been performed on the link, this field displays two hyphens (**--**).
Delay(ms)	Packet round-trip delay calculated during the last link quality probe cycle. If the calculated delay exceeds 3000 ms or no link quality probe operation has been performed on the link, this field displays two hyphens (**--**).
State	State of the link: **Active** or **Inactive**.

Display brief information about all IPsec smart link policies.

```
<Sysname> display ipsec smart-link policy brief
Name           Active link ID    Loss(%)           Delay(ms)
policy1        1                 0                 10
policy2        2                 --                --
```

Table 7 Command output

Field	Description
Name	Name of an IPsec smart link policy.

Field	Description
Active link ID	ID of the link over which the IPsec tunnel is established.
Loss(%)	Packet loss ratio calculated during the last link quality probe cycle. If no link quality probe operation has been performed on the link, this field displays two hyphens (**--**).
Delay(ms)	Packet round-trip delay calculated during the last link quality probe cycle. If the calculated delay exceeds 3000 ms or no link quality probe operation has been performed on the link, this field displays two hyphens (**--**).

Related commands

ipsec smart-link policy

display ipsec statistics

Use **display ipsec statistics** to display IPsec packet statistics.

Syntax

display ipsec statistics [**tunnel-id** *tunnel-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

tunnel-id *tunnel-id*: Specifies an IPsec tunnel by its ID. The value range for the *tunnel-id* argument is 0 to 4294967294. You can use the **display ipsec tunnel brief** command to view the IDs of established IPsec tunnels.

Usage guidelines

If you do not specify any parameters, this command displays statistics for all IPsec packets.

Examples

Display statistics for all IPsec packets.

```
<Sysname> display ipsec statistics
  IPsec packet statistics:
    Received/sent packets: 47/64
    Received/sent bytes: 3948/5208
    Received/sent packet rate: 5/5 packets/sec
    Received/sent byte rate: 290/290 bytes/sec
    Dropped packets (received/sent): 0/45

    Dropped packets statistics
      No available SA: 0
      Wrong SA: 0
      Invalid length: 0
```

```
      Authentication failure: 0
      Encapsulation failure: 0
      Decapsulation failure: 0
      Replayed packets: 0
      ACL check failure: 45
      MTU check failure: 0
      Loopback limit exceeded: 0
      Crypto speed limit exceeded: 0
```

Display statistics for the packets of IPsec tunnel 1.

```
<Sysname> display ipsec statistics tunnel-id 1
  IPsec packet statistics:
    Received/sent packets: 5124/8231
    Received/sent bytes: 52348/64356
    Received/sent packet rate: 4/4 packets/sec
    Received/sent byte rate: 232/232 bytes/sec
    Dropped packets (received/sent): 0/0

    Dropped packets statistics
      No available SA: 0
      Wrong SA: 0
      Invalid length: 0
      Authentication failure: 0
      Encapsulation failure: 0
      Decapsulation failure: 0
      Replayed packets: 0
      ACL check failure: 0
      MTU check failure: 0
      Loopback limit exceeded: 0
      Crypto speed limit exceeded: 0
```

Table 8 Command output

Field	Description
Received/sent packets	Number of received/sent IPsec-protected packets.
Received/sent bytes	Number of bytes of received/sent IPsec-protected packets.
Received/sent packet rate	Receiving or sending rate (in pps) of IPsec-protected packets.
Received/sent bytes rate	Receiving or sending rate (in Bps) of bytes of IPsec-protected packets.
Dropped packets (received/sent)	Number of dropped IPsec-protected packets (received/sent).
No available SA	Number of packets dropped due to lack of available IPsec SA.
Wrong SA	Number of packets dropped due to wrong IPsec SA.
Invalid length	Number of packets dropped due to invalid packet length.
Authentication failure	Number of packets dropped due to authentication failure.
Encapsulation failure	Number of packets dropped due to encapsulation failure.
Decapsulation failure	Number of packets dropped due to decapsulation failure.
Replayed packets	Number of dropped replayed packets.

Field	Description
ACL check failure	Number of packets dropped due to ACL check failure.
MTU check failure	Number of packets dropped due to MTU check failure.
Loopback limit exceeded	Number of packets dropped due to loopback limit exceeded.
Crypto speed limit exceeded	Number of packets dropped due to crypto speed limit exceeded.

Related commands

reset ipsec statistics

display ipsec transform-set

Use **display ipsec transform-set** to display information about IPsec transform sets.

Syntax

display ipsec transform-set [*transform-set-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

transform-set-name: Specifies an IPsec transform set by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

If you do not specify an IPsec transform set, this command displays information about all IPsec transform sets.

Examples

Display information about all IPsec transform sets.

```
<Sysname> display ipsec transform-set
IPsec transform set: mytransform
  State: incomplete
  Encapsulation mode: tunnel
  ESN: Enabled
  PFS:
  Transform: ESP

IPsec transform set: completeTransform
  State: complete
  Encapsulation mode: transport
  ESN: Enabled
  PFS:
```

```
Transform: AH-ESP
AH protocol:
  Integrity: SHA1
ESP protocol:
  Integrity: SHA1
  Encryption: AES-CBC-128
```

Table 9 Command output

Field	Description
IPsec transform set	Name of the IPsec transform set.
State	Whether the IPsec transform set is complete.
Encapsulation mode	Encapsulation mode used by the IPsec transform set: **transport** or **tunnel**.
ESN	Whether Extended Sequence Number (ESN) is enabled.
PFS	Perfect Forward Secrecy (PFS) used by the IPsec policy for negotiation: • 768-bit Diffie-Hellman group (**dh-group1**). • 1024-bit Diffie-Hellman group (**dh-group2**). • 1536-bit Diffie-Hellman group (**dh-group5**). • 2048-bit Diffie-Hellman group (**dh-group14**). • 2048-bit and 256_bit subgroup Diffie-Hellman group (**dh-group24**). • 256-bit ECP Diffie-Hellman group (**dh-group19**). • 384-bit ECP Diffie-Hellman group (**dh-group20**).
Transform	Security protocols used by the IPsec transform set: AH, ESP, or both. If both protocols are configured, IPsec uses ESP before AH.
AH protocol	AH settings.
ESP protocol	ESP settings.
Integrity	Authentication algorithm used by the security protocol.
Encryption	Encryption algorithm used by the security protocol.

Related commands

ipsec transform-set

display ipsec tunnel

Use **display ipsec tunnel** to display information about IPsec tunnels.

Syntax

display ipsec tunnel { **brief** | **count** | **tunnel-id** *tunnel-id* }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

brief: Displays brief information about all IPsec tunnels.

count: Displays information about the specified number of IPsec tunnels.

tunnel-id *tunnel-id*: Specifies an IPsec tunnel by its ID. The value range for the *tunnel-id* argument is 0 to 4294967294.

Usage guidelines

IPsec is a Layer 3 VPN technology that transmits data in a secure channel established between two endpoints (such as two security gateways). Such a secure channel is usually called an IPsec tunnel.

Examples

Display brief information about all IPsec tunnels.

```
<Sysname> display ipsec tunnel brief
-------------------------------------------------------------------------------
Tunn-id   Src Address     Dst Address     Inbound SPI   Outbound SPI  Status
-------------------------------------------------------------------------------
0         --              --              1000          2000          Active
                                          3000          4000
1         1.2.3.1         2.2.2.2         5000          6000          Active
                                          7000          8000
```

Table 10 Command output

Field	Description
Src Address	Source IP address of the IPsec tunnel. For IPsec SAs created by using IPsec profiles, this field displays two hyphens (**--**).
Dst Address	Destination IP address of the IPsec tunnel. For IPsec SAs created by using IPsec profiles, this field displays two hyphens (**--**).
Inbound SPI	Valid SPI in the inbound direction of the IPsec tunnel. If the tunnel uses two security protocols, two SPIs in the inbound direction are displayed in two lines.
Outbound SPI	Valid SPI in the outbound direction of the IPsec tunnel. If the tunnel uses two security protocols, two SPIs in the outbound direction are displayed in two lines.
Status	Status of the IPsec SA, which can only be **Active**.

Display the number of IPsec tunnels.

```
<Sysname> display ipsec tunnel count
Total IPsec Tunnel Count: 2
```

Display detailed information about all IPsec tunnels.

```
<Sysname> display ipsec tunnel
Tunnel ID: 0
Status: Active
Perfect forward secrecy:
Inside vpn-instance:
SA's SPI:
    outbound:  2000        (0x000007d0)   [AH]
    inbound:   1000        (0x000003e8)   [AH]
    outbound:  4000        (0x00000fa0)   [ESP]
```

```
    inbound:   3000        (0x00000bb8)   [ESP]
Tunnel:
    local  address:
    remote address:
Flow:

Tunnel ID: 1
Status: Active
Perfect forward secrecy:
Inside vpn-instance:
SA's SPI:
    outbound:  6000        (0x00001770)   [AH]
    inbound:   5000        (0x00001388)   [AH]
    outbound:  8000        (0x00001f40)   [ESP]
    inbound:   7000        (0x00001b58)   [ESP]
Tunnel:
    local  address: 1.2.3.1
    remote address: 2.2.2.2
Flow:
    as defined in ACL 3100
```

Display detailed information about IPsec tunnel 1.

```
<Sysname> display ipsec tunnel tunnel-id 1
Tunnel ID: 1
Status: Active
Perfect forward secrecy:
Inside vpn-instance:
SA's SPI:
    outbound:  6000        (0x00001770)   [AH]
    inbound:   5000        (0x00001388)   [AH]
    outbound:  8000        (0x00001f40)   [ESP]
    inbound:   7000        (0x00001b58)   [ESP]
Tunnel:
    local  address: 1.2.3.1
    remote address: 2.2.2.2
Flow:
    as defined in ACL 3100
```

Table 11 Command output

Field	Description
Tunnel ID	IPsec ID, used to uniquely identify an IPsec tunnel.
Status	IPsec tunnel status, which can only be **Active**.
Perfect forward secrecy	Perfect Forward Secrecy (PFS) used by the IPsec policy for negotiation: • 768-bit Diffie-Hellman group (**dh-group1**). • 1024-bit Diffie-Hellman group (**dh-group2**). • 1536-bit Diffie-Hellman group (**dh-group5**). • 2048-bit Diffie-Hellman group (**dh-group14**). • 2048-bit and 256_bit subgroup Diffie-Hellman group (**dh-group24**). • 256-bit ECP Diffie-Hellman group (**dh-group19**).

Field	Description
	• 384-bit ECP Diffie-Hellman group (**dh-group20**).
Inside vpn-instance	Name of the VPN instance to which the IPsec-protected data belongs.
SA's SPI	SPIs of the inbound and outbound SAs.
Tunnel	Local and remote addresses of the IPsec tunnel.
local address	Local end IP address of the IPsec tunnel.
remote address	Remote end IP address of the IPsec tunnel.
Flow	Information about the data flow protected by the IPsec tunnel, including source IP address, destination IP address, source port, destination port, and protocol.
as defined in ACL 3001	Range of data flow protected by the IPsec tunnel that is established manually. This information shows that the IPsec tunnel protects all data flows defined by ACL 3001.

encapsulation-mode

Use **encapsulation-mode** to set the encapsulation mode that the security protocol uses to encapsulate IP packets.

Use **undo encapsulation-mode** to restore the default.

Syntax

encapsulation-mode { **transport** | **tunnel** }

undo encapsulation-mode

Default

IP packets are encapsulated in tunnel mode.

Views

IPsec transform set view

Predefined user roles

network-admin

context-admin

Parameters

transport: Uses the transport mode for IP packet encapsulation.

tunnel: Uses the tunnel mode for IP packet encapsulation.

Usage guidelines

IPsec supports the following encapsulation modes:

- **Transport mode**—The security protocols protect the upper layer data of an IP packet. Only the transport layer data is used to calculate the security protocol headers. The calculated security protocol headers and the encrypted data (only for ESP encapsulation) are placed after the original IP header. You can use the transport mode when end-to-end security protection is required (the secured transmission start and end points are the actual start and end points of the data). The transport mode is typically used for protecting host-to-host communications.
- **Tunnel mode**—The security protocols protect the entire IP packet. The entire IP packet is used to calculate the security protocol headers. The calculated security protocol headers and the encrypted data (only for ESP encapsulation) are encapsulated in a new IP packet. In this mode,

the encapsulated packet has two IP headers. The inner IP header is the original IP header. The outer IP header is added by the network device that provides the IPsec service. You must use the tunnel mode when the secured transmission start and end points are not the actual start and end points of the data packets (for example, when two gateways provide IPsec but the data start and end points are two hosts behind the gateways). The tunnel mode is typically used for protecting gateway-to-gateway communications.

The IPsec transform sets at both ends of the IPsec tunnel must have the same encapsulation mode.

Examples

Configure IPsec transform set **tran1** to use the transport mode for IP packet encapsulation.

```
<Sysname> system-view
[Sysname] ipsec transform-set tran1
[Sysname-ipsec-transform-set-tran1] encapsulation-mode transport
```

Related commands

ipsec transform-set

esn enable

Use **esn enable** to enable the Extended Sequence Number (ESN) feature.

Use **undo esn enable** to disable the ESN feature.

Syntax

esn enable [**both**]

undo esn enable

Default

The ESN feature is disabled.

Views

IPsec transform set view

Predefined user roles

network-admin

context-admin

Parameters

both: Specifies IPsec to support both extended sequence number and traditional sequence number. If you do not specify this keyword, IPsec only supports extended sequence number.

Usage guidelines

The ESN feature applies only to IPsec SAs negotiated by IKEv2.

The ESN feature extends the sequence number length from 32 bits to 64 bits. This feature prevents the sequence number space from being exhausted when large volumes of data are transmitted at high speeds over an IPsec SA. If the sequence number space is not exhausted, the IPsec SA does not need to be renegotiated.

This feature must be enabled at both the initiator and the responder.

Examples

Enable the ESN feature in IPsec transform set **tran1**.

```
<Sysname> system-view
[Sysname] ipsec transform-set tran1
```

```
[Sysname-ipsec-transform-set-tran1] esn enable
```

Related commands

display ipsec transform-set

esp authentication-algorithm

Use **esp authentication-algorithm** to specify authentication algorithms for ESP.

Use **undo esp authentication-algorithm** to restore the default.

Syntax

esp authentication-algorithm { **aes-xcbc-mac** | **md5** | **sha1** | **sha256** | **sha384** | **sha512** | **sm3** } *

undo esp authentication-algorithm

Default

ESP does not use any authentication algorithms.

Views

IPsec transform set view

Predefined user roles

network-admin

context-admin

Parameters

aes-xcbc-mac: Specifies the HMAC-AES-XCBC-96 algorithm, which uses a 128-bit key. This keyword is available only for IKEv2.

md5: Specifies the HMAC-MD5-96 algorithm, which uses a 128-bit key.

sha1: Specifies the HMAC-SHA1-96 algorithm, which uses a 160-bit key.

sha256: Specifies the HMAC-SHA256 algorithm, which uses a 256-bit key.

sha384: Specifies the HMAC-SHA384 algorithm, which uses a 384-bit key.

sha512: Specifies the HMAC-SHA512 algorithm, which uses a 512-bit key.

sm3: Specifies the HMAC-SM3-96 algorithm, which uses a 256-bit key. This keyword is available only for IKEv1.

Usage guidelines

You can specify multiple ESP authentication algorithms for one IPsec transform set, and the algorithm specified earlier has a higher priority.

For a manual or IKEv1-based IPsec policy, the first specified ESP authentication algorithm takes effect. To make sure an IPsec tunnel can be established successfully, the IPsec transform sets specified at both ends of the tunnel must have the same first ESP authentication algorithm.

Examples

Configure IPsec transform set **tran1** to use the HMAC-SHA1 algorithm as the ESP authentication algorithm.

```
<Sysname> system-view
[Sysname] ipsec transform-set tran1
[Sysname-ipsec-transform-set-tran1] esp authentication-algorithm sha1
```

Related commands

ipsec transform-set

esp encryption-algorithm

Use **esp encryption-algorithm** to specify encryption algorithms for ESP.

Use **undo esp encryption-algorithm** to restore the default.

Syntax

esp encryption-algorithm { **3des-cbc** | **aes-cbc-128** | **aes-cbc-192** | **aes-cbc-256** | **aes-ctr-128** | **aes-ctr-192** | **aes-ctr-256** | **camellia-cbc-128** | **camellia-cbc-192** | **camellia-cbc-256** | **des-cbc** | **gmac-128** | **gmac-192** | **gmac-256** | **gcm-128** | **gcm-192** | **gcm-256** | **null** | **sm1-cbc-128** | **sm4-cbc** } *

undo esp encryption-algorithm

Default

ESP does not use any encryption algorithms.

Views

IPsec transform set view

Predefined user roles

network-admin

context-admin

Parameters

3des-cbc: Specifies the 3DES algorithm in CBC mode, which uses a 168-bit key.

aes-cbc-128: Specifies the AES algorithm in CBC mode, which uses a 128-bit key.

aes-cbc-192: Specifies the AES algorithm in CBC mode, which uses a 192-bit key.

aes-cbc-256: Specifies the AES algorithm in CBC mode, which uses a 256-bit key.

aes-ctr-128: Specifies the AES algorithm in CTR mode, which uses a 128-bit key. This keyword is available only for IKEv2.

aes-ctr-192: Specifies the AES algorithm in CTR mode, which uses a 192-bit key. This keyword is available only for IKEv2.

aes-ctr-256: Specifies the AES algorithm in CTR mode, which uses a 256-bit key. This keyword is available only for IKEv2.

camellia-cbc-128: Specifies the Camellia algorithm in CBC mode, which uses a 128-bit key. This keyword is available only for IKEv2.

camellia-cbc-192: Specifies the Camellia algorithm in CBC mode, which uses a 192-bit key. This keyword is available only for IKEv2.

camellia-cbc-256: Specifies the Camellia algorithm in CBC mode, which uses a 256-bit key. This keyword is available only for IKEv2.

des-cbc: Specifies the DES algorithm in CBC mode, which uses a 64-bit key.

gmac-128: Specifies the GMAC algorithm, which uses a 128-bit key. This keyword is available only for IKEv2.

gmac-192: Specifies the GMAC algorithm, which uses a 192-bit key. This keyword is available only for IKEv2.

gmac-256: Specifies the GMAC algorithm, which uses a 256-bit key. This keyword is available only for IKEv2.

gcm-128: Specifies the GCM algorithm, which uses a 128-bit key. This keyword is available only for IKEv2.

gcm-192: Specifies the GCM algorithm, which uses a 192-bit key. This keyword is available only for IKEv2.

gcm-256: Specifies the GCM algorithm, which uses a 256-bit key. This keyword is available only for IKEv2.

null: Specifies the NULL algorithm, which means encryption is not performed.

sm1-cbc-128: Specifies the SM1 algorithm in CBC mode, which uses a 128-bit key. This keyword is available only for IKEv1.

sm4-cbc: Uses the SM4 algorithm in CBC mode, which uses a 128-bit key. This keyword is available only for IKEv1.

Usage guidelines

You can specify multiple ESP encryption algorithms for one IPsec transform set, and the algorithm specified earlier has a higher priority.

For a manual or IKEv1-based IPsec policy, the first specified ESP encryption algorithm takes effect. To make sure an IPsec tunnel can be established successfully, the IPsec transform sets specified at both ends of the tunnel must have the same first ESP encryption algorithm.

GCM and GMAC algorithms are combined mode algorithms. GCM algorithms provide encryption and authentication services. GMAC algorithms only provide authentication service. Combined mode algorithms can be used only when ESP is used alone without AH. Combined mode algorithms cannot be used together with ordinary ESP authentication algorithms.

Examples

Configure IPsec transform set **tran1** to use the AES-CBC-128 algorithm as the ESP encryption algorithm.

```
<Sysname> system-view
[Sysname] ipsec transform-set tran1
[Sysname-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128
```

Related commands

ipsec transform-set

gateway

Use **gateway** to specify the gateway address for an interface that uses a manually configured IP address.

Use **undo gateway** to delete the gateway address together with the default route that uses the gateway address as the next hop address.

Syntax

gateway *gateway-address* [**no-route**]

undo gateway

Default

An interface that uses a manually configured IP address does not have a gateway address.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

gateway-address: Specifies the gateway IP address in dotted decimal notation.

no-route: Disables generation of a default route with the gateway address as the next hop address. If you do not specify this keyword, a default route with the gateway address as the next hop address will be generated.

Usage guidelines

You must configure the gateway address for an interface that uses a manually configured IP address if the following conditions are met:

- The interface is configured as the local interface of a link in an IPsec smart link policy (by using the **link** command).
- The **nexthop** *nexthop-address* option is not specified in the **link** command.

The **gateway** command does not take effect if the interface acquires its IP address through DHCP or PPPoE. Such interfaces always use the gateway address assigned by the DHCP or PPPoE server.

The automatically generated default route (which uses the gateway address as the next hop address) cannot be deleted by using the **undo ip route-static** command.

Examples

Specify 10.1.1.254 as the gateway address for GigabitEthernet 1/0/1, and disable generation of a default route that uses the gateway address as the next hop address.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] gateway 10.1.1.254 no-route
```

Related commands

link

ike-profile

Use **ike-profile** to specify an IKE profile for an IPsec policy, IPsec profile, or IPsec policy template.

Use **undo ike-profile** to restore the default.

Syntax

ike-profile *profile-name*

undo ike-profile

Default

No IKE profile is specified.

Views

IPsec policy view

IPsec policy template view

IPsec profile view

Predefined user roles

network-admin

context-admin

Parameters

profile-name: Specifies an IKE profile by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

If no IKE profile is specified for an IPsec policy, IPsec profile, or IPsec policy template, the device selects an IKE profile configured in system view for negotiation. If no IKE profile is configured in system view, the device uses the global IKE settings.

The IKE profile specified for an IPsec policy, IPsec profile, or IPsec policy template defines the parameters used for IKE negotiation.

You can specify only one IKE profile for an IPsec policy, IPsec profile, or IPsec policy template.

Examples

Specify IKE profile **profile1** for IPsec policy **policy1**.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 10 isakmp
[Sysname-ipsec-policy-isakmp-policy1-10] ike-profile profile1
```

Related commands

ike profile

ikev2-profile

Use **ikev2-profile** to specify an IKEv2 profile for an IPsec policy, IPsec profile, or IPsec policy template.

Use **undo ikev2-profile** to restore the default.

Syntax

ikev2-profile *profile-name*

undo ikev2-profile

Default

No IKEv2 profile is specified.

Views

IPsec policy view

IPsec policy template view

IPsec profile view

Predefined user roles

network-admin

context-admin

Parameters

profile-name: Specifies an IKEv2 profile by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

The IKEv2 profile specified for an IPsec policy, IPsec profile, or IPsec policy template defines the parameters used for IKEv2 negotiation.

You can specify only one IKEv2 profile for an IPsec policy, IPsec profile, or IPsec policy template. On the initiator, an IKEv2 profile is required. On the responder, an IKEv2 profile is optional. If you do not specify an IKEv2 profile, the responder can use any IKEv2 profile for negotiation.

Examples

Specify IKEv2 profile **profile1** for IPsec policy **policy1**.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 10 isakmp
[Sysname-ipsec-policy-isakmp-policy1-10] ikev2-profile profile1
```

Related commands

display ipsec ipv6-policy

display ipsec policy

ikev2 profile

ipsec { ipv6-policy | policy }

Use **ipsec** { **ipv6-policy** | **policy** } to create an IPsec policy entry and enter its view, or enter the view of an existing IPsec policy entry.

Use **undo ipsec** { **ipv6-policy** | **policy** } to delete an IPsec policy.

Syntax

ipsec { **ipv6-policy** | **policy** } *policy-name seq-number* [**isakmp** | **manual**]

undo ipsec { **ipv6-policy** | **policy** } *policy-name* [*seq-number*]

Default

No IPsec policies exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-policy: Specifies an IPv6 IPsec policy.

policy: Specifies an IPv4 IPsec policy.

policy-name: Specifies a name for the IPsec policy, a case-insensitive string of 1 to 63 characters.

seq-number: Specifies a sequence number for the IPsec policy entry, in the range of 1 to 65535.

isakmp: Establishes IPsec SAs through IKE negotiation.

manual: Establishes IPsec SAs manually.

Usage guidelines

When you create an IPsec policy, you must specify the SA setup mode (**isakmp** or **manual**). When you enter the view of an existing IPsec policy, you do not need to specify the SA setup mode.

You cannot change the SA setup mode of an existing IPsec policy.

An IPsec policy is a set of IPsec policy entries that have the same name but different sequence numbers. In the same IPsec policy, an IPsec policy entry with a smaller sequence number has a higher priority.

If you specify the *seq-number* argument, the **undo** command deletes the specified IPsec policy entry. If you do not specify this argument, the **undo** command deletes the specified IPsec policy.

An IPv4 IPsec policy and IPv6 IPsec policy can have the same name.

Examples

Create an IKE-based IPsec policy entry and enter the IPsec policy view. The policy name is **policy1** and the sequence number is 100.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 isakmp
[Sysname-ipsec-policy-isakmp-policy1-100]
```

Create a manual IPsec policy entry and enter the IPsec policy view. The policy name is **policy1** and the sequence number is 101.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 101 manual
[Sysname-ipsec-policy-manual-policy1-101]
```

Related commands

display ipsec { **ipv6-policy** | **policy** }

ipsec apply

ipsec { ipv6-policy | policy } template

Use **ipsec** { **ipv6-policy** | **policy** } **template** to create an IPsec policy entry by using an IPsec policy template.

Use **undo ipsec** { **ipv6-policy** | **policy** } to delete an IPsec policy.

Syntax

ipsec { **ipv6-policy** | **policy** } *policy-name seq-number* **isakmp template** *template-name*

undo ipsec { **ipv6-policy** | **policy** } *policy-name* [*seq-number*]

Default

No IPsec policies exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-policy: Specifies an IPv6 IPsec policy.

policy: Specifies an IPv4 IPsec policy.

policy-name: Specifies a name for the IPsec policy, a case-insensitive string of 1 to 63 characters.

seq-number: Specifies a sequence number for the IPsec policy entry, in the range of 1 to 65535. A smaller number indicates a higher priority.

isakmp: Specifies the IKE mode for the IPsec policy entry.

template *template-name*: Specifies the IPsec policy template to be used to create the IPsec policy entry. The template name is a case-insensitive string of 1 to 63 characters.

Usage guidelines

If you specify the *seq-number* argument, the **undo** command deletes the specified IPsec policy entry. If you do not specify this argument, the **undo** command deletes the specified IPsec policy.

An interface applied with an IPsec policy that is configured by using an IPsec policy template cannot initiate an SA negotiation, but it can respond to a negotiation request. The parameters not defined in the template are determined by the initiator. When the remote end's information (such as the IP address) is unknown, this method allows the remote end to initiate negotiations with the local end.

Examples

Create an IKE-based IPsec policy entry by using IPsec policy template **temp1**, and specify the IPsec policy name as **policy2** and the sequence number as 200.

```
<Sysname> system-view
[Sysname] ipsec policy policy2 200 isakmp template temp1
```

Related commands

display ipsec { **ipv6-policy** | **policy** }

ipsec { **ipv6-policy-template** | **policy-template** }

ipsec { ipv6-policy | policy } local-address

Use **ipsec** { **ipv6-policy** | **policy** } **local-address** to bind an IPsec policy to a source interface.

Use **undo ipsec** { **ipv6-policy** | **policy** } **local-address** to remove the binding between an IPsec policy and a source interface.

Syntax

ipsec { **ipv6-policy** | **policy** } *policy-name* **local-address** *interface-type interface-number*

undo ipsec { **ipv6-policy** | **policy** } *policy-name* **local-address**

Default

No IPsec policy is bound to a source interface.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-policy: Specifies an IPv6 IPsec policy.

policy: Specifies an IPv4 IPsec policy.

policy-name: Specifies an IPsec policy name, a case-insensitive string of 1 to 63 characters.

local-address *interface-type interface-number*: Specifies the shared source interface by its type and number.

Usage guidelines

For high availability, two interfaces can operate in backup mode. After an IPsec policy is applied to the two interfaces, they negotiate with their peers to establish IPsec SAs separately. When one interface fails and a link failover occurs, the other interface needs to take some time to renegotiate SAs, resulting in service interruption.

To solve these problems, bind a source interface to an IPsec policy and apply the policy to both interfaces. This enables the two physical interfaces to use the same source interface to negotiate IPsec SAs. As long as the source interface is up, the negotiated IPsec SAs will not be removed and will keep working, regardless of link failover.

After an IPsec policy is applied to a service interface and IPsec SAs have been established, if you bind the IPsec policy to a source interface, the existing IPsec SAs are deleted.

Only an IKE-based IPsec policy can be bound to a source interface.

An IPsec policy can be bound to only one source interface. If you execute this command multiple times, the most recent configuration takes effect.

A source interface can be bound to multiple IPsec policies.

As a best practice, use a stable interface, such as a Loopback interface, as a source interface.

Examples

Bind IPsec policy **map** to source interface Loopback 11.

```
<Sysname> system-view
[Sysname] ipsec policy map local-address loopback 11
```

Related commands

ipsec { **ipv6-policy** | **policy** }

ipsec { ipv6-policy-template | policy-template }

Use **ipsec** { **ipv6-policy-template** | **policy-template** } to create an IPsec policy template entry and enter its view, or enter the view of an existing IPsec policy template entry.

Use **undo ipsec** { **ipv6-policy-template** | **policy-template** } to delete an IPsec policy template.

Syntax

ipsec { **ipv6-policy-template** | **policy-template** } *template-name seq-number*

undo ipsec { **ipv6-policy-template** | **policy-template** } *template-name* [*seq-number*]

Default

No IPsec policy templates exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-policy-template: Specifies an IPv6 IPsec policy template.

policy-template: Specifies an IPv4 IPsec policy template.

template-name: Specifies a name for the IPsec policy template, a case-insensitive string of 1 to 63 characters.

seq-number: Specifies a sequence number for the IPsec policy template entry, in the range of 1 to 65535. A smaller number indicates a higher priority.

Usage guidelines

The configurable parameters for an IPsec policy template are similar to the parameters that you use when you configure an IKE-based IPsec policy. However, all parameters except for the IPsec transform sets and the IKE peer are optional for an IPsec policy template.

An IPsec policy template is a set of IPsec policy template entries that have the same name but different sequence numbers.

With the *seq-number* argument specified, the **undo** command deletes an IPsec policy template entry.

An IPv4 IPsec policy template and an IPv6 IPsec policy template can have the same name.

Examples

Create an IPsec policy template entry and enter the IPsec policy template view. The template name is **template1** and the sequence number is 100.

```
<Sysname> system-view
[Sysname] ipsec policy-template template1 100
[Sysname-ipsec-policy-template-template1-100]
```

Related commands

display ipsec { **ipv6-policy-template** | **policy-template** }

ipsec { **ipv6-policy** | **policy** }

ipsec { **ipv6-policy** | **policy** } **isakmp template**

ipsec anti-replay check

Use **ipsec anti-replay check** to enable IPsec anti-replay checking.

Use **undo ipsec anti-replay check** to disable IPsec anti-replay checking.

Syntax

ipsec anti-replay check

undo ipsec anti-replay check

Default

IPsec anti-replay checking is enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

IPsec packet de-encapsulation involves complicated calculation. De-encapsulation of replayed packets is not necessary but consumes large amounts of resources and degrades performance, resulting in DoS. IPsec anti-replay checking, when enabled, is performed before the de-encapsulation process, reducing resource waste.

In some situations, service data packets are received in a different order than their original order. The IPsec anti-replay feature drops them as replayed packets, which impacts communications. If this happens, disable IPsec anti-replay checking or adjust the size of the anti-replay window as required.

Only IPsec SAs negotiated by IKE support anti-replay checking. Manually created IPsec SAs do not support anti-replay checking. Enabling or disabling IPsec anti-replay checking does not affect manually created IPsec SAs.

Examples

Enable IPsec anti-replay checking.

```
<Sysname> system-view
[Sysname] ipsec anti-replay check
```

Related commands

ipsec anti-replay window

ipsec anti-replay window

Use **ipsec anti-replay window** to set the anti-replay window size.

Use **undo ipsec anti-replay window** to restore the default.

Syntax

ipsec anti-replay window *width*

undo ipsec anti-replay window

Default

The anti-replay window size is 64.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

width: Specifies the size for the anti-replay window. It can be 64, 128, 256, 512, or 1024 packets.

Usage guidelines

Service data packets might be received in a very different order than their original order, and the IPsec anti-replay feature might drop them as replayed packets, affecting normal communications. If this happens, disable IPsec anti-replay checking or adjust the size of the anti-replay window as required.

Changing the anti-replay window size affects only the IPsec SAs negotiated later.

Examples

Set the size of the anti-replay window to 128.

```
<Sysname> system-view
```

```
[Sysname] ipsec anti-replay window 128
```

Related commands

ipsec anti-replay check

ipsec apply

Use **ipsec apply** to apply an IPsec policy to an interface.

Use **undo ipsec apply** to remove an IPsec policy application from an interface.

Syntax

ipsec apply { **ipv6-policy** | **policy** } *policy-name*

undo ipsec apply { **ipv6-policy** | **policy** }

Default

No IPsec policy is applied to an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-policy: Specifies an IPv6 IPsec policy.

policy: Specifies an IPv4 IPsec policy.

policy-name: Specifies an IPsec policy name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

On an interface, you can apply a maximum of two IPsec policies: one IPv4 IPsec policy and one IPv6 IPsec policy.

An IKE-based IPsec policy that is bound to a source interface can be applied to multiple interfaces. A manual IPsec policy can be applied to only one interface.

Examples

Apply IPsec policy **policy1** to GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipsec apply policy policy1
```

Related commands

display ipsec { **ipv6-policy** | **policy** }

ipsec { **ipv6-policy** | **policy** }

ipsec decrypt-check enable

Use **ipsec decrypt-check enable** to enable ACL checking for de-encapsulated IPsec packets.

Use **undo ipsec decrypt-check** to disable ACL checking for de-encapsulated IPsec packets.

Syntax

ipsec decrypt-check enable

undo ipsec decrypt-check enable

Default

ACL checking for de-encapsulated IPsec packets is enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

In tunnel mode, the IP packet encapsulated in an inbound IPsec packet might not be under the protection of the ACL specified in the IPsec policy. After being de-encapsulated, such packets bring threats to the network security. In this scenario, you can enable ACL checking for de-encapsulated IPsec packets. All packets failing the checking are discarded, improving the network security.

Examples

Enable ACL checking for de-encapsulated IPsec packets.

```
<Sysname> system-view
[Sysname] ipsec decrypt-check enable
```

ipsec df-bit

Use **ipsec df-bit** to configure the DF bit for the outer IP header of IPsec packets on an interface.

Use **undo ipsec df-bit** to restore the default.

Syntax

ipsec df-bit { **clear** | **copy** | **set** }

undo ipsec df-bit

Default

The DF bit is not configured for the outer IP header of IPsec packets on an interface. The global DF bit setting is used.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

clear: Clears the DF bit in the outer IP header. IPsec packets can be fragmented.

copy: Copies the DF bit setting of the original IP header to the outer IP header.

set: Sets the DF bit in the outer IP header. IPsec packets cannot be fragmented.

Usage guidelines

This command is effective only when the IPsec encapsulation mode is tunnel mode. It is not effective in transport mode because the outer IP header is not added in transport mode.

This command does not change the DF bit for the original IP header of IPsec packets.

If multiple interfaces use an IPsec policy that is bound to a source interface, you must use the same DF bit setting on these interfaces.

Packet fragmentation and reassembly might cause packet forwarding to be delayed. You can set the DF bit to avoid the forwarding delay. However, to prevent the IPsec packets from being discarded, you must make sure the path MTU is larger than the IPsec packet size. As a best practice, clear the DF bit if you cannot make sure the path MTU is larger than the IPsec packet size.

Examples

Set the DF bit in the outer IP header of IPsec packets on GigabitEthernet 1/0/2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] ipsec df-bit set
```

Related commands

ipsec global-df-bit

ipsec flow-overlap check enable

Use **ipsec flow-overlap check enable** to enable IPsec flow overlap check.

Use **undo ipsec flow-overlap check enable** to disable IPsec flow overlap check.

Syntax

ipsec flow-overlap check enable

undo ipsec flow-overlap check enable

Default

IPsec flow overlap check is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

In a hub-spoke network, the hub typically uses an IPsec policy template to negotiate IPsec SAs with spokes. The data flows to be protected by the IPsec SAs might overlap with each other. To avoid IPsec flow overlapping, you can enable IPsec flow overlap check on the hub device. When negotiating an IPsec SA for a data flow, the device checks whether the data flow overlaps with an existing protected data flow. If yes, the new IPsec SA negotiation fails and the device generates an IPsec flow overlap notification. On receiving such notifications, you must reconfigure the ACL settings for IPsec on the spoke devices.

This feature checks the destination IP address of a data flow to be protected with the destination IP addresses of the existing protected data flows. If an overlap exists, the feature determines that the data flow overlaps.

The following applies to the IPsec flow overlap check feature:

- As a best practice, enable this feature on the hub device of a hub-spoke network.
- This feature takes effect only on IPsec SAs negotiated by using IPsec policy templates.
- This feature takes effect only for new IPsec SA negotiations. It does not take effect on existing IPsec SAs.
- This feature takes effect only on IPsec SAs negotiated on the same interface and in the same VPN instance.
- This feature does not take effect on renegotiated IPsec SAs.
- This feature does not check overlaps for source IP addresses of data flows.
- This feature impacts device performance, enable this feature only when necessary (for example, for network upgrade or expansion) and disable it in time.

Examples

Enable IPsec flow overlap check.

```
<Sysname> system-view
[Sysname] ipsec flow-overlap check enable
```

ipsec fragmentation

Use **ipsec fragmentation** to configure the IPsec fragmentation feature.

Use **undo ipsec fragmentation** to restore the default.

Syntax

ipsec fragmentation { **after-encryption** | **before-encryption** }

undo ipsec fragmentation

Default

The device fragments packets before IPsec encapsulation.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

after-encryption: Fragments packets after IPsec encapsulation.

before-encryption: Fragments packets before IPsec encapsulation.

Usage guidelines

If you configure the device to fragment packets before IPsec encapsulation, the device predetermines the encapsulated packet size before the actual encapsulation. If the encapsulated packet size exceeds the MTU of the output interface and the DF bit is not set, the device fragments the packet before encapsulation. If the packet's DF bit is set, the device drops the packet and sends an ICMP error message.

If you configure the device to fragment packets after IPsec encapsulation, the device directly encapsulates the packets and fragments the encapsulated packets in subsequent service modules.

Examples

Configure the device to fragment packets after IPsec encapsulation.

```
<Sysname>system-view
```

```
[Sysname] ipsec fragmentation after-encryption
```

ipsec global-df-bit

Use **ipsec global-df-bit** to configure the DF bit for the outer IP header of IPsec packets on all interfaces.

Use **undo ipsec global-df-bit** to restore the default.

Syntax

ipsec global-df-bit { **clear** | **copy** | **set** }

undo ipsec global-df-bit

Default

The DF bit setting of the original IP header is copied to the outer IP header for IPsec packets.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

clear: Clears the DF bit in the outer IP header. IPsec packets can be fragmented.

copy: Copies the DF bit setting of the original IP header to the outer IP header.

set: Sets the DF bit in the outer IP header. IPsec packets cannot be fragmented.

Usage guidelines

This command is effective only when the IPsec encapsulation mode is tunnel mode. It is not effective in transport mode because the outer IP header is not added in transport mode.

This command does not change the DF bit for the original IP header of IPsec packets.

Packet fragmentation and reassembly might cause packet forwarding to be delayed. You can set the DF bit to avoid the forwarding delay. However, to prevent IPsec packets from being discarded, you must make sure the path MTU is larger than the IPsec packet size. As a best practice, clear the DF bit if you cannot make sure the path MTU is larger than the IPsec packet size.

Examples

Set the DF bit in the outer IP header of IPsec packets on all interfaces.

```
<Sysname> system-view
[Sysname] ipsec global-df-bit set
```

Related commands

ipsec df-bit

ipsec limit max-tunnel

Use **ipsec limit max-tunnel** to set the maximum number of IPsec tunnels.

Use **undo ipsec limit max-tunnel** to restore the default.

Syntax

ipsec limit max-tunnel *tunnel-limit*

undo ipsec limit max-tunnel

Default

The number of IPsec tunnels is not limited.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

tunnel-limit: Specifies the maximum number of IPsec tunnels, in the range of 1 to 4294967295.

Usage guidelines

To maximize concurrent performance of IPsec when memory is sufficient, increase the maximum number of IPsec tunnels. To ensure service availability when memory is insufficient, decrease the maximum number of IPsec tunnels.

Examples

Set the maximum number of IPsec tunnels to 5000.

```
<Sysname> system-view
[Sysname] ipsec limit max-tunnel 5000
```

Related commands

ike limit

ipsec logging negotiation enable

Use **ipsec logging negotiation enable** to enable logging for IPsec negotiation.

Use **undo ipsec logging negotiation packet enable** to disable logging for IPsec negotiation.

Syntax

ipsec logging negotiation enable

undo ipsec logging negotiation enable

Default

Logging for IPsec negotiation is enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command enables the device to output logs for the IPsec negotiation process.

Examples

Enable logging for IPsec negotiation.

```
<Sysname> system-view
```

```
[Sysname] ipsec logging negotiation enable
```

ipsec logging packet enable

Use **ipsec logging packet enable** to enable logging for IPsec packets.

Use **undo ipsec logging packet enable** to disable logging for IPsec packets.

Syntax

ipsec logging packet enable

undo ipsec logging packet enable

Default

Logging for IPsec packets is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

After logging for IPsec packets is enabled, the device outputs a log when an IPsec packet is discarded. IPsec packets might be discarded due to lack of inbound SA, AH/ESP authentication failure, or ESP encryption failure. A log contains the source and destination IP addresses, SPI, and sequence number of the packet, and the reason it was discarded.

Examples

Enable logging for IPsec packets.

```
<Sysname> system-view
[Sysname] ipsec logging packet enable
```

ipsec netmask-filter

Use **ipsec netmask-filter** to configure IPsec netmask filtering.

Use **undo ipsec netmask-filter** to restore the default.

Syntax

ipsec netmask-filter { **destination-mask** *mask-length* | **source-mask** *mask-length* } *

undo ipsec netmask-filter [**destination-mask** | **source-mask**]

Default

IPsec netmask filtering is not configured.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

destination-mask *mask-length*: Specifies the minimum mask length for IPv4 flow destination addresses, in the range of the 1 to 32.

source-mask *mask-length*: Specifies the minimum mask length for IPv4 flow source IP addresses, in the range of the 1 to 32.

Usage guidelines

This feature is supported only on IPv4 networks.

This feature takes effect only IPsec SAs negotiated by using IPsec policy templates.

As a best practice, configure this feature on the hub device of a hub-spoke network.

On a hub-spoke network, if the IPsec data flow range configured on a spoke is too large, traffic of other spokes might be directed to that spoke incorrectly. To avoid incorrect packet forwarding, you can enable IPsec netmask filtering on the hub device. When negotiating an IPsec SA for a data flow, the device checks the mask lengths of the data flow. The IPsec SA negotiation proceeds only if the mask lengths of the source and destination IP addresses of the data flow are greater than or equal to those configured by IPsec netmask filtering. If the data flow fails to pass the netmask filtering, the IPsec SA negotiation fails and the device generates a corresponding SA negotiation failure notification. On receiving such notifications, you must reconfigure the ACL settings for IPsec on the spoke devices.

If you execute this command multiple times, the most recent configuration takes effect.

If you do not specify any parameters, the **undo ipsec netmask-filter** command disables both the destination and source netmask filtering features.

Examples

Configure IPsec netmask filtering: set the source IP mask length to 24 and destination IP mask length to 24.

```
<Sysname> system-view
[Sysname] ipsec netmask-filter source-mask 24 destination-mask 24
```

ipsec profile

Use **ipsec profile** to create an IPsec profile and enter its view, or enter the view of an existing IPsec profile.

Use **undo ipsec profile** to delete an IPsec profile.

Syntax

ipsec profile *profile-name* [**manual** | **isakmp**]

undo ipsec profile *profile-name*

Default

No IPsec profiles exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

profile-name: Specifies a name for the IPsec profile, a case-insensitive string of 1 to 63 characters.

manual: Specifies the IPsec SA setup mode as manual.

isakmp: Specifies the IPsec SA setup mode as IKE.

Usage guidelines

When you create an IPsec profile, you must specify the IPsec SA setup mode (**manual** or **isakmp**). When you enter the view of an existing IPsec profile, you do not need to specify the IPsec SA setup mode.

A manual IPsec profile is similar to a manual IPsec policy. It is used exclusively for IPsec protection for application protocols, including OSPFv3, IPv6 BGP, and RIPng.

An IKE-based IPsec profile is similar to an IKE-based IPsec policy. It uses IKE negotiation to establish IPsec SAs to protect IPv4 and IPv6 application protocols, such as ADVPN. An IKE-based IPsec profile does not require you to specify the remote end address or an ACL.

Examples

Create a manual IPsec profile named **profile1**.

```
<Sysname> system-view
[Sysname] ipsec profile profile1 manual
[Sysname-ipsec-profile-manual-profile1]
```

Create an IKE-based IPsec profile named **profile1**.

```
<Sysname> system-view
[Sysname] ipsec profile profile1 isakmp
[Sysname-ipsec-profile-isakmp-profile1]
```

Related commands

display ipsec profile

ipsec redundancy enable

Use **ipsec redundancy enable** to enable IPsec redundancy.

Use **undo ipsec redundancy enable** to disable IPsec redundancy.

Syntax

ipsec redundancy enable

undo ipsec redundancy enable

Default

IPsec redundancy is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

With IPsec redundancy enabled, the system synchronizes the following information from the active device to the standby device at configurable intervals:

- Lower bound values of the IPsec anti-replay window for inbound packets.
- IPsec anti-replay sequence numbers for outbound packets.

The synchronization ensures uninterrupted IPsec traffic forwarding and anti-replay protection when the active device fails.

To configure synchronization intervals, use the **redundancy replay-interval** command.

Examples

Enable IPsec redundancy.

```
<Sysname> system-view
[Sysname] ipsec redundancy enable
```

Related commands

redundancy replay-interval

ipsec sa global-duration

Use **ipsec sa global-duration** to configure the global IPsec SA lifetime.

Use **undo ipsec sa global-duration** to restore the default.

Syntax

ipsec sa global-duration { **time-based** *seconds* | **traffic-based** *kilobytes* }

undo ipsec sa global-duration { **time-based** | **traffic-based** }

Default

The time-based global IPsec SA lifetime is 3600 seconds, and the traffic-based global lifetime is 1843200 Kilobytes.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

time-based *seconds*: Specifies the time-based global lifetime for IPsec SAs, in the range of 180 to 604800 seconds.

traffic-based *kilobytes*: Specifies the traffic-based global lifetime for IPsec SAs, in the range of 2560 to 4294967295 Kilobytes. When traffic on an SA reaches this value, the SA expires.

Usage guidelines

You can also configure IPsec SA lifetimes in IPsec policy view or IPsec policy template view. The device prefers the IPsec SA lifetimes configured in IPsec policy view or IPsec policy template view over the global IPsec SA lifetimes.

When IKE negotiates IPsec SAs, it uses the local lifetime settings or those proposed by the peer, whichever are smaller.

An IPsec SA can have both a time-based lifetime and a traffic-based lifetime. The IPsec SA expires when either lifetime expires. Before the IPsec SA expires, IKE negotiates a new IPsec SA, which takes over immediately after its creation.

Examples

Configure the global IPsec SA lifetime as 7200 seconds.

```
<Sysname> system-view
[Sysname] ipsec sa global-duration time-based 7200
```

Configure the global IPsec SA lifetime as 10240 Kilobytes.

```
[Sysname] ipsec sa global-duration traffic-based 10240
```

Related commands

display ipsec sa

sa duration

ipsec sa global-soft-duration buffer

Use **ipsec sa global-soft-duration buffer** to set the global time-based or traffic-based IPsec SA soft lifetime buffer.

Use **undo ipsec sa global-soft-duration buffer** to restore the default.

Syntax

ipsec sa global-soft-duration buffer { **time-based** *seconds* | **traffic-based** *kilobytes* }

undo ipsec sa global-soft-duration buffer { **time-based** | **traffic-based** }

Default

The global time-based and traffic-based IPsec SA soft lifetime buffers are not configured.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

time-based *seconds*: Specifies the time-based IPsec SA soft lifetime buffer, in seconds. The value range is 20 to 201600.

traffic-based *kilobytes*: Specifies the traffic-based IPsec SA soft lifetime buffer, in Kilobytes. The value range is 1000 to 4294901760.

Usage guidelines

This command takes effect only when IKEv1 is used.

The IPsec SA soft lifetime buffers are used to determine the IPsec SA soft lifetimes.

If no IPsec SA soft lifetime buffers are configured, the system calculates a default time-based and a default traffic-based IPsec SA soft lifetime.

If IPsec SA soft lifetime buffers are configured, the system calculates IPsec SA soft lifetimes as follows:

- Time-based IPsec SA soft lifetime = time-based IPsec SA lifetime – time-based IPsec SA soft lifetime buffer.

  If the calculated time-based IPsec SA soft lifetime is shorter than or equal to 20 seconds, the system uses the default time-based IPsec SA soft lifetime.
- Traffic-based IPsec SA soft lifetime = traffic-based IPsec SA lifetime – traffic-based IPsec SA soft lifetime buffer.

If the calculated traffic-based IPsec SA soft lifetime is smaller than or equal to 1000 Kilobytes, the system uses the default traffic-based IPsec SA soft lifetime.

You can also configure IPsec SA soft lifetime buffers in IPsec policy view or IPsec profile view. The device prefers the IPsec SA lifetime buffers configured in IPsec policy view or IPsec profile view over the global lifetime buffers configured in system view.

Examples

Set the global time-based IPsec SA soft lifetime buffer to 600 seconds.

```
<Sysname> system-view
[Sysname] ipsec sa global-soft-duration buffer time-based 600
```

Set the global traffic-based IPsec SA soft lifetime buffer to 10000 Kilobytes.

```
<Sysname> system-view
[Sysname] ipsec sa global-soft-duration buffer traffic-based 10000
```

Related commands

sa soft-duration buffer

ipsec sa idle-time

Use **ipsec sa idle-time** to enable the global IPsec SA idle timeout feature and set the idle timeout.

Use **undo ipsec sa idle-time** to disable the global IPsec SA idle timeout feature.

Syntax

ipsec sa idle-time *seconds*

undo ipsec sa idle-time

Default

The global IPsec SA idle timeout feature is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies the IPsec SA idle timeout in the range of 60 to 86400 seconds.

Usage guidelines

This feature applies only to IPsec SAs negotiated by IKE.

The IPsec SA idle timer starts when an IPsec SA is created. If no traffic matches the IPsec SA within the idle timeout interval, the IPsec SA is deleted.

The IPsec SA idle timeout can also be configured in IPsec policy view, IPsec profile view, or IPsec policy template view, which takes precedence over the global IPsec SA timeout.

Examples

Enable the global IPsec SA idle timeout feature and set the IPsec SA idle timeout to 600 seconds.

```
<Sysname> system-view
[Sysname] ipsec sa idle-time 600
```

Related commands

display ipsec sa

sa idle-time

ipsec smart-link policy

Use **ipsec smart-link policy** to create an IPsec smart link policy and enter its view, or enter the view of an existing IPsec smart link policy.

Use **undo ipsec smart-link policy** to delete an IPsec smart link policy.

Syntax

ipsec smart-link policy *policy-name*

undo ipsec smart-link policy *policy-name*

Default

No IPsec smart link policies exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies a name for the IPsec smart link policy. The policy name is a case-insensitive string of 1 to 63 characters and can contain only letters, digits, hyphens (-), and underscores (_).

Usage guidelines

An IPsec smart link policy defines the link quality probe parameters, link switchover thresholds, and links for smart link selection.

The device supports a maximum of three IPsec smart link policies.

An IPsec smart link policy takes effect after it is applied to an IKE-based IPsec policy. You cannot apply an IPsec smart link policy to a manual IPsec policy or an IPsec policy created by using an IPsec policy template.

An IPsec smart link policy can be applied to only one IPsec policy, and an IPsec policy can use only one IPsec smart link policy.

Examples

Created an IPsec smart link policy named **smlkpolicy1**.

```
<Sysname> system-view
[Sysname] ipsec smart-link policy smlkpolicy1
[Sysname-ipsec-smart-link-policy-smlkpolicy1]
```

Related commands

display ipsec smart-link policy

ipsec transform-set

Use **ipsec transform-set** to create an IPsec transform set and enter its view, or enter the view of an existing IPsec transform set.

Use **undo ipsec transform-set** to delete an IPsec transform set.

Syntax

ipsec transform-set *transform-set-name*

undo ipsec transform-set *transform-set-name*

Default

No IPsec transform sets exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

transform-set-name: Specifies a name for the IPsec transform set, a case-insensitive string of 1 to 63 characters.

Usage guidelines

An IPsec transform set, part of an IPsec policy, defines the security parameters for IPsec SA negotiation, including the security protocol, encryption algorithms, authentication algorithms, and encapsulation mode.

Examples

Create an IPsec transform set named **tran1** and enter its view.

```
<Sysname> system-view
[Sysname] ipsec transform-set tran1
[Sysname-transform-set-tran1]
```

Related commands

display ipsec transform-set

link

Use **link** to configure a link for IPsec smart link selection.

Use **undo link** to delete a link from IPsec smart link selection.

Syntax

link *link-id* **interface** *interface-type interface-number* [**local** *local-address* **nexthop** *nexthop-address*] **remote** *remote-address*

undo link *link-id*

Default

An IPsec smart link policy does not contain any links.

Views

IPsec smart link policy view

Predefined user roles

network-admin

context-admin

Parameters

link-id: Specifies a link ID in the range of 1 to 10.

interface *interface-type interface-number*: Specifies the local interface of the link.

local *local-address*: Specifies the local IP address of the link, in dotted decimal notation. The specified local IP address must be the same as the IP address of the link local interface. By default, the IP address of the local interface is used.

nexthop *nexthop-address*: Specifies the next hop IP address for the link, in dotted decimal notation. The specified next hop address must be the same as the gateway address on the local interface of the link. If you do not specify a next hop IP address, the gateway address of the link local interface is used. If the gateway address of the link local interface cannot be obtained, the remote IP address of the link is used.

remote *remote-address*: Specifies the remote IP address for the link, in dotted decimal notation.

Usage guidelines

A maximum of 10 links can be configured in an IPsec smart link policy. A link configured earlier is given a higher priority than the one configured later. You can use the **move link** command to adjust the priorities of the links. During link switchover, IPsec traffic will be switched over the links in descending order of the link priority.

After a link is selected, the device applies the IPsec policy that uses the IPsec smart link policy to the local interface of the link. The local and remote IP addresses of the link will be set as the local and remote IP addresses of the IPsec tunnel.

To correctly forward IKE negotiation packets and IPsec packets, the device automatically generates a route for the active link over which the IPsec tunnel is established. The remote address and next hop address of the link are used as the destination address and next hop address of the route.

Examples

Configure link 1 with local interface GigabitEthernet 1/0/1, local IP address 1.1.1.1, next hop IP address 1.1.1.254, and remote IP address 3.3.3.3.

```
<Sysname> system-view
[Sysname] ipsec smart-link policy smlkpolicy1
[Sysname-ipsec-smart-link-policy-smlkpolicy1] link 1 interface gigabitethernet 1/0/1
local 1.1.1.1 nexthop 1.1.1.254 remote 3.3.3.3
```

Related commands

gateway

link-probe

Use **link-probe** to set the number of link quality probe packets sent in each probe cycle and the probe packet sending interval.

Use **undo link-probe** to restore the default.

Syntax

link-probe { **count** *number* | **interval** *interval* }

undo link-probe { **count** | **interval** }

Default

The device sends 10 probe packets in each probe cycle and the probe packet sending interval is 1 second.

Views

IPsec smart link policy view

Predefined user roles

network-admin

context-admin

Parameters

count *number*: Specifies the number of probe packets sent in each probe cycle. The value range is 1 to 30.

interval *interval*: Specifies probe packet sending interval in seconds. The value range is 1 to 3.

Usage guidelines

After sending the specified number of probe packets over the active link, the device calculates the packet loss ratio and delay, and compares the results with the configured thresholds. If the packet loss ratio or delay over the link exceeds the threshold, a link switchover is triggered.

Examples

Set the interval for sending link quality probe packets to 2 seconds and the number of probe packets sent in each probe cycle to 15.

```
<Sysname> system-view
[Sysname] ipsec smart-link policy smlkpolicy1
[Sysname-ipsec-smart-link-policy-smlkpolicy1] link-probe interval 2
[Sysname-ipsec-smart-link-policy-smlkpolicy1] link-probe count 15
```

Related commands

link-probe source

link-switch threshold

link-probe source

Use **link-probe source** to specify the source and destination IP addresses for link quality probe packets.

Use **undo link-probe source** to remove the source and destination IP addresses configured for link quality probe packets.

Syntax

link-probe source *source-address* **destination** *destination-address*

undo link-probe source *source-address* **destination** *destination-address*

Default

The source and destination IP addresses of link quality probe packets are the local and remote IP addresses of the link over which the packets are sent.

Views

IPsec smart link policy view

Predefined user roles

network-admin

context-admin

Parameters

source *source-address*: Specifies the source IP address for link quality probe packets, in dotted decimal notation.

destination *destination-address*: Specifies the destination IP address for link quality probe packets, in dotted decimal notation.

Usage guidelines

IPsec uses ICMP packets as probe packets for link quality probe. The *source-address* of the probe packets can be any address on the local subnet. The *destination-address* can be the IP address of a device on the remote subnet or an interface IP address of the remote gateway. The *destination-address* and *source-address* must be reachable to each other.

To ensure that probe packets can be sent over the IPsec tunnel to the destination, the branch gateway performs the following operations:

- Adds a static route destined for the probe destination address. The next hop address of the route is the local IP address of the IPsec tunnel at the headquarters (the link remote IP address configured on the branch gateway).

  The link remote address refers to the address specified by the *remote-address* argument in the **link** command.
- Adds the following rule to the ACL used by the IPsec policy:

  rule permit ip source *source-address* 0 **destination** *dest-address* 0

For the remote device (the headquarters gateway) to correctly receive and respond to the probe packets, configure the following settings on the remote device:

- In the ACL used by the IPsec policy template, add ACL rules to permit the data flows that need IPsec protection.
- Enable IPsec RRI or add a static route destined for the source address of the probe packets..

Examples

Set the source and destination IP addresses for link quality probe packets to 10.3.1.10 and 10.3.2.10, respectively.

```
<Sysname> system-view
[Sysname] ipsec smart-link policy smlkpolicy1
[Sysname-ipsec-smart-link-policy-smlkpolicy1] link-probe source 10.3.1.10 destination
10.3.2.10
```

Related commands

link-probe

link-switch cycles

Use **link-switch cycles** to set the maximum number of link switchover cycles.

Use **undo link-switch cycles** to restore the default.

Syntax

link-switch cycles *number*

undo link-switch cycles

Default

The maximum number of link switchover cycles is 3.

Views

IPsec smart link policy view

Predefined user roles

network-admin

context-admin

Parameters

number: Specifies the maximum number of link switchover cycles. The value range is 0 to 5. Value 0 indicates that the number of link switchover cycles is not limited.

Usage guidelines

If the delay or packet loss ratio over the active link exceeds the configured threshold, the device performs cyclic link switchovers in descending order of the link priorities. The first link switchover cycle starts from the current active link. For example, suppose a smart link policy contains four links and the active link is link 3. The first link switchover cycle is 3 > 4. The subsequent link switchover cycles each are 1 > 2 > 3 > 4.

Cyclic link switchover probes the available links one by one in descending order of the link priority, and uses the first qualified link to transfer traffic. If no links are qualified when the maximum number of link switchover cycles is reached, the device selects a link for traffic as follows:

- Selects the link with the lowest packet loss ratio.
- Selects the link with the lowest delay if the links have the same packet loss ratio.
- Selects the link with the lowest priority if the links have the same packet loss ratio and delay.

After 10 minutes, the device starts link quality probing and cyclic link switchovers again.

If the maximum number of link switchover cycles is set to 0, the device never stops link quality probing and cyclic link switchovers.

Examples

Set the maximum number of link switchover cycles to 2.

```
<Sysname> system-view
[Sysname] ipsec smart-link policy smlkpolicy1
[Sysname-ipsec-smart-link-policy-smlkpolicy1] link-switch cycles 2
```

Related commands

link-switch threshold

link-switch threshold

Use **link-switch threshold** to set the link switchover thresholds.

Use **undo link-switch threshold** to restore the default.

Syntax

link-switch threshold { **delay** *delay* | **loss** *loss-ratio* }

undo link-switch threshold { **delay** | **loss** }

Default

The packet loss ratio threshold is 30%, and the delay threshold is 500 milliseconds.

Views

IPsec smart link policy view

Predefined user roles

network-admin

context-admin

Parameters

delay *delay*: Specifies the delay threshold, in milliseconds. The value range is 1 to 3000.

loss *loss-ratio*: Specifies the packet loss ratio threshold, in percentages. The value range is 1 to 100.

Usage guidelines

After sending the specified number of probe packets (a probe cycle), the device calculates the average delay and packet loss ratio and compares the results with the configured thresholds. A link switchover is triggered if either threshold is exceeded.

The packet loss ratio within a link quality probe cycle is calculated as follows: Packet loss ratio = number of received response packets / total number of link quality probe packets sent.

The delay is calculated as follows: Delay = time when a response packet is received – time when the probe packet is sent. The device calculates the delay of each probe packet within a probe cycle and takes an average.

Examples

Set the packet loss ratio threshold to 10% and the delay threshold to 300 milliseconds.

```
<Sysname> system-view
[Sysname] ipsec smart-link policy smlkpolicy1
[Sysname-ipsec-smart-link-policy-smlkpolicy1] link-switch threshold loss 10
[Sysname-ipsec-smart-link-policy-smlkpolicy1] link-switch threshold delay 300
```

Related commands

link-probe interval

local-address

Use **local-address** to configure the local IP address for the IPsec tunnel.

Use **undo local-address** to restore the default.

Syntax

local-address { *ipv4-address* | **ipv6** *ipv6-address* }

undo local-address

Default

The primary IPv4 address of the interface to which the IPsec policy is applied is used as the local IPv4 address. The first IPv6 address of the interface to which the IPsec policy is applied is used as the local IPv6 address.

Views

IPsec policy view

IPsec policy template view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-address: Specifies the local IPv4 address for the IPsec tunnel.

ipv6 *ipv6-address*: Specifies the local IPv6 address for the IPsec tunnel.

Usage guidelines

The remote IP address on the IKE negotiation initiator must be the same as the local address on the IKE negotiation responder.

The local address cannot be a secondary IP address of the interface where the IPsec policy is applied.

Examples

Configure local address 1.1.1.1 for the IPsec tunnel.

```
<Sysname> system-view
[Sysname] ipsec policy map 1 isakmp
[Sysname-ipsec-policy-isakmp-map-1] local-address 1.1.1.1
```

Related commands

remote-address

move link

Use **move link** to move links in an IPsec smart link policy to adjust their priorities.

Syntax

move link *link-id1* **before** *link-id2*

Views

IPsec smart link policy view

Predefined user roles

network-admin

context-admin

Parameters

link-id1: Specifies the ID of the link to be moved. The value range is 1 to 10. The specified link ID must already exist.

before: Moves *link-id1* to the front of *link-id2*.

link-id2: Specifies the target link ID. The value range is 1 to 10. The specified link ID must already exist.

Usage guidelines

By default, a link configured earlier is given a higher priority in IPsec smart link selection. You can use this command to adjust the link priorities in an IPsec smart link policy.

To view the links and their priorities in an IPsec smart link policy, use the **display ipsec smart-link policy** command.

Examples

Move link 5 in IPsec smart link policy **smlkpolicy1** to the front of link 1 so that link 5 takes precedence over link 1.

```
<Sysname> system-view
[Sysname] ipsec smart-link policy smlkpolicy1
[Sysname-ipsec-smart-link-policy-smlkpolicy1] move link 5 before 1
```

Related commands

display ipsec smart-link policy

pfs

Use **pfs** to enable the Perfect Forward Secrecy (PFS) feature for an IPsec transform set.

Use **undo pfs** to restore the default.

Syntax

pfs { **dh-group1** | **dh-group2** | **dh-group5** | **dh-group14** | **dh-group19** | **dh-group20** | **dh-group24** }

undo pfs

Default

The PFS feature is disabled for the IPsec transform set.

Views

IPsec transform set view

Predefined user roles

network-admin

context-admin

Parameters

dh-group1: Uses 768-bit Diffie-Hellman group.

dh-group2: Uses 1024-bit Diffie-Hellman group.

dh-group5: Uses 1536-bit Diffie-Hellman group.

dh-group14: Uses 2048-bit Diffie-Hellman group.

dh-group24: Uses 2048-bit and 256-bit subgroup Diffie-Hellman group.

dh-group19: Uses 256-bit ECP Diffie-Hellman group. This keyword is available only for IKEv2.

dh-group20: Uses 384-bit ECP Diffie-Hellman group. This keyword is available only for IKEv2.

dh-group24: Uses 2048-bit and 256-bit subgroup Diffie-Hellman group.

Usage guidelines

In terms of security and required calculation time, the following groups are in descending order:

- 384-bit ECP Diffie-Hellman group (**dh-group20**).
- 256-bit ECP Diffie-Hellman group (**dh-group19**).
- 2048-bit and 256-bit subgroup Diffie-Hellman group (**dh-group24**).
- 2048-bit Diffie-Hellman group (**dh-group14**).
- 1536-bit Diffie-Hellman group (**dh-group5**).
- 1024-bit Diffie-Hellman group (**dh-group2**).

- 768-bit Diffie-Hellman group (**dh-group1**).

If IKEv1 is used, the security level of the Diffie-Hellman group of the initiator must be higher than or equal to that of the responder. This restriction does not apply to IKEv2.

The end without the PFS feature performs IKE negotiation according to the PFS requirements of the peer end.

Examples

Enable PFS using 2048-bit Diffie-Hellman group for IPsec transform set **tran1**.

```
<Sysname> system-view
[Sysname] ipsec transform-set tran1
[Sysname-ipsec-transform-set-tran1] pfs dh-group14
```

protocol

Use **protocol** to specify a security protocol for an IPsec transform set.

Use **undo protocol** to restore the default.

Syntax

protocol { **ah** | **ah-esp** | **esp** }

undo protocol

Default

The IPsec transform set uses the ESP protocol.

Views

IPsec transform set view

Predefined user roles

network-admin

context-admin

Parameters

ah: Specifies the AH protocol.

ah-esp: Specifies using the ESP protocol first and then using the AH protocol.

ah: Specifies the AH protocol.

Usage guidelines

The two tunnel ends must use the same security protocol in the IPsec transform set.

Examples

Specify the AH protocol for the IPsec transform set.

```
<Sysname> system-view
[Sysname] ipsec transform-set tran1
[Sysname-ipsec-transform-set-tran1] protocol ah
```

qos pre-classify

Use **qos pre-classify** to enable the QoS pre-classify feature.

Use **undo qos pre-classify** to disable the QoS pre-classify feature.

Syntax

qos pre-classify

undo qos pre-classify

Default

The QoS pre-classify feature is disabled. QoS uses the new IP header of IPsec packets to perform traffic classification.

Views

IPsec policy view

IPsec policy template view

Predefined user roles

network-admin

context-admin

Usage guidelines

The QoS pre-classify feature enables QoS to classify packets by using the IP header of the original IP packets.

Examples

Enable the QoS pre-classify feature.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] qos pre-classify
```

redundancy replay-interval

Use **redundancy replay-interval** to set the anti-replay window lower bound value synchronization interval for inbound packets and the sequence number synchronization interval for outbound packets.

Use **undo redundancy replay-interval** to restore the default.

Syntax

redundancy replay-interval inbound *inbound-interval* **outbound** *outbound-interval*

undo redundancy replay-interval

Default

The active device synchronizes the anti-replay window lower bound value every time it receives 1000 packets and synchronizes the sequence number every time it sends 100000 packets.

Views

IPsec policy view

IPsec policy template view

IPsec profile view

Predefined user roles

network-admin

context-admin

Parameters

inbound *inbound-interval*: Specifies the interval at which the active device synchronizes the lower bound value of the IPsec anti-replay window to the standby device. This interval is expressed in the number of received packets, in the range of 0 to 1000. If you set the value to 0, the lower bound value of the anti-replay window will not be synchronized.

outbound *outbound-interval*: Specifies the interval at which the active device synchronizes the IPsec anti-replay sequence number to the standby device. This interval is expressed in the number of sent packets, in the range of 1000 to 100000.

Usage guidelines

The intervals take effect only after you enable IPsec redundancy by using the **ipsec redundancy enable** command.

A short interval improves the anti-replay information consistency between the active device and the standby device, but it sacrifices the forwarding performance of the devices.

Examples

Set the anti-replay window lower bound value synchronization interval for inbound packets to 800. Set the sequence number synchronization interval for outbound packets to 50000.

```
<Sysname> system-view
[Sysname] ipsec policy test 1 manual
[sysname-ipsec-policy-manual-test-1] redundancy replay-interval inbound 800 outbound
50000
```

Related commands

ipsec anti-replay check

ipsec anti-replay window

ipsec redundancy enable

remote-address

Use **remote-address** to configure the remote IP address for the IPsec tunnel.

Use **undo remote-address** to restore the default.

Syntax

remote-address { [**ipv6**] *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [**primary**]

undo remote-address { [**ipv6**] *host-name* | *ipv4-address* | **ipv6** *ipv6-address* }

Default

No remote IP address is configured for the IPsec tunnel.

Views

IPsec policy view

IPsec policy template view

Predefined user roles

network-admin

context-admin

Parameters

ipv6: Specifies the remote address or host name of an IPv6 IPsec tunnel. To specify the remote address or host name of an IPv4 IPsec tunnel, do not specify this keyword.

hostname: Specifies the remote host name, a case-insensitive string of 1 to 253 characters. The host name can be resolved to an IP address by the DNS server.

ipv4-address: Specifies a remote IPv4 address.

ipv6-address: Specifies a remote IPv6 address.

primary: Sets the specified remote address as the primary address, which has the highest priority in tunnel setup. If you do not set a primary address, the address specified earlier has a higher priority.

Usage guidelines

This remote IP address configuration is required on the IKE negotiation initiator and optional on the responder if the responder uses an IPsec policy template.

A manual IPsec policy does not support DNS. Therefore, you must specify a remote IP address rather than a remote host name for the manual IPsec policy.

If you configure a remote host name, the local end resolves the host name into the latest IP address of the remote end.

- If a DNS server is used for resolution, the local end queries the remote IP address again from the DNS server after the previously cached remote IP address expires. This mechanism ensures that the local end can always obtain the latest remote IP address.
- If a static DNS entry is used for resolution, the local end always obtains the latest remote IP address corresponding to the host name.

For example, the local end has a static DNS entry which maps the host name **test** to the IP address 1.1.1.1. Configure the following commands:

Configure the remote host name to **test** for the IPsec tunnel in the IPsec policy **policy1**.

```
[Sysname] ipsec policy policy1 1 isakmp
[Sysname-ipsec-policy-isakmp-policy1-1] remote-address test
```

Change the IP address for the host **test** to 2.2.2.2.

```
[Sysname] ip host test 2.2.2.2
```

In this case, the local end obtains the latest IP address of the remote host, which is 2.2.2.2.

You can execute this command multiple times to specify multiple remote IP addresses. When establishing an IPsec tunnel, the local end initiates IPsec negotiation to the first specified IP address. If the negotiation succeeds, the local end establishes the IPsec tunnel with this IP address. If the negotiation fails, the local end tries IPsec tunnel setup to the second IP address, and so forth to the last IP address.

If a primary remote address is set, the primary address has the highest priority in tunnel setup. The local end starts IPsec negotiation first to the primary address for each tunnel setup.

Each IPsec policy can have only one primary remote address. To change the primary address, you must first execute the **undo remote-address** command, and then use the **remote-address** command to specify a new primary address.

Examples

Specify remote IP address 10.1.1.2 for the IPsec tunnel.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 10 manual
[Sysname-ipsec-policy-manual-policy1-10] remote-address 10.1.1.2
```

Related commands

ip host (*Layer 3—IP Services Command Reference*)

local-address

reset ipsec sa

Use **reset ipsec sa** to clear IPsec SAs.

Syntax

reset ipsec sa [{ **ipv6-policy** | **policy** } *policy-name* [*seq-number*] | **profile** *policy-name* | **remote** { *ipv4-address* | **ipv6** *ipv6-address* } | **spi** { *ipv4-address* | **ipv6** *ipv6-address* } { **ah** | **esp** } *spi-num*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

{ **ipv6-policy** | **policy** } *policy-name* [*seq-number*]: Clears IPsec SAs for the specified IPsec policy.

- **ipv6-policy**: Specifies an IPv6 IPsec policy.
- **policy**: Specifies an IPv4 IPsec policy.
- *policy-name*: Specifies the name of the IPsec policy, a case-insensitive string of 1 to 63 characters.
- *seq-number*: Specifies the sequence number of an IPsec policy entry, in the range of 1 to 65535. If you do not specify this argument, all the entries in the IPsec policy are specified.

profile *profile-name*: Clears IPsec SAs for the IPsec profile specified by its name, a case-insensitive string of 1 to 63 characters.

remote: Clears IPsec SAs for the specified remote address.

ipv4-address: Specifies a remote IPv4 address.

ipv6 *ipv6-address*: Specifies a remote IPv6 address.

spi { *ipv4-address* | **ipv6** *ipv6-address* } { **ah** | **esp** } *spi-num*: Clears IPsec SAs matching the specified SA triplet: the remote address, the security protocol, and the SPI.

- *ipv4-address*: Specifies a remote IPv4 address.
- **ipv6** *ipv6-address*: Specifies a remote IPv6 address.
- **ah**: Specifies the AH protocol.
- **esp**: Specifies the ESP protocol.

spi-num: Specifies the security parameter index in the range of 256 to 4294967295.

Usage guidelines

If you do not specify any parameters, this command clears all IPsec SAs.

If you specify an SA triplet, this command clears the IPsec SA matching the triplet, and all the other IPsec SAs that were established during the same negotiation process, including the corresponding

IPsec SA in the other direction, and the inbound and outbound IPsec SAs using the other security protocol (AH or ESP).

An outbound SA is uniquely identified by an SA triplet and an inbound SA is uniquely identified by an SPI. To clear IPsec SAs by specifying a triplet in the outbound direction, you should provide the remote IP address, the security protocol, and the SPI, where the remote IP address can be any valid address if the SAs are established by IPsec profiles. To clear IPsec SAs by specifying a triplet in the inbound direction, you should provide the SPI and use any valid values for the other two parameters.

After a manual IPsec SA is cleared, the system automatically creates a new SA based on the parameters of the IPsec policy. After IKE negotiated SAs are cleared, the system creates new SAs only when IKE negotiation is triggered by packets.

Examples

Clear all IPsec SAs.

```
<Sysname> reset ipsec sa
```

Clear the inbound and outbound IPsec SAs for the triplet of SPI 256, remote IP address 10.1.1.2, and security protocol AH.

```
<Sysname> reset ipsec sa spi 10.1.1.2 ah 256
```

Clear all IPsec SAs for remote IP address 10.1.1.2.

```
<Sysname> reset ipsec sa remote 10.1.1.2
```

Clear all IPsec SAs for entry 10 of IPsec policy **policy1**.

```
<Sysname> reset ipsec sa policy policy1 10
```

Clear all IPsec SAs for IPsec policy **policy1**.

```
<Sysname> reset ipsec sa policy policy1
```

Related commands

display ipsec sa

reset ipsec statistics

Use **reset ipsec statistics** to clear IPsec packet statistics.

Syntax

reset ipsec statistics[**tunnel-id** *tunnel-id*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

tunnel-id *tunnel-id*: Clears IPsec packet statistics for the specified IPsec tunnel. The value range for the *tunnel-id* argument is 0 to 4294967295. If you do not specify this option, the command clears all IPsec packet statistics.

Examples

Clear IPsec packet statistics.

```
<Sysname> reset ipsec statistics
```

Related commands

display ipsec statistics

reverse-route dynamic

Use **reverse-route dynamic** to enable IPsec reverse route inject (RRI).

Use **undo reverse-route dynamic** to disable IPsec RRI.

Syntax

reverse-route [**next-hop** [**ipv6**] *ip-address*] **dynamic**

undo reverse-route dynamic

Default

IPsec RRI is disabled.

Views

IPsec policy view

IPsec policy template view

Predefined user roles

network-admin

context-admin

Parameters

next-hop: Specifies a next hop IP address for the IPsec RRI-created static route. If you do not specify a next hop IP address, the static route uses the remote IP address of the IPsec tunnel as the next hop IP address.

ipv6: Specifies an IPv6 address.

ip-address: Specifies the next hop IPv4 or IPv6 address.

Usage guidelines

IPsec RRI is usually used on a gateway device at the headquarters side in an IPsec VPN. After IPsec RRI is enabled for an IPsec policy or an IPsec policy template on a gateway device, the gateway device automatically creates a static route upon IPsec SA creation according to this IPsec policy or IPsec policy template. By default, the static route uses the protected peer private network as the destination IP address and the remote IP address of the IPsec tunnel as the next hop address. If there are multiple paths to the remote tunnel end, you can use the **next-hop** keyword to specify a next hop IP address for the static route.

When you enable IPsec RRI for an IPsec policy, the device deletes all IPsec SAs that are created according to this IPsec policy. Upon IPsec SAs are renegotiated, the static routes are created.

When you disable IPsec RRI for an IPsec policy, the device deletes all IPsec SAs that are created according to this IPsec policy, and the associated static routes.

To display the static routes created by RRI, use the **display ip routing-table** command.

Examples

Enable IPsec RRI to create a static route according to the IPsec SA negotiated by the specified IPsec policy. The destination IP address is the protected peer private network 3.0.0.0/24, and the next hop is the IP address (1.1.1.2) of the remote tunnel interface.

```
<Sysname> system-view
[Sysname] ipsec policy 1 1 isakmp
[Sysname-ipsec-policy-isakmp-1-1] reverse-route dynamic
[Sysname-ipsec-policy-isakmp-1-1] quit
```

Display the routing table. You can see a created static route. (Other information is not shown.)

```
[Sysname] display ip routing-table

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
3.0.0.0/24          Static 60   0            1.1.1.2         GE1/0/1
```

Enable IPsec RRI to create a static route according to the IPsec SA negotiated by the specified IPsec policy. Set the next hop IP address of the static route to 2.2.2.3.

```
<Sysname> system-view
[Sysname] ipsec policy 1 1 isakmp
[Sysname-ipsec-policy-isakmp-1-1] reverse-route next-hop 2.2.2.3 dynamic
[Sysname-ipsec-policy-isakmp-1-1] quit
```

Display the routing table. You can see a created static route. (Other information is not shown.)

```
[Sysname] display ip routing-table
Destination/Mask    Proto  Pre  Cost         NextHop         Interface
4.0.0.0/24          Static 60   0            2.2.2.3         GE1/0/1
```

Related commands

display ip routing-table (*Layer 3—IP Routing Command Reference*)

ipsec policy

ipsec policy-template

reverse-route preference

Use **reverse-route preference** to set the preference of the static routes created by IPsec RRI.

Use **undo reverse-route preference** to restore the default.

Syntax

reverse-route preference *number*

undo reverse-route preference

Default

The preference for the static routes created by IPsec RRI is 60.

Views

IPsec policy view

IPsec policy template view

Predefined user roles

network-admin

context-admin

Parameters

number: Specifies a preference value. The value range is 1 to 255. A smaller value represents a higher preference.

Usage guidelines

When you change this preference in an IPsec policy, the device deletes all IPsec SAs created according to this IPsec policy, and the associated static routes.

Examples

Change the preference to 100 for static routes created by IPsec RRI.

```
<Sysname> system-view
[Sysname] ipsec policy 1 1 isakmp
[Sysname-ipsec-policy-isakmp-1-1] reverse-route preference 100
```

Related commands

ipsec policy

ipsec policy-template

reverse-route tag

Use **reverse-route tag** to set a route tag for the static routes created by IPsec RRI.

Use **undo reverse-route tag** to restore the default.

Syntax

reverse-route tag *tag-value*

undo reverse-route tag

Default

The route tag value is 0 for the static routes created by IPsec RRI.

Views

IPsec policy view

IPsec policy template view

Predefined user roles

network-admin

context-admin

Parameters

tag-value: Specifies a tag value. The value range is 1 to 4294967295.

Usage guidelines

The tag value set by this command helps in implementing flexible route control through routing policies.

When you change this tag value in an IPsec policy, the device deletes all IPsec SAs created by this IPsec policy, and all associated static routes.

Examples

Set the tag value to 50 for the static routes created by IPsec RRI.

```
<Sysname>system-view
[Sysname] ipsec policy 1 1 isakmp
[Sysname-ipsec-policy-isakmp-1-1] reverse-route tag 50
```

Related commands

ipsec policy

ipsec policy-template

sa df-bit

Use **sa df-bit** to configure the DF bit for the outer IP header of IPsec packets.

Use **undo sa df-bit** to restore the default.

Syntax

sa df-bit { **clear** | **copy** | **set** }

undo sa df-bit

Default

The DF bit is not configured for the outer IP header of IPsec packets. The interface-specific or global DF bit setting is used.

Views

IPsec policy view

IPsec policy template view

IPsec profile view

Predefined user roles

network-admin

context-admin

Parameters

clear: Clears the DF bit in the outer IP header. IPsec packets can be fragmented.

copy: Copies the DF bit setting of the original IP header to the outer IP header.

set: Sets the DF bit in the outer IP header. IPsec packets cannot be fragmented.

Usage guidelines

This command is effective only when the IPsec encapsulation mode is tunnel mode. It is not effective in transport mode because the outer IP header is not added in transport mode.

This command is supported only when the IKE negotiation mode is used for IPsec SA setup.

This command does not change the DF bit for the original IP header of IPsec packets.

Packet fragmentation and reassembly might cause packet forwarding to be delayed. You can set the DF bit to avoid the forwarding delay. If the DF bit is set, make sure the path MTU is larger than the IPsec packet size to prevent the IPsec packets from being discarded. Clear the DF bit if you cannot make sure the path MTU is larger than the IPsec packet size.

If the DF bit setting is not configured in the IPsec policy, IPsec profile, or IPsec policy template, the interface-specific DF bit setting is used. If the interface-specific DF bit setting is not configured either, the global DF bit setting is used.

Examples

Set the DF bit in the outer IP header of IPsec packets in IPsec policy **policy1**.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 isakmp
[Sysname-ipsec-policy-isakmp-policy1-100] sa df-bit set
```

Related commands

ipsec df-bit

ipsec global-df-bit

sa duration

Use **sa duration** to set an SA lifetime.

Use **undo sa duration** to remove an SA lifetime.

Syntax

sa duration { **time-based** *seconds* | **traffic-based** *kilobytes* }

undo sa duration { **time-based** | **traffic-based** }

Default

The SA lifetime of an IPsec policy, IPsec profile, or IPsec policy template is the current global SA lifetime.

Views

IPsec policy view

IPsec policy template view

IPsec profile view

Predefined user roles

network-admin

context-admin

Parameters

time-based *seconds*: Specifies the time-based SA lifetime in the range of 180 to 604800 seconds.

traffic-based *kilobytes*: Specifies the traffic-based SA lifetime in the range of 2560 to 4294967295 Kilobytes.

Usage guidelines

IKE prefers the SA lifetime of the IPsec policy, IPsec profile, or IPsec policy template over the global SA lifetime configured by the **ipsec sa global-duration** command. If the IPsec policy, IPsec profile, or IPsec policy template is not configured with the SA lifetime, IKE uses the global SA lifetime for SA negotiation.

During SA negotiation, IKE selects the shorter SA lifetime between the local SA lifetime and the remote SA lifetime.

Examples

Set the SA lifetime to 7200 seconds for IPsec policy **policy1**.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 isakmp
[Sysname-ipsec-policy-isakmp-policy1-100] sa duration time-based 7200
```

Set the SA lifetime to 20 MB for IPsec policy **policy1**. The IPsec SA expires after transmitting 20480 Kilobytes.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 isakmp
[Sysname-ipsec-policy-isakmp-policy1-100] sa duration traffic-based 20480
```

Related commands

display ipsec sa

ipsec sa global-duration

sa hex-key authentication

Use **sa hex-key authentication** to configure a hexadecimal authentication key for manual IPsec SAs.

Use **undo sa hex-key authentication** to remove the hexadecimal authentication key.

Syntax

sa hex-key authentication { **inbound** | **outbound** } { **ah** | **esp** } { **cipher** | **simple** } *string*

undo sa hex-key authentication { **inbound** | **outbound** } { **ah** | **esp** }

Default

No hexadecimal authentication key is configured for manual IPsec SAs.

Views

IPsec policy view

IPsec profile view

Predefined user roles

network-admin

context-admin

Parameters

inbound: Specifies a hexadecimal authentication key for the inbound SA.

outbound: Specifies a hexadecimal authentication key for the outbound SA.

ah: Uses AH.

esp: Uses ESP.

cipher: Specifies a key in encrypted form.

simple: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. Its plaintext form is case insensitive and must be a 16-byte hexadecimal string for HMAC-MD5, a 32-byte hexadecimal string for HMAC-SM3, and a 20-byte hexadecimal string for HMAC-SHA1. Its encrypted form is a case-sensitive string of 1 to 85 characters.

Usage guidelines

This command applies only to manual IPsec policies and IPsec profiles.

You must set an authentication key for both the inbound and outbound SAs.

The local inbound SA must use the same authentication key as the remote outbound SA, and the local outbound SA must use the same authentication key as the remote inbound SA.

In an IPsec profile to be applied to an IPv6 routing protocol, the local authentication keys of the inbound and outbound SAs must be identical.

The keys for the IPsec SAs at the two tunnel ends must be input in the same format (either in hexadecimal or character format). Otherwise, they cannot establish an IPsec tunnel.

If you execute this command multiple times for the same protocol and direction, the most recent configuration takes effect.

Examples

Configure plaintext authentication keys **0x112233445566778899aabbccddeeff00** and **0xaabbccddeeff001100aabbccddeeff00** for the inbound and outbound SAs that use AH.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] sa hex-key authentication inbound ah simple
11223344556778899aabbccddeeff00
[Sysname-ipsec-policy-manual-policy1-100] sa hex-key authentication outbound ah simple
aabbccddeeff001100aabbccddeeff00
```

Related commands

display ipsec sa

sa string-key

sa hex-key encryption

Use **sa encryption-hex** configure a hexadecimal encryption key for manual IPsec SAs.

Use **undo sa encryption-hex** remove the hexadecimal encryption key.

Syntax

sa hex-key encryption { **inbound** | **outbound** } **esp** { **cipher** | **simple** } *string*

undo sa hex-key encryption { **inbound** | **outbound** } **esp**

Default

No hexadecimal encryption key is configured for manual IPsec SAs.

Views

IPsec policy view

IPsec profile view

Predefined user roles

network-admin

context-admin

Parameters

inbound: Specifies a hexadecimal encryption key for the inbound SA.

outbound: Specifies a hexadecimal encryption key for the outbound SA.

esp: Uses ESP.

cipher: Specifies a key in encrypted form.

simple: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. Its encrypted form is a case-sensitive string of 1 to 117 characters. Its plaintext form is a case-insensitive hexadecimal string and the key length varies by algorithm.

The following matrix shows the key length for the algorithms:

Algorithm	Key length (bytes)
DES-CBC	8
3DES-CBC	24
AES128-CBC	16
AES192-CBC	24

Algorithm	Key length (bytes)
AES256-CBC	32
SM1128-CBC	16
SM4128-CBC	16

Usage guidelines

This command applies only to manual IPsec policies and IPsec profiles.

You must set an encryption key for both the inbound and outbound SAs.

The local inbound SA must use the same encryption key as the remote outbound SA, and the local outbound SA must use the same encryption key as the remote inbound SA.

In an IPsec profile to be applied to an IPv6 routing protocol, the local encryption keys of the inbound and outbound SAs must be identical.

The keys for the IPsec SAs at the two tunnel ends must be configured in the same format (either in hexadecimal or character format). Otherwise, they cannot establish an IPsec tunnel.

If you execute this command multiple times for the same direction, the most recent configuration takes effect.

Examples

Configure plaintext encryption keys **0x1234567890abcdef** and **0xabcdefabcdef1234** for the inbound and outbound IPsec SAs that use ESP.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] sa hex-key encryption inbound esp simple
1234567890abcdef
[Sysname-ipsec-policy-manual-policy1-100] sa hex-key encryption outbound esp simple
abcdefabcdef1234
```

Related commands

display ipsec sa

sa string-key

sa idle-time

Use **sa idle-time** to set the IPsec SA idle timeout.

Use **undo sa idle-time** to restore the default.

Syntax

sa idle-time *seconds*

undo sa idle-time

Default

An IPsec policy, IPsec profile, or IPsec policy template uses the global IPsec SA idle timeout.

Views

IPsec policy view

IPsec policy template view

IPsec profile view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies the IPsec SA idle timeout in the range of 60 to 86400 seconds.

Usage guidelines

This feature applies only to IPsec SAs negotiated by IKE and takes effect after the **ipsec sa idle-time** command is configured.

The IPsec SA idle timer starts when an IPsec SA is created. If no traffic matches the IPsec SA within the idle timeout interval, the IPsec SA is deleted.

The IPsec SA idle timeout configured by this command takes precedence over the global IPsec SA timeout configured by the **ipsec sa idle-time** command. If the IPsec policy, IPsec profile, or IPsec policy template is not configured with the SA idle timeout, IKE uses the global SA idle timeout.

Examples

Set the IPsec SA idle timeout to 600 seconds for IPsec policy **map**.

```
<Sysname> system-view
[Sysname] ipsec policy map 100 isakmp
[Sysname-ipsec-policy-isakmp-map-100] sa idle-time 600
```

Related commands

display ipsec sa

ipsec sa idle-time

sa soft-duration buffer

Use **sa soft-duration buffer** to set the time-based or traffic-based IPsec SA soft lifetime buffer.

Use **undo sa soft-duration buffer** to restore the default.

Syntax

sa soft-duration buffer { **time-based** *seconds* | **traffic-based** *kilobytes* }

undo sa soft-duration buffer { **time-based** | **traffic-based** }

Default

The time-based and traffic-based IPsec SA soft lifetime buffers are not configured.

Views

IPsec policy view

IPsec profile view

Predefined user roles

network-admin

context-admin

Parameters

time-based *seconds*: Specifies the time-based IPsec SA soft lifetime buffer in seconds. The value range is 20 to 201600.

traffic-based *kilobytes*: Specifies the traffic-based IPsec SA soft lifetime buffer in Kilobytes. The value range is 1000 to 4294901760.

Usage guidelines

This command takes effect only when IKEv1 is used.

The IPsec SA soft lifetime buffers are used to determine the IPsec SA soft lifetimes.

If no IPsec SA soft lifetime buffers are configured, the system calculates a default time-based and a default traffic-based IPsec SA soft lifetime.

If IPsec SA soft lifetime buffers are configured, the system calculates IPsec SA soft lifetimes as follows:

- Time-based IPsec SA soft lifetime = time-based IPsec SA lifetime – time-based IPsec SA soft lifetime buffer.

  If the calculated time-based IPsec SA soft lifetime is shorter than or equal to 20 seconds, the system uses the default time-based IPsec SA soft lifetime.
- Traffic-based IPsec SA soft lifetime = traffic-based IPsec SA lifetime – traffic-based IPsec SA soft lifetime buffer.

  If the calculated traffic-based IPsec SA soft lifetime is smaller than or equal to 1000 Kilobytes, the system uses the default traffic-based IPsec SA soft lifetime.

Examples

Set the time-based IPsec SA soft lifetime buffer to 600 seconds in IPsec policy **example 1**.

```
<Sysname> system-view
[Sysname] ipsec policy example 1 isakmp
[Sysname-ipsec-policy-isakmp-example-1] sa soft-duration buffer time-based 600
```

Set the traffic-based IPsec SA soft lifetime buffer to 10000 Kilobytes in IPsec policy **example 1**.

```
<Sysname> system-view
[Sysname] ipsec policy example 1 isakmp
[Sysname-ipsec-policy-isakmp-example-1] sa soft-duration buffer traffic-based 10000
```

Related commands

ipsec sa global-soft-duration buffer

sa spi

Use **sa spi** to configure an SPI for IPsec SAs.

Use **undo sa spi** to remove the SPI.

Syntax

sa spi { **inbound** | **outbound** } { **ah** | **esp** } *spi-number*

undo sa spi { **inbound** | **outbound** } { **ah** | **esp** }

Default

No SPI is configured for IPsec SAs.

Views

IPsec policy view

IPsec profile view

Predefined user roles

network-admin

context-admin

Parameters

inbound: Specifies an SPI for inbound SAs.

outbound: Specifies an SPI for outbound SAs.

ah: Uses AH.

esp: Uses ESP.

spi-number: Specifies a security parameters index (SPI) in the range of 256 to 4294967295.

Usage guidelines

This command applies only to manual IPsec policies and IPsec profiles.

You must configure an SPI for both inbound and outbound SAs, and make sure the SAs in each direction are unique: For an outbound SA, make sure its triplet (remote IP address, security protocol, and SPI) is unique. For an inbound SA, make sure its SPI is unique.

The local inbound SA must use the same SPI as the remote outbound SA, and the local outbound SA must use the same SPI as the remote inbound SA.

When you configure an IPsec profile for an IPv6 routing protocol, follow these guidelines:

- The local inbound and outbound SAs must use the same SPI.
- The IPsec SAs on the devices in the same scope must have the same SPI. The scope is defined by protocols. For OSPFv3, the scope consists of OSPFv3 neighbors or an OSPFv3 area. For RIPng, the scope consists of directly-connected neighbors or a RIPng process. For BGP4+, the scope consists of BGP4+ peers or a BGP4+ peer group.

Examples

Set the SPI for the inbound SA to 10000 and the SPI for the outbound SA to 20000 in a manual IPsec policy.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] sa spi inbound ah 10000
[Sysname-ipsec-policy-manual-policy1-100] sa spi outbound ah 20000
```

Related commands

display ipsec sa

sa string-key

Use **sa string-key** to set a key string (a key in character format) for manual IPsec SAs.

Use **undo sa string-key** to remove the key string.

Syntax

sa string-key { **inbound** | **outbound** } { **ah** | **esp** } [**cipher** | **simple**] *string*

undo sa string-key { **inbound** | **outbound** } { **ah** | **esp** }

Default

No key string is configured for manual IPsec SAs.

Views

IPsec policy view

IPsec profile view

Predefined user roles

network-admin

context-admin

Parameters

inbound: Sets a key string for inbound IPsec SAs.

outbound: Sets a key string for outbound IPsec SAs.

ah: Uses AH.

esp: Uses ESP.

cipher: Specifies a key string in encrypted form.

simple: Specifies a key string in plaintext form. For security purposes, the key string specified in plaintext form will be stored in encrypted form.

string: Specifies the key string. Its encrypted form is a case-sensitive string of 1 to 373 characters. Its plaintext form is a case-sensitive string of 1 to 255 characters. Using the key string, the system automatically generates keys that meet the algorithm requirements. When the protocol is ESP, the system automatically generates keys for the authentication algorithm and encryption algorithm.

Usage guidelines

This command applies only to manual IPsec policies and IPsec profiles.

You must set a key for both inbound and outbound SAs.

The local inbound SA must use the same key as the remote outbound SA, and the local outbound SA must use the same key as the remote inbound SA.

The keys for the IPsec SAs at the two tunnel ends must be input in the same format (either in hexadecimal or character format). Otherwise, they cannot establish an IPsec tunnel.

When you configure an IPsec profile for an IPv6 routing protocol, follow these guidelines:

- The local inbound and outbound SAs must use the same key.
- The IPsec SAs on the devices in the same scope must have the same key. The scope is defined by protocols. For OSPFv3, the scope consists of OSPFv3 neighbors or an OSPFv3 area. For RIPng, the scope consists of directly-connected neighbors or a RIPng process. For BGP, the scope consists of BGP peers or a BGP peer group.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure the inbound and outbound SAs that use AH to use plaintext keys **abcdef** and **efcdab**, respectively.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] sa string-key inbound ah simple abcdef
[Sysname-ipsec-policy-manual-policy1-100] sa string-key outbound ah simple efcdab
```

In an IPv6 IPsec policy, configure the inbound and outbound SAs that use AH to use plaintext key **abcdef**.

```
<Sysname> system-view
[Sysname] ipsec ipv6-policy policy1 100 manual
[Sysname-ipsec-ipv6-policy-manual-policy1-100] sa string-key inbound ah simple abcdef
[Sysname-ipsec-ipv6-policy-manual-policy1-100] sa string-key outbound ah simple abcdef
```

Related commands

display ipsec sa

sa hex-key

sa trigger-mode

Use **sa trigger-mode** to set the IPsec SA negotiation triggering mode.

Use **undo sa trigger-mode** to restore the default.

Syntax

sa trigger-mode { **auto** | **traffic-based** }

undo sa trigger-mode

Default

IPsec SA negotiation is triggered when traffic requires IPsec protection.

Views

IPsec policy view

Predefined user roles

network-admin

context-admin

Parameters

auto: Triggers IPsec SA negotiation when required IPsec configuration is complete.

traffic-based: Triggers IPsec SA negotiation when traffic requires IPsec protection.

Usage guidelines

You can specify the IPsec SA negotiation triggering mode only for IKE-based IPsec policies.

Compared to the auto mode, the traffic-based mode is more economical in terms of resource usage because it triggers IPsec SA negotiation only when traffic requires IPsec protection. However, the traffic-based mode leaves traffic unprotected before IPsec SAs are successfully established.

This command does not take effect if a smart link policy with smart link selection enabled is applied to the IPsec policy.

The IPsec SA negotiation triggering modes on the local and remote ends of an IPsec tunnel can be different.

Modifying the IPsec SA negotiation triggering mode does not affect existing IPsec SAs.

If the IPsec SA negotiation triggering mode is set to **auto**, change the mode to **traffic-based** as a best practice after IPsec SA establishment is complete.

If the ACL for an IPsec policy or IPsec policy template uses the aggregation or the per-host mode, the IPsec policy or IPsec policy template cannot trigger IPsec SA negotiation in auto mode.

Examples

Set the IPsec SA negotiation triggering mode to **auto** for IPsec policy **policy1**.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 10 isakmp
[Sysname-ipsec-policy-isakmp-policy1-10] sa trigger-mode auto
```

security acl

Use **security acl** to specify an ACL for an IPsec policy or IPsec policy template.

Use **undo security acl** to restore the default.

Syntax

security acl [**ipv6**] { *acl-number* | **name** *acl-name* } [**aggregation** | **per-host**]

undo security acl

Default

An IPsec policy or IPsec policy template does not use any ACL.

Views

IPsec policy view

IPsec policy template view

Predefined user roles

network-admin

context-admin

Parameters

ipv6: Specifies an IPv6 ACL.

acl-number: Specifies an ACL by its number in the range of 3000 to 3999.

name *acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters.

aggregation: Specifies the data protection mode as aggregation. The device does not support protecting IPv6 data flows in aggregation mode.

per-host: Specifies the data protection mode as per-host.

Usage guidelines

An IKE-based IPsec policy supports the following data flow protection modes:

- **Standard mode**—One IPsec tunnel protects one data flow. The data flow permitted by an ACL rule is protected by one IPsec tunnel that is established solely for it. The standard mode is used if you do not specify the aggregation or the per-host mode.
- **Aggregation mode**—One IPsec tunnel protects all data flows permitted by all the rules of an ACL. This mode is only used to communicate with old-version devices.
- **Per-host mode**—One IPsec tunnel protects one host-to-host data flow. One host-to-host data flow is identified by one ACL rule and protected by one IPsec tunnel established solely for it. This mode consumes more system resources when multiple data flows exist between two subnets to be protected.

A manual IPsec policy supports only the aggregation mode.

If the ACL for an IPsec policy or IPsec policy template uses the aggregation or the per-host mode, the IPsec policy or IPsec policy template cannot trigger IPsec SA negotiation in auto mode.

If the specified ACL does not exist or does not contain rules, the IPsec policy does not take effect.

If the **vpn-instance** keyword is specified in an ACL rule, the rule applies only to VPN packets. If the **vpn-instance** keyword is not specified in an ACL rule, the rule applies only to public network packets.

Examples

Specify IPv4 advanced ACL 3001 for IPsec policy **policy1**.

```
<Sysname> system-view
[Sysname] acl advanced 3001
```

```
[Sysname-acl-ipv4-adv-3001] rule permit tcp source 10.1.1.0 0.0.0.255 destination
10.1.2.0 0.0.0.255
[Sysname-acl-ipv4-adv-3001] quit
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] security acl 3001
```

Specify IPv4 advanced ACL 3002 for IPsec policy **policy2** and specify the data protection mode as aggregation.

```
<Sysname> system-view
[Sysname] acl advanced 3002
[Sysname-acl-ipv4-adv-3002] rule 0 permit ip source 10.1.2.1 0.0.0.255 destination
10.1.2.2 0.0.0.255
[Sysname-acl-ipv4-adv-3002] rule 1 permit ip source 10.1.3.1 0.0.0.255 destination
10.1.3.2 0.0.0.255
[Sysname-acl-ipv4-adv-3002] quit
[Sysname] ipsec policy policy2 1 isakmp
[Sysname-ipsec-policy-isakmp-policy2-1] security acl 3002 aggregation
```

Related commands

display ipsec sa

display ipsec tunnel

smart-link enable

Use **smart-link enable** to enable IPsec smart link selection.

Use **undo smart-link enable** to disable IPsec smart link selection.

Syntax

smart-link enable

undo smart-link enable

Default

IPsec smart link selection is disabled in an IPsec smart link policy.

Views

IPsec smart link policy view

Predefined user roles

network-admin

context-admin

Usage guidelines

The device performs link quality probing and cyclic link switchovers only when IPsec smart link selection is enabled in the IPsec smart link policy. After you disable IPsec smart link selection in the IPsec smart link policy, the IPsec tunnel created based on the policy still takes effect but no link switchover will occur.

Examples

Disable IPsec smart link selection in IPsec smart link policy **smlkpolicy1**.

```
<Sysname> system-view
[Sysname] ipsec smart-link policy smlkpolicy1
[Sysname-ipsec-smart-link-policy-smlkpolicy1] undo smart-link enable
```

Related commands

smart-link policy

smart-link policy

Use **smart-link policy** to apply an IPsec smart link policy to an IPsec policy.

Use **undo smart-link policy** to restore the default.

Syntax

smart-link policy *policy-name*

undo smart-link policy

Default

An IPsec smart link policy is not applied to an IPsec policy.

Views

IPsec policy view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies an existing IPsec smart link policy by its name.

Usage guidelines

An IPsec smart link policy takes effect after it is applied to an IKE-based IPsec policy.

You can apply only one IPsec smart link policy to an IPsec policy.

After the device selects a link to establish the IPsec tunnel, it applies the IPsec policy that uses the IPsec smart link policy to the local interface of the link.

Examples

Apply IPsec smart link policy **smlkpolicy1** to IPsec policy **policy1**.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 1 isakmp
[Sysname-ipsec-policy-isakmp-policy1-1] smart-link policy smlkpolicy1
```

Related commands

smart-link enable

snmp-agent trap enable ipsec

Use **snmp-agent trap enable ipsec** command to enable SNMP notifications for IPsec.

Use **undo snmp-agent trap enable ipsec** command to disable SNMP notifications for IPsec.

Syntax

snmp-agent trap enable ipsec [**auth-failure** | **connection-start** | **connection-stop** | **decrypt-failure** | **encrypt-failure** | **global** | **invalid-sa-failure** | **no-sa-failure** | **policy-add** | **policy-attach** | **policy-delete** | **policy-detach** | **tunnel-start** | **tunnel-stop**] *

undo snmp-agent trap enable ipsec [**auth-failure** | **connection-start** | **connection-stop** | **decrypt-failure** | **encrypt-failure** | **global** | **invalid-sa-failure** | **no-sa-failure** | **policy-add** | **policy-attach** | **policy-delete** | **policy-detach** | **tunnel-start** | **tunnel-stop**] *

Default

All SNMP notifications for IPsec are disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

auth-failure: Specifies notifications about authentication failures.

connection-start: Specifies notifications about successful establishment of the first IPsec tunnel under IPsec policy entries with the same description.

connection-stop: Specifies notifications about successful removal of the last IPsec tunnel under IPsec policy entries with the same description.

decrypt-failure: Specifies notifications about decryption failures.

encrypt-failure: Specifies notifications about encryption failures.

global: Specifies notifications globally.

invalid-sa-failure: Specifies notifications about invalid-SA failures.

no-sa-failure: Specifies notifications about SA-not-found failures.

policy-add: Specifies notifications about events of adding IPsec policies.

policy-attach: Specifies notifications about events of applying IPsec policies to interfaces.

policy-delete: Specifies notifications about events of deleting IPsec policies.

policy-detach: Specifies notifications about events of removing IPsec policies from interfaces.

tunnel-start: Specifies notifications about events of creating IPsec tunnels.

tunnel-stop: Specifies notifications about events of deleting IPsec tunnels.

Usage guidelines

If you do not specify any keywords, this command enables or disables all SNMP notifications for IPsec.

To generate and output SNMP notifications for a specific IPsec failure type or event type, perform the following tasks:

1. Enable SNMP notifications for IPsec globally.
2. Enable SNMP notifications for the failure type or event type.

Examples

Enable SNMP notifications for IPsec globally.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable ipsec global
```

Enable SNMP notifications for events of creating IPsec tunnels.

```
[Sysname] snmp-agent trap enable ipsec tunnel-start
```

tfc enable

Use **tfc enable** to enable Traffic Flow Confidentiality (TFC) padding.

Use **undo tfc enable** to disable TFC padding.

Syntax

tfc enable

undo tfc enable

Default

TFC padding is disabled.

Views

IPsec policy view

IPsec policy template view

Predefined user roles

network-admin

context-admin

Usage guidelines

TFC padding applies only to IPsec SAs negotiated by IKEv2.

TFC padding can hide the length of the original packet, and might affect the packet encapsulation and de-encapsulation performance. This feature takes effect on UDP packets encapsulated by ESP in transport mode and on original IP packets encapsulated by ESP in tunnel mode.

Examples

Enable TFC padding for IPsec policy **policy1**.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 10 isakmp
[Sysname-ipsec-policy-isakmp-policy1-10] tfc enable
```

Related commands

display ipsec ipv6-policy

display ipsec policy

transform-set

Use **transform-set** to specify an IPsec transform set for an IPsec policy, IPsec profile, or IPsec policy template.

Use **undo transform-set** to remove the IPsec transform set specified for an IPsec policy, IPsec profile, or IPsec policy template.

Syntax

transform-set *transform-set-name*&<1-6>

undo transform-set [*transform-set-name*]

Default

No IPsec transform set is specified for an IPsec policy, IPsec profile, or IPsec policy template.

Views

IPsec policy view

IPsec policy template view

IPsec profile view

Predefined user roles

network-admin

context-admin

Parameters

transform-set-name&<1-6>: Specifies a space-separated list of up to six IPsec transform sets. The specified transform set names must be different. A transform set name is a case-insensitive string of 1 to 63 characters.

Usage guidelines

You can specify only one IPsec transform set for a manual IPsec policy. If you execute this command multiple times, the most recent configuration takes effect.

You can specify a maximum of six IPsec transform sets for an IKE-based IPsec policy. During an IKE negotiation, IKE searches for a fully matched IPsec transform set at the two ends of the IPsec tunnel. If no match is found, no SA can be set up, and the packets expecting to be protected will be dropped.

If you do not specify the *transform-set-name* argument, the **undo transform-set** command removes all IPsec transform sets specified for the IPsec policy, IPsec profile, or IPsec policy template.

Examples

Specify IPsec transform set **prop1** for IPsec policy **policy1**.

```
<Sysname> system-view
[Sysname] ipsec transform-set prop1
[Sysname-ipsec-transform-set-prop1] quit
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] transform-set prop1
```

Related commands

ipsec { **ipv6-policy** | **policy** }

ipsec profile

ipsec transform-set

tunnel protection ipsec

Use **tunnel protection ipsec** to apply an IPsec profile to a tunnel interface.

Use **undo tunnel protection ipsec** to restore the default.

Syntax

tunnel protection ipsec profile *profile-name* [**acl** [**ipv6**] { *acl-number* | **name** *acl-name* }]

undo tunnel protection ipsec profile

Default

No IPsec profile is applied to a tunnel interface.

Views

Tunnel interface view

Predefined user roles

network-admin

context-admin

Parameters

profile *profile-name*: Specify an IPsec profile by its name, a case-insensitive string of 1 to 63 characters. The specified IPsec profile must be an IKE-based IPsec profile.

ipv6: Specifies an IPv6 ACL. To specify an IPv4 ACL, do not specify this keyword.

acl-number: Specifies an ACL by its number in the range of 3000 to 3999.

name *acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

After an IPsec profile is applied to a tunnel interface, the peers negotiate an IPsec tunnel through IKE to protect data transmitted through the tunnel interface.

If you specify an ACL when applying an IPsec profile to a tunnel interface, only the ACL-permitted data on the tunnel interface can be protected by IPsec. To protect the traffic of a VPN instance on the tunnel interface, do not specify the VPN instance in the ACL. If you do so, the IPsec profile cannot initiate IPsec negotiation. Instead, you should bind the VPN instance to the tunnel interface. Therefore, the VPN instance of the IPsec SAs negotiated by using the IPsec profile is the VPN instance bound to the tunnel interface.

Specify an IPv4 ACL if the IPsec profile is applied to an IPv4 tunnel interface.

Specify an IPv6 ACL if the IPsec profile is applied to an IPv6 tunnel interface.

Examples

Apply IPsec profile **prf1** to tunnel interface Tunnel 1.

```
<Sysname> system-view
[Sysname] interface tunnel 1 mode advpn gre
[Sysname-Tunnel1] tunnel protection ipsec profile prf1
```

Apply IPsec profile **prf1** to IPv4 tunnel interface Tunnel 1 and use IPv4 ACL 3000 to filter the data to be protected by IPsec on the tunnel interface.

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule 0 permit ip source 1.0.0.0 0.0.0.255 destination 2.0.0.0
0.0.0.255
[Sysname-acl-ipv4-adv-3000] quit
[Sysname] interface tunnel 1 mode ipsec
[Sysname-Tunnel1] tunnel protection ipsec profile prf1 acl 3000
```

Apply IPsec profile **prf1** to IPv6 tunnel interface Tunnel 1 and use IPv6 ACL 3000 to filter the data to be protected by IPsec on the tunnel interface.

```
<Sysname> system-view
[Sysname] acl ipv6 advanced 3000
[Sysname-acl-ipv6-adv-3000] rule 0 permit ipv6 source 1:1::/64 destination 2:2::/64
[Sysname-acl-ipv6-adv-3000] quit
[Sysname] interface tunnel 1 mode ipsec ipv6
[Sysname-Tunnel1] tunnel protection ipsec profile prf1 acl ipv6 3000
```

Related commands

interface tunnel (*VPN Command Reference*)

display interface tunnel (*VPN Command Reference*)

ipsec profile

IKE commands

aaa authorization

Use **aaa authorization** to enable IKE AAA authorization.

Use **undo aaa authorization** to disable IKE AAA authorization.

Syntax

aaa authorization domain *domain-name* **username** *user-name*

undo aaa authorization

Default

IKE AAA authorization is disabled.

Views

IKE profile view

Predefined user roles

network-admin

context-admin

Parameters

domain *domain-name*: Specifies the ISP domain used for requesting authorization attributes. The ISP domain name is a case-insensitive string of 1 to 255 characters and must meet the following requirements:

- The name cannot contain a forward slash (/), backslash (\), vertical bar (|), quotation mark ("), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or an at sign (@).
- The name cannot be **d**, **de**, **def**, **defa**, **defau**, **defaul**, **default**, **i**, **if**, **if-**, **if-u**, **if-un**, **if-unk**, **if-unkn**, **if-unkno**, **if-unknow**, or **if-unknown**.

username *user-name*: Specifies the username used for requesting authorization attributes. The username is a case-sensitive string of 1 to 55 characters and must meet the following requirements:

- The username cannot contain the domain name.
- The username cannot contain a forward slash (/), backslash (\), vertical bar (|), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or an at sign (@).
- The username cannot be **a**, **al**, or **all**.

Usage guidelines

The AAA authorization feature enables IKE to request authorization attributes, such as the IKE address pool, from AAA.

IKE uses the ISP domain and username to request authorization attributes. AAA uses the authorization settings in the ISP domain to request the user's authorization attributes from the remote AAA server or the local user database. After IKE passes the username authentication, it obtains the authorization attributes.

This feature is applicable when AAA is used to centrally manage and deploy authorization attributes.

Examples

Create IKE profile **profile1**.

```
<Sysname> system-view
```

```
[Sysname] ike profile profile1
```

Enable AAA authorization. Specify ISP domain **abc** and username **test**.

```
[Sysname-ike-profile-profile1] aaa authorization domain abc username test
```

app-dev-info

Use **app-dev-info** to specify a GD-quantum access ID.

Use **undo app-dev-info** to restore the default.

Syntax

app-dev-info *app-dev-info*

undo app-dev-info

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480	Yes
NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	No

Default

No GD-quantum access ID is specified.

Views

IKE GD-quantum view

Predefined user roles

network-admin

context-admin

Parameters

app-dev-info: Specifies a GD-quantum access ID, a nine-digit string.

Usage guidelines

The GD-quantum access IDs are uniformly distributed by the GD-quantum server, unique one for each device. You can use a GD-quantum access ID and a GD-quantum authentication key to log in to the GD-quantum server.

To obtain a GD-quantum access ID, contact the administrator of the GD-quantum server.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure the GD-quantum access ID **185110851**.

```
<Sysname> system-view
[Sysname] ike gd-quantum
[Sysname-ike-gdquantum] app-dev-info 185110851
```

authentication-algorithm

Use **authentication-algorithm** to specify an authentication algorithm for an IKE proposal.

Use **undo authentication-algorithm** to restore the default.

Syntax

authentication-algorithm { **md5** | **sha** | **sha256** | **sha384** | **sha512** | **sm3** }

undo authentication-algorithm

Default

The IKE proposal uses the HMAC-SHA1 authentication algorithm.

Views

IKE proposal view

Predefined user roles

network-admin

context-admin

Parameters

md5: Specifies the HMAC-MD5 algorithm.

sha: Specifies the HMAC-SHA1 algorithm.

sha256: Specifies the HMAC-SHA256 algorithm.

sha384: Specifies the HMAC-SHA384 algorithm.

sha512: Specifies the HMAC-SHA512 algorithm.

sm3: Specifies the HMAC-SM3 algorithm.

Examples

Specify HMAC-SHA1 as the authentication algorithm for IKE proposal 1.

```
<Sysname> system-view
[Sysname] ike proposal 1
[Sysname-ike-proposal-1] authentication-algorithm sha
```

Related commands

display ike proposal

authentication-method

Use **authentication-method** to specify an authentication method to be used in an IKE proposal.

Use **undo authentication-method** to restore the default.

Syntax

authentication-method { **dsa-signature** | **pre-share** | **rsa-de** | **rsa-signature** | **sm2-de** }

undo authentication-method

Default

The preshared key authentication method is used.

Views

IKE proposal view

Predefined user roles

network-admin

context-admin

Parameters

dsa-signature: Specifies the DSA signature authentication method.

pre-share: Specifies the preshared key authentication method.

rsa-de: Specifies the RSA digital envelope authentication method.

rsa-signature: Specifies the RSA signature authentication method.

sm2-de: Specifies the SM2 digital envelope authentication method.

Usage guidelines

Preshared key authentication does not require certificates as signature authentication does, and it is usually used on a simple network.

Signature authentication provides higher security, and it is usually deployed on a large-scale network, such as a network with many branches.

On a network with many branches, using preshared key authentication requires the headquarters to configure a preshared key for each branch. Using signature authentication only requires the headquarters to configure one PKI domain.

The digital envelope authentication method is supported only in IKEv1 and must be used if the device is subject to China OSCCA regulations.

Authentication methods configured on both IKE ends must match.

If you specify the RSA or DSA signature authentication method, you must configure the IKE peer to obtain certificates from a CA.

If you specify the preshared key authentication method, you must configure the same preshared key on both IKE ends.

Examples

Specify the preshared key authentication method for IKE proposal 1.

```
<Sysname> system-view
[Sysname] ike proposal 1
[Sysname-ike-proposal-1] authentication-method pre-share
```

Related commands

display ike proposal

ike keychain

pre-shared-key

auth-key

Use **auth-key** to configure a GD-quantum authentication key.

Use **undo auth-key** to restore the default.

Syntax

auth-key { **cipher** | **simple** } *key-value*

undo auth-key

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480	Yes
NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	No

Default

No GD-quantum authentication key is configured.

Views

IKE GD-quantum view

Predefined user roles

network-admin

context-admin

Parameters

cipher: Specifies a GD-quantum authentication key in encrypted form.

simple: Specifies a GD-quantum authentication key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

key-value: Specifies the GD-quantum authentication key. The key is case sensitive. Its plaintext form is a 64-bit hexadecimal number, and its encrypted form is a 117-bit hexadecimal number.

Usage guidelines

The GD-quantum authentication keys are used by the GD-quantum server for identity authentication. Each GD-quantum authentication key corresponds to one GD-quantum access ID (specified by using the **app-dev-info** command). Only devices with correct GD-quantum access IDs and GD-quantum authentication keys can successfully log in to the GD-quantum server when sending login requests to the server.

To obtain a GD-quantum authentication key, contact the administrator of the GD-quantum server.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure the GD-quantum authentication key **0x66c7f0f462eeedd9d1f2d46bdc10e4e24167c4875cf2f7a2297da02b8f4ba8e0** for logging in to the GD-quantum server.

```
<Sysname> system-view
[Sysname] ike gd-quantum
[Sysname-ike-gdquantum] auth-key simple
66c7f0f462eeedd9d1f2d46bdc10e4e24167c4875cf2f7a2297da02b8f4ba8e0
```

certificate domain

Use **certificate domain** to specify a PKI domain for signature authentication.

Use **undo certificate domain** to remove a PKI domain for signature authentication.

Syntax

certificate domain *domain-name*

undo certificate domain *domain-name*

Default

No PKI domains are specified for signature authentication.

Views

IKE profile view

Predefined user roles

network-admin

context-admin

Parameters

domain-name: Specifies the name of a PKI domain, a case-insensitive string of 1 to 31 characters.

Usage guidelines

You can specify a maximum of six PKI domains for an IKE profile by executing this command multiple times.

IKE uses the specified PKI domains for enrollment, authentication, certificate issuing, validation, and signature. If you do not specify any PKI domains, IKE uses all PKI domains configured on the device.

Follow these restrictions and guidelines for the device to obtain the CA certificate during IKE negotiation:

- On the initiator:
  - If the IKE profile has a PKI domain and the automatic certificate request mode is configured for the PKI domain, the initiator automatically obtains the CA certificate.
  - If the IKE profile has no PKI domain, you must manually obtain the CA certificate.
- On the responder:
  - If main mode is used in IKE phase 1, the responder does not automatically obtain the CA certificate. You must manually obtain the CA certificate.
  - If aggressive mode is used in IKE phase 1, the responder automatically obtains the CA certificate if the following conditions are met:
    - A matching IKE profile is found.
    - An PKI domain is specified in the IKE profile.
    - The automatic certificate request mode is configured for the PKI domain.

    If the conditions are not met, you must manually obtain the CA certificate.

IKE first automatically obtains the CA certificate, and then requests a local certificate. If the CA certificate already exists locally, IKE automatically requests a local certificate.

Examples

Specify PKI domain **abc** for IKE profile 1.

```
<Sysname> system-view
[Sysname] ike profile 1
[Sysname-ike-profile-1] certificate domain abc
```

Related commands

authentication-method

pki domain

client-authentication

Use **client-authentication** to enable client authentication.

Use **undo client-authentication** to disable client authentication.

Syntax

client-authentication xauth

undo client-authentication xauth

Default

Client authentication is disabled.

Views

IKE profile view

Predefined user roles

network-admin

context-admin

Parameters

xauth: Uses Extended Authentication within ISAKMP/Oakley (XAUTH) for authentication.

Usage guidelines

Client authentication enables an IPsec gateway to authenticate remote users through a RADIUS server in IKE negotiation. Remote users who provide the correct username and password pass the authentication and continue with the IKE negotiation. This feature simplifies the configuration on the IPsec gateway and ensures the validity of the remote users. If you do not use this feature, you must configure an IPsec policy and an authentication password for each remote user.

Examples

Enable XAUTH client authentication.

```
<Sysname> system-view
[Sysname] ike profile test
[Sysname-ike-profile-test] client-authentication xauth
```

Related commands

local-user

client-authentication xauth user

Use **client-authentication xauth user** to specify the username and password for client authentication.

Use **undo client-authentication xauth user** to restore the default.

Syntax

client-authentication xauth user *username* **password** { **cipher** | **simple** } string

undo client-authentication xauth user

Default

The username and password for client authentication are not specified.

Views

IKE profile view

Predefined user roles

network-admin

context-admin

Parameters

username: Specifies the username for client authentication. The username is a case-sensitive string of 1 to 55 characters and must meet the following requirements:

- The username cannot contain a forward slash (/), backslash (\), vertical bar (|), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or an at sign (@).
- The username cannot be **a**, **al**, or **all**.

password: Specifies the password for client authentication.

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password string. Its plaintext form is a case-sensitive string of 1 to 63 characters. Its encrypted form is a case-sensitive string of 1 to 110 characters.

Usage guidelines

Configure this command in the IKE profile used by a branch gateway. The branch gateway can then use the username and password to pass AAA authentication and establish an IPsec tunnel with the IPsec gateway at the enterprise center.

Examples

Specify username **abc** and password **123456TESTplat&!** for client authentication.

```
<Sysname> system-view
[Sysname] ike profile test
[Sysname-ike-profile-test] client-authentication xauth user abc password simple
123456TESTplat&!
```

decrypt-quantum-key

Use **decrypt-quantum-key** to configure a GD-quantum decryption key.

Use **undo decrypt-quantum-key** to restore the default.

Syntax

decrypt-quantum-key { **cipher** | **simple** } *key-value*

undo decrypt-quantum-key

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480	Yes
NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	No

Default

No GD-quantum decryption key is configured.

Views

IKE GD-quantum view

Predefined user roles

network-admin

context-admin

Parameters

cipher: Specifies a GD-quantum decryption key in encrypted form.

simple: Specifies a GD-quantum decryption key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

key-value: Specifies the GD-quantum decryption key. The key is case sensitive. Its plaintext form is a 64-bit hexadecimal number, and its encrypted form is a 117-bit hexadecimal number.

Usage guidelines

A device can request encrypted GD-quantum keys from the GD-quantum server after successfully logging in to the server. Use this command to configure GD-quantum decryption keys for decryption so as to be used in IPsec.

To obtain a GD-quantum decryption key, contact the administrator of the GD-quantum server.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure the GD-quantum decryption key **0x66c7f0f462eeedd9d1f2d46bdc10e4e24167c4875cf2f7a2297da02b8f4ba8e0**.

```
<Sysname> system-view
[Sysname] ike gd-quantum
[Sysname-ike-gdquantum] decrypt-quantum-key simple
66c7f0f462eeedd9d1f2d46bdc10e4e24167c4875cf2f7a2297da02b8f4ba8e0
```

description

Use **description** to configure a description for an IKE proposal.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

An IKE proposal does not have a description.

Views

IKE proposal view

Predefined user roles

network-admin

context-admin

Parameters

text: Specifies the description, a case-sensitive string of 1 to 80 characters.

Usage guidelines

When multiple IKE proposals exist, you configure different descriptions for them to distinguish them.

Examples

Configure a description of **test** for IKE proposal 1.

```
<Sysname> system-view
[Sysname] ike proposal 1
[Sysname-ike-proposal-1] description test
```

dh

Use **dh** to specify the DH group to be used for key negotiation in IKE phase 1.

Use **undo dh** to restore the default.

Syntax

dh { **group1** | **group14** | **group2** | **group24** | **group5** }

undo dh

Default

The 768-bit Diffie-Hellman group (**group1**) is used.

Views

IKE proposal view

Predefined user roles

network-admin

context-admin

Parameters

group1: Uses the 768-bit Diffie-Hellman group.

group14: Uses the 2048-bit Diffie-Hellman group.

group2: Uses the 1024-bit Diffie-Hellman group.

group24: Uses the 2048-bit Diffie-Hellman group with the 256-bit prime order subgroup.

group5: Uses the 1536-bit Diffie-Hellman group.

Usage guidelines

A DH group with a higher group number provides higher security but needs more time for processing. To achieve the best trade-off between processing performance and security, choose a proper Diffie-Hellman group for your network.

Examples

Specify the 2048-bit Diffie-Hellman group **group1** to be used for key negotiation in IKE phase 1 in IKE proposal 1.

```
<Sysname> system-view
[Sysname] ike proposal 1
[Sysname-ike-proposal-1] dh group14
```

Related commands

display ike proposal

display ike proposal

Use **display ike proposal** to display configuration information about all IKE proposals.

Syntax

display ike proposal

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Usage guidelines

This command displays the configuration information about all IKE proposals in descending order of proposal priorities. If no IKE proposal is configured, this command displays the default IKE proposal.

Examples

Display the configuration information about all IKE proposals.

```
<Sysname> display ike proposal
 Priority Authentication Authentication Encryption  Diffie-Hellman Duration
              method       algorithm    algorithm       group      (seconds)
------------------------------------------------------------------------------
 1        RSA-SIG            SHA1        DES-CBC     Group 1        5000
 11       PRE-SHARED-KEY     SHA1        DES-CBC     Group 1        50000
 default  PRE-SHARED-KEY     SHA1       DES-CBC     Group 1        86400
```

Table 12 Command output

Field	Description
Priority	Priority of the IKE proposal
Authentication method	Authentication method used by the IKE proposal.
Authentication algorithm	Authentication algorithm used in the IKE proposal: • **MD5**—HMAC-MD5 algorithm. • **SHA1**—HMAC-SHA1 algorithm. • **SHA256**—HMAC-SHA256 algorithm. • **SHA384**—HMAC-SHA384 algorithm. • **SHA512**—HMAC-SHA512 algorithm. • **SM3**—HMAC-SM3 algorithm.
Encryption algorithm	Encryption algorithm used by the IKE proposal: • **3DES-CBC**—168-bit 3DES algorithm in CBC mode. • **AES-CBC-128**—128-bit AES algorithm in CBC mode. • **AES-CBC-192**—192-bit AES algorithm in CBC mode. • **AES-CBC-256**—256-bit AES algorithm in CBC mode. • **DES-CBC**—56-bit DES algorithm in CBC mode. • **SM1-CBC-128**—128-bit SM1 algorithm in CBC mode. • **SM4-CBC**—128-bit SM4 algorithm in CBC mode.
Diffie-Hellman group	DH group used in IKE negotiation phase 1.
Duration (seconds)	IKE SA lifetime (in seconds) of the IKE proposal

Related commands

ike proposal

display ike sa

Use **display ike sa** to display information about IKE SAs.

Syntax

display ike sa [**verbose** [**connection-id** *connection-id* | **remote-address** [**ipv6**] *remote-address* [**vpn-instance** *vpn-instance-name*]]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

verbose: Displays detailed information.

connection-id *connection-id*: Displays detailed information about IKE SAs by connection ID in the range of 1 to 2000000000.

remote-address: Displays detailed information about IKE SAs with the specified remote address.

ipv6: Specifies an IPv6 address.

remote-address: Remote IP address.

vpn-instance *vpn-instance-name*: Displays detailed information about IKE SAs in an MPLS L3VPN instance. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays detailed information about IKE SAs for the public network.

Usage guidelines

If you do not specify any parameters, this command displays summary information about all IKE SAs.

Examples

Display summary information about all IKE SAs.

```
<Sysname> display ike sa
    Connection-ID  Remote          Flag        DOI
  -------------------------------------------------------------
      1            202.38.0.2/500  RD          IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY
```

Table 13 Command output

Field	Description
Connection-ID	Identifier of the IKE SA.

Field	Description
Remote	Remote IP address and port number of the SA.
Flags	Status of the SA: • **RD--READY**—The SA has been established. • **RL--REPLACED**—The SA has been replaced by a new one and will be deleted later. • **FD-FADING**—The SA is in use, but it is about to expire and will be deleted soon. • **RK-REKEY**—The SA is a Rekey SA. • **Unknown**—The SA status is unknown.
DOI	Interpretation domain to which the SA belongs. **IPsec**—The SA belongs to an IPsec DOI.

Display detailed information about all IKE SAs.

```
<Sysname> display ike sa verbose
    -----------------------------------------
    Connection ID: 2
    Outside VPN: 1
    Inside VPN: 1
    Profile: prof1
    Transmitting entity: Initiator
    Initiator cookie: 1bcf453f0a217259
    Responder cookie: 5e32a74dfa66a0a4
    -----------------------------------------
    Local IP/port: 4.4.4.4/500
    Local ID type: IPV4_ADDR
    Local ID: 4.4.4.4

    Remote IP/port: 4.4.4.5/500
    Remote ID type: IPV4_ADDR
    Remote ID: 4.4.4.5

    Authentication-method: PRE-SHARED-KEY
    Authentication-algorithm: SHA1
    Encryption-algorithm: AES-CBC-128

    Life duration(sec): 86400
    Remaining key duration(sec): 86379
    Exchange-mode: Main
    Diffie-Hellman group: Group 1
    NAT traversal: Not detected

    Extend authentication: Enabled
    Assigned IP address: 192.168.2.1
    Vendor ID index: 0xa1d
    Vendor ID sequence number: 0x0
```

Display detailed information about the IKE SA with a remote address of 4.4.4.5.

```
<Sysname> display ike sa verbose remote-address 4.4.4.5
    ----------------------------------------------
    Connection ID: 2
    Outside VPN: 1
    Inside VPN: 1
    Profile: prof1
    Transmitting entity: Initiator
    Initiator cookie: 1bcf453f0a217259
    Responder cookie: 5e32a74dfa66a0a4
    ----------------------------------------------
    Local IP/port: 4.4.4.4/500
    Local ID type: IPV4_ADDR
    Local ID: 4.4.4.4

    Remote IP/port: 4.4.4.5/500
    Remote ID type: IPV4_ADDR
    Remote ID: 4.4.4.5

    Authentication-method: PRE-SHARED-KEY
    Authentication-algorithm: SHA1
    Encryption-algorithm: AES-CBC-128

    Life duration(sec): 86400
    Remaining key duration(sec): 86379
    Exchange-mode: Main
    Diffie-Hellman group: Group 1
    NAT traversal: Not detected

    Extend authentication: Enabled
    Assigned IP address: 192.168.2.1
    Vendor ID index: 0xa1d
    Vendor ID sequence number: 0x0
```

Table 14 Command output

Field	Description
Connection ID	Identifier of the IKE SA.
Outside VPN	VPN instance name of the MPLS L3VPN to which the receiving interface belongs.
Inside VPN	VPN instance name of the MPLS L3VPN to which the protected data belongs.
Profile	Name of the matching IKE profile found in the IKE SA negotiation. If no matching profile is found, this field displays nothing.
Transmitting entity	Role of the IKE negotiation entity: **Initiator** or **Responder**.
Initiator cookie	IKE SA initiator cookie.
Responder cookie	IKE SA responder cookie.
Local IP/port	IP address and port number of the local gateway.

Field	Description
Local ID type	Identifier type of the local gateway.
Local ID	Identifier of the local gateway.
Remote IP/port	IP address and port number of the remote gateway.
Remote ID type	Identifier type of the remote gateway.
Remote ID	Identifier of the remote security gateway.
Authentication-method	Authentication method used by the IKE proposal: • **DSA-SIG**—DSA signature. • **PRE-SHARED-KEY**—Preshared key. • **RSA-DE**—RSA digital envelop. • **RSA-SIG**—RSA signature. • **SM2-DE**—SM2 digital envelop.
Authentication-algorithm	Authentication algorithm used by the IKE proposal: • **MD5**—HMAC-MD5 algorithm. • **SHA1**—HMAC-SHA1 algorithm. • **SHA256**—HMAC-SHA256 algorithm. • **SHA384**—HMAC-SHA384 algorithm. • **SHA512**—HMAC-SHA512 algorithm. • **SM3**—HMAC-SM3 algorithm.
Encryption-algorithm	Encryption algorithm used by the IKE proposal: • **3DES-CBC**—168-bit 3DES algorithm in CBC mode. • **AES-CBC-128**—128-bit AES algorithm in CBC mode. • **AES-CBC-192**—192-bit AES algorithm in CBC mode. • **AES-CBC-256**—256-bit AES algorithm in CBC mode. • **DES-CBC**—56-bit DES algorithm in CBC mode. • **SM1-CBC-128**—128-bit SM1 algorithm in CBC mode. • **SM4-CBC**—128-bit SM4 algorithm in CBC mode.
Life duration(sec)	Lifetime of the IKE SA in seconds.
Remaining key duration(sec)	Remaining lifetime of the IKE SA in seconds.
Exchange-mode	IKE negotiation mode in phase 1: **Main**, **GM-main**, or **Aggressive**.
Diffie-Hellman group	DH group used for key negotiation in IKE phase 1. This field is not displayed if the IKE negotiation mode in phase 1 is GM main.
NAT traversal	Whether a NAT gateway is detected.
Extend authentication	Whether extended authentication for clients is enabled.
Assigned IP address	IP address assigned to the remote peer. This field is not displayed if no IP address is assigned.
Vendor ID index	Vendor ID index used when the IKE negotiation was triggered.
Vendor ID sequence number	Vendor ID sequence number used when the IKE negotiation was triggered.

display ike statistics

Use **`display ike statistics`** to display IKE statistics.

Syntax

display ike statistics

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display IKE statistics.

```
<Sysname> display ike statistics
IKE statistics:
  No matching proposal: 0
  Invalid ID information: 0
  Unavailable certificate: 0
  Unsupported DOI: 0
  Unsupported situation: 0
  Invalid proposal syntax: 0
  Invalid SPI: 0
  Invalid protocol ID: 0
  Invalid certificate: 0
  Authentication failure: 0
  Invalid flags: 0
  Invalid message id: 0
  Invalid cookie: 0
  Invalid transform ID: 0
  Malformed payload: 0
  Invalid key information: 0
  Invalid hash information: 0
  Unsupported attribute: 0
  Unsupported certificate type: 0
  Invalid certificate authority: 0
  Invalid signature: 0
  Unsupported exchange type: 0
  No available SA: 1
  Retransmit timeout: 0
  Not enough memory: 0
  Enqueue fails: 0
  Failures to send R_U_THERE DPD packets: 0
  Failures to receive R_U_THERE DPD packets: 0
  Failures to send ACK DPD packets: 0
  Failures to receive ACK DPD packets: 0
  Sent P1 SA lifetime change packets: 0
  Received P1 SA lifetime change packets: total=0, process failures=0 (no SA=0, failures
to reset SA soft lifetime=0, failures to reset SA hard lifetime=0)
```

```
Sent P2 SA lifetime change packets: 0
Received P2 SA lifetime change packets: total=0, process failures=0
```

Related commands

reset ike statistics

dpd

Use **dpd** to configure IKE DPD.

Use **undo dpd** to disable IKE DPD.

Syntax

dpd interval *interval* [**retry** *seconds*] { **on-demand** | **periodic** }

undo dpd interval

Default

IKE DPD is disabled.

Views

IKE profile view

Predefined user roles

network-admin

context-admin

Parameters

interval *interval*: Specifies a DPD triggering interval in the range of 1 to 300 seconds.

retry *seconds*: Specifies the DPD retry interval in the range of 1 to 60 seconds. The default is 5 seconds.

on-demand: Triggers DPD on demand. The device triggers DPD if it has IPsec traffic to send and has not received any IPsec packets from the peer for the specified interval.

periodic: Triggers DPD at regular intervals. The device triggers DPD at the specified interval.

Usage guidelines

DPD is triggered periodically or on-demand. As a best practice, use the on-demand mode when the device communicates with a large number of IKE peers. For an earlier detection of dead peers, use the periodic triggering mode, which consumes more bandwidth and CPU.

When DPD settings are configured in both IKE profile view and system view, the DPD settings in IKE profile view apply. If DPD is not configured in IKE profile view, the DPD settings in system view apply.

It is a good practice to set the triggering interval longer than the retry interval so that a DPD detection does not occur during a DPD retry.

Examples

Configure DPD to be triggered every 10 seconds and every 5 seconds between retries if the peer does not respond.

```
<Sysname> system-view
[Sysname] ike profile 1
[Sysname-ike-profile-1] dpd interval 10 retry 5 on-demand
```

Related commands

ike dpd

encryption-algorithm

Use **encryption-algorithm** to specify an encryption algorithm for an IKE proposal.

Use **undo encryption-algorithm** to restore the default.

Syntax

encryption-algorithm { **3des-cbc** | **aes-cbc-128** | **aes-cbc-192** | **aes-cbc-256** | **des-cbc** | **sm1-cbc-128** | **sm4-cbc** }

undo encryption-algorithm

Default

An IKE proposal uses the 56-bit DES encryption algorithm in CBC mode.

Views

IKE proposal view

Predefined user roles

network-admin

context-admin

Parameters

3des-cbc: Specifies the 3DES algorithm in CBC mode. The 3DES algorithm uses a 168-bit key for encryption.

aes-cbc-128: Specifies the AES algorithm in CBC mode. The AES algorithm uses a 128-bit key for encryption.

aes-cbc-192: Specifies the AES algorithm in CBC mode. The AES algorithm uses a 192-bit key for encryption.

aes-cbc-256: Specifies the AES algorithm in CBC mode. The AES algorithm uses a 256-bit key for encryption.

des-cbc: Specifies the DES algorithm in CBC mode. The DES algorithm uses a 56-bit key for encryption.

sm1-cbc-128: Specifies the SM1 algorithm in CBC mode. The SM1 algorithm uses a 128-bit key for encryption.

sm4-cbc: Uses the SM4 algorithm in CBC mode as the encryption algorithm. The SM4 algorithm uses a 128-bit key.

Examples

Use the 128-bit AES algorithm in CBC mode as the encryption algorithm for IKE proposal 1.

```
<Sysname> system-view
[Sysname] ike proposal 1
[Sysname-ike-proposal-1] encryption-algorithm aes-cbc-128
```

Related commands

display ike proposal

exchange-mode

Use **exchange-mode** to select an IKE negotiation mode for phase 1.

Use **undo exchange-mode** to restore the default.

Syntax

exchange-mode { **aggressive** | **gm-main** | **main** }

undo exchange-mode

Default

Main mode is used for phase 1.

Views

IKE profile view

Predefined user roles

network-admin

context-admin

Parameters

aggressive: Specifies the aggressive mode.

gm-main: Specifies the GM main mode.

main: Specifies the main mode.

Usage guidelines

As a best practice, specify the **aggressive** mode at the local end if the following conditions are met:

- The local end, for example, a dialup user, obtains an IP address automatically.
- Preshared key authentication is used.

If you specify the GM main mode for phase 1 IKE negotiation, make sure the authentication method is RSA-DE or SM2-DE digital envelope authentication.

Examples

Specify that IKE negotiation operates in GM main mode.

```
<Sysname> system-view
[Sysname] ike profile 1
[Sysname-ike-profile-1] exchange-mode gm-main
```

Specify that IKE negotiation operates in main mode.

```
<Sysname> system-view
[Sysname] ike profile 1
[Sysname-ike-profile-1] exchange-mode main
```

Related commands

display ike proposal

ike address-group

Use **ike address-group** to configure an IKE IPv4 address pool for assigning IPv4 addresses to remote peers.

Use **undo ike address-group** to delete an IKE IPv4 address pool.

Syntax

ike address-group *group-name start-ipv4-address end-ipv4-address* [*mask* | *mask-length*]

undo ike address-group *group-name*

Default

No IKE IPv4 address pools exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a name for the IKE IPv4 address pool, a case-insensitive string of 1 to 63 characters.

start-ipv4-address end-ipv4-address: Specifies an IPv4 address range. The *start-ipv4-address* argument specifies the start IPv4 address. The *end-ipv4-address* argument specifies the end IPv4 address.

mask: Specifies the IPv4 address mask.

mask-length: Specifies the length of the IPv4 address mask.

Usage guidelines

An IKE IPv4 address pool can contain a maximum of 8192 IPv4 addresses.

To modify or delete an address pool, you must delete all IKE SAs and IPsec SAs. Otherwise, the assigned IPv4 addresses might not be reclaimed.

Examples

Configure an IKE IPv4 address pool with name **ipv4group**, address range 1.1.1.1 to 1.1.1.2, and mask 255.255.255.0.

```
<Sysname> system-view
[Sysname] ike address-group ipv4group 1.1.1.1 1.1.1.2 255.255.255.0
```

Configure an IKE IPv4 address pool with name **ipv4group**, address range 1.1.1.1 to 1.1.1.2, and mask length 32.

```
<Sysname> system-view
[Sysname] ike address-group ipv4group 1.1.1.1 1.1.1.2 32
```

Related commands

aaa authorization

ike compatible-gm-main enable

Use **ike compatible-gm-main enable** to enable GM main mode compatibility.

Use **undo ike compatible-gm-main enable** to restore the default.

Syntax

ike compatible-gm-main enable

undo ike compatible-gm-main enable

Default

The GM main mode compatibility is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

IKE peers running different software versions might have the GM main mode compatibility issue (signature verification failure) during IKE negotiation. If the device encounters this issue with its peer, you can execute this command on the device.

Do not execute this command on the device if the device does not have the GM main mode compatibility issue with its peers.

Examples

Enable GM main mode compatibility.

```
<Sysname> system-view
[Sysname] ike compatible-gm-main enable
```

ike compatible-sm4 enable

Use **ike compatible-sm4 enable** to enable SM4-CBC key length compatibility.

Use **undo ike compatible-sm4 enable** to restore the default.

Syntax

ike compatible-sm4 enable

undo ike compatible-sm4 enable

Default

SM4-CBC key length compatibility is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

By default, IKE negotiation between two peers using the SM4-CBC encryption algorithm will fail if the peers use different SM4-CBC key lengths. You can enable SM4-CBC key length compatibility so the local IKE peer can successfully negotiate with a remote peer that uses a different SM4-CBC key length.

Examples

Enable SM4-CBC key length compatibility.

```
<Sysname> system-view
[Sysname] ike compatible-sm4 enable
```

ike dpd

Use **ike dpd** to configure global IKE DPD.

Use **undo ike dpd** to disable global IKE DPD.

Syntax

ike dpd interval *interval* [**retry** *seconds*] { **on-demand** | **periodic** }

undo ike dpd interval

Default

Global IKE DPD is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interval *interval*: Specifies a DPD triggering interval in the range of 1 to 300 seconds.

retry *seconds*: Specifies the DPD retry interval in the range of 1 to 60 seconds. The default is 5 seconds.

on-demand: Triggers DPD on demand. The device triggers DPD if it has IPsec traffic to send and has not received any IPsec packets from the peer for the specified interval.

periodic: Triggers DPD at regular intervals. The device triggers DPD at the specified interval.

Usage guidelines

DPD is triggered periodically or on-demand. As a best practice, use the on-demand mode when the device communicates with a large number of IKE peers. For an earlier detection of dead peers, use the periodical triggering mode, which consumes more bandwidth and CPU.

When DPD settings are configured in both IKE profile view and system view, the DPD settings in IKE profile view apply. If DPD is not configured in IKE profile view, the DPD settings in system view apply.

It is a good practice to set the triggering interval longer than the retry interval so that a DPD detection does not occur during a DPD retry.

Examples

Configure DPD to be triggered every 10 seconds and every 5 seconds between retries if the peer does not respond.

```
<Sysname> system-view
[Sysname] ike dpd interval 10 retry 5 on-demand
```

Related commands

dpd

ike gd-quantum

Use **ike gd-quantum** to enable GD-quantum encryption for IKE and enter IKE GD-quantum view.

Use **undo ike gd-quantum** to disable GD-quantum encryption for IKE.

Syntax

ike gd-quantum

undo ike gd-quantum

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480	Yes
NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	No

Default

GD-quantum encryption for IKE is disabled.

Views

system view

Predefined user roles

network-admin

context-admin

Usage guidelines

After enabling GD-quantum encryption for IKE, the device can use the symmetric key provided by the GD-quantum server to encrypt the IPsec protected data, which further enhance the security of IPsec.

The device obtains keys from the GD-quantum server in the following steps:

1. **Connecting the GD-quantum server**—After all commands in IKE GD-quantum view are configured, the device establishes a connection with the specified GD-quantum server.
2. **Logging in to the GD-quantum server**—After the connection is established, the device sends a login request to the GD-quantum server, carrying the GD-quantum access ID and the GD-quantum authentication key. Only devices with verified GD-quantum access IDs and GD-quantum authentication keys can successfully log in to the GD-quantum server.
3. **Obtaining the GD-quantum keys**—After successful login and the IKE phase 1 negotiation, the device obtains the encrypted GD-quantum keys from the GD-quantum server, decrypt them with the GD-quantum decryption keys configured on the device, and finally obtain the GD-quantum keys for IPsec.

When enabling GD-quantum encryption for IKE, the device enters IKE GD-quantum view. Configure the IP address and port number of the GD-quantum server, the GD-quantum access IDs and GD-quantum authentication keys, and the GD-quantum decryption keys in this view.

Examples

Enable GD-quantum encryption for IKE and enter IKE GD-quantum view.

```
<Sysname> system-view
[Sysname] ike gd-quantum
[Sysname-ike-gdquantum]
```

ike gm-main sm4-version

Use **ike gm-main sm4-version** to specify the SM4 algorithm version used in IKE GM main negotiation.

Use **undo ike gm-main sm4-version** to restore the default.

Syntax

ike gm-main sm4-version { **draft** | **standard** }

undo ike gm-main sm4-version

Default

The standard SM4 algorithm is used in IKE GM main negotiation.

Views

IKE profile view

Predefined user roles

network-admin

context-admin

Parameters

draft: Specifies the draft version of the SM4 algorithm. The attribute value for the standard SM4 is 127.

standard: Specifies the standard version of the SM4 algorithm. The attribute value for the standard SM4 is 129.

Usage guidelines

Specify the SM4 version used by the device to initiate an IKE negotiation with a device from other vendors to make sure the two devices use the same SM4 version in the negotiation.

This command takes effect only on negotiations for new IKE SAs. It does not apply to existing IKE SAs.

Examples

In IKE profile view, configure the IKE GM main negotiation to use the draft SM4 algorithm.

```
<Sysname> system-view
[Sysname] ike profile prof1
[Sysname-ike-profile-prof1] ike gm-main sm4-version draft
```

ike identity

Use **ike identity** to specify the global identity used by the local end during IKE negotiations.

Use **undo ike identity** to restore the default.

Syntax

ike identity { **address** { *ipv4-address* | **ipv6** *ipv6-address* }| **dn** | **fqdn** [*fqdn-name*] | **user-fqdn** [*user-fqdn-name*] }

undo ike identity

Default

The IP address of the interface where the IPsec policy applies is used as the IKE identity.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

address { *ipv4-address* | **ipv6** *ipv6-address* }: Uses an IPv4 or IPv6 address as the identity.

dn: Uses the DN in the digital signature as the identity.

fqdn *fqdn-name*: Uses the FQDN name as the identity. The *fqdn-name* argument is a case-sensitive string of 1 to 255 characters, for example, www.test.com. If you do not specify this argument, the device name configured by using the **sysname** command is used as the local FQDN.

user-fqdn *user-fqdn-name*: Uses the user FQDN name as the identity. The *user-fqdn-name* argument is a case-sensitive string of 1 to 255 characters, for example, abc@test.com. If you do not specify this argument, the device name configured by using the **sysname** command is used as the user FQDN.

Usage guidelines

The global local identity can be used for all IKE SA negotiations. The local identity (set by the **local-identity** command for an IKE profile) can be used only for IKE SA negotiations that use the IKE profile.

If the local authentication method is signature authentication, you can set an identity of any type. If the local authentication method is preshared key authentication, you cannot set the DN as the identity.

The **ike signature-identity from-certificate** command sets the local device to always use the identity information obtained from the local certificate for signature authentication. If the **ike signature-identity from-certificate** command is not set, the **local-identity** command configuration, if configured, takes precedence over the **ike identity** command configuration.

Examples

Specify IP address 2.2.2.2 as the identity.

```
<sysname> system-view
[sysname] ike identity address 2.2.2.2
```

Related commands

local-identity

ike signature-identity from-certificate

ike invalid-spi-recovery enable

Use **ike invalid-spi-recovery enable** to enable invalid security parameter index (SPI) recovery.

Use **undo ike invalid-spi-recovery enable** to disable invalid SPI recovery.

Syntax

ike invalid-spi-recovery enable

undo ike invalid-spi-recovery enable

Default

Invalid SPI recovery is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

IPsec "black hole" occurs when one IPsec peer fails (for example, a peer can fail if a reboot occurs). One peer fails and loses its SAs with the other peer. When an IPsec peer receives a data packet for which it cannot find an SA, an invalid SPI is encountered. The peer drops the data packet and tries to send an SPI invalid notification to the data originator. This notification is sent by using the IKE SA. When no IKE SA is available, the notification is not sent. The originating peer continues sending the data by using the IPsec SA that has the invalid SPI, and the receiving peer keeps dropping the traffic.

The invalid SPI recovery feature enables the receiving peer to set up an IKE SA with the originator so that an SPI invalid notification can be sent. Upon receiving the notification, the originating peer deletes the IPsec SA that has the invalid SPI. If the originator has data to send, new SAs will be set up.

Use caution when you enable the invalid SPI recovery feature, because using this feature can result in a DoS attack. Attackers can make a great number of invalid SPI notifications to the same peer.

Examples

Enable invalid SPI recovery.

```
<Sysname> system-view
[Sysname] ike invalid-spi-recovery enable
```

ike ipv6-address-group

Use **ike ipv6-address-group** to configure an IKE IPv6 address pool for assigning IPv6 addresses to remote peers.

Use **undo ike ipv6-address-group** to delete an IKE IPv6 address pool.

Syntax

ike ipv6-address-group *group-name* **prefix** *prefix/prefix-len* **assign-len** *assign-len*

undo ike ipv6-address-group *group-name*

Default

No IKE IPv6 address pools exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a name for the IKE IPv6 address pool. The *group-name* argument is a case-insensitive string of 1 to 63 characters.

prefix *prefix/prefix-len*: Specifies an IPv6 prefix in the format of *prefix*/*prefix length*. The value range for the *prefix-len* argument is 1 to 128.

assign-len *assign-len*: Specifies the assigned prefix length. The value range for the *assign-len* argument is 1 to 128, and the value must be greater than or equal to *prefix-len*. The difference between *assign-len* and *prefix-len* must be equal to or less than 16.

Usage guidelines

Different from the IKE IPv4 address pool, the device assigns an IPv6 subnet to a peer from the IKE IPv6 address pool. The peer can use the assigned IPv6 subnet to assign IPv6 addresses to other devices.

IKE IPv6 address pools cannot overlap with each other.

Examples

Configure an IKE IPv6 address pool with name **ipv6group**, prefix 1:1::/64, and assigned prefix length 80.

```
<Sysname> system-view
[Sysname] ike ipv6-address-group ipv6group prefix 1:1::/64 assign-len 80
```

Related commands

aaa authorization

ike keepalive interval

Use **ike keepalive interval** to set the IKE keepalive interval.

Use **undo ike keepalive interval** to restore the default.

Syntax

ike keepalive interval *interval*

undo ike keepalive interval

Default

No IKE keepalives are sent.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies the number of seconds between IKE keepalives, in the range of 20 to 28800.

Usage guidelines

To detect the status of the peer, configure IKE DPD instead of the IKE keepalive feature, unless IKE DPD is not supported on the peer.

The keepalive timeout time configured at the local must be longer than the keepalive interval configured at the peer. Because more than three consecutive packets are rarely lost on a network, you can set the keepalive timeout time to three times as long as the keepalive interval.

Examples

Set the keepalive interval to 200 seconds

```
<Sysname> system-view
[Sysname] ike keepalive interval 200
```

Related commands

ike keepalive timeout

ike keepalive timeout

Use **ike keepalive timeout** to set the IKE keepalive timeout time.

Use **undo ike keepalive timeout** to restore the default.

Syntax

ike keepalive timeout *seconds*

undo ike keepalive timeout

Default

The IKE keepalive timeout time is not set.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies the number of seconds between IKE keepalives. The value range for this argument is 20 to 28800.

Usage guidelines

If the local end receives no keepalive packets from the peer during the timeout time, the IKE SA is deleted along with the IPsec SAs it negotiated.

The keepalive timeout time configured at the local end must be longer than the keepalive interval configured at the peer. Because more than three consecutive packets are rarely lost on a network, you can set the keepalive timeout time to three times as long as the keepalive interval.

Examples

Set the keepalive timeout time to 20 seconds.

```
<Sysname> system-view
[Sysname] ike keepalive timeout 20
```

Related commands

ike keepalive interval

ike keychain

Use **ike keychain** to create an IKE keychain and enter its view, or enter the view of an existing IKE keychain.

Use **undo ike keychain** to delete an IKE keychain.

Syntax

ike keychain *keychain-name* [**vpn-instance** *vpn-instance-name*]

undo ike keychain *keychain-name* [**vpn-instance** *vpn-instance-name*]

Default

No IKE keychains exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

keychain-name: Specifies an IKE keychain name, a case-insensitive string of 1 to 63 characters.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the IKE keychain belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. To create an IKE keychain for the public network, do not specify this option.

Usage guidelines

To use preshared key authentication, you must create and specify an IKE keychain for the IKE profile.

Examples

Create IKE keychain **key1** and enter its view.

```
<Sysname> system-view
[Sysname] ike keychain key1
[Sysname-ike-keychain-key1]
```

Related commands

authentication-method

pre-shared-key

ike limit

Use **ike limit** to set the maximum number of half-open or established IKE SAs.

Use **undo ike limit** to restore the default.

Syntax

ike limit { **max-negotiating-sa** *negotiation-limit* | **max-sa** *sa-limit* }

undo ike limit { **max-negotiating-sa** | **max-sa** }

Default

The maximum number of half-open IKE SAs and IPsec SAs is 200, and there is no limit to the maximum number of established IKE SAs.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

max-negotiating-sa *negotiation-limit*: Specifies the maximum number of half-open IKE SAs and IPsec SAs. The value range for the *negotiation-limit* argument is 1 to 99999.

max-sa *sa-limit*: Specifies the maximum number of established IKE SAs. The value range for the *sa-limit* argument is 1 to 99999.

Usage guidelines

The supported maximum number of half-open IKE SAs depends on the device's processing capability. Adjust the maximum number of half-open IKE SAs to make full use of the device's processing capability without affecting the IKE SA negotiation efficiency.

The supported maximum number of established IKE SAs depends on the device's memory space. Adjust the maximum number of established IKE SAs to make full use of the device's memory space without affecting other applications in the system.

Examples

Set the maximum number of half-open IKE SAs and IPsec SAs to 200.

```
<Sysname> system-view
[Sysname] ike limit max-negotiating-sa 200
```

Set the maximum number of established IKE SAs to 5000.

```
<Sysname> system-view
[Sysname] ike limit max-sa 5000
```

ike logging negotiation enable

Use **ike logging negotiation enable** to enable logging for IKE negotiation.

Use **undo ike logging negotiation packet enable** to disable logging for IKE negotiation.

Syntax

ike logging negotiation enable

undo ike logging negotiation enable

Default

Logging for IKE negotiation is enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command enables the device to output logs for the IKE negotiation process.

Examples

Enable logging for IKE negotiation.

```
<Sysname> system-view
[Sysname] ike logging negotiation enable
```

ike nat-keepalive

Use **ike nat-keepalive** to set the NAT keepalive interval.

Use **undo ike nat-keepalive** to restore the default.

Syntax

ike nat-keepalive *seconds*

undo ike nat-keepalive

Default

The NAT keepalive interval is 20 seconds.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies the NAT keepalive interval in seconds, in the range of 5 to 300.

Usage guidelines

This command takes effect only for a device that resides in the private network behind a NAT gateway. The device behind the NAT gateway needs to send NAT keepalives to its peer to keep the NAT session alive, so that the peer can access the device.

The NAT keepalive interval must be shorter than the NAT session lifetime.For information about how to display the lifetime of NAT sessions, see *NAT Command Reference.*

Examples

Set the NAT keepalive interval to 5 seconds.

```
<Sysname> system-view
[Sysname] ike nat-keepalive 5
```

ike profile

Use **ike profile** to create an IKE profile and enter its view, or enter the view of an existing IKE profile.

Use **undo ike profile** to delete an IKE profile.

Syntax

ike profile *profile-name*

undo ike profile *profile-name*

Default

No IKE profiles exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

profile-name: Specifies an IKE profile name, a case-insensitive string of 1 to 63 characters.

Examples

Create IKE profile 1 and enter its view.

```
<Sysname> system-view
[Sysname] ike profile 1
[Sysname-ike-profile-1]
```

ike proposal

Use **ike proposal** to create an IKE proposal and enter its view, or enter the view of an existing IKE proposal.

Use **undo ike proposal** to delete an IKE proposal.

Syntax

ike proposal proposal-number

undo ike proposal *proposal-number*

Default

An IKE proposal exists, which has the lowest priority and uses the following settings:

- **Encryption algorithm**—DES-CBC.
- **Authentication algorithm**—HMAC-SHA1.
- **Authentication method**—Preshared key authentication.
- **DH group**—768-bit Diffie-Hellman group.
- **IKE SA lifetime**—86400 seconds.

You cannot change the settings of the default IKE proposal.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

proposal-number: Specifies an IKE proposal number in the range of 1 to 65535. The lower the number, the higher the priority of the IKE proposal.

Usage guidelines

During IKE negotiation:

- The initiator sends its IKE proposals to the peer.
  - If the initiator is using an IPsec policy with an IKE profile, the initiator sends all IKE proposals specified for the IKE profile to the peer. An IKE proposal specified earlier for the IKE profile has a higher priority.
  - If the initiator is using an IPsec policy with no IKE profile, the initiator sends all its IKE proposals to the peer. An IKE proposal with a smaller number has a higher priority.
- The peer searches its own IKE proposals for a match. The search starts from the IKE proposal with the highest priority and proceeds in descending order of priority until a match is found. The matching IKE proposals are used to establish the IKE SA. If all user-defined IKE proposals are mismatched, the two peers use their default IKE proposals to establish the IKE SA.

Examples

Create IKE proposal 1 and enter its view.

```
<Sysname> system-view
[Sysname] ike proposal 1
[Sysname-ike-proposal-1]
```

Related commands

display ike proposal

ike signature-identity from-certificate

Use **ike signature-identity from-certificate** to configure the local device to obtain the identity information from the local certificate for signature authentication.

Use **undo ike signature-identity from-certificate** to restore the default.

Syntax

ike signature-identity from-certificate

undo ike signature-identity from-certificate

Default

The local end uses the identity information specified by the **local-identity** or **ike identity** command for signature authentication.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command requires the local device to always use the identity information in the local certificate for signature authentication, regardless of the **local-identity** or **ike identity** configuration.

Configure this command when the aggressive mode and signature authentication are used and the device interconnects with a NF-based peer device. NF supports only DN for signature authentication.

If the **ike signature-identity from-certificate** command is not configured, the **local-identity** command configuration, if configured, takes precedence over the **ike identity** command configuration.

Examples

Configure the local device to always obtain the identity information from the local certificate for signature authentication.

```
<Sysname> system-view
[sysname] ike signature-identity from-certificate
```

Related commands

local-identity

ike identity

inside-vpn

Use **inside-vpn** to specify an inside VPN instance.

Use **undo inside-vpn** to restore the default.

Syntax

inside-vpn vpn-instance *vpn-instance-name*

undo inside-vpn

Default

No inside VPN instance is specified for an IKE profile. The device forwards protected data to the VPN instance where the interface that receives the data resides.

Views

IKE profile view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the device forwards protected data. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

This command determines where the device should forward received IPsec protected data. If you configure this command, the device looks for a route in the specified VPN instance to forward the data. If you do not configure this command, the device looks for a route in the VPN instance where the receiving interface resides to forward the data.

The inside VPN instance specified in an IKE profile takes effect only on IPsec policies that use the IKE profile. It does not take effect on IPsec profiles that use the IKE profile.

Examples

Specify inside VPN instance **vpn1** for IKE profile **prof1**.

```
<Sysname> system-view
[Sysname] ike profile prof1
[Sysname-ike-profile-prof1] inside-vpn vpn-instance vpn1
```

keychain

Use **keychain** to specify an IKE keychain for preshared key authentication.

Use **undo keychain** to remove an IKE keychain.

Syntax

keychain *keychain-name*

undo keychain *keychain-name*

Default

No IKE keychain is specified for preshared key authentication.

Views

IKE profile view

Predefined user roles

network-admin

context-admin

Parameters

keychain-name: Specifies an IKE keychain name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

You can specify a maximum of six IKE keychains for an IKE profile. An IKE keychain specified earlier has a higher priority.

Examples

Specify IKE keychain **abc** for IKE profile **1**.

```
<Sysname> system-view
[Sysname] ike profile 1
[Sysname-ike-profile-1] keychain abc
```

Related commands

ike keychain

local-identity

Use **local-identity** to configure the local ID, the ID that the device uses to identify itself to the peer during IKE negotiation.

Use **undo local-identity** to restore the default.

Syntax

local-identity { **address** { *ipv4-address* | **ipv6** *ipv6-address* } | **dn** | **fqdn** [*fqdn-name*] | **user-fqdn** [*user-fqdn-name*] }

undo local-identity

Default

No local ID is configured for an IKE profile. An IKE profile uses the local ID configured in system view by using the **ike identity** command. If the local ID is not configured in system view, the IKE profile uses the IP address of the interface to which the IPsec policy is applied as the local ID.

Views

IKE profile view

Predefined user roles

network-admin

context-admin

Parameters

address { *ipv4-address* | **ipv6** *ipv6-address* }: Uses an IPv4 or IPv6 address as the local ID.

dn: Uses the DN in the local certificate as the local ID.

fqdn *fqdn-name*: Uses an FQDN as the local ID. The *fqdn-name* argument is a case-sensitive string of 1 to 255 characters, such as www.test.com. If you do not specify this argument, the device name configured by using the **sysname** command is used as the local FQDN.

user-fqdn *user-fqdn-name*: Uses a user FQDN as the local ID. The *user-fqdn-name* argument is a case-sensitive string of 1 to 255 characters, such as adc@test.com. If you do not specify this argument, the device name configured by using the **sysname** command is used as the user FQDN.

Usage guidelines

For digital signature authentication, the device can use any type of ID. For preshared key authentication, the device can use any type of ID other than the DN.

In digital signature authentication, if the local ID is an IP address that is different from the IP address in the local certificate, the device uses its FQDN instead. The FQDN is the device name configured by using the **sysname** command.

In aggressive mode, for digital signature authentication, if the local ID is the DN in the local certificate, the device uses its FQDN instead for IKE negotiation. To use the DN in the local certificate as the local ID for IKE negotiation, execute the **ike signature-identity from-certificate** command in system view.

The initiator uses the local ID to identify itself to the responder. The responder compares the initiator's ID with the peer IDs configured by the **match remote** command to look for a matching IKE profile.

An IKE profile can have only one local ID.

An IKE profile with no local ID specified uses the local ID configured by using the **ike identity** command in system view.

Examples

Set the local ID to IP address **2.2.2.2**.

```
<Sysname> system-view
[Sysname] ike profile prof1
[Sysname-ike-profile-prof1] local-identity address 2.2.2.2
```

Related commands

match remote

ike identity

ike signature-identity from-certificate

match local address (IKE keychain view)

Use **match local address** to specify a local interface or IP address to which an IKE keychain can be applied.

Use **undo match local address** to restore the default.

Syntax

match local address { *interface-type interface-number* | { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] }

undo match local address

Default

An IKE keychain can be applied to any local interface or IP address.

Views

IKE keychain view

Predefined user roles

network-admin

context-admin

Parameters

interface-type interface-number: Specifies a local interface. It can be any Layer 3 interface.

ipv4-address: Specifies the IPv4 address of a local interface.

ipv6 *ipv6-address*: Specifies the IPv6 address of a local interface.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the IPv4 or IPv6 address belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the IPv4 or IPv6 address belongs to the public network, do not specify this option.

Usage guidelines

Use this command to specify which address or interface can use the IKE keychain for IKE negotiation. Specify the local address configured in IPsec policy or IPsec policy template view (using the **local-address** command) for this command. If no local address is configured, specify the IP address of the interface that uses the IPsec policy.

You can specify a maximum of six IKE keychains for an IKE profile. An IKE keychain specified earlier has a higher priority. To give an IKE keychain a higher priority, you can configure this command for the keychain. For example, suppose you specified IKE keychain A before specifying IKE keychain B, and you configured the peer ID 2.2.0.0/16 for IKE keychain A and the peer ID 2.2.2.0/24 for IKE keychain B. For the local interface with the IP address 3.3.3.3 to negotiate with the peer 2.2.2.6, IKE keychain A is preferred because IKE keychain A was specified earlier. To use IKE keychain B, you can use this command to restrict the application scope of IKE keychain B to address 3.3.3.3.

Examples

Create IKE keychain **key1**.

```
<Sysname> system-view
[Sysname] ike keychain key1
```

Apply IKE keychain **key1** to IP address 2.2.2.2.

```
[sysname-ike-keychain-key1] match local address 2.2.2.1
```

Apply IKE keychain **key1** to the interface with IP address 2.2.2.2 in VPN instance **vpn1**.

```
[sysname-ike-keychain-key1] match local address 2.2.2.2 vpn-instance vpn1
```

match local address (IKE profile view)

Use **match local address** to specify a local interface or IP address to which an IKE profile can be applied.

Use **undo match local address** to restore the default.

Syntax

match local address { *interface-type interface-number* | { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] }

undo match local address

Default

An IKE profile can be applied to any local interface or IP address.

Views

IKE profile view

Predefined user roles

network-admin

context-admin

Parameters

interface-type interface-number: Specifies a local interface. It can be any Layer 3 interface.

ipv4-address: Specifies the IPv4 address of a local interface.

ipv6 *ipv6-address*: Specifies the IPv6 address of a local interface.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the IPv4 or IPv6 address belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the IPv4 or IPv6 address belongs to the public network, do not specify this option.

Usage guidelines

Use this command to specify which address or interface can use the IKE profile for IKE negotiation. Specify the local address configured in IPsec policy or IPsec policy template view (using the **local-address** command) for this command. If no local address is configured, specify the IP address of the interface that uses the IPsec policy.

An IKE profile configured earlier has a higher priority. To give an IKE profile that is configured later a higher priority, you can configure this command for the profile. For example, suppose you configured IKE profile A before configuring IKE profile B, and you configured the **match remote identity address range 2.2.2.1 2.2.2.100** command for IKE profile A and the **match remote identity address range 2.2.2.1 2.2.2.10** command for IKE profile B. For the local interface with the IP address 3.3.3.3 to negotiate with the peer 2.2.2.6, IKE profile A is preferred because IKE profile A was configured earlier. To use IKE profile B, you can use this command to restrict the application scope of IKE profile B to address 3.3.3.3.

Examples

Create IKE profile **prof1**.

```
<Sysname> system-view
[Sysname] ike profile prof1
```

Apply IKE profile **prof1** to IP address 2.2.2.2.

```
[sysname-ike-profile-prof1] match local address 2.2.2.1
```

Apply IKE profile **prof1** to the interface with IP address 2.2.2.2 in VPN instance **vpn1**.

```
[sysname-ike-profile-prof1] match local address 2.2.2.2 vpn-instance vpn1
```

match remote

Use **match remote** to configure a peer ID for IKE profile matching.

Use **undo match remote** to delete a peer ID for IKE profile matching.

Syntax

match remote { **certificate** *policy-name* | **identity** { **address** { { *ipv4-address* [*mask* | *mask-length*] | **range** *low-ipv4-address*

high-ipv4-address } | **ipv6** { *ipv6-address* [*prefix-length*] | **range** *low-ipv6-address high-ipv6-address* } } [**vpn-instance** *vpn-instance-name*] | **fqdn** *fqdn-name* | **user-fqdn** *user-fqdn-name* } }

undo match remote { **certificate** *policy-name* | **identity** { **address** { { *ipv4-address* [*mask* | *mask-length*] | **range** *low-ipv4-address high-ipv4-address* } | **ipv6** { *ipv6-address* [*prefix-length*] | **range** *low-ipv6-address high-ipv6-address* } } [**vpn-instance** *vpn-instance-name*] | **fqdn** *fqdn-name* | **user-fqdn** *user-fqdn-name* } }

Default

No peer ID is configured for IKE profile matching.

Views

IKE profile view

Predefined user roles

network-admin

context-admin

Parameters

certificate *policy-name*: Uses the DN in the peer's digital certificate as the peer ID for IKE profile matching. The *policy-name* argument is a string of 1 to 31 characters.

identity: Uses the specified information as the peer ID for IKE profile matching. The specified information is configured on the peer by using the **local-identity** command.

- **address** *ipv4-address* [*mask* | *mask-length*]: Uses an IPv4 host address or an IPv4 subnet address as the peer ID for IKE profile matching. The value range for the *mask-length* argument is 0 to 32, and the default is 32.
- **address range** *low-ipv4-address high-ipv4-address*: Uses a range of IPv4 addresses as the peer ID for IKE profile matching. The end address must be higher than the start address.
- **address ipv6** *ipv6-address* [*prefix-length*]: Uses an IPv6 host address or an IPv6 subnet address as the peer ID for IKE profile matching. The value range for the *prefix-length* argument is 0 to 128, and the default is 128.
- **address ipv6 range** *low-ipv6-address high-ipv6-address*: Uses a range of IPv6 addresses as the peer ID for IKE profile matching. The end address must be higher than the start address.
- **fqdn** *fqdn-name*: Uses the peer's FQDN as the peer ID for IKE profile matching. The *fqdn-name* argument is a case-sensitive string of 1 to 255 characters, such as www.test.com.
- **user-fqdn** *user-fqdn-name*: Uses the peer's user FQDN as the peer ID for IKE profile matching. The *user-fqdn-name* argument is a case-sensitive string of 1 to 255 characters, such as adc@test.com.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the specified address or addresses belong. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the address or addresses belong to the public network, do not specify this option.

Usage guidelines

The responder compares the initiator's ID it received with the peer IDs of its local IKE profiles. If a match is found, the responder uses the IKE profile with the matching peer ID for IKE negotiation with the initiator.

On the responder, each IKE profile must have at least one peer ID configured. To make sure only one IKE profile is matched for a peer, do not configure the same peer ID for two or more IKE profiles.

If you configure the same peer ID for two or more IKE profiles, which IKE profile is selected for IKE negotiation is unpredictable.

For an IKE profile, you can configure multiple peer IDs. A peer ID configured earlier has a higher priority.

Examples

Create IKE profile **prof1**.

```
<Sysname> system-view
[Sysname] ike profile prof1
```

Configure a peer ID with the identity type of FQDN and the value of **www.test.com**.

```
[Sysname-ike-profile-prof1] match remote identity fqdn www.test.com
```

Configure a peer ID with the identity type of IP address and the value of **10.1.1.1**.

```
[Sysname-ike-profile-prof1] match remote identity address 10.1.1.1
```

Related commands

local-identity

pre-shared-key

Use **pre-shared-key** to configure a preshared key.

Use **undo pre-shared-key** to delete a preshared key.

Syntax

pre-shared-key { **address** { *ipv4-address* [*mask* | *mask-length*] | **ipv6** *ipv6-address* [*prefix-length*] } | **hostname** *host-name* } **key** { **cipher** | **simple** } *string*

undo pre-shared-key { **address** { *ipv4-address* [*mask* | *mask-length*] | **ipv6** *ipv6-address* [*prefix-length*] } | **hostname** *host-name* }

Default

No preshared key is configured.

Views

IKE keychain view

Predefined user roles

network-admin

context-admin

Parameters

address: Specifies a peer by its address.

ipv4-address: Specifies the IPv4 address of the peer.

mask: Specifies the mask in dotted decimal notation. The default mask is 255.255.255.255.

mask-length: Specifies the mask length in the range of 0 to 32. The default mask length is 32.

ipv6: Specifies an IPv6 peer.

ipv6-address: Specifies the IPv6 address of the peer.

prefix-length: Specifies the prefix length in the range of 0 to 128. The default prefix length is 128.

hostname *host-name*: Specifies a peer by its hostname, a case-sensitive string of 1 to 255 characters.

key: Specifies a preshared key.

cipher: Specifies a preshared key in encrypted form.

simple: Specifies a preshared key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the preshared key. The key is case sensitive.Its plaintext form is a string of 1 to 128 characters and its encrypted form is a string of 1 to 201 characters.

Usage guidelines

The address option or the hostname option specifies the peer with which the device can use the preshared key to perform IKE negotiation.

If you specify the peer by using the **hostname** option, the device can act as only a responder in IKE negotiation and it must use the aggressive mode in IKE phase 1. The peer device ID must be the peer FQDN that matches the hostname.

Two peers must be configured with the same preshared key to pass preshared key authentication.

Examples

Create IKE keychain **key1** and enter IKE keychain view.

```
<Sysname> system-view
[Sysname] ike keychain key1
```

Set the preshared key to be used for IKE negotiation with peer 1.1.1.2 to **123456TESTplat&!**.

```
[Sysname-ike-keychain-key1] pre-shared-key address 1.1.1.2 255.255.255.255 key simple
123456TESTplat&!
```

Related commands

authentication-method

keychain

priority (IKE keychain view)

Use **priority** to specify a priority for an IKE keychain.

Use **undo priority** to restore the default.

Syntax

priority *priority*

undo priority

Default

The priority of an IKE keychain is 100.

Views

IKE keychain view

Predefined user roles

network-admin

context-admin

Parameters

priority *priority*: Specifies a priority number in the range of 1 to 65535. The lower the priority number, the higher the priority.

Usage guidelines

To determine the priority of an IKE keychain, the device examines the existence of the **match local address** command before examining the priority number. An IKE keychain with the **match local address** command configured has a higher priority than an IKE keychain that does not have the **match local address** command configured.

Examples

Set the priority to 10 for IKE keychain **key1**.

```
<Sysname> system-view
[Sysname] ike keychain key1
[Sysname-ike-keychain-key1] priority 10
```

priority (IKE profile view)

Use **priority** to specify a priority for an IKE profile.

Use **undo priority** to restore the default.

Syntax

priority *priority*

undo priority

Default

The priority of an IKE profile is 100.

Views

IKE profile view

Predefined user roles

network-admin

context-admin

Parameters

priority *priority*: Specifies a priority number in the range of 1 to 65535. The smaller the priority number, the higher the priority.

Usage guidelines

To determine the priority of an IKE profile, the device examines the existence of the **match local address** command before examining the priority number. An IKE profile with the **match local address** command configured has a higher priority than an IKE profile that does not have the **match local address** command configured.

Examples

Set the priority to 10 for IKE profile **prof1**.

```
<Sysname> system-view
[Sysname] ike profile prof1
[Sysname-ike-profile-prof1] priority 10
```

proposal

Use **proposal** to specify IKE proposals for an IKE profile.

Use **undo proposal** to restore the default.

Syntax

proposal *proposal-number*&<1-6>

undo proposal

Default

No IKE proposals are specified for an IKE profile and the IKE proposals configured in system view are used for IKE negotiation.

Views

IKE profile view

Predefined user roles

network-admin

context-admin

Parameters

proposal-number&<1-6>: Specifies a space-separated list of up to six IKE proposals by their numbers in the range of 1 to 65535. An IKE proposal specified earlier has a higher priority.

Usage guidelines

When acting as the initiator, the device sends the specified IKE proposals to its peer for IKE negotiation. When acting as the responder, the device uses the IKE proposals configured in system view to match the IKE proposals received from the initiator.

Examples

Specify IKE proposal **10** for IKE profile **prof1**.

```
<Sysname> system-view
[Sysname] ike profile prof1
[Sysname-ike-profile-prof1] proposal 10
```

Related commands

ike proposal

reset ike sa

Use **reset ike sa** to delete IKE SAs.

Syntax

reset ike sa [**connection-id** *connection-id*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

connection-id *connection-id*: Specifies the connection ID of the IKE SA to be cleared, in the range of 1 to 2000000000.

Usage guidelines

When you delete an IKE SA, the device automatically sends a notification to the peer.

Examples

Display the current IKE SAs.

```
<Sysname> display ike sa
    Connection-ID  Remote            Flag        DOI
  -------------------------------------------------------
      1            202.38.0.2        RD          IPsec
      2            202.38.0.3        RD          IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY
```

Delete the IKE SA with the connection ID 2.

```
<Sysname> reset ike sa connection-id 2
```

Display the current IKE SAs.

```
<Sysname> display ike sa
    Connection-ID  Remote            Flag        DOI
  -------------------------------------------------------
      1            202.38.0.2        RD          IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY
```

reset ike statistics

Use **reset ike statistics** command to clear IKE MIB statistics.

Syntax

reset ike statistics

Views

User view

Predefined user roles

network-admin

context-admin

Examples

Clears IKE MIB statistics.

```
<Sysname> reset ike statistics
```

Related commands

snmp-agent trap enable ike

sa duration

Use **sa duration** to set the IKE SA lifetime for an IKE proposal.

Use **undo sa duration** to restore the default.

Syntax

sa duration *seconds*

undo sa duration

Default

The IKE SA lifetime is 86400 seconds for an IKE proposal.

Views

IKE proposal view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies the IKE SA lifetime in seconds, in the range of 60 to 604800.

Usage guidelines

Before an IKE SA expires, IKE negotiates a new SA. The new SA takes effect immediately after it is negotiated. The old IKE SA will be cleared when it expires.

If the communicating peers are configured with different IKE SA lifetime settings, the smaller setting takes effect.

If the IPsec SA lifetime is also configured, set the IKE SA lifetime longer than the IPsec SA lifetime as a best practice.

Examples

Set the IKE SA lifetime to 600 seconds for IKE **proposal 1**.

```
<Sysname> system-view
[Sysname] ike proposal 1
[Sysname-ike-proposal-1] sa duration 600
```

Related commands

display ike proposal

sa soft-duration buffer

Use **sa soft-duration buffer** to set the IKE SA soft lifetime buffer time.

Use **undo sa soft-duration buffer** to restore the default.

Syntax

sa soft-duration buffer *seconds*

undo sa soft-duration buffer

Default

The IKE SA soft lifetime buffer time is not configured.

Views

IKE profile view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies the IKE SA soft lifetime buffer time, in seconds. The value range is 10 to 36000.

Usage guidelines

This command takes effect only when IKEv1 is used.

The IKE SA soft lifetime buffer time is used determine the IKE SA soft lifetime. A new IKE SA will be negotiated when the IKE SA soft lifetime expires.

The IKE SA soft lifetime is calculated as follows: IKE SA soft lifetime = IKE SA lifetime – IKE SA soft lifetime buffer time.

If the IKE SA soft lifetime buffer time is not configured, the system calculates a default IKE SA soft lifetime based on the IKE SA lifetime.

The default IKE SA soft lifetime is also used if the IKE soft lifetime calculated based on the soft lifetime buffer is shorter than or equal to 10 seconds.

Examples

Set the IKE SA soft lifetime buffer time to 600 seconds.

```
<Sysname> system-view
[Sysname] ike profile abc
[Sysname-ike-profile-abc] sa soft-duration buffer 600
```

Related commands

display ike sa

server-address

Use **server-address** to specify the IP address and port number of the GD-quantum server.

Use **undo server-address** to restore the default.

Syntax

server-address *ip-address* [**port** *port-number*]

undo server-address

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480	Yes
NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	No

Default

No IP address or port number of the GD-quantum server is specified.

Views

IKE GD-quantum view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the IPv4 address of the GD-quantum server.

port *port-number*: Specifies the port number of the GD-quantum server, in the range of 1 to 65535. The default value for the *port-number* argument is 8013.

Usage guidelines

The device interacts with the GD-quantum server specified in this command to obtain the GD-quantum keys. Make sure you specify the IP address and port number that the GD-quantum server actually uses.

Any change to this command does affect the established connection between the device and the GD-quantum server.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the IP address of the GD-quantum server as 192.168.0.111, and the port number as 5656.

```
<Sysname> system-view
[Sysname] ike gd-quantum
[Sysname-ike-gdquantum] server-address 192.168.0.111 port 5656
```

snmp-agent trap enable ike

Use **snmp-agent trap enable ike** command to enable SNMP notifications for IKE.

Use **undo snmp-agent trap enable ike** to disable SNMP notifications for IKE.

Syntax

snmp-agent trap enable ike [**attr-not-support** | **auth-failure** | **cert-type-unsupport** | **cert-unavailable** | **decrypt-failure** | **encrypt-failure** | **global** | **invalid-cert-auth** | **invalid-cookie** | **invalid-id** | **invalid-proposal** | **invalid-protocol** | **invalid-sign** | **no-sa-failure** | **proposal-add** | **proposal–delete** | **tunnel-start** | **tunnel-stop** | **unsupport-exch-type**] *

undo snmp-agent trap enable ike [**attr-not-support** | **auth-failure** | **cert-type-unsupport** | **cert-unavailable** | **decrypt-failure** | **encrypt-failure** | **global** | **invalid-cert-auth** | **invalid-cookie** | **invalid-id** | **invalid-proposal** | **invalid-protocol** | **invalid-sign** | **no-sa-failure** | **proposal-add** | **proposal–delete** | **tunnel-start** | **tunnel-stop** | **unsupport-exch-type**] *

Default

All SNMP notifications for IKE are disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

attr-not-support: Specifies notifications about attribute-unsupported failures.

auth-failure: Specifies notifications about authentication failures.

cert-type-unsupport: Specifies notifications about certificate-type-unsupported failures.

cert-unavailable: Specifies notifications about certificate-unavailable failures.

decrypt-failure: Specifies notifications about decryption failures.

encrypt-failure: Specifies notifications about encryption failures.

global: Specifies notifications globally.

invalid-cert-auth: Specifies notifications about invalid-certificate-authentication failures.

invalid-cookie: Specifies notifications about invalid-cookie failures.

invalid-id: Specifies notifications about invalid-ID failures.

invalid-proposal: Specifies notifications about invalid-IKE-proposal failures.

invalid-protocol: Specifies notifications about invalid-protocol failures.

invalid-sign: Specifies notifications about invalid-signature failures.

no-sa-failure: Specifies notifications about SA-not-found failures.

proposal-add: Specifies notifications about events of adding IKE proposals.

proposal-delete: Specifies notifications about events of deleting IKE proposals.

tunnel-start: Specifies notifications about events of creating IKE tunnels.

tunnel-stop: Specifies notifications about events of deleting IKE tunnels.

unsupport-exch-type: Specifies notifications about negotiation-type-unsupported failures.

Usage guidelines

If you do not specify any keywords, this command enables or disables all SNMP notifications for IKE.

To generate and output SNMP notifications for a specific IKE failure type or event type, perform the following tasks:

1. Enable SNMP notifications for IKE globally.
2. Enable SNMP notifications for the failure type or event type.

Examples

Enable SNMP notifications for IKE globally.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable ike global
```

Enable SNMP notifications for events of creating IKE tunnels.

```
[Sysname] snmp-agent trap enable ike tunnel-start
```

IKEv2 commands

aaa authorization

Use **aaa authorization** to enable IKEv2 AAA authorization.

Use **undo aaa authorization** to disable IKEv2 AAA authorization.

Syntax

aaa authorization domain *domain-name* **username** *user-name*

undo aaa authorization

Default

IKEv2 AAA authorization is disabled.

Views

IKEv2 profile view

Predefined user roles

network-admin

context-admin

Parameters

domain *domain-name*: Specifies the ISP domain used for requesting authorization attributes. The ISP domain name is a case-insensitive string of 1 to 255 characters and must meet the following requirements:

- The name cannot contain a forward slash (/), backslash (\), vertical bar (|), quotation mark ("), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or an at sign (@).
- The name cannot be **d**, **de**, **def**, **defa**, **defau**, **defaul**, **default**, **i**, **if**, **if-**, **if-u**, **if-un**, **if-unk**, **if-unkn**, **if-unkno**, **if-unknow**, or **if-unknown**.

username *user-name*: Specifies the username used for requesting authorization attributes. The username is a case-sensitive string of 1 to 55 characters and must meet the following requirements:

- The username cannot contain the domain name.
- The username cannot contain a forward slash (/), backslash (\), vertical bar (|), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or an at sign (@).
- The username cannot be **a**, **al**, or **all**.

Usage guidelines

The AAA authorization feature enables IKEv2 to request authorization attributes, such as the IKEv2 address pool, from AAA.

IKEv2 uses the ISP domain and username to request authorization attributes. AAA uses the authorization settings in the ISP domain to request the user's authorization attributes from the remote AAA server or the local user database. After IKEv2 passes the username authentication, it obtains the authorization attributes.

This feature is applicable when AAA is used to centrally manage and deploy authorization attributes.

Examples

Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

Enable AAA authorization. Specify ISP domain name **abc** and username **test**.

```
[Sysname-ikev2-profile-profile1] aaa authorization domain abc username test
```

Related commands

display ikev2 profile

address

Use **address** to specify the IP address or IP address range of an IKEv2 peer.

Use **undo address** to restore the default.

Syntax

address { *ipv4-address* [*mask* | *mask-length*] | **ipv6** *ipv6-address* [*prefix-length*] }

undo address

Default

The IKEv2 peer's IP address or IP address range is not specified.

Views

IKEv2 peer view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-address: Specifies the IPv4 address of the IKEv2 peer.

mask: Specifies the subnet mask of the IPv4 address.

mask-length: Specifies the subnet mask length of the IPv4 address, in the range of 0 to 32.

ipv6 *ipv6-address*: Specifies the IPv6 address of the IKEv2 peer.

prefix-length: Specifies the prefix length of the IPv6 address, in the range of 0 to 128.

Usage guidelines

Both the initiator and the responder can look up an IKEv2 peer by IP address in IKEv2 negotiation.

The IP addresses of different IKEv2 peers in the same IKEv2 keychain cannot be the same.

Examples

Create an IKEv2 keychain named **key1**.

```
<Sysname> system-view
[Sysname] ikev2 keychain key1
```

Create an IKEv2 peer named **peer1**.

```
[Sysname-ikev2-keychain-key1] peer peer1
```

Specify the IKEv2 peer's IP address 3.3.3.3 with subnet mask 255.255.255.0.

```
[Sysname-ikev2-keychain-key1-peer-peer1] address 3.3.3.3 255.255.255.0
```

Related commands

ikev2 keychain

peer

authentication-method

Use **authentication-method** to specify the local or remote identity authentication method.

Use **undo authentication-method** to remove the local or remote identity authentication method.

Syntax

authentication-method { **local** | **remote** } { **dsa-signature** | **ecdsa-signature** | **pre-share** | **rsa-signature** }

undo authentication-method local

undo authentication-method remote { **dsa-signature** | **ecdsa-signature** | **pre-share** | **rsa-signature** }

Default

No local or remote identity authentication method is specified.

Views

IKEv2 profile view

Predefined user roles

network-admin

context-admin

Parameters

local: Specifies the local identity authentication method.

remote: Specifies the remote identity authentication method.

dsa-signature: Specifies the DSA signatures as the identity authentication method.

ecdsa-signature: Specifies the ECDSA signatures as the identity authentication method.

pre-share: Specifies the preshared key as the identity authentication method.

rsa-signature: Specifies the RSA signatures as the identity authentication method.

Usage guidelines

The local and remote identity authentication methods must both be specified and they can be different.

You can specify only one local identity authentication method. You can specify multiple remote identity authentication methods by executing this command multiple times when there are multiple remote ends whose authentication methods are unknown.

If you use RSA, DSA, or ECDSA signature authentication, you must specify PKI domains for obtaining certificates. You can specify PKI domains by using the **certificate domain** command in IKEv2 profile view. If you do not specify PKI domains in IKEv2 profile view, the PKI domains configured by the **pki domain** command in system view will be used.

If you specify the preshared key method, you must specify a preshared key for the IKEv2 peer in the keychain used by the IKEv2 profile.

Examples

Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

Specify the preshared key and RSA signatures as the local and remote authentication methods, respectively.

```
[Sysname-ikev2-profile-profile1] authentication-method local pre-share
[Sysname-ikev2-profile-profile1] authentication-method remote rsa-signature
```

Specify PKI domain **genl** as the PKI domain for obtaining certificates.

```
[Sysname-ikev2-profile-profile1] certificate domain genl
```

Specify IKEv2 keychain **keychain1**.

```
[Sysname-ikev2-profile-profile1] keychain keychain1
```

Related commands

display ikev2 profile

certificate domain (IKEv2 profile view)

keychain (IKEv2 profile view)

certificate domain

Use **certificate domain** to specify a PKI domain for signature authentication in IKEv2 negotiation.

Use **undo certificate domain** to remove a PKI domain for signature authentication in IKEv2 negotiation.

Syntax

certificate domain *domain-name* [**sign** | **verify**]

undo certificate domain *domain-name*

Default

PKI domains configured in system view are used for signature authentication.

Views

IKEv2 profile view

Predefined user roles

network-admin

context-admin

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters.

sign: Uses the local certificate in the PKI domain to generate a signature.

verify: Uses the CA certificate in the PKI domain to verify the remote end's certificate.

Usage guidelines

If you do not specify the **sign** or **verify** keyword, the PKI domain is used for both **sign** and **verify** purposes. You can specify a PKI domain for each purpose by executing this command multiple times. If you specify the same PKI domain for both purposes, the later configuration takes

effect. For example, if you execute **certificate domain abc sign** and **certificate domain abc verify** successively, the PKI domain **abc** will be used only for verification.

If the local end uses RSA, DSA, or ECDSA signature authentication, you must specify a PKI domain for signature generation. If the remote end uses RSA, DSA, or ECDSA signature authentication, you must specify a PKI domain for verifying the remote end's certificate. If you do not specify PKI domains, the PKI domains configured in system view will be used.

Examples

Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

Specify PKI domain **abc** for signature. Specify PKI domain **def** for verification.

```
[Sysname-ikev2-profile-profile1] certificate domain abc sign
[Sysname-ikev2-profile-profile1] certificate domain def verify
```

Related commands

authentication-method

pki domain

config-exchange

Use **config-exchange** to enable configuration exchange.

Use **undo config-exchange** to disable configuration exchange.

Syntax

config-exchange { **request** | **set** { **accept** | **send** } }

undo config-exchange { **request** | **set** { **accept** | **send** } }

Default

Configuration exchange is disabled.

Views

IKEv2 profile view

Predefined user roles

network-admin

context-admin

Parameters

request: Enables the device to send request messages carrying the configuration request payload during the IKE_AUTH exchange.

set: Specifies the configuration set payload exchange.

accept: Enables the device to accept the configuration set payload carried in Info messages.

send: Enables the device to send Info messages carrying the configuration set payload.

Usage guidelines

The configuration exchange feature enables the local and remote ends to exchange configuration data, such as gateway address, internal IP address, and route. The exchange includes data request and response, and data push and response. The enterprise center can push IP addresses to branches. The branches can request IP addresses, but the requested IP addresses cannot be used.

You can specify both **request** and **set** for the device.

If you specify **request** for the local end, the remote end will respond if it can obtain the requested data through AAA authorization.

If you specify **set send** for the local end, you must specify **set accept** for the remote end.

The device with **set send** specified pushes an IP address after the IKEv2 SA is set up if it does not receive any configuration request from the peer.

Examples

Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

Enable the local end to add the configuration request payload to the request message of IKE_AUTH exchange.

```
[Sysname-ikev2-profile-profile1] config-exchange request
```

Related commands

aaa authorization

display ikev2 profile

dh

Use **dh** to specify DH groups to be used in IKEv2 key negotiation.

Use **undo group** to restore the default.

Syntax

dh { **group1** | **group14** | **group2** | **group24** | **group5** | **group19** | **group20** } *

undo dh

Default

No DH group is specified for an IKEv2 proposal.

Views

IKEv2 proposal view

Predefined user roles

network-admin

context-admin

Parameters

group1: Uses the 768-bit Diffie-Hellman group.

group2: Uses the 1024-bit Diffie-Hellman group.

group5: Uses the 1536-bit Diffie-Hellman group.

group14: Uses the 2048-bit Diffie-Hellman group.

group24: Uses the 2048-bit Diffie-Hellman group with the 256-bit prime order subgroup.

group19: Uses the 256-bit ECP Diffie-Hellman group.

group20: Uses the 384-bit ECP Diffie-Hellman group.

Usage guidelines

A DH group with a higher group number provides higher security but needs more time for processing. To achieve the best trade-off between processing performance and security, choose proper DH groups for your network.

You must specify a minimum of one DH group for an IKEv2 proposal. Otherwise, the proposal is incomplete and useless.

You can specify multiple DH groups for an IKEv2 proposal. A group specified earlier has a higher priority.

Examples

Specify DH group 1 for IKEv2 proposal 1.

```
<Sysname> system-view
[Sysname] ikev2 proposal 1
[Sysname-ikev2-proposal-1] dh group1
```

Related commands

ikev2 proposal

display ikev2 policy

Use **display ikev2 policy** to display the IKEv2 policy configuration.

Syntax

display ikev2 policy [*policy-name* | **default**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

policy-name: Specifies an IKEv2 policy by its name, a case-insensitive string of 1 to 63 characters.

default: Specifies the default IKEv2 policy.

Usage guidelines

If you do not specify any parameters, this command displays the configuration of all IKEv2 policies.

Examples

Display the configuration of all IKEv2 policies.

```
<Sysname> display ikev2 policy
IKEv2 policy: 1
  Priority: 100
  Match local address: 1.1.1.1
  Match local address ipv6: 1:1::1:1
  Match VRF: vpn1
  Proposal: 1
```

```
  Proposal: 2
IKEv2 policy: default
  Match VRF: any
  Proposal: default
```

Table 15 Command output

Field	Description
IKEv2 policy	Name of the IKEv2 policy.
Priority	Priority of the IKEv2 policy.
Match local address	IPv4 address to which the IKEv2 policy can be applied.
Match local address ipv6	IPv6 address to which the IKEv2 policy can be applied.
Match VRF	VPN instance to which the IKEv2 policy can be applied.
Proposal	IKEv2 proposal that the IKEv2 policy uses.

Related commands

ikev2 policy

display ikev2 profile

Use **display ikev2 profile** to display the IKEv2 profile configuration.

Syntax

display ikev2 profile [*profile-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

profile-name: Specifies an IKEv2 profile by its name, a case-insensitive string of 1 to 63 characters. If you do not specify an IKEv2 profile, this command displays the configuration of all IKEv2 profiles.

Examples

Display the configuration of all IKEv2 profiles.

```
<Sysname> display ikev2 profile
IKEv2 profile: 1
  Priority: 100
  Match criteria:
    Local address 1.1.1.1
    Local address GigabitEthernet1/0/1
    Local address 1:1::1:1
    Remote identity ipv4 address 3.3.3.3/32
```

```
  VRF vrf1
Inside-vrf:
Local identity: address 1.1.1.1
Local authentication method: pre-share
Remote authentication methods: pre-share
Keychain: Keychain1
Sign certificate domain:
   Domain1
   abc
Verify certificate domain:
   Domain2
   yy
SA duration: 500
DPD: Interval 32, retry 23, periodic
Config-exchange: Request, Set send, Set accept
NAT keepalive: 10
AAA authorization: Domain domain1, username ikev2
```

Table 16 Command output

Field	Description
IKEv2 profile	Name of the IKEv2 profile.
Priority	Priority of the IKEv2 profile.
Match criteria	Criteria for looking up the IKEv2 profile.
Inside-vrf	Inside VPN instance.
Local identity	ID of the local end.
Local authentication method	Method that the local end uses for authentication.
Remote authentication methods	Methods that the remote end uses for authentication.
Keychain	IKEv2 keychain that the IKEv2 profile uses.
Sign certificate domain	PKI domain used for signature generation.
Verify certificate domain	PKI domain used for verifying the remote end's certificate.
SA duration	Lifetime of the IKEv2 SA.
DPD	DPD settings: • Detection interval in seconds. • Retry interval in seconds. • Detection mode, on demand or periodically. If DPD is disabled, this field displays **Disabled**.
Config-exchange	Configuration exchange settings: • **Request**—The local end sends request messages carrying the configuration request payload during the IKE_AUTH exchange. • **Set accept**—The local end accepts the configuration set payload carried in Info messages. • **Set send**—The local end sends Info messages carrying the configuration set payload.
NAT keepalive	NAT keepalive interval in seconds.
AAA authorization	AAA authorization settings:

Field	Description
	• ISP domain name. • Username.

Related commands

ikev2 profile

display ikev2 proposal

Use **display ikev2 proposal** to display the IKEv2 proposal configuration.

Syntax

display ikev2 proposal [*name* | **default**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

name: Specifies an IKEv2 proposal by its name, a case-insensitive string of 1 to 63 characters.

default: Specifies the default IKEv2 proposal.

Usage guidelines

This command displays IKEv2 proposals in descending order of priorities. If you do not specify any parameters, this command displays the configuration of all IKEv2 proposals.

Examples

Display the configuration of all IKEv2 proposals.

```
<Sysname> display ikev2 proposal
IKEv2 proposal : 1
  Encryption: 3DES-CBC AES-CBC-128 AES-CTR-192 CAMELLIA-CBC-128
  Integrity: MD5 SHA256 AES-XCBC-MAC
  PRF: MD5 SHA256 AES-XCBC-MAC
  DH Group: MODP1024/Group2 MODP1536/Group5

IKEv2 proposal : default
  Encryption: AES-CBC-128 3DES-CBC
  Integrity: SHA1 MD5
  PRF: SHA1 MD5
  DH Group: MODP1536/Group5 MODP1024/Group2
```

Table 17 Command output

Field	Description
IKEv2 proposal	Name of the IKEv2 proposal.

Field	Description
Encryption	Encryption algorithms that the IKEv2 proposal uses.
Integrity	Integrity protection algorithms that the IKEv2 proposal uses.
PRF	PRF algorithms that the IKEv2 proposal uses.
DH Group	DH groups that the IKEv2 proposal uses.

Related commands

ikev2 proposal

display ikev2 sa

Use **display ikev2 sa** to display the IKEv2 SA information.

Syntax

display ikev2 sa [**count** | [{ **local** | **remote** } { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]] [**verbose** [**tunnel** *tunnel-id*]]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

count: Displays the number of IKEv2 SAs.

local: Displays IKEv2 SA information for a local IP address.

remote: Displays IKEv2 SA information for a remote IP address.

ipv4-address: Specifies a local or remote IPv4 address.

ipv6 *ipv6-address*: Specifies a local or remote IPv6 address.

vpn-instance *vpn-instance-name*: Displays information about the IKEv2 SAs in an MPLS L3VPN instance. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays information about IKEv2 SAs for the public network.

verbose: Displays detailed information. If you do not specify this keyword, the command displays the summary information.

tunnel *tunnel-id*: Displays detailed IKEv2 SA information for an IPsec tunnel. The *tunnel-id* argument specifies an IPsec tunnel by its ID in the range of 1 to 2000000000.

Usage guidelines

If you do not specify any parameters, this command displays summary information about all IKEv2 SAs.

Examples

Display summary information about all IKEv2 SAs.

```
<Sysname> display ikev2 sa
     Tunnel ID          Local             Remote             Status
  ------------------------------------------------------------------------
     1                  1.1.1.1/500       1.1.1.2/500        EST
     2                  2.2.2.1/500       2.2.2.2/500        EST
  Status:
  IN-NEGO: Negotiating, EST: Established, DEL: Deleting
```

Display summary IKEv2 SA information for the remote IP address 1.1.1.2.

```
<Sysname> display ikev2 sa remote 1.1.1.2
     Tunnel ID          Local             Remote             Status
  ------------------------------------------------------------------------
     1                  1.1.1.1/500       1.1.1.2/500        EST
  Status:
  IN-NEGO: Negotiating, EST: Established, DEL: Deleting
```

Table 18 Command output

Field	Description
Tunnel ID	ID of the IPsec tunnel to which the IKEv2 SA belongs.
Local	Local IP address of the IKEv2 SA.
Remote	Remote IP address of the IKEv2 SA.
Status	Status of the IKEv2 SA: • **IN-NEGO (Negotiating)**—The IKEv2 SA is under negotiation. • **EST (Established)**—The IKEv2 SA has been set up. • **DEL (Deleting)**—The IKEv2 SA is about to be deleted.

Display detailed information about all IKEv2 SAs.

```
<Sysname> display ikev2 sa verbose
  Tunnel ID: 1
  Local IP/Port: 1.1.1.1/500
  Remote IP/Port: 1.1.1.2/500
  Outside VRF: -
  Inside VRF: -
  Local SPI: 8f8af3dbf5023a00
  Remote SPI: 0131565b9b3155fa

  Local ID type: FQDN
  Local ID: device_a
  Remote ID type: FQDN
  Remote ID: device_b

  Auth sign method: Pre-shared key
  Auth verify method: Pre-shared key
  Integrity algorithm: HMAC_MD5
  PRF algorithm: HMAC_MD5
  Encryption algorithm: AES-CBC-192

  Life duration: 86400 secs
```

```
  Remaining key duration: 85604 secs
  Diffie-Hellman group: MODP1024/Group2
  NAT traversal: Not detected
  DPD: Interval 20 secs, retry interval 2 secs
  Transmitting entity: Initiator

  Local window: 1
  Remote window: 1
  Local request message ID: 2
  Remote request message ID:2
  Local next message ID: 0
  Remote next message ID: 0

  Pushed IP address: 192.168.1.5
  Assigned IP address: 192.168.2.24
```

Display detailed IKEv2 SA information for the remote IP address 1.1.1.2.

```
<Sysname> display ikev2 sa remote 1.1.1.2 verbose
  Tunnel ID: 1
  Local IP/Port: 1.1.1.1/500
  Remote IP/Port: 1.1.1.2/500
  Outside VRF: -
  Inside VRF: -
  Local SPI: 8f8af3dbf5023a00
  Remote SPI: 0131565b9b3155fa

  Local ID type: FQDN
  Local ID: device_a
  Remote ID type: FQDN
  Remote ID: device_b

  Auth sign method: Pre-shared key
  Auth verify method: Pre-shared key
  Integrity algorithm: HMAC_MD5
  PRF algorithm: HMAC_MD5
  Encryption algorithm: AES-CBC-192

  Life duration: 86400 secs
  Remaining key duration: 85604 secs
  Diffie-Hellman group: MODP1024/Group2
  NAT traversal: Not detected
  DPD: Interval 30 secs, retry interval 10 secs
  Transmitting entity: Initiator

  Local window: 1
  Remote window: 1
  Local request message ID: 2
  Remote request message ID: 2
```

```
Local next message ID: 0
Remote next message ID: 0

Pushed IP address: 192.168.1.5
Assigned IP address: 192.168.2.24
```

Table 19 Command output

Field	Description
Tunnel ID	ID of the IPsec tunnel to which the IKEv2 SA belongs.
Local IP/Port	IP address and port number of the local security gateway.
Remote IP/Port	IP address and port number of the remote security gateway.
Outside VRF	Name of the VPN instance to which the protected outbound data flow belongs. If the protected outbound data flow belongs to the public network, this field displays a hyphen (**-**).
Inside VRF	Name of the VPN instance to which the protected inbound data flow belongs. If the protected inbound data flow belongs to the public network, this field displays a hyphen (**-**).
Local SPI	SPI that the local end uses.
Remote SPI	SPI that the remote end uses.
Local ID type	ID type of the local security gateway.
Local ID	ID of the local security gateway.
Remote ID type	ID type of the remote security gateway.
Remote ID	ID of the remote security gateway.
Auth sign method	Signature method that the IKEv2 proposal uses in authentication.
Auth verify method	Verification method that the IKEv2 proposal uses in authentication.
Integrity algorithm	Integrity protection algorithms that the IKEv2 proposal uses.
PRF algorithm	PRF algorithms that the IKEv2 proposal uses.
Encryption algorithm	Encryption algorithms that the IKEv2 proposal uses.
Life duration	Lifetime of the IKEv2 SA, in seconds.
Remaining key duration	Remaining lifetime of the IKEv2 SA, in seconds.
Diffie-Hellman group	DH groups used in IKEv2 key negotiation.
NAT traversal	Whether a NAT gateway is detected between the local and remote ends.
DPD	DPD settings: • Detection interval in seconds. • Retry interval in seconds. If DPD is disabled, this field displays **Interval 0 secs, retry interval 0 secs**.
Transmitting entity	Role of the local end in IKEv2 negotiation, initiator or responder.

Field	Description
Local window	Window size that the local end uses.
Remote window	Window size that the remote end uses.
Local request message ID	ID of the request message that the local end is about to send.
Remote request message ID	ID of the request message that the remote end is about to send.
Local next message ID	ID of the message that the local end expects to receive.
Remote next message ID	ID of the message that the remote end expects to receive.
Pushed IP address	IP address pushed to the local end by the remote end.
Assigned IP address	IP address assigned to the remote end by the local end .

Display the number of IKEv2 SAs.

```
[Sysname] display ikev2 sa count
IKEv2 SAs count: 0
```

display ikev2 statistics

Use **`display ikev2 statistics`** to display IKEv2 statistics.

Syntax

`display ikev2 statistics`

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display IKEv2 statistics.

```
<Sysname> display ikev2 statistics
IKEv2 statistics:
  Unsupported critical payload: 0
  Invalid IKE SPI: 0
  Invalid major version: 0
  Invalid syntax: 0
  Invalid message ID: 0
  Invalid SPI: 0
  No proposal chosen: 0
  Invalid KE payload: 0
  Authentication failed: 0
  Single pair required: 0
  TS unacceptable: 0
  Invalid selectors: 0
```

```
Temporary failure: 0
No child SA: 0
Unknown other notify: 0
No enough resource: 0
Enqueue error: 0
No IKEv2 SA: 0
Packet error: 0
Other error: 0
Retransmit timeout: 0
DPD detect error: 0
Del child for IPsec message: 1
Del child for deleting IKEv2 SA: 1
Del child for receiving delete message: 0
```

Related commands

reset ikev2 statistics

dpd

Use **dpd** to configure IKEv2 DPD.

Use **undo dpd** to disable IKEv2 DPD.

Syntax

dpd interval *interval* [**retry** *seconds*] { **on-demand** | **periodic** }

undo dpd interval

Default

IKEv2 DPD is disabled. The global IKEv2 DPD settings are used.

Views

IKEv2 profile view

Predefined user roles

network-admin

context-admin

Parameters

interval *interval*: Specifies a DPD triggering interval in the range of 10 to 3600 seconds.

retry *seconds* Specifies the DPD retry interval in the range of 2 to 60 seconds. The default is 5 seconds.

on-demand: Triggers DPD on demand. The device triggers DPD if it has IPsec traffic to send and has not received any IPsec packets from the peer for the specified interval.

periodic: Triggers DPD at regular intervals. The device triggers DPD at the specified interval.

Usage guidelines

DPD is triggered periodically or on-demand. As a best practice, use the on-demand mode when the device communicates with a large number of IKEv2 peers. For an earlier detection of dead peers, use the periodic triggering mode, which consumes more bandwidth and CPU.

The triggering interval must be longer than the retry interval, so that the device will not trigger a new round of DPD during a DPD retry.

Examples

Configure on-demand IKEv2 DPD. Set the DPD triggering interval to 10 seconds and the retry interval to 5 seconds.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
[Sysname-ikev2-profile-profile1] dpd interval 10 retry 5 on-demand
```

Related commands

ikev2 dpd

encryption

Use **encryption** to specify encryption algorithms for an IKEv2 proposal.

Use **undo encryption** to restore the default.

Syntax

encryption { **3des-cbc** | **aes-cbc-128** | **aes-cbc-192** | **aes-cbc-256** | **aes-ctr-128** | **aes-ctr-192** | **aes-ctr-256** | **camellia-cbc-128** | **camellia-cbc-192** | **camellia-cbc-256** | **des-cbc** } *

undo encryption

Default

No encryption algorithm is specified for an IKEv2 proposal.

Views

IKEv2 proposal view

Predefined user roles

network-admin

context-admin

Parameters

3des-cbc: Specifies the 3DES algorithm in CBC mode, which uses a 168-bit key.

aes-cbc-128: Specifies the AES algorithm in CBC mode, which uses a 128-bit key.

aes-cbc-192: Specifies the AES algorithm in CBC mode, which uses a 192-bit key.

aes-cbc-256: Specifies the AES algorithm in CBC mode, which uses a 256-bit key.

aes-ctr-128: Specifies the AES algorithm in CTR mode, which uses a 128-bit key.

aes-ctr-192: Specifies the AES algorithm in CTR mode, which uses a 192-bit key.

aes-ctr-256: Specifies the AES algorithm in CTR mode, which uses a 256-bit key.

camellia-cbc-128: Specifies the Camellia algorithm in CBC mode, which uses a 128-bit key.

camellia-cbc-192: Specifies the Camellia algorithm in CBC mode, which uses a 192-bit key.

camellia-cbc-256: Specifies the Camellia algorithm in CBC mode, which uses a 256-bit key.

des-cbc: Specifies the DES algorithm in CBC mode, which uses a 56-bit key.

Usage guidelines

You must specify a minimum of one encryption algorithm for an IKEv2 proposal. Otherwise, the proposal is incomplete and useless. You can specify multiple encryption algorithms for an IKEv2 proposal. An algorithm specified earlier has a higher priority.

Examples

Specify the 168-bit 3DES algorithm in CBC mode as the encryption algorithm for IKE proposal **prop1**.

```
<Sysname> system-view
[Sysname] ikev2 proposal prop1
[Sysname-ikev2-proposal-prop1] encryption 3des-cbc
```

Related commands

ikev2 proposal

hostname

Use **hostname** to specify the host name of an IKEv2 peer.

Use **undo hostname** to restore the default.

Syntax

hostname *name*

undo hostname

Default

The IKEv2 peer's host name is not specified.

Views

IKEv2 peer view

Predefined user roles

network-admin

context-admin

Parameters

name: Specifies the host name of the IKEv2 peer, a case-insensitive string of 1 to 253 characters.

Usage guidelines

Only the initiator can look up an IKEv2 peer by host name in IKEv2 negotiation, and the initiator must use an IPsec policy rather than an IPsec profile.

Examples

Create an IKEv2 keychain named **key1**.

```
<Sysname> system-view
[Sysname] ikev2 keychain key1
```

Create an IKEv2 peer named **peer1**.

```
[Sysname-ikev2-keychain-key1] peer peer1
```

Specify host name **test** of the IKEv2 peer.

```
[Sysname-ikev2-keychain-key1-peer-peer1] hostname test
```

Related commands

ikev2 keychain

peer

identity

Use **identity** to specify the ID of an IKEv2 peer.

Use **undo identity** to restore the default.

Syntax

identity { **address** { *ipv4-address* | **ipv6** { *ipv6-address* } } | **fqdn** *fqdn-name* | **email** *email-string* | **key-id** *key-id-string* }

undo identity

Default

The IKEv2 peer's ID is not specified.

Views

IKEv2 peer view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-address: Specifies the IPv4 address of the peer.

ipv6 *ipv6-address*: Specifies the IPv6 address of the peer.

fqdn *fqdn-name*: Specifies the FQDN of the peer. The *fqdn-name* argument is a case-sensitive string of 1 to 255 characters, such as www.test.com.

email *email-string*: Specifies the email address of the peer. The *email-string* argument is a case-sensitive string of 1 to 255 characters in the format defined by RFC 822, such as esec@test.com.

key-id *key-id-string*: Specifies the remote gateway's key ID. The *key-id-string* argument is a case-sensitive string of 1 to 255 characters, and is usually a vendor-specific string for doing proprietary types of identification.

Usage guidelines

Only the responder can look up an IKEv2 peer by ID in IKEv2 negotiation. The initiator does not know the peer ID when initiating the IKEv2 negotiation, so it cannot use an ID for IKEv2 peer lookup.

Examples

Create an IKEv2 keychain named **key1**.

```
<Sysname> system-view
[Sysname] ikev2 keychain key1
```

Create an IKEv2 peer named **peer1**.

```
[Sysname-ikev2-keychain-key1] peer peer1
```

Specify IPv4 address 1.1.1.2 as the ID of the IKEv2 peer.

```
[Sysname-ikev2-keychain-key1-peer-peer1] identity address 1.1.1.2
```

Related commands

ikev2 keychain

peer

identity local

Use **identity local** to configure the local ID, the ID that the device uses to identify itself to the peer during IKEv2 negotiation..

Use **undo identity local** to restore the default.

Syntax

identity local { **address** { *ipv4-address* | **ipv6** *ipv6-address* } | **dn** | **email** *email-string* | **fqdn** *fqdn-name* | **key-id** *key-id-string* }

undo identity local

Default

No local ID is configured. The IP address of the interface to which the IPsec policy is applied is used as the local ID.

Views

IKEv2 profile view

Predefined user roles

network-admin

context-admin

Parameters

address { *ipv4-address* | **ipv6** *ipv6-address* }: Uses an IPv4 or IPv6 address as the local ID.

dn: Uses the DN in the local certificate as the local ID.

email *email-string*: Uses an email address as the local ID. The *email-string* argument is a case-sensitive string of 1 to 255 characters in the format defined by RFC 822, such as sec@abc.com.

fqdn *fqdn-name*: Uses an FQDN as the local ID. The *fqdn-name* argument is a case-sensitive string of 1 to 255 characters, such as www.test.com.

key-id *key-id-string*: Uses the device's key ID as the local ID. The *key-id-string* argument is a case-sensitive string of 1 to 255 characters, and is usually a vendor-specific string for doing proprietary types of identification.

Usage guidelines

Peers exchange local IDs for identifying each other in negotiation.

Examples

Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

Use IP address 2.2.2.2 as the local ID.

```
[Sysname-ikev2-profile-profile1] identity local address 2.2.2.2
```

Related commands

peer

ikev2 address-group

Use **ikev2 address-group** to configure an IKEv2 IPv4 address pool for assigning IPv4 addresses to remote peers.

Use **undo ikev2 address-group** to delete an IKEv2 IPv4 address pool.

Syntax

ikev2 address-group *group-name start-ipv4-address end-ipv4-address* [*mask* | *mask-length*]

undo ikev2 address-group *group-name* [*start-ipv4-address* [*end-ipv4-address*]]

Default

No IKEv2 IPv4 address pools exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies an name for the IKEv2 IPv4 address pool. The *group-name* argument is a case-insensitive string of 1 to 63 characters.

start-ipv4-address end-ipv4-address: Specifies an IPv4 address range. The *start-ipv4-address* argument specifies the start IPv4 address. The *end-ipv4-address* argument specifies the end IPv4 address.

mask: Specifies the IPv4 address mask.

mask-length: Specifies the length of the IPv4 address mask.

Usage guidelines

An IKE IPv4 address pool can contain a maximum of 8192 IPv4 addresses.

Follow these guidelines when you delete IKEv2 IPv4 address pools:

- To delete all IPv4 address pools with a designated group name, use the **undo ikev2 address-group** *group-name* command.
- To delete an IPv4 address pool that contains only one IP address, use the **undo ikev2 address-group** *group-name start-ipv4-address* command.
- To delete a specific IPv4 address pool, use the **ikev2 address-group** *group-name start-ipv4-address end-ipv4-address* command.
- If the IPv4 address pool with the specified name and address range does not exist, no address group will be deleted.

Examples

Configure an IKEv2 IPv4 address pool with name **ipv4group**, address range 1.1.1.1 to 1.1.1.2, and mask 255.255.255.0.

```
<Sysname> system-view
[Sysname] ikev2 address-group ipv4group 1.1.1.1 1.1.1.2 255.255.255.0
```

Configure an IKEv2 IPv4 address pool with name **ipv4group**, address range 1.1.1.1 to 1.1.1.2, and mask length 32.

```
<Sysname> system-view
[Sysname] ikev2 address-group ipv4group 1.1.1.1 1.1.1.2 32
```

Delete IKEv2 IPv4 address pool **ipv4group** with address range 1.1.1.1 to 1.1.1.2.

```
<Sysname> system-view
[Sysname] undo ikev2 address-group ipv4group 1.1.1.1 1.1.1.2
```

Related commands

address-group

ikev2 cookie-challenge

Use **ikev2 cookie-challenge** to enable the cookie challenging feature.

Use **undo ikev2 cookie-challenge** to disable the cookie challenging feature.

Syntax

ikev2 cookie-challenge *number*

undo ikev2 cookie-challenge

Default

The cookie challenging feature is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

number: Specifies the threshold for triggering the cookie challenging feature. The value range for this argument is 0 to 1000 half-open IKE SAs.

Usage guidelines

When an IKEv2 responder maintains a threshold number of half-open IKE SAs, it starts the cookie challenging mechanism. The responder generates a cookie and includes it in the response sent to the initiator. If the initiator initiates a new IKE_SA_INIT request that carries the correct cookie, the responder considers the initiator valid and proceeds with the negotiation. If the carried cookie is incorrect, the responder terminates the negotiation.

This feature can protect the responder against DoS attacks which aim to exhaust the responder's system resources by using a large number of IKE_SA_INIT requests with forged source IP addresses.

Examples

Enable the cookie challenging feature and set the threshold to 450.

```
<Sysname> system-view
[Sysname] ikev2 cookie-challenge 450
```

ikev2 dpd

Use **ikev2 dpd** to configure global IKEv2 DPD.

Use **undo ikev2 dpd** to disable global IKEv2 DPD.

Syntax

ikev2 dpd interval *interval* [**retry** *seconds*] { **on-demand** | **periodic** }

undo ikev2 dpd interval

Default

The global IKEv2 DPD feature is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interval *interval*: Specifies a DPD triggering interval in the range of 10 to 3600 seconds.

retry *seconds*: Specifies the DPD retry interval in the range of 2 to 60 seconds. The default is 5 seconds.

on-demand: Triggers DPD on demand. The device triggers DPD if it has IPsec traffic to send and has not received any IPsec packets from the peer for the specified interval.

periodic: Triggers DPD at regular intervals. The device triggers DPD at the specified interval.

Usage guidelines

DPD is triggered periodically or on-demand. As a best practice, use the on-demand mode when the device communicates with a large number of IKEv2 peers. For an earlier detection of dead peers, use the periodic triggering mode, which consumes more bandwidth and CPU.

The triggering interval must be longer than the retry interval, so that the device will not trigger a new round of DPD during a DPD retry.

You can configure IKEv2 DPD in both IKEv2 profile view and system view. The IKEv2 DPD settings in IKEv2 profile view apply. If you do not configure IKEv2 DPD in IKEv2 profile view, the IKEv2 DPD settings in system view apply.

Examples

Configure the device to trigger IKEv2 DPD if it has IPsec traffic to send and has not received any IPsec packets from the peer for 15 seconds.

```
<Sysname> system-view
[Sysname] ikev2 dpd interval 15 on-demand
```

Configure the device to trigger IKEv2 DPD every 15 seconds.

```
<Sysname> system-view
[Sysname] ikev2 dpd interval 15 periodic
```

Related commands

dpd (IKEv2 profile view)

ikev2 ipv6-address-group

Use **ikev2 ipv6-address-group** to configure an IKEv2 IPv6 address pool for assigning IPv6 addresses to remote peers.

Use **undo ikev2 ipv6-address-group** to delete an IKEv2 IPv6 address pool.

Syntax

ikev2 ipv6-address-group *group-name* **prefix** *prefix/prefix-len* **assign-len** *assign-len*

undo ikev2 ipv6-address-group *group-name*

Default

No IKEv2 IPv6 address pools exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a name for the IKEv2 IPv6 address pool. The *group-name* argument is a case-insensitive string of 1 to 63 characters.

prefix *prefix/prefix-len*: Specifies an IPv6 prefix in the format of *prefix*/*prefix length*. The value range for the *prefix-len* argument is 1 to 128.

assign-len *assign-len*: Specifies the assigned prefix length. The value range for the *assign-len* argument is 1 to 128, and the value must be greater than or equal to *prefix-len*. The difference between *assign-len* and *prefix-len* must be no more than 16.

Usage guidelines

Different from the IKEv2 IPv4 address pool, the device assigns an IPv6 subnet to a peer from the IKEv2 IPv6 address pool. The peer can use the assigned IPv6 subnet to assign IPv6 addresses to other devices.

IKEv2 IPv6 address pools cannot overlap with each other.

Examples

Configure an IKEv2 IPv6 address pool with name **ipv6group**, prefix 1:1::/64, and assigned prefix length 80.

```
<Sysname> system-view
[Sysname] ikev2 ipv6-address-group ipv6group prefix 1:1::/64 assign-len 80
```

Related commands

ipv6-address-group

ikev2 keychain

Use **ikev2 keychain** to create an IKEv2 keychain and enter its view, or enter the view of an existing IKEv2 keychain.

Use **undo ikev2 keychain** to delete an IKEv2 keychain.

Syntax

ikev2 keychain *keychain-name*

undo ikev2 keychain *keychain-name*

Default

No IKEv2 keychains exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

keychain-name: Specifies a name for the IKEv2 keychain. The keychain name is a case-insensitive string of 1 to 63 characters and cannot contain a hyphen (-).

Usage guidelines

An IKEv2 keychain is required on both ends if either end uses preshared key authentication. The preshared key configured on both ends must be the same.

You can configure multiple IKEv2 peers in an IKEv2 keychain.

Examples

Create an IKEv2 keychain named **key1** and enter IKEv2 keychain view.

```
<Sysname> system-view
[Sysname] ikev2 keychain key1
[Sysname-ikev2-keychain-key1]
```

ikev2 nat-keepalive

Use **ikev2 nat-keepalive** to set the NAT keepalive interval.

Use **undo ikev2 nat-keepalive** to restore the default.

Syntax

ikev2 nat-keepalive *seconds*

undo ikev2 nat-keepalive

Default

The NAT keepalive interval is 10 seconds.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies the NAT keepalive interval in seconds, in the range of 5 to 3600.

Usage guidelines

This command takes effect when the device resides in the private network behind a NAT device. The device must send NAT keepalive packets regularly to its peer to keep the NAT session alive, so that the peer can access the device.

The NAT keepalive interval must be shorter than the NAT session lifetime.

Examples

Set the NAT keepalive interval to 5 seconds.

```
<Sysname> system-view
[Sysname] ikev2 nat-keepalive 5
```

ikev2 policy

Use **ikev2 policy** to create an IKEv2 policy and enter its view, or enter the view of an existing IKEv2 policy.

Use **undo ikev2 policy** to delete an IKEv2 policy.

Syntax

ikev2 policy *policy-name*

undo ikev2 policy *policy-name*

Default

An IKEv2 policy named **default** exists, which uses the default IKEv2 proposal and matches any local addresses.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies a name for the IKEv2 policy. The policy name is a case-insensitive string of 1 to 63 characters.

Usage guidelines

Each end must have an IKEv2 policy for the IKE_SA_INIT exchange. The initiator looks up an IKEv2 policy by the IP address of the interface to which the IPsec policy is applied and the VPN instance to which the interface belongs. The responder looks up an IKEv2 policy by the IP address of the interface that receives the IKEv2 packet and the VPN instance to which the interface belongs. An IKEv2 policy uses IKEv2 proposals to define the encryption algorithms, integrity protection algorithms, PRF algorithms, and DH groups to be used for negotiation.

You can configure multiple IKEv2 policies. An IKEv2 policy must have a minimum of one IKEv2 proposal. Otherwise, the policy is incomplete.

If the initiator uses an IPsec policy that is bound to a source interface, the initiator looks up an IKEv2 policy by the IP address of the source interface.

You can set priorities to adjust the match order of IKEv2 policies that have the same match criteria.

If no IKEv2 policy is configured, the default IKEv2 policy is used. You cannot enter the view of the default IKEv2 policy, nor modify it.

Examples

Create an IKEv2 policy named **policy1** and enter IKEv2 policy view.

```
<Sysname> system-view
[Sysname] ikev2 policy policy1
[Sysname-ikev2-policy-policy1]
```

Related commands

display ikev2 policy

ikev2 profile

Use **ikev2 profile** to create an IKEv2 profile and enter its view, or enter the view of an existing IKEv2 profile.

Use **undo ikev2 profile** to delete an IKEv2 profile.

Syntax

ikev2 profile *profile-name*

undo ikev2 profile *profile-name*

Default

No IKEv2 profiles exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

profile-name: Specifies a name for the IKEv2 profile. The profile name is a case-insensitive string of 1 to 63 characters.

Usage guidelines

An IKEv2 profile contains the IKEv2 SA parameters that are not negotiated, such as the identity information and authentication methods of the peers, and the matching criteria for profile lookup.

Examples

Create an IKEv2 profile named **profile1** and enter IKEv2 profile view.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
[Sysname-ikev2-profile-profile1]
```

Related commands

display ikev2 profile

ikev2 proposal

Use **ikev2 proposal** to create an IKEv2 proposal and enter its view, or enter the view of an existing IKEv2 proposal.

Use **undo ikev2 proposal** to delete an IKEv2 proposal.

Syntax

ikev2 proposal *proposal-name*

undo ikev2 proposal *proposal-name*

Default

An IKEv2 proposal named **default** exists.

The default IKEv2 proposal has the lowest priority and uses the following settings:

- **Encryption algorithm**—AES-CBC-128 and 3DES.

- **Integrity protection algorithm**—HMAC-SHA1 and HMAC-MD5.
- **PRF algorithm**—HMAC-SHA1 and HMAC-MD5.
- **DH group**—Group 5 and group 2.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

proposal-name: Specifies a name for the IKEv2 proposal. The proposal name is a case-insensitive string of 1 to 63 characters and cannot be **default**.

Usage guidelines

An IKEv2 proposal contains security parameters used in IKE_SA_INIT exchanges, including the encryption algorithms, integrity protection algorithms, PRF algorithms, and DH groups.

An IKEv2 proposal must have a minimum of one set of security parameters, including one encryption algorithm, one integrity protection algorithm, one PRF algorithm, and one DH group.

In an IKEv2 proposal, you can specify multiple parameters of the same type. The parameters of different types combine and form multiple sets of security parameters. If you want to use only one set of security parameters, configure only one set of security parameters for the IKEv2 proposal.

Examples

Create an IKEv2 proposal named **prop1**. Specify encryption algorithm AES-CBC-128, integrity protection algorithm SHA1, PRF algorithm SHA1, and DH group 2.

```
<Sysname> system-view
[Sysname] ikev2 proposal prop1
[Sysname-ikev2-proposal-prop1] encryption aes-cbc-128
[Sysname-ikev2-proposal-prop1] integrity sha1
[Sysname-ikev2-proposal-prop1] prf sha1
[Sysname-ikev2-proposal-prop1] dh group2
```

Related commands

encryption-algorithm

integrity

prf

dh

inside-vrf

Use **inside-vrf** to specify an inside VPN instance.

Use **undo inside-vrf** to restore the default.

Syntax

inside-vrf *vrf-name*

undo inside-vrf

Default

No inside VPN instance is specified. The internal and external networks are in the same VPN instance. The device forwards protected data to this VPN instance.

Views

IKEv2 profile view

Predefined user roles

network-admin

context-admin

Parameters

vrf-name: Specifies the VPN instance to which the protected data belongs. The *vrf-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

This command determines where the device should forward received IPsec packets after it de-encapsulates them. If you configure this command, the device looks for a route in the specified VPN instance to forward the packets. If you do not configure this command, the internal and external networks are in the same VPN instance. The device looks for a route in this VPN instance to forward the packets.

The inside VPN instance specified in an IKEv2 profile takes effect only on IPsec policies that use the IKEv2 profile. It does not take effect on IPsec profiles that use the IKEv2 profile.

Examples

Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

Specify inside VPN instance **vpn1**.

```
[Sysname-ikev2-profile-profile1] inside-vrf vpn1
```

integrity

Use **integrity** to specify integrity protection algorithms for an IKEv2 proposal.

Use **undo integrity** to restore the default.

Syntax

integrity { **aes-xcbc-mac** | **md5** | **sha1** | **sha256** | **sha384** | **sha512** } *

undo integrity

Default

No integrity protection algorithm is specified for an IKEv2 proposal.

Views

IKEv2 proposal view

Predefined user roles

network-admin

context-admin

Parameters

aes-xcbc-mac: Uses the HMAC-AES-XCBC-MAC algorithm.

md5: Uses the HMAC-MD5 algorithm.

sha1: Uses the HMAC-SHA1 algorithm.

sha256: Uses the HMAC-SHA256 algorithm.

sha384: Uses the HMAC-SHA384 algorithm.

sha512: Uses the HMAC-SHA512 algorithm.

Usage guidelines

You must specify a minimum of one integrity protection algorithm for an IKEv2 proposal. Otherwise, the proposal is incomplete and useless. You can specify multiple integrity protection algorithms for an IKEv2 proposal. An algorithm specified earlier has a higher priority.

Examples

Create an IKEv2 proposal named **prop1**.

```
<Sysname> system-view
[Sysname] ikev2 proposal prop1
```

Specify HMAC-SHA1 and HMAC-MD5 as the integrity protection algorithms, with HMAC-SHA1 preferred.

```
[Sysname-ikev2-proposal-prop1] integrity sha1 md5
```

Related commands

ikev2 proposal

keychain

Use **keychain** to specify an IKEv2 keychain for preshared key authentication.

Use **undo keychain** to restore the default.

Syntax

keychain *keychain-name*

undo keychain

Default

No IKEv2 keychain is specified for an IKEv2 profile.

Views

IKEv2 profile view

Predefined user roles

network-admin

context-admin

Parameters

keychain-name: Specifies an IKEv2 keychain by its name. The keychain name is a case-insensitive string of 1 to 63 characters and cannot contain a hyphen (-).

Usage guidelines

An IKEv2 keychain is required on both ends if either end uses preshared key authentication. You can specify only one IKEv2 keychain for an IKEv2 profile.

You can specify the same IKEv2 keychain for different IKEv2 profiles.

Examples

Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

Specify IKEv2 keychain **keychain1**.

```
[Sysname-ikev2-profile-profile1] keychain keychain1
```

Related commands

display ikev2 profile

ikev2 keychain

match local (IKEv2 profile view)

Use **match local** to specify a local interface or a local IP address to which an IKEv2 profile can be applied.

Use **undo match local** to remove a local interface or a local IP address to which an IKEv2 profile can be applied.

Syntax

match local address { *interface-type interface-number* | *ipv4-address* | **ipv6** *ipv6-address* }

undo match local address { *interface-type interface-number* | *ipv4-address* | **ipv6** *ipv6-address* }

Default

An IKEv2 profile can be applied to any local interface or IP address.

Views

IKEv2 profile view

Predefined user roles

network-admin

context-admin

Parameters

address: Specifies a local interface or IP address to which an IKEv2 profile can be applied.

interface-type interface-number: Specifies a local interface by its type and number. It can be any Layer 3 interface.

ipv4-address: Specifies the IPv4 address of a local interface.

ipv6 *ipv6-address*: Specifies the IPv6 address of a local interface.

Usage guidelines

Use this command to specify which address or interface can use the IKEv2 profile for IKEv2 negotiation. The interface is the interface that receives IKEv2 packets. The IP address is the IP address of the interface that receives IKEv2 packets.

An IKEv2 profile configured earlier has a higher priority. To give an IKEv2 profile that is configured later a higher priority, you can configure the **priority** command or this command for the profile. For example, suppose you configured IKEv2 profile A before configuring IKEv2 profile B, and you configured the **match remote identity address range 2.2.2.1 2.2.2.100** command for IKEv2 profile A and the **match remote identity address range 2.2.2.1 2.2.2.10**

command for IKEv2 profile B. For the local interface with the IP address 3.3.3.3 to negotiate with the peer 2.2.2.6, IKEv2 profile A is preferred because IKEv2 profile A was configured earlier. To use IKEv2 profile B, you can use this command to restrict the application scope of IKEv2 profile B to IPv4 address 3.3.3.3.

You can specify multiple applicable local interfaces or IP addresses for an IKEv2 profile.

Examples

Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

Apply IKEv2 profile **profile1** to the interface whose IP address is 2.2.2.2.

```
[Sysname-ikev2-profile-profile1] match local address 2.2.2.2
```

Related commands

match remote

match local address (IKEv2 policy view)

Use **match local address** to specify a local interface or a local address that an IKEv2 policy matches.

Use **undo match local address** to remove a local interface or a local address that an IKEv2 policy matches.

Syntax

match local address { *interface-type interface-number* | *ipv4-address* | **ipv6** *ipv6-address* }

undo match local address { *interface-type interface-number* | *ipv4-address* | **ipv6** *ipv6-address* }

Default

No local interface or local address is specified, and the IKEv2 policy matches any local interface or local address.

Views

IKEv2 policy view

Predefined user roles

network-admin

context-admin

Parameters

interface-type interface-number: Specifies a local interface by its type and number. It can be any Layer 3 interface.

ipv4-address: Specifies the IPv4 address of a local interface.

ipv6 *ipv6-address*: Specifies the IPv6 address of a local interface.

Usage guidelines

IKEv2 policies with this command configured are looked up before those that do not have this command configured.

Examples

Configure IKEv2 policy **policy1** to match local address 3.3.3.3.

```
<Sysname> system-view
[Sysname] ikev2 policy policy1
[Sysname-ikev2-policy-policy1] match local address 3.3.3.3
```

Related commands

display ikev2 policy

match vrf

match remote

Use **match remote** to configure a peer ID that an IKEv2 profile matches.

Use **undo match remote** to delete a peer ID that an IKEv2 profile matches.

Syntax

match remote { **certificate** *policy-name* | **identity** { **address** { { *ipv4-address* [*mask* | *mask-length*] | **range** *low-ipv4-address high-ipv4-address* } | **ipv6** { *ipv6-address* [*prefix-length*] | **range** *low-ipv6-address high-ipv6-address* } } | **fqdn** *fqdn-name* | **email** *email-string* | **key-id** *key-id-string* } }

undo match remote { **certificate** *policy-name* | **identity** { **address** { { *ipv4-address* [*mask* |*mask-length*] | **range** *low-ipv4-address high-ipv4-address* } | **ipv6** { *ipv6-address* [*prefix-length*] | **range** *low-ipv6-address high-ipv6-address* } } | **fqdn** *fqdn-name* | **email** *email-string* | **key-id** *key-id-string* } }

Default

No matching peer ID is configured for the IKEv2 profile.

Views

IKEv2 profile view

Predefined user roles

network-admin

context-admin

Parameters

certificate *policy-name*: Uses the information in the peer's digital certificate as the peer ID for IKEv2 profile matching. The *policy-name* argument specifies a certificate-based access control policy by its name, a case-insensitive string of 1 to 31 characters.

identity: Uses the specified information as the peer ID for IKEv2 profile matching. The specified information is configured on the peer by using the **identity local** command.

- **address** *ipv4-address* [*mask* | *mask-length*]: Uses an IPv4 host address or an IPv4 subnet address as the peer ID for IKEv2 profile matching. The value range for the *mask-length* argument is 0 to 32, and the default is 32.
- **address range** *low-ipv4-address high-ipv4-address*: Uses a range of IPv4 addresses as the peer ID for IKEv2 profile matching. The end address must be higher than the start address.
- **address ipv6** *ipv6-address* [*prefix-length*]: Uses an IPv6 host address or an IPv6 subnet address as the peer ID for IKEv2 profile matching. The value range for the *prefix-length* argument is 0 to 128, and the default is 128.

- **address ipv6 range** *low-ipv6-address high-ipv6-address*: Uses a range of IPv6 addresses as the peer ID for IKEv2 profile matching. The end address must be higher than the start address.
- **fqdn** *fqdn-name*: Uses the peer's FQDN as the peer ID for IKEv2 profile matching. The *fqdn-name* argument is a case-sensitive string of 1 to 255 characters, such as www.test.com.
- **email** *email-string*: Uses peer's email address as the peer ID for IKEv2 profile matching. The *email-string* argument is a case-sensitive string of 1 to 255 characters in the format defined by RFC 822, such as sec@abc.com.
- **key-id** *key-id-string*: Uses the peer's key ID as the peer ID for IKEv2 profile matching. The *key-id-string* argument is a case-sensitive string of 1 to 255 characters, and is usually a vendor-specific string for doing proprietary types of identification.

Usage guidelines

The device compares the received peer ID with the peer IDs configured in local IKEv2 profiles. If a match is found, it uses the IKEv2 profile with the matching peer ID for IKEv2 negotiation.

If the device has the **match remote**, **match vrf**, and **match local address** commands configured, it uses the IKEv2 profile that matches all the criteria configured by the commands.

To make sure only one IKEv2 profile is matched for a peer, do not configure the same peer ID for two or more IKEv2 profiles. If you configure the same peer ID for two or more IKEv2 profiles, which IKEv2 profile is selected for IKEv2 negotiation is unpredictable.

You can configure an IKEv2 profile to match multiple peer IDs. A peer ID configured earlier has a higher priority.

Examples

Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

Configure the IKEv2 profile to match the peer ID that is FQDN name www.test.com.

```
[Sysname-ikev2-profile-profile1] match remote identity fqdn www.test.com
```

Configure the IKEv2 profile to match the peer ID that is IP address 10.1.1.1.

```
[Sysname-ikev2-profile-profile1]match remote identity address 10.1.1.1
```

Related commands

identity local

match local address

match vrf

match vrf (IKEv2 policy view)

Use **match vrf** to specify a VPN instance that an IKEv2 policy matches.

Use **undo match vrf** to restore the default.

Syntax

match vrf { **name** *vrf-name* | **any** }

undo match vrf

Default

No VPN instance is specified, and the IKEv2 policy matches all local IP addresses in the public network.

Views

IKEv2 policy view

Predefined user roles

network-admin

context-admin

Parameters

name *vrf-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters.

any: Specifies the public network and all VPN instances.

Usage guidelines

Each end must have an IKEv2 policy for the IKE_SA_INIT exchange. The initiator looks up an IKEv2 policy by the IP address of the interface to which the IPsec policy is applied and the VPN instance to which the interface belongs. The responder looks up an IKEv2 policy by the IP address of the interface that receives the IKEv2 packet and the VPN instance to which the interface belongs.

IKEv2 policies with this command configured are looked up before those that do not have this command configured.

Examples

Create an IKEv2 policy named **policy1**.

```
<Sysname> system-view
[Sysname] ikev2 policy policy1
```

Configure the IKEv2 policy to match VPN instance **vpn1**.

```
[Sysname-ikev2-policy-policy1] match vrf name vpn1
```

Related commands

display ikev2 policy

match local address

match vrf (IKEv2 profile view)

Use **match vrf** to specify a VPN instance for an IKEv2 profile.

Use **undo match vrf** to restore the default.

Syntax

match vrf { **name** *vrf-name* | **any** }

undo match vrf

Default

The IKEv2 profile belongs to the public network.

Views

IKEv2 profile view

Predefined user roles

network-admin

context-admin

Parameters

name *vrf-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters.

any: Specifies the public network and all VPN instances.

Usage guidelines

If an IKEv2 profile belongs to a VPN instance, only interfaces in the VPN instance can use the IKEv2 profile for IKEv2 negotiation. The VPN instance is the VPN instance to which the interface that receives IKEv2 packets belongs. If you specify the **any** keyword, interfaces in any VPN instance can use the IKEv2 profile for IKEv2 negotiation.

Examples

Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

Specify **vrf1** as the VPN instance that the IKEv2 profile belongs to.

```
[Sysname-ikev2-profile-profile1] match vrf name vrf1
```

Related commands

match remote

nat-keepalive

Use **nat-keepalive** to set the NAT keepalive interval.

Use **undo nat-keepalive** to restore the default.

Syntax

nat-keepalive *seconds*

undo nat-keepalive

Default

The NAT keepalive interval set in system view is used.

Views

IKEv2 profile view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies the NAT keepalive interval in seconds, in the range of 5 to 3600.

Usage guidelines

This command takes effect when the device resides in the private network behind a NAT device. The device must send NAT keepalive packets regularly to its peer to keep the NAT session alive, so that the peer can access the device.

The NAT keepalive interval must be shorter than the NAT session lifetime.

Examples

Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
```

```
[Sysname] ikev2 profile profile1
```

Set the NAT keepalive interval to 1200 seconds.

```
[Sysname-ikev2-profile-profile1]nat-keepalive 1200
```

Related commands

display ikev2 profile

ikev2 nat-keepalive

peer

Use **peer** to create an IKEv2 peer and enter its view, or enter the view of an existing IKEv2 peer.

Use **undo peer** to delete an IKEv2 peer.

Syntax

peer *name*

undo peer *name*

Default

No IKEv2 peers exist.

Views

IKEv2 keychain view

Predefined user roles

network-admin

context-admin

Parameters

name: Specifies a name for the IKEv2 peer. The peer name is a case-insensitive string of 1 to 63 characters.

Usage guidelines

An IKEv2 peer contains a preshared key and the criteria for looking up the peer. The criteria for peer lookup includes the peer's host name, IP address, IP address range, and ID. The IKEv2 negotiation initiator uses the peer's host name, IP address, or IP address range to look up its peer. The responder uses the peer's IP address, IP address range, or ID to look up its peer.

Examples

Create an IKEv2 keychain named **key1** and enter IKEv2 keychain view.

```
<Sysname> system-view
[Sysname] ikev2 keychain key1
```

Create an IKEv2 peer named **peer1**.

```
[Sysname-ikev2-keychain-key1] peer peer1
```

Related commands

address

hostname

identity

ikev2 keychain

pre-shared-key

Use **pre-shared-key** to configure a preshared key.

Use **undo pre-shared-key** to delete a preshared key.

Syntax

pre-shared-key [**local** | **remote**] { **ciphertext** | **plaintext** } *string*

undo pre-shared-key [**local** | **remote**]

Default

No preshared key exists.

Views

IKEv2 peer view

Predefined user roles

network-admin

context-admin

Parameters

local: Specifies a preshared key for certificate signing.

remote: Specifies a preshared key for certificate authentication.

ciphertext: Specifies a preshared key in encrypted form.

plaintext: Specifies a preshared key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the preshared key. The key is case sensitive. Its plaintext form is a string of 1 to 128 characters and its encrypted form is a string of 1 to 201 characters.

Usage guidelines

If you specify the **local** or **remote** keyword, you configure an asymmetric key. If you specify neither the **local** nor the **remote** keyword, you configure a symmetric key.

To delete a key by using the **undo** command, you must specify the correct key type. For example, if you configure a key by using the **pre-shared-key local** command, you cannot delete the key by using the **undo pre-shared-key** or **undo pre-shared-key remote** command.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

- On the initiator:

  # Create an IKEv2 keychain named **key1**.

  ```
  <Sysname> system-view
  [Sysname] ikev2 keychain key1
  ```

  # Create an IKEv2 peer named **peer1**.

  ```
  [Sysname-ikev2-keychain-key1] peer peer1
  ```

  # Configure **111-key** as the symmetric plaintext preshared key.

  ```
  [Sysname-ikev2-keychain-key1-peer-peer1] pre-shared-key plaintext 111-key
  [Sysname-ikev2-keychain-key1-peer-peer1] quit
  ```

  # Create an IKEv2 peer named **peer2**.

  ```
  [Sysname-ikev2-keychain-key1] peer peer2
  ```

Configure asymmetric plaintext preshared keys. The key for certificate signing is **111-key-a** and the key for certificate authentication is **111-key-b**.

```
[Sysname-ikev2-keychain-key1-peer-peer2] pre-shared-key local plaintext 111-key-a
[Sysname-ikev2-keychain-key1-peer-peer2] pre-shared-key remote plaintext 111-key-b
```

- On the responder:

  # Create an IKEv2 keychain named **telecom**.

```
<Sysname> system-view
[Sysname] ikev2 keychain telecom
```

  # Create an IKEv2 peer named **peer1**.

```
[Sysname-ikev2-keychain-telecom] peer peer1
```

  # Configure **111-key** as the symmetric plaintext preshared key.

```
[Sysname-ikev2-keychain-telecom-peer-peer1] pre-shared-key plaintext 111-key
[Sysname-ikev2-keychain-telecom-peer-peer1] quit
```

  # Create an IKEv2 peer named **peer2**.

```
[Sysname-ikev2-keychain-telecom] peer peer2
```

  # Configure asymmetric plaintext preshared keys. The key for certificate signing is **111-key-b** and the key for certificate authentication is **111-key-a**.

```
[Sysname-ikev2-keychain-telecom-peer-peer2] pre-shared-key local plaintext
111-key-b
[Sysname-ikev2-keychain-telecom-peer-peer2] pre-shared-key remote plaintext
111-key-a
```

Related commands

ikev2 keychain

peer

prf

Use **prf** to specify pseudo-random function (PRF) algorithms for an IKEv2 proposal.

Use **undo prf** to restore the default.

Syntax

prf { **aes-xcbc-mac** | **md5** | **sha1** | **sha256** | **sha384** | **sha512** } *

undo prf

Default

An IKEv2 proposal uses the integrity protection algorithms as the PRF algorithms.

Views

IKEv2 proposal view

Predefined user roles

network-admin

context-admin

Parameters

aes-xcbc-mac: Uses the HMAC-AES-XCBC-MAC algorithm.

md5: Uses the HMAC-MD5 algorithm.

sha1: Uses the HMAC-SHA1 algorithm.

sha256: Uses the HMAC-SHA256 algorithm.

sha384: Uses the HMAC-SHA384 algorithm.

sha512: Uses the HMAC-SHA512 algorithm.

Usage guidelines

You can specify multiple PRF algorithms for an IKEv2 proposal. An algorithm specified earlier has a higher priority.

Examples

Create an IKEv2 proposal named **prop1**.

```
<Sysname> system-view
[Sysname] ikev2 proposal prop1
```

Specify HMAC-SHA1 and HMAC-MD5 as the PRF algorithms, with HMAC-SHA1 preferred.

```
[Sysname-ikev2-proposal-prop1] prf sha1 md5
```

Related commands

ikev2 proposal

integrity

priority (IKEv2 policy view)

Use **priority** to set a priority for an IKEv2 policy.

Use **undo priority** to restore the default.

Syntax

priority *priority*

undo priority

Default

The priority of an IKEv2 policy is 100.

Views

IKEv2 policy view

Predefined user roles

network-admin

context-admin

Parameters

priority: Specifies the priority of the IKEv2 policy, in the range of 1 to 65535. A smaller number represents a higher priority.

Usage guidelines

The priority set by this command can only be used to adjust the match order of IKEv2 policies.

Examples

Set the priority to 10 for IKEv2 policy **policy1**.

```
<Sysname> system-view
[Sysname] ikev2 policy policy1
[Sysname-ikev2-policy-policy1] priority 10
```

Related commands

display ikev2 policy

priority (IKEv2 profile view)

Use **priority** to set a priority for an IKEv2 profile.

Use **undo priority** to restore the default.

Syntax

priority *priority*

undo priority

Default

The priority of an IKEv2 profile is 100.

Views

IKEv2 profile view

Predefined user roles

network-admin

context-admin

Parameters

priority: Specifies the priority of the IKEv2 profile, in the range of 1 to 65535. A smaller number represents a higher priority.

Usage guidelines

The priority set by this command can only be used to adjust the match order of IKEv2 profiles.

Examples

Set the priority to 10 for IKEv2 profile **profile1**.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
[Sysname-ikev2-profile-profile1] priority 10
```

proposal

Use **proposal** to specify an IKEv2 proposal for an IKEv2 policy.

Use **undo proposal** to remove an IKEv2 proposal from an IKEv2 policy.

Syntax

proposal *proposal-name*

undo proposal *proposal-name*

Default

No IKEv2 proposal is specified for an IKEv2 policy.

Views

IKEv2 policy view

Predefined user roles

network-admin

context-admin

Parameters

proposal-name: Specifies an IKEv2 proposal by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

You can specify multiple IKEv2 proposals for an IKEv2 policy. A proposal specified earlier has a higher priority.

Examples

Specify IKEv2 proposal **proposal1** for IKEv2 policy **policy1**.

```
<Sysname> system-view
[Sysname] ikev2 policy policy1
[Sysname-ikev2-policy-policy1] proposal proposal1
```

Related commands

display ikev2 policy

ikev2 proposal

reset ikev2 sa

Use **reset ikev2 sa** to delete IKEv2 SAs.

Syntax

reset ikev2 sa [[{ **local** | **remote** } { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]] | **tunnel** *tunnel-id*] [**fast**]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

local: Deletes IKEv2 SAs for a local IP address.

remote: Deletes IKEv2 SAs for a remote IP address.

ipv4-address: Specifies a local or remote IPv4 address.

ipv6 *ipv6-address*: Specifies a local or remote IPv6 address.

vpn-instance *vpn-instance-name*: Deletes IKEv2 SAs in a VPN instance. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command deletes IKEv2 SAs for the public network.

tunnel *tunnel-id*: Deletes IKEv2 SAs for an IPsec tunnel. The *tunnel-id* argument specifies an IPsec tunnel by its ID in the range of 1 to 2000000000.

fast: Notifies the peers of the deletion and deletes IKEv2 SAs directly before receiving the peers' responses. If you do not specify this keyword, the device notifies the peers of the deletion and deletes IKEv2 SAs after it receives the peers' responses.

Usage guidelines

Deleting an IKEv2 SA will also delete the child SAs negotiated through the IKEv2 SA.

If you do not specify any parameters, this command deletes all IKEv2 SAs and the child SAs negotiated through the IKEv2 SAs.

Examples

Display information about IKEv2 SAs.

```
<Sysname> display ikev2 sa
     Tunnel ID          Local             Remote             Status
  ----------------------------------------------------------------------
     1                  1.1.1.1/500       1.1.1.2/500        EST
     2                  2.2.2.1/500       2.2.2.2/500        EST
  Status:
  IN-NEGO: Negotiating, EST: Established, DEL: Deleting
```

Delete the IKEv2 SA whose remote IP address is 1.1.1.2.

```
<Sysname> reset ikev2 sa remote 1.1.1.2
```

Display information about IKEv2 SAs again. Verify that the IKEv2 SA is deleted.

```
<Sysname> display ikev2 sa
     Tunnel ID          Local             Remote             Status
  ----------------------------------------------------------------------
     2                  2.2.2.1/500       2.2.2.2/500        EST
  Status:
  IN-NEGO: Negotiating, EST: Established, DEL: Deleting
```

Related commands

`display ikev2 sa`

reset ikev2 statistics

Use **`reset ikev2 statistics`** to clear IKEv2 statistics.

Syntax

`reset ikev2 statistics`

Views

User view

Predefined user roles

network-admin

context-admin

Examples

Clear IKEv2 statistics.

```
<Sysname> reset ikev2 statistics
```

Related commands

`display ikev2 statistics`

sa duration

Use **sa duration** to set the IKEv2 SA lifetime.

Use **undo sa duration** to restore the default.

Syntax

sa duration *seconds*

undo sa duration

Default

The IKEv2 SA lifetime is 86400 seconds.

Views

IKEv2 profile view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies the IKEv2 SA lifetime in seconds, in the range of 120 to 86400.

Usage guidelines

An IKEv2 SA can be used for subsequent IKEv2 negotiations before its lifetime expires, saving a lot of negotiation time. However, the longer the lifetime, the higher the possibility that attackers collect enough information and initiate attacks.

Two peers can have different IKEv2 SA lifetime settings, and they do not perform lifetime negotiation. The peer with a shorter lifetime always initiates the rekeying.

Examples

Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

Set the IKEv2 SA lifetime to 1200 seconds.

```
[Sysname-ikev2-profile-profile1] sa duration 1200
```

Related commands

display ikev2 profile

Contents

ADVPN commands

VAM server commands

The following compatibility matrixes show the support of hardware platforms for VAM server:

Models	VAM server compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080	Yes
NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	No

authentication-algorithm

Use **authentication-algorithm** to specify the algorithms for VAM protocol packet authentication and their priorities.

Use **undo authentication-algorithm** to restore the default.

Syntax

authentication-algorithm { **aes-xcbc-mac** | **md5** | **none** | **sha-1** | **sha-256** } *

undo authentication-algorithm

Default

SHA-1 is used for protocol packet authentication.

Views

ADVPN domain view

Predefined user roles

network-admin

context-admin

Parameters

aes-xcbc-mac: Uses the AES-XCBC-MAC authentication algorithm.

md5: Uses the MD5 authentication algorithm.

none: Performs no authentication.

sha-1: Uses the SHA-1 authentication algorithm.

sha-256: Uses the SHA-256 authentication algorithm.

Usage guidelines

The VAM server and client use SHA-1 for connection request and response packet authentication, and use the negotiated algorithms for negotiation acknowledgment and subsequent VAM protocol packet authentication.

An authentication algorithm specified earlier by using this command has a higher priority during algorithm negotiation between a VAM server and a client. The VAM server compares its algorithms

in descending order of priority with the algorithms sent by the client, and sends the matching algorithm with the highest priority to the client.

The configuration of this command does not affect registered VAM clients. It applies to subsequently registered VAM clients.

Examples

Specify the authentication algorithms as MD5, SHA-1, and SHA-256 in descending order of priority for ADVPN domain 1.

```
<Sysname> system-view
[Sysname] vam server advpn-domain 1
[Sysname-vam-server-domain-1] authentication-algorithm md5 sha-1 sha-256
```

authentication-method

Use **authentication-method** to specify an authentication mode that the VAM server uses to authenticate clients.

Use **undo authentication-method** to restore the default.

Syntax

authentication-method { **none** | { **chap** | **pap** } [**domain** *isp-name*] }

undo authentication-method

Default

The authentication method is CHAP, and the default domain is used.

Views

ADVPN domain view

Predefined user roles

network-admin

context-admin

Parameters

none: Performs no authentication on clients.

chap: Performs CHAP authentication.

pap: Performs PAP authentication.

domain *isp-name*: Specifies an ISP domain for authentication. The *isp-name* argument is a case-insensitive string of 1 to 255 characters. It cannot include back slashes (\), vertical bars (|), slashes (/), colons (:), asterisks (*), question marks (?), quotation marks ("), left angle brackets (<), right angle brackets (>), and at signs (@). If you do not specify this option, the default domain is used for authentication.

Usage guidelines

If the specified ISP domain does not exist, the authentication will fail.

A newly configured authentication method does not affect registered VAM clients. It applies to subsequently registered VAM clients.

Examples

Configure the VAM server to use CHAP to authenticate clients.

```
<Sysname> system-view
[Sysname] vam server advpn-domain 1
```

```
[Sysname-vam-server-domain-1] authentication-method chap
```

display vam server address-map

Use **display vam server address-map** to display IPv4 private-public address mapping information for VAM clients registered with the VAM server.

Syntax

display vam server address-map [**advpn-domain** *domain-name* [**private-address** *private-ip-address*]] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

advpn-domain *domain-name*: Displays IPv4 address mapping information for VAM clients in the specified ADVPN domain. The *domain-name* argument is a case-insensitive string of 1 to 31 characters that can include only letters, digits, and dots (.). If you do not specify this option, the command displays address mapping information for VAM clients in all ADVPN domains.

private-address *private-ip-address*: Displays IPv4 address mapping information for the VAM client with the specified private IPv4 address. If you do not specify this option, the command displays mapping information for VAM clients in the specified domain or all ADVPN domains.

verbose: Displays detailed address mapping information. If you do not specify this keyword, the command displays brief address mapping information.

Examples

Display IPv4 address mapping information for VAM clients in all ADVPN domains.

```
<Sysname> display vam server address-map
ADVPN domain name: 1
Total private address mappings: 2
Group      Private address  Public address             Type   NAT  Holding time
1          10.0.0.1         2001::1                   Hub    No   0H 13M 34S
1          10.0.0.3         74.125.128.102            Spoke  Yes  0H 4M 21S

ADVPN domain name: 2
Total private address mappings: 0

ADVPN domain name: 3
Total private address mappings: 1
Group      Private address  Public address             Type   NAT  Holding time
1          30.0.0.1         113.124.136.1             Hub    No   0H 0M 2S

ADVPN domain name: 4
Total private address mappings: 1
Group      Private address  Public address             Type   NAT  Holding time
```

```
1          40.0.0.1         4001::1                    Hub    No   1H 8M 22S

ADVPN domain name: 5
Total private address mappings: 1
Group      Private address  Public address             Type   NAT  Holding time
1          50.0.0.1         115.194.156.1              Hub    No   132H 41M 29S
```

Display IPv4 address mapping information for VAM clients in ADVPN domain 1.

```
<Sysname> display vam server address-map advpn-domain 1
ADVPN domain name: 1
Total private address mappings: 2
Group      Private address  Public address             Type   NAT  Holding time
1          10.0.0.1         2001::1                    Hub    No   0H 13M 34S
1          10.0.0.3         74.125.128.102             Spoke  Yes  0H 4M 21S
```

Display IPv4 address mapping information for the VAM client with private IPv4 address 10.0.0.1 in ADVPN domain 1.

```
<Sysname> display vam server address-map advpn-domain 1 private-address 10.0.0.1
Group      Private address  Public address             Type   NAT  Holding time
1          10.0.0.1         2001::1                    Hub    No   0H 13M 34S
```

Table 1 Command output

Field	Description
Group	Hub group to which the VAM client belongs.
Private address	Private address that the VAM client has registered with the VAM server.
Public address	Public address that the VAM client has registered with the VAM server.
Type	VAM client type: **Hub** or **Spoke**.
NAT	Whether NAT traversal is used: **No** or **Yes**.
Holding time	Duration time that elapses since the VAM client successfully registered with the server, in the format of xH yM zS.

Display detailed IPv4 address mapping information for VAM clients in all ADVPN domains.

```
<Sysname> display vam server address-map verbose
ADVPN domain name : 1
Private address   : 10.0.0.1
Type              : Hub
Hub group         : 1
Holding time      : 0H 13M 34S
Link protocol     : UDP
Public address    : 2001::1
Public port       : 10018
Registered address: 2001::1
Registered port   : 10018
Behind NAT        : No

ADVPN domain name : 1
Private address   : 10.0.0.3
Type              : Spoke
Hub group         : 1
```

```
Holding time      : 0H 4M 21S
Link protocol     : UDP
Public address    : 74.125.128.102
Public port       : 11297
Registered address: 192.168.23.6
Registered port   : 2158
Behind NAT        : Yes

ADVPN domain name : 3
Private address   : 30.0.0.1
Type              : Hub
Hub group         : 1
Holding time      : 0H 0M 2S
Link protocol     : GRE
Public address    : 113.124.136.1
Registered address: 113.124.136.1
Behind NAT        : No

ADVPN domain name : 4
Private address   : 40.0.0.1
Hub group         : 1
Holding time      : 1H 8M 22S
Link protocol     : IPsec-UDP
Public address    : 4001::1
Registered address: 4001::1
Registered port   : 4072
Behind NAT        : No

ADVPN domain name : 5
Private address   : 50.0.0.1
Type              : Hub
Hub group         : 1
Holding time      : 132H 41M 29S
Link protocol     : IPsec-GRE
Public address    : 115.194.156.1
Registered address: 115.194.156.1
Behind NAT        : No
```

Display detailed IPv4 address mapping information for VAM clients in ADVPN domain 1.

```
<Sysname> display vam server address-map advpn-domain 1 verbose
ADVPN domain name : 1
Private address   : 10.0.0.1
Type              : Hub
Hub group         : 1
Holding time      : 0H 13M 34S
Link protocol     : UDP
Public address    : 2001::1
Public port       : 10018
Registered address: 2001::1
```

```
Registered port   : 10018
Behind NAT        : No

ADVPN domain name : 1
Private address   : 10.0.0.3
Type              : Spoke
Hub group         : 1
Holding time      : 0H 4M 21S
Link protocol     : UDP
Public address    : 74.125.128.102
Public port       : 11297
Registered address: 192.168.23.6
Registered port   : 2158
Behind NAT        : Yes
```

Display detailed IPv4 address mapping information for the VAM client with private IPv4 address 10.0.0.1 in ADVPN domain 1.

```
<Sysname> display vam server address-map advpn-domain 1 private-address 10.0.0.1 verbose
ADVPN domain name : 1
Private address   : 10.0.0.1
Type              : Hub
Hub group         : 1
Holding time      : 0H 13M 34S
Link protocol     : UDP
Public address    : 2001::1
Public port       : 10018
Registered address: 2001::1
Registered port   : 10018
Behind NAT        : No
```

Table 2 Command output

Field	Description
Private address	Private address that the VAM client has registered with the VAM server.
Type	VAM client type: **Hub** or **Spoke**.
Hub group	Hub group to which the VAM client belongs.
Holding time	Duration time that elapses since the VAM client successfully registered with the server, in the format of xH yM zS.
Link protocol	Link layer protocol used by the VAM client for ADVPN tunnel establishment: • **UDP**. • **GRE**. • **IPsec-UDP**. • **IPsec-GRE**.
Public address	VAM client's public IP address that has been NATed.
Public port	VAM client's ADVPN port number that has been NATed. This field is displayed when the **Link protocol** is **UDP** or **IPsec-UDP**.
Registered address	Public address that the VAM client has registered with the VAM server.

Field	Description
Registered port	ADVPN port number that the VAM client has registered with the VAM server. This field is displayed when the **Link protocol** is **UDP** or **IPsec-UDP**.
IPsec address	IP address used by the VAM client for IPsec tunnel establishment. This field is displayed when the **Link protocol** is **IPsec-UDP** or **IPsec-GRE**.
IPsec port	UDP port number used by the VAM client for IPsec tunnel establishment. This field is displayed when the **Link protocol** is **IPsec-UDP** or **IPsec-GRE**.
Behind NAT	Whether NAT traversal is used: **No** or **Yes**.

Related commands

reset vam server address-map

display vam server ipv6 address-map

Use **display vam server ipv6 address-map** to display IPv6 private-public address mapping information for VAM clients registered with the VAM server.

Syntax

display vam server ipv6 address-map [**advpn-domain** *domain-name* [**private-address** *private-ipv6-address*]] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

advpn-domain *domain-name*: Displays IPv6 address mapping information for VAM clients in the specified ADVPN domain. The *domain-name* argument is a case-insensitive string of 1 to 31 characters that can include only letters, digits, and dots (.). If you do not specify this option, the command displays address mapping information for VAM clients in all ADVPN domains.

private-address *private-ipv6-address*: Displays IPv6 address mapping information for the VAM client with the specified private IPv6 address. If you do not specify this option, the command displays mapping information for VAM clients in the specified domain or all ADVPN domains.

verbose: Displays detailed address mapping information. If you do not specify this keyword, the command displays brief address mapping information.

Examples

Display IPv6 address mapping information for VAM clients in all ADVPN domains.

```
<Sysname> display vam server ipv6 address-map
ADVPN domain name: 1
Total private address mappings: 2
Group      Private address       Public address         Type   NAT  Holding time
```

```
1          1000::1:0:0:1         2001::1               Hub    No   0H 13M 34S
2          1000::2:0:0:1         220.181.111.85        Spoke  Yes  0H 4M 21S

ADVPN domain name: 2
Total private address mappings: 0

ADVPN domain name: 3
Total private address mappings: 1
Group      Private address       Public address        Type   NAT  Holding time
1          1003::1:0:0:1         3001::1               Hub    No   0H 0M 2S

ADVPN domain name: 4
Total private address mappings: 1
Group      Private address       Public address        Type   NAT  Holding time
1          1004::1:0:0:1         202.108.231.125       Hub    No   1H 8M 22S

ADVPN domain name: 5
Total private address mappings: 1
Group      Private address       Public address        Type   NAT  Holding time
1          1005::1:0:0:1         5001::1               Hub    No   132H 41M 29S
```

Display IPv6 address mapping information for VAM clients in ADVPN domain 1.

```
<Sysname> display vam server ipv6 address-map advpn-domain 1
ADVPN domain name: 1
Total private address mappings: 2
Group      Private address       Public address        Type   NAT  Holding time
1          1000::1:0:0:1         2001::1               Hub    No   0H 13M 34S
2          1000::2:0:0:1         220.181.111.85        Spoke  Yes  0H 4M 21S
```

Display IPv6 address mapping information for the VAM client with private IPv6 address 1000::1:0:0:1 in ADVPN domain 1.

```
<Sysname> display vam server ipv6 address-map advpn-domain 1 private-address 1000::1:0:0:1
Group      Private address       Public address        Type   NAT  Holding time
1          1000::1:0:0:1         2001::1               Hub    No   0H 13M 34S
```

Table 3 Command output

Field	Description
Group	Hub group to which the VAM client belongs.
Private address	Private address that the VAM client has registered with the VAM server.
Public address	Public address that the VAM client has registered with the VAM server.
Type	VAM client type: **Hub** or **Spoke**.
NAT	Whether NAT traversal is used: **No** or **Yes**.
Holding time	Duration time that elapses since the VAM client successfully registered with the server, in the format of xH yM zS.

Display detailed IPv6 address mapping information for VAM clients in all ADVPN domains.

```
<Sysname> display vam server ipv6 address-map verbose
ADVPN domain name : 1
Private address   : 1000::1:0:0:1
```

```
Link local address: FE80::50:4
Type              : Hub
Hub group         : 1
Holding time      : 0H 13M 34S
Link protocol     : UDP
Public address    : 2001::1
Public port       : 2098
Registered address: 2001::1
Registered port   : 2098
Behind NAT        : No

ADVPN domain name : 1
Private address   : 1000::2:0:0:1
Link local address: FE80::60:4
Type              : Spoke
Hub group         : 2
Holding time      : 0H 4M 21S
Link protocol     : UDP
Public address    : 220.181.111.85
Public port       : 10018
Registered address: 10.158.26.14
Registered port   : 2694
Behind NAT        : Yes

ADVPN domain name : 3
Private address   : 1003::1:0:0:1
Link local address: FE80::70:4
Type              : Hub
Hub group         : 1
Holding time      : 0H 0M 2S
Link protocol     : GRE
Public address    : 3001::1
Registered address: 3001::1
Behind NAT        : No

ADVPN domain name : 4
Private address   : 1004::1:0:0:1
Link local address: FE80::80:4
Hub group         : 1
Holding time      : 1H 8M 22S
Link protocol     : IPsec-UDP
Public address    : 202.108.231.125
Registered address: 202.108.231.125
Registered port   : 4072
Behind NAT        : No

ADVPN domain name : 5
Private address   : 1005::1:0:0:1
```

```
Link local address: FE80::90:4
Type              : Hub
Hub group         : 1
Holding time      : 132H 41M 29S
Link protocol     : IPsec-GRE
Public address    : 5001::1
Registered address: 5001::1
Behind NAT        : No
```

Display detailed IPv6 address mapping information for VAM clients in ADVPN domain 1.

```
<Sysname> display vam server ipv6 address-map advpn-domain 1 verbose
ADVPN domain name : 1
Private address   : 1000::1:0:0:1
Link local address: FE80::50:4
Type              : Hub
Hub group         : 1
Holding time      : 0H 13M 34S
Link protocol     : UDP
Public address    : 2001::1
Public port       : 2098
Registered address: 2001::1
Registered port   : 2098
Behind NAT        : No

ADVPN domain name : 1
Private address   : 1000::2:0:0:1
Link local address: FE80::60:4
Type              : Spoke
Hub group         : 2
Holding time      : 0H 4M 21S
Link protocol     : UDP
Public address    : 220.181.111.85
Public port       : 10018
Registered address: 10.158.26.14
Registered port   : 2694
Behind NAT        : Yes
```

Display detailed IPv6 address mapping information for the VAM client with private IPv6 address 1000::1:0:0:1 in ADVPN domain 1.

```
<Sysname> display vam server ipv6 address-map advpn-domain 1 ipv6 private-address
1000::1:0:0:1 verbose
ADVPN domain name : 1
Private address   : 1000::1:0:0:1
Link local address: FE80::50:4
Type              : Hub
Hub group         : 1
Holding time      : 0H 13M 34S
Link protocol     : UDP
Public address    : 2001::1
Public port       : 2098
```

```
Registered address: 2001::1
Registered port   : 2098
Behind NAT        : No
```

Table 4 Command output

Field	Description
Private address	Private address that the VAM client has registered with the VAM server.
Link local address	Link local address that the VAM client has registered with the VAM server.
Type	VAM client type: **Hub** or **Spoke**.
Hub group	Hub group to which the VAM client belongs.
Holding time	Duration time that elapses since the VAM client successfully registered with the server, in the format of xH yM zS.
Link protocol	Link layer protocol used by the VAM client for ADVPN tunnel establishment: • **UDP**. • **GRE**. • **IPsec-UDP**. • **IPsec-GRE**.
Public address	VAM client's public IP address that has been NATed.
Public port	VAM client's ADVPN port number that has been NATed. This field is displayed when the **Link protocol** is **UDP** or **IPsec-UDP**.
Registered address	Public address that the VAM client has registered with the VAM server.
Registered port	ADVPN port number that the VAM client has registered with the VAM server. This field is displayed when the **Link protocol** is **UDP** or **IPsec-UDP**.
IPsec address	IP address used by the VAM client for IPsec tunnel establishment. This field is displayed when the **Link protocol** is **IPsec-UDP** or **IPsec-GRE**.
IPsec port	UDP port number used by the VAM client for IPsec tunnel establishment. This field is displayed when the **Link protocol** is **IPsec-UDP** or **IPsec-GRE**.
Behind NAT	Whether NAT traversal is used: **No** or **Yes**.

Related commands

reset vam server ipv6 address-map

display vam server ipv6 private-network

Use **display vam server ipv6 private-network** to display IPv6 private networks for VAM clients registered with the VAM server.

Syntax

display vam server ipv6 private-network [**advpn-domain** *domain-name* [**private-address** *private-ipv6-address*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

advpn-domain *domain-name*: Displays IPv6 private networks for VAM clients in the specified ADVPN domain. The *domain-name* argument is a case-insensitive string of 1 to 31 characters that can include only letters, digits, and dots (.). If you do not specify this option, the command displays IPv6 private networks for VAM clients in all ADVPN domains.

private-address *private-ipv6-address*: Displays IPv6 private networks for the VAM client with the specified private IPv6 address. If you do not specify this option, the command displays IPv6 private networks for VAM clients in the specified domain or all ADVPN domains.

Examples

Display IPv6 private networks for VAM clients in all ADVPN domains.

```
<Sysname> display vam server ipv6 private-network
ADVPN domain name: 1
Total private networks: 5
Network/Prefix                    Private address                   Preference
1000::1:0:0:0/96                  1000::1:0:0:2                     80
1000::1:0:0:0/100                 1000::1:0:0:1                     80
1000::1:1:0:0/96                  1000::1:0:0:1                     80
1000::2:0:0:0/96                  1000::1:0:0:2                     80
1000::2:0:0:0/96                  1000::2:0:0:2                     80

ADVPN domain name: 2
Total private networks: 0

ADVPN domain name: 3
Total private networks: 1
Network/Prefix                    Private address                   Preference
1001::1:0:0:0/100                 1001::1:0:0:1                     80
```

Display IPv6 private networks for VAM clients in ADVPN domain 1.

```
<Sysname> display vam server ipv6 private-network advpn-domain 1
ADVPN domain name: 1
Total private networks: 5
Network/Prefix                    Private address                   Preference
1000::1:0:0:0/96                  1000::1:0:0:2                     80
1000::1:0:0:0/100                 1000::1:0:0:1                     80
1000::1:1:0:0/96                  1000::1:0:0:1                     80
1000::2:0:0:0/96                  1000::1:0:0:2                     80
1000::2:0:0:0/96                  1000::2:0:0:2                     80
```

Display IPv6 private networks for the VAM client with private IPv6 address 1000::1:0:0:1.

```
<Sysname> display vam server ipv6 private-network advpn-domain 1 private-address
1000::1:0:0:1
Total private networks: 2
```

```
Network/Prefix                  Private address                 Preference
1000::1:0:0:0/100               1000::1:0:0:1                   80
1000::1:1:0:0/96                1000::1:0:0:1                   80
```

Table 5 Command output

Field	Description
Network/Prefix	Private network address/prefix length for an ADVPN tunnel interface.
Private address	Private address that the VAM client has registered with the VAM server.
Preference	Preference of the private route that the VAM client has registered with the VAM server.

display vam server private-network

Use **display vam server private-network** to display IPv4 private networks for VAM clients registered with the VAM server.

Syntax

display vam server private-network [**advpn-domain** *domain-name* [**private-address** *private-ip-address*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

advpn-domain *domain-name*: Displays IPv4 private networks for VAM clients in the specified ADVPN domain. The *domain-name* argument is a case-insensitive string of 1 to 31 characters that can include only letters, digits, and dots (.). If you do not specify this option, the command displays IPv4 private networks for VAM clients in all ADVPN domains.

private-address *private-ip-address*: Displays IPv4 private networks for the VAM client with the specified private IPv4 address. If you do not specify this option, the command displays IPv6 private networks for VAM clients in the specified domain or all ADVPN domains.

Examples

Display IPv4 private networks for VAM clients in all ADVPN domains.

```
<Sysname> display vam server private-network
ADVPN domain name: 1
Total private networks: 5
Network/Mask              Private address        Preference
192.168.0.0/24            10.0.0.2               80
192.168.0.0/28            10.0.0.1               80
192.168.1.0/24            10.0.0.1               80
192.168.100.0/24          10.0.0.2               80
192.168.100.0/24          10.0.0.3               80
```

```
ADVPN domain name: 2
Total private networks: 0

ADVPN domain name: 3
Total private networks: 1
Network/Mask              Private address        Preference
192.168.200.0/24          20.0.0.1               80
```

Display IPv4 private networks for VAM clients in ADVPN domain 1.

```
<Sysname> display vam server private-network advpn-domain 1
ADVPN domain name: 1
Total private networks: 5
Network/Mask              Private address        Preference
192.168.0.0/24            10.0.0.2               80
192.168.0.0/28            10.0.0.1               80
192.168.1.0/24            10.0.0.1               80
192.168.100.0/24          10.0.0.2               80
192.168.100.0/24          10.0.0.3               80
```

Display IPv4 private networks for the VAM client with private IPv4 address 10.0.0.1.

```
<Sysname> display vam server private-network advpn-domain 1 private-address 10.0.0.1
Total private networks: 5
Network/Mask              Private address        Preference
192.168.0.0/28            10.0.0.1               80
192.168.1.0/24            10.0.0.1               80
```

Table 6 Command output

Field	Description
Network/Mask	Private network address/mask length for an ADVPN tunnel interface.
Private address	Private address that the VAM client has registered with the VAM server.
Preference	Preference of the private route that the VAM client has registered with the VAM server.

display vam server statistics

Use **display vam server statistics** to display ADVPN domain statistics on the VAM server.

Syntax

display vam server statistics [**advpn-domain** *domain-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

advpn-domain *domain-name*: Displays statistics for the specified ADVPN domain. The *domain-name* argument is a case-insensitive string of 1 to 31 characters that can include only letters, digits, and dots (.). If you do not specify this option, the command displays statistics for all ADVPN domains on the VAM server.

Examples

Display statistics for all ADVPN domains.

```
<Sysname> display vam server statistics
Total ADVPN number: 3
Total spoke number: 121
Total hub number  : 3

ADVPN domain name      : 1
Server status          : Enabled
Holding time           : 0H 1M 47S
Registered spoke number: 98
Registered hub number  : 2
Packets received:
  Initialization request        : 100
  Initialization complete       : 100
  Register request              : 100
  Authentication information    : 100
  Address resolution request    : 203
  Network registration request  : 59
  Update request                : 196
  Logout request                : 0
  Hub information response      : 2
  Data flow information response: 0
  Keepalive                     : 642
  Error notification            : 0
  Unknown                       : 0
Packets sent:
  Initialization response      : 100
  Initialization complete      : 100
  Authentication request       : 100
  Register response            : 100
  Address resolution response  : 203
  Network registration response: 59
  Update response              : 196
  Hub information request      : 2
  Data flow information request: 0
  Logout response              : 0
  Keepalive                    : 642
  Error notification           : 0

ADVPN domain name      : 2
Server status          : Disabled
```

```
ADVPN domain name      : 3
Server status          : Enabled
Holding time           : 0H 33M 53S
Registered spoke number: 23
Registered hub number  : 1
Packets received:
  Initialization request        : 24
  Initialization complete       : 24
  Register request              : 24
  Authentication information    : 24
  Address resolution request    : 23
  Network registration request  : 0
  Update request                : 5
  Logout request                : 0
  Hub information response      : 2
  Data flow information response: 0
  Keepalive                     : 362
  Error notification            : 0
  Unknown                       : 0
Packets sent:
  Initialization response      : 24
  Initialization complete      : 24
  Authentication request       : 24
  Register response            : 24
  Address resolution response  : 23
  Network registration response: 0
  Update response              : 0
  Hub information request      : 2
  Data flow information request: 0
  Logout response              : 0
  Keepalive                    : 362
  Error notification           : 0
```

Display statistics for ADVPN domain 1.

```
<Sysname> display vam server statistics advpn-domain 1
ADVPN domain name      : 1
Server status          : Enabled
Holding time           : 0H 1M 47S
Registered spoke number: 98
Registered hub number  : 2
Packets received:
  Initialization request        : 100
  Initialization complete       : 100
  Register request              : 100
  Authentication information    : 100
  Address resolution request    : 203
  Network registration request  : 59
  Update request                : 196
  Logout request                : 0
```

```
  Hub information response      : 2
  Data flow information response: 0
  Keepalive                     : 642
  Error notification            : 0
  Unknown                       : 0
Packets sent:
  Initialization response      : 100
  Initialization complete      : 100
  Authentication request       : 100
  Register response            : 100
  Address resolution response  : 203
  Network registration response: 59
  Update response              : 196
  Hub information request      : 2
  Data flow information request: 0
  Logout response              : 0
  Keepalive                    : 642
  Error notification           : 0
```

Table 7 Command output

Field	Description
Server status	Whether the VAM server is enabled: **Enabled** or **Disabled**.
Holding time	Duration time that elapses after the VAM service is enabled, in the format of xH yM zS.

Related commands

reset vam server statistics

encryption-algorithm

Use **encryption-algorithm** to specify the algorithms for VAM protocol packet encryption and their priorities.

Use **undo encryption-algorithm** to restore the default.

Syntax

encryption-algorithm { **3des-cbc** | **aes-cbc-128** | **aes-cbc-192** | **aes-cbc-256** | **aes-ctr-128** | **aes-ctr-192** | **aes-ctr-256** | **des-cbc** | **none** } *

undo encryption-algorithm

Default

The following encryption algorithms are available (in descending order of priority):

- AES-CBC-256
- AES-CBC-192
- AES-CBC-128
- AES-CTR-256
- AES-CTR-192
- AES-CTR-128
- 3DES-CBC

- DES-CBC

Views

ADVPN domain view

Predefined user roles

network-admin

context-admin

Parameters

3des-cbc: Uses the 3DES-CBC encryption algorithm.

aes-cbc-128: Uses the AES-CBC encryption algorithm, with a key length of 128 bits.

aes-cbc-192: Uses the AES-CBC encryption algorithm, with a key length of 192 bits.

aes-cbc-256: Uses the AES-CBC encryption algorithm, with a key length of 256 bits.

aes-ctr-128: Uses the AES-CTR encryption algorithm, with a key length of 128 bits.

aes-ctr-192: Uses the AES-CTR encryption algorithm, with a key length of 192 bits.

aes-ctr-256: Uses the AES-CTR encryption algorithm, with a key length of 256 bits.

des-cbc: Uses the DES-CBC encryption algorithm.

none: Performs no encryption.

Usage guidelines

The VAM server and client use AES-CBC-128 for connection request and response packet encryption, and use the negotiated algorithms for negotiation acknowledgment and subsequent VAM protocol packet encryption.

An encryption algorithm specified earlier by using this command has a higher priority during algorithm negotiation between a VAM server and a client. The VAM server compares its algorithms in descending order of priority with the algorithms sent by the client, and sends the matching algorithm with the highest priority to the client.

The configuration of this command does not affect registered VAM clients. It applies to subsequently registered VAM clients.

Examples

Specify the encryption algorithms as AES-CBC-128 and 3DES-CBC for ADVPN domain 1, where AES-CBC-128 has a higher priority.

```
<Sysname> system-view
[Sysname] vam server advpn-domain 1
[Sysname-vam-server-domain-1] encryption-algorithm aes-cbc-128 3des-cbc
```

hub ipv6 private-address

Use **hub ipv6 private-address** to configure a hub private IPv6 address in a hub group.

Use **undo hub ipv6 private-address** to remove a hub private IPv6 address from a hub group.

Syntax

hub ipv6 private-address *private-ipv6-address* [**public-address** { *public-ipv4-address* | *public-ipv6-address* } [**advpn-port** *port-number*]]

undo hub ipv6 private-address *private-ipv6-address*

Default

No hub private IPv6 address is configured.

Views

Hub group view

Predefined user roles

network-admin

context-admin

Parameters

*private-ipv6-address*s: Specifies the private IPv6 address of a hub. The address must be a global unicast address.

public-address: Specifies the public address of the hub. If you do not specify this keyword, the VAM server uses the public address registered by the hub.

public-ipv4-address: Specifies the public IPv4 address of the hub. The address must be a unicast address.

public-ipv6-address: Specifies the public IPv6 address of the hub. The address must be a global unicast address.

advpn-port *port-number*: Specifies the ADVPN port number of the hub, in the range of 1025 to 65535. If you do not specify this option, the VAM server uses the port number registered by the hub.

Usage guidelines

For a hub to traverse a NAT gateway, configure a static mapping between the hub's registered public address/ADVPN port number and a NATed address/port number on the NAT gateway. To use this command to add the hub to a hub group, specify the NATed address and port number as the public address and ADVPN port number.

You can configure multiple hub private IPv6 addresses for a hub group.

If you execute this command multiple times for a private IPv6 address, the most recent configuration takes effect.

Examples

Add a hub to hub group 1 in ADVPN domain 1 with private IPv6 address 1000::1:0:0:1, public IPv6 address 2001::1, and ADVPN port number 8000.

```
<Sysname> system-view
[Sysname] vam server advpn-domain 1
[Sysname-vam-server-domain-1] hub-group 1
[Sysname-vam-server-domain-1-hub-group-1] hub ipv6 private-address 1000::1:0:0:1
public-address 2001::1 advpn-port 8000
```

hub private-address

Use **hub private-address** to configure a hub private IPv4 address in a hub group.

Use **undo hub private-address** to remove a hub private IPv4 address from a hub group.

Syntax

hub private-address *private-ip-address* [**public-address** { *public-ipv4-address* | *public-ipv6-address* } [**advpn-port** *port-number*]]

undo hub private-address *private-ip-address*

Default

No hub private IPv4 address is configured.

Views

Hub group view

Predefined user roles

network-admin

context-admin

Parameters

private-ip-address: Specifies the private IPv4 address of a hub. The address must be a unicast address.

public-address: Specifies the public address of the hub. If you do not specify this keyword, the VAM server uses the public address registered by the hub.

public-ipv4-address: Specifies the public IPv4 address of the hub. The address must be a unicast address.

public-ipv6-address: Specifies the public IPv6 address of the hub. The address must be a global unicast address.

advpn-port *port-number*: Specifies the ADVPN port number of the hub, in the range of 1025 to 65535. If you do not specify this option, the VAM server uses the port number registered by the hub.

Usage guidelines

For a hub to traverse a NAT gateway, configure a static mapping between the hub's registered public address/ADVPN port number and a NATed address/port number on the NAT gateway. To use this command to add the hub to a hub group, specify the NATed address and port number as the public address and ADVPN port number.

You can configure a maximum of four hub private IPv4 addresses for a hub group.

If you execute this command multiple times for a private IPv4 address, the most recent configuration takes effect.

Examples

Add a hub to hub group 1 in ADVPN domain 1 with private IPv4 address 10.1.1.1, public IPv4 address 123.0.0.1, and ADVPN port number 8000.

```
<Sysname> system-view
[Sysname] vam server advpn-domain 1
[Sysname-vam-server-domain-1] hub-group 1
[Sysname-vam-server-domain-1-hub-group-1] hub private-address 10.1.1.1 public-address
123.0.0.1 advpn-port 8000
```

hub-group

Use **hub-group** to create a hub group and enter its view, or enter the view of an existing hub group.

Use **undo hub-group** to delete a hub group.

Syntax

hub-group *group-name*

undo hub-group *group-name*

Default

No hub groups exist.

Views

ADVPN domain view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a group by its name. A group name is a case-insensitive string of 1 to 31 characters that can include only letters, digits, and dots (.).

Usage guidelines

Hub groups apply to large ADVPN networks. You can classify spokes to different hub groups, and specify one or more hubs for each group.

When a VAM client registers with the VAM server, the VAM server selects a hub group for the client as follows:

1. The server matches the private address of the client against the private addresses of hubs in different hub groups in lexicographic order.
2. If a match is found, the server assigns the client to the hub group as a hub.
3. If no match is found, the server matches the client's private address against the private addresses of spokes in different hub groups in lexicographic order.
4. If a match is found, the server assigns the client to the hub group as a spoke.
5. If no match is found, the registration fails.

The VAM server only assigns hub information in the matching hub group to the client. The client only establishes permanent ADVPN tunnels to the hubs in the matching hub group.

Examples

Create hub group 1 in ADVPN domain 1, and enter hub group view.

```
<Sysname> system-view
[Sysname] vam server advpn-domain 1
[Sysname-vam-server-domain-1] hub-group 1
[Sysname-vam-server-domain-1-hub-group-1]
```

keepalive

Use **keepalive** to set a keepalive interval and a maximum number of keepalive retries for VAM clients.

Use **undo keepalive** to restore the default.

Syntax

keepalive interval *interval* **retry** *retries*

undo keepalive

Default

The keepalive interval is 180 seconds and the maximum number of keepalive retries is 3.

Views

ADVPN domain view

Predefined user roles

network-admin

context-admin

Parameters

interval *interval*: Specifies the keepalive interval in the range of 5 to 65535 seconds.

retry *retries*: Specifies the maximum number of keepalive retries, in the range of 1 to 6.

Usage guidelines

The VAM server assigns the configured keepalive parameters to clients in the ADVPN domain.

A client sends keepalives to the server at the specified interval. If a client receives no responses from the server after maximum keepalive attempts (keepalive retries + 1), the client stops sending keepalives. If the VAM server receives no keepalives from a client before the timeout timer expires, the server removes information about the client and logs off the client. The timeout time is the product of the keepalive interval and keepalive attempts.

Newly configured keepalive parameters do not affect registered VAM clients. They apply to subsequently registered clients.

If a device configured with dynamic NAT exists between the VAM server and VAM clients, configure the keepalive interval to be shorter than the aging time of NAT entries.

Configure proper values for the keepalive parameters depending on the network condition.

Examples

Set the keepalive interval for VAM clients in ADVPN domain 1 to 30 seconds, and the maximum number of keepalive retries to 5.

```
<Sysname> system-view
[Sysname] vam server advpn-domain 1
[Sysname-vam-server-domain-1] keepalive interval 30 retry 5
```

pre-shared-key (ADVPN domain view)

Use **pre-shared-key** to configure a preshared key for the VAM server.

Use **undo pre-shared-key** to remove the configuration.

Syntax

pre-shared-key { **cipher** | **simple** } *string*

undo pre-shared-key

Default

No preshared key is configured.

Views

ADVPN domain view

Predefined user roles

network-admin

context-admin

Parameters

cipher: Specifies a preshared key in encrypted form.

simple: Specifies a preshared key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the preshared key. Its plaintext form is a case-sensitive string of 1 to 31 characters. Its encrypted form is a case-sensitive string of 1 to 73 characters.

Usage guidelines

The preshared key is used to generate initial encryption and authentication keys during connection initialization. It is also used to generate encryption and authentication keys for subsequent packets if encryption and authentication are needed.

The VAM server and all clients in an ADVPN domain must have the same preshared key.

Examples

Set the key to **123** in plaintext form for the VAM server in ADVPN domain 1.

```
<Sysname> system-view
[Sysname] vam server advpn-domain 1
[Sysname-vam-server-domain-1] pre-shared-key simple 123
```

Related commands

pre-shared-key (VAM client view)

reset vam server address-map

Use **reset vam server address-map** to clear IPv4 private-public address mapping information for VAM clients registered with the VAM server.

Syntax

reset vam server address-map [**advpn-domain** *domain-name* [**private-address** *private-ip-address*]]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

advpn-domain *domain-name*: Clears IPv4 address mapping information for VAM clients in the specified ADVPN domain. The *domain-name* argument is a case-insensitive string of 1 to 31 characters that can include only letters, digits, and dots (.). If you do not specify this option, the command clears address mapping information for VAM clients in all ADVPN domains.

private-address *private-ip-address*: Clears IPv4 address mapping information for the VAM client with the specified private IPv4 address. If you do not specify this option, the command clears address mapping information for VAM clients in the specified domain or all ADVPN domains.

Usage guidelines

CAUTION:

When this command is executed, the system sends an error notification to VAM clients that have registered the private IPv4 addresses and logs off the clients.

Executing this command also clears IPv4 private network information for the private IPv4 addresses.

Examples

Clear IPv4 address mapping information for clients in all ADVPN domains.

```
<Sysname> reset vam server address-map
```

Clear IPv4 address mapping information for clients in ADVPN domain 1.

```
<Sysname> reset vam server address-map advpn-domain 1
```

Clear IPv4 address mapping information for the client with private IPv4 address 10.0.0.1 in ADVPN domain 1.

```
<Sysname> reset vam server address-map advpn-domain 1 private-address 10.0.0.1
```

Related commands

display vam server address-map

reset vam server ipv6 address-map

Use **reset vam server ipv6 address-map** to clear IPv6 private-public address mapping information for VAM clients registered with the VAM server.

Syntax

reset vam server ipv6 address-map [**advpn-domain** *domain-name* [**private-address** *private-ipv6-address*]]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

advpn-domain *domain-name*: Clears IPv6 address mapping information for VAM clients in the specified ADVPN domain. The *domain-name* argument is a case-insensitive string of 1 to 31 characters that can include only letters, digits, and dots (.). If you do not specify this option, the command clears address mapping information for VAM clients in all ADVPN domains.

private-address *private-ipv6-address*: Clears IPv6 address mapping information for the VAM client with the specified private IPv6 address. If you do not specify this option, the command clears address mapping information for VAM clients in the specified domain or all ADVPN domains.

Usage guidelines

CAUTION:

When this command is executed, the system sends an error notification to VAM clients that have registered the private IPv6 addresses and logs off the clients.

Executing this command also clears IPv6 private network information for the private IPv6 addresses.

Examples

Clear IPv6 address mapping information for clients in all ADVPN domains.

```
<Sysname> reset vam server ipv6 address-map
```

Clear IPv6 address mapping information for clients in ADVPN domain 1.

```
<Sysname> reset vam server ipv6 address-map advpn-domain 1
```

Clear IPv6 address mapping information for the client with private IPv6 address 1000::1:0:0:1 in ADVPN domain 1.

```
<Sysname> reset vam server ipv6 address-map advpn-domain 1 private-address 1000::1:0:0:1
```

Related commands

display vam server ipv6 address-map

reset vam server statistics

Use **reset vam server statistics** to clear ADVPN domain statistics on the VAM server.

Syntax

reset vam server statistics [**advpn-domain** *domain-name*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

advpn-domain *domain-name*: Clears statistics for the specified ADVPN domain. The *domain-name* argument is a case-insensitive string of 1 to 31 characters that can include only letters, digits, and dots (.). If you do not specify this option, the command clears statistics for all ADVPN domains on the server.

Examples

Clear statistics for ADVPN domain **abc**.

```
<Sysname> reset vam server statistics advpn-domain abc
```

Clear statistics for all ADVPN domains.

```
<Sysname> reset vam server statistics
```

Related commands

display vam server statistics

retry interval

Use **retry interval** to set the retry timer for the VAM server.

Use **undo retry interval** to restore the default.

Syntax

retry interval *interval*

undo retry interval

Default

The retry timer is 5 seconds.

Views

ADVPN domain view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies the retry timer in the range of 3 to 30 seconds.

Usage guidelines

The VAM server starts the retry timer after it sends a request to a client. If the server receives no response from the client before the retry timer expires, the server resends the request. The server stops sending the request after receiving a response from the client or after the timeout timer (product of the keepalive interval and keepalive attempts) expires.

Examples

Set the retry timer to 20 seconds for the VAM server in ADVPN domain 1.

```
<Sysname> system-view
[Sysname] vam server advpn-domain 1
[Sysname-vam-server-domain-1] retry interval 20
```

server enable

Use **server enable** to enable the VAM server for an ADVPN domain.

Use **undo server enable** to disable the VAM server for an ADVPN domain.

Syntax

server enable

undo server enable

Default

The VAM server is disabled for an ADVPN domain.

Views

ADVPN domain view

Predefined user roles

network-admin

context-admin

Usage guidelines

You can also execute the **vam server enable** command in system view to enable the VAM server for one or all ADVPN domains.

Examples

Enable the VAM server for ADVPN domain 1.

```
<Sysname> system-view
[Sysname] vam server advpn-domain 1
[Sysname-vam-server-domain-1] server enable
```

Related commands

vam server enable

shortcut interest

Use **shortcut interest** to specify an ACL to control establishing IPv4 spoke-to-spoke tunnels.

Use **undo shortcut interest** to restore the default.

Syntax

shortcut interest { **acl** { *acl-number* | **name** *acl-name* } **all** }

undo shortcut interest

Default

Spokes are not allowed to establish direct tunnels.

Views

Hub group view

Predefined user roles

network-admin

context-admin

Parameters

acl: Specifies an ACL to control establishing IPv4 spoke-to-spoke tunnels.

acl-number: Specifies an IPv4 ACL by its number:

- 2000 to 2999 for IPv4 basic ACLs.
- 3000 to 3999 for IPv4 advanced ACLs.

name *acl-name*: Specifies an ACL by its name. An ACL name is a case-insensitive string of 1 to 63 characters. It must start with an English letter and to avoid confusion, it cannot be **all**.

all: Allows establishing IPv4 spoke-to-spoke tunnels between all spokes in different hub groups.

Usage guidelines

The VAM server assigns the specified ACL to an online hub. When receiving an IPv4 spoke-to-spoke packet from a spoke, the hub sends a redirect packet to the spoke if **all** is specified or if the packet matches an ACL rule. Then, the spoke sends the VAM server the destination address of the packet, obtains the remote spoke information, and establishes a direct tunnel to the remote spoke.

After a spoke-spoke tunnel is established, the spokes directly exchange packets.

When you specify an IPv4 ACL, follow these guidelines:

- If the ACL does not exist, the configuration does not take effect. The hub does not send any redirect packets to the spoke.
- If the ACL is an IPv4 basic ACL, this command supports only rules that match source addresses.
- If the ACL is an IPv4 advanced ACL, this command supports rules that match protocol numbers, source/destination addresses, and source/destination ports. It does not support rules that exclude a source/destination port.
- If the ACL contains an unsupported rule, the rule does not take effect.

Examples

Specify ACL 3000 to control establishing IPv4 spoke-to-spoke tunnels.

```
<Sysname> system-view
[Sysname] vam server advpn-domain 1
[Sysname-vam-server-domain-1] hub-group 1
[Sysname-vam-server-domain-1-hub-group-1] shortcut interest acl 3000
```

shortcut ipv6 interest

Use **shortcut ipv6 interest** to specify an ACL to control establishing IPv6 spoke-to-spoke tunnels.

Use **undo shortcut ipv6 interest** to restore the default.

Syntax

shortcut ipv6 interest { **acl** { *ipv6-acl-number* | **name** *ipv6-acl-name* } **all** }

undo shortcut ipv6 interest

Default

Spokes are not allowed to establish direct tunnels.

Views

Hub group view

Predefined user roles

network-admin

context-admin

Parameters

acl: Specifies an ACL to control establishing IPv6 spoke-to-spoke tunnels.

ipv6-acl-number: Specifies an IPv6 ACL by its number:

- 2000 to 2999 for IPv6 basic ACLs.
- 3000 to 3999 for IPv6 advanced ACLs.

name *ipv6-acl-name*: Specifies an IPv6 ACL by its name. An IPv6 ACL name is a case-insensitive string of 1 to 63 characters. It must start with an English letter and to avoid confusion, it cannot be **all**.

all: Allows establishing IPv6 spoke-to-spoke tunnels between all spokes in different hub groups.

Usage guidelines

The VAM server assigns the specified ACL to an online hub. When receiving an IPv6 spoke-to-spoke packet from a spoke, the hub sends a redirect packet to the spoke if **all** is specified or if the packet matches an ACL rule. Then, the spoke sends the destination address of the packet to the VAM server, obtains the remote spoke information, and establishes a direct tunnel to the remote spoke.

After a spoke-spoke tunnel is established, the spokes directly exchange packets.

When you specify an IPv6 ACL, follow these guidelines:

- If the ACL does not exist, the configuration does not take effect. The hub does not send any redirect packets to the spoke.
- If the ACL is an IPv6 basic ACL, this command supports only rules that match source addresses.
- If the ACL is an IPv6 advanced ACL, this command supports rules that match protocol numbers, source/destination addresses, and source/destination ports. It does not support rules that exclude a source/destination port.
- If the ACL contains an unsupported rule, the rule does not take effect.

Examples

Specify ACL 3000 to control establishing IPv6 spoke-to-spoke tunnels.

```
<Sysname> system-view
[Sysname] vam server advpn-domain 1
[Sysname-vam-server-domain-1] hub-group 1
[Sysname-vam-server-domain-1-hub-group-1] shortcut ipv6 interest acl 3000
```

spoke ipv6 private-address

Use **spoke ipv6 private-address** to configure a spoke private IPv6 address range in a hub group.

Use **undo ipv6 spoke private-address** to delete a spoke private IPv6 address range in a hub group.

Syntax

spoke ipv6 private-address { **network** *prefix prefix-length* | **range** *start-ipv6-address end-ipv6-address* }

undo spoke ipv6 private-address { **network** *prefix prefix-length* | **range** *start-ipv6-address end-ipv6-address* }

Default

No spoke private IPv6 address range is configured.

Views

Hub group view

Predefined user roles

network-admin

context-admin

Parameters

network *prefix prefix-length*: Specifies a prefix and prefix length. The value range for *prefix-length* is 0 to 128.

range *start-ipv6-address end-ipv6-address*: Specifies a start IPv6 address and an end IPv6 address.

Usage guidelines

If you specify a prefix and prefix length, the system automatically transforms them to a start address and an end address.

You can configure multiple spoke private IPv6 address ranges in a hub group. The ranges are listed from low to high.

The spoke private IPv6 address range to be deleted must be the same as the configured one.

Examples

Configure a spoke private IPv6 address range in IPv6 network address format as 1000::/64 for hub group 1.

```
<Sysname> system-view
[Sysname] vam server advpn-domain 1
[Sysname-vam-server-domain-1] hub-group 1
[Sysname-vam-server-domain-1-hub-group-1] spoke ipv6 private-address network 1000:: 64
```

spoke private-address

Use **spoke private-address** to configure a spoke private IPv4 address range in a hub group.

Use **undo spoke private-address** to delete a spoke private IPv4 address range in a hub group.

Syntax

spoke private-address { **network** *ip-address* { *mask-length* | *mask* } | **range** *start-ipv4-address end-ipv4-address* }

undo spoke private-address { **network** *ip-address* { *mask-length* | *mask* } | **range** *start-ipv4-address end-ipv4-address* }

Default

No spoke private IPv4 address range is configured.

Views

Hub group view

Predefined user roles

network-admin

context-admin

Parameters

network *ip-address* { *mask-length* | *mask* }: Specifies an IPv4 address and its mask length (or mask). The value range for *mask-length* is 0 to 32.

range *start-address end-address*: Specifies a start IPv4 address and an end IPv4 address.

Usage guidelines

If you specify an IPv4 address and its mask length (or mask), the system automatically transforms them to a start address and an end address.

You can configure multiple spoke private IPv4 address ranges in a hub group. The ranges are listed from low to high.

The spoke private IPv4 address range to be deleted must be the same as the configured one.

Examples

Configure a spoke private IPv4 address range in IPv4 network address format as 1.1.1.0/24 for hub group 1.

```
<Sysname> system-view
[Sysname] vam server advpn-domain 1
[Sysname-vam-server-domain-1] hub-group 1
[Sysname-vam-server-domain-1-hub-group-1] spoke private-address network 1.1.1.0
255.255.255.0
```

vam server advpn-domain

Use **vam server advpn-domain** to create an ADVPN domain and enter its view, or enter the view of an existing ADVPN domain.

Use **undo vam server advpn-domain** to remove an ADVPN domain.

Syntax

vam server advpn-domain *domain-name* [**id** *domain-id*]

undo vam server advpn-domain *domain-name*

Default

No ADVPN domains exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

domain-name: Specifies an ADVPN domain by its name. An ADVPN domain name is a case-insensitive string of 1 to 31 characters that can include only letters, digits, and dots (.).

id *domain-id*: Specifies the ID of an ADVPN domain, in the range of 1 to 65535.

Usage guidelines

An ADVPN domain ID is required only when you create the ADVPN domain.

You must specify a unique domain ID for an ADVPN domain.

Examples

Create ADVPN domain 1 with domain ID 1, and enter its view.

```
<Sysname> system-view
[Sysname] vam server advpn-domain 1 id 1
[Sysname-vam-server-domain-1]
```

vam server enable

Use **vam server enable** to enable the VAM server for ADVPN domains.

Use **undo vam server enable** to disable the VAM server for ADVPN domains.

Syntax

vam server enable [**advpn-domain** *domain-name*]

undo vam server enable [**advpn-domain** *domain-name*]

Default

The VAM server is disabled for an ADVPN domain.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

advpn-domain *domain-name*: Enables the VAM server for the specified ADVPN domain. The *domain-name* argument is a case-insensitive string of 1 to 31 characters that can include only letters, digits, and dots (.). If you do not specify this option, the command enables the VAM server for all ADVPN domains.

Usage guidelines

You can also execute the **server enable** command in ADVPN domain view to enable the VAM server for an ADVPN domain.

Examples

Enable the VAM server for all ADVPN domains.

```
<Sysname> system-view
[Sysname] vam server enable
```

Enable the VAM server for ADVPN domain 1.

```
<Sysname> system-view
[Sysname] vam server enable advpn-domain 1
```

Related commands

server enable

vam server listen-port

Use **vam server listen-port** to set the port number of the VAM server.

Use **undo vam server listen-port** to restore the default.

Syntax

vam server listen-port *port-number*

undo vam server listen-port

Default

The port number of the VAM server is 18000.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

port-number: Specifies the port number in the range of 1025 to 65535.

Usage guidelines

The port number of the VAM server must be the same as the port configured on the VAM clients.

Examples

Set the port number to 10000.

```
<Sysname> system-view
[Sysname] vam server listen-port 10000
```

Related commands

server primary

server secondary

VAM client commands

advpn-domain

Use **advpn-domain** to specify an ADVPN domain for a VAM client.

Use **undo advpn-domain** to remove the ADVPN domain.

Syntax

advpn-domain *domain-name*

undo advpn-domain

Default

No ADVPN domain is specified for a VAM client.

Views

VAM client view

Predefined user roles

network-admin

context-admin

Parameters

domain-name: Specifies an ADVPN domain by its name. An ADVPN domain name is a case-insensitive string of 1 to 31 characters that can include only letters, digits, and dots (.).

Usage guidelines

An ADVPN domain can contain multiple VAM clients.

Examples

Specify ADVPN domain 100 for VAM client **abc**.

```
<Sysname> system-view
[Sysname] vam client name abc
[Sysname-vam-client-abc] advpn-domain 100
```

client enable

Use **client enable** to enable a VAM client.

Use **undo client enable** to disable a VAM client.

Syntax

client enable

undo client enable

Default

The VAM client is disabled.

Views

VAM client view

Predefined user roles

network-admin

context-admin

Usage guidelines

You can also execute the **vam client enable** command in system view to enable one or all VAM clients.

Examples

Enable VAM client **abc**.

```
<Sysname> system-view
[Sysname] vam client name abc
[Sysname-vam-client-abc] client enable
```

Related commands

vam client enable

display vam client fsm

Use **display vam client fsm** to display FSM information for VAM clients.

Syntax

display vam client fsm [**name** *client-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

name *client-name*: Displays FSM information for the specified VAM client. The *client-name* argument is a case-insensitive string of 1 to 63 characters that can include only letters, digits, and dots (.). If you do not specify this option, the command displays FSM information for all VAM clients.

Usage guidelines

This command only displays the configured parameters and dynamically obtained information.

Examples

Display FSM information for all VAM clients.

```
<Sysname> display vam client fsm
Client name      : abc
Status           : Enabled
ADVPN domain name: 1
  Primary server: abc.com (28.1.1.23)
    Private address: 10.0.0.12
    Interface      : Tunnel1
      Current state           : Online (active)
      Client type             : Hub
      Holding time            : 9H 20M 30S
      Encryption algorithm    : AES-CBC-128
      Authentication algorithm: SHA1
      Keepalive               : 30 seconds, 3 times
      Number of hubs          : 1
    Private address: 1000::22
    Interface      : Tunnel2
```

```
      Current state           : Online (active)
      Client type             : Spoke
      Holding time            : 9H 20M 30S
      Encryption algorithm    : AES-CBC-128
      Authentication algorithm: SHA1
      Keepalive               : 30 seconds, 3 times
      Number of hubs          : 1
  Secondary server: 2811::24
    Private address: 10.0.0.12
    Interface      : Tunnel1
      Current state           : Offline
      Client type             : Unknown
      Holding time            : 0H 0M 0S
      Encryption algorithm    : AES-CBC-128
      Authentication algorithm: SHA1
      Keepalive               : 0 seconds, 0 times
      Number of hubs          : 0
    Private address: 1000::22
    Interface      : Tunnel2
      Current state           : Offline
      Client type             : Unknown
      Holding time            : 0H 0M 0S
      Encryption algorithm    : AES-CBC-128
      Authentication algorithm: SHA1
      Keepalive               : 0 seconds, 0 times
      Number of hubs          : 0

Client name      : hub
Status           : Enabled
ADVPN domain name: 2
  Primary server: 202.159.36.24
    Private address: 10.0.0.12
    Interface      : Tunnel20
      Current state           : Online (active)
      Client type             : Hub
      Holding time            : 0H 0M 47S
      Encryption algorithm    : AES-CBC-128
      Authentication algorithm: SHA1
      Keepalive               : 30 seconds, 3 times
      Number of hubs          : 1

Client name      : spoke
Status           : Disabled
ADVPN domain name:
```

Table 8 Command output

Field	Description
Status	VAM client status: **Enabled** or **Disabled**.

Field	Description
Primary server	Public address of the primary VAM server.
Private address	Private address that the VAM client has registered with the VAM server.
Interface	ADVPN tunnel interface for the VAM client.
Current state	Current state of the VAM client: • **Offline**. • **Init**. • **Reg**. • **Online**. • **Dumb**.
Client type	VAM client type: • **Hub**. • **Spoke**. • **Unknown**.
Holding time	Duration time since the VAM client stayed in its current state, in the format of xH yM zS.
Encryption algorithm	Negotiated encryption algorithm.
Authentication algorithm	Negotiated authentication algorithm.
Keepalive	Keepalive interval (in seconds) and number of retransmissions configured on the VAM server.
Secondary server	Public address of the secondary VAM server.

Related commands

`reset vam client fsm`

display vam client shortcut interest

Use **`display vam client shortcut interest`** to display IPv4 spoke-to-spoke tunnel establishment rules for VAM clients.

Syntax

`display vam client shortcut interest` [**`name`** *`client-name`*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

`name` *`client-name`*: Displays IPv4 spoke-to-spoke tunnel establishment rules for the specified VAM client. The *`client-name`* argument is a case-insensitive string of 1 to 63 characters that can include only letters, digits, and dots (.). If you do not specify this option, the command displays IPv4 spoke-to-spoke tunnel establishment rules for all VAM clients.

Usage guidelines

The VAM server assigns the rules for establishing IPv4 spoke-to-spoke tunnels only to hubs. If the specified VAM client is a spoke, the number of rules is displayed as 0.

Examples

Display IPv4 spoke-to-spoke tunnel establishment rules for all VAM clients.

```
<Sysname> display vam client shortcut interest
Client name      : abc
ADVPN domain name: 1
Client type      : Spoke
ACL rules        : 0

Client name      : hub
ADVPN domain name: 2
Client type      : Hub
ACL rules        : 2
  Rule 1: Permit
    Protocol   : 6 (TCP)
    Source     : Address 0.0.0.0-255.255.255.255, port 0-65535
    Destination: Address 192.168.114.100-192.168.114.200, port 10000-20000
  Rule 2: Deny
    Protocol   : 0 (IP)
    Source     : Address 0.0.0.0-255.255.255.255, port 0-65535
    Destination: Address 0.0.0.0-255.255.255.255, port 0-65535

Client name      : spoke
ADVPN domain name: 3
Client type      : Unknown
ACL rules        : 0
```

Display IPv4 spoke-to-spoke tunnel establishment rules for VAM client **abc**.

```
<Sysname> display vam client shortcut interest name abc
Client name      : abc
ADVPN domain name: 1
Client type      : Spoke
ACL rules        : 0
```

Table 9 Command output

Field	Description
Client type	VAM client type: • **Hub**. • **Spoke**. • **Unknown**.
ACL rules	Number of ACL rules received by the VAM client.
Rule *n*: *Operation*	*n* represents the number of an ACL rule. Rule operation: • **Permit**—Allows the spokes to establish direct tunnels. • **Deny**—Disallows the spokes to establish direct tunnels. • **Discard**—Discards packets.

Field	Description
Protocol	Matching protocol number.
Source	Matching source IP address range and port number range.
Destination	Matching destination IP address range and port number range.

display vam client shortcut ipv6 interest

Use **display vam client shortcut ipv6 interest** to display IPv6 spoke-to-spoke tunnel establishment rules for VAM clients.

Syntax

display vam client shortcut ipv6 interest [**name** *client-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

name *client-name*: Displays IPv6 spoke-to-spoke tunnel establishment rules for the specified VAM client. The *client-name* argument is a case-insensitive string of 1 to 63 characters that can include only letters, digits, and dots (.). If you do not specify this option, the command displays IPv6 spoke-to-spoke tunnel establishment rules for all VAM clients.

Usage guidelines

The VAM server assigns the rules for establishing IPv6 spoke-to-spoke tunnels only to hubs. If the specified VAM client is a spoke, the number of rules is displayed as 0.

Examples

Display IPv6 spoke-to-spoke tunnel establishment rules for all VAM clients.

```
<Sysname> display vam client shortcut ipv6 interest
Client name      : abc
ADVPN domain name: 1
Client type      : Spoke
ACL rules        : 0

Client name      : hub
ADVPN domain name: 2
Client type      : Hub
ACL rules        : 2
  Rule 1: Permit
    Protocol                : TCP
    Start source address    : 0::0
    End source address      : FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
    Start source port       : 0
```

```
    End source port          : 65535
    Start destination address: 2000::0
    End destination address  : 2000:1::0
    Start destination port   : 0
    End destination port     : 65535
  Rule 2: Deny
    Protocol                 : All
    Start source address     : 0::0
    End source address       : FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
    Start source port        : 0
    End source port          : 65535
    Start destination address: 0::0
    End destination address  : FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
    Start destination port   : 0
    End destination port     : 65535

Client name      : spoke
ADVPN domain name:
Client type      : Unknown
ACL rules        : 0
```

Display IPv6 spoke-to-spoke tunnel establishment rules for VAM client **abc**.

```
<Sysname> display vam client shortcut ipv6 interest name abc
Client name      : spoke
ADVPN domain name:
Client type      : Unknown
ACL rules        : 0
```

Table 10 Command output

Field	Description
Client type	VAM client type: • **Hub**. • **Spoke**. • **Unknown**.
ACL rules	Number of ACL rules received by the VAM client.
Rule *n*: *operation*	*n* represents the number of an ACL rule. Rule operation: • **Permit**—Allows the spokes to establish direct tunnels. • **Deny**—Disallows the spokes to establish direct tunnels. • **Discard**—Discards packets.
Protocol	Matching protocol number.
Start source address	Matching start address of the source IPv6 address range.
End source address	Matching end address of the source IPv6 address range.
Start source port	Matching start port number of the source port number range.
End source port	Matching end port number of the source port number range.
Start destination address	Matching start address of the destination IPv6 address range.
End destination address	Matching end address of the destination IPv6 address range.

Field	Description
Start destination port	Matching start port number of the destination port number range.
End destination port	Matching end port number of the destination port number range.

display vam client statistics

Use **display vam client statistics** to display VAM client statistics.

Syntax

display vam client statistics [**name** *client-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

name *client-name*: Displays statistics for the specified VAM client. The *client-name* argument is a case-insensitive string of 1 to 63 characters that can include only letters, digits, and dots (.). If you do not specify this option, the command displays statistics for all VAM clients.

Examples

Display statistics for all VAM clients.

```
<Sysname> display vam client statistics
Client name: abc
Status     : Enabled
  Primary server: abc.com
    Packets sent:
      Initialization request        : 1
      Initialization complete       : 1
      Register request              : 1
      Authentication information    : 1
      Address resolution request    : 9
      Network registration request  : 0
      Update request                : 0
      Logout request                : 0
      Hub information response      : 0
      Data flow information response: 0
      Keepalive                     : 35
      Error notification            : 0
    Packets received:
      Initialization response      : 1
      Initialization complete      : 1
      Authentication request       : 1
      Register response            : 1
```

```
      Address resolution response  : 9
      Network registration response: 0
      Update response              : 0
      Hub information request      : 0
      Data flow information request: 0
      Logout response              : 0
      Keepalive                    : 35
      Error notification           : 0
      Unknown                      : 0
  Secondary server: 28.1.1.24
    Packets sent:
      Initialization request        : 15
      Initialization complete       : 0
      Register request              : 0
      Authentication information    : 0
      Address resolution request    : 0
      Network registration request  : 0
      Update request                : 0
      Logout request                : 0
      Hub information response      : 0
      Data flow information response: 0
      Keepalive                     : 0
      Error notification            : 0
    Packets received:
      Initialization response      : 0
      Initialization complete      : 0
      Register response            : 0
      Authentication request       : 0
      Address resolution response  : 0
      Network registration response: 0
      Update response              : 0
      Hub information request      : 0
      Data flow information request: 0
      Logout response              : 0
      Keepalive                    : 0
      Error notification           : 0
      Unknown                      : 0

Client name: hub
Status     : Disabled

Client name: spoke
Status     : Enabled
  Primary server: test.com
    Packets sent:
      Initialization request        : 3
      Initialization complete       : 3
      Register request              : 3
```

```
      Authentication information    : 3
      Address resolution request    : 0
      Network registration request  : 0
      Update request                : 0
      Logout request                : 0
      Hub information response      : 0
      Data flow information response: 0
      Keepalive                     : 124
      Error notification            : 0
    Packets received:
      Initialization response      : 3
      Initialization complete      : 3
      Authentication request       : 3
      Register response            : 3
      Address resolution response  : 0
      Network registration response: 0
      Update response              : 0
      Hub information request      : 0
      Data flow information request: 0
      Logout response              : 0
      Keepalive                    : 114
      Error notification           : 0
      Unknown                      : 0
```

Display statistics for VAM client **abc**.

```
<Sysname> display vam client statistics name abc
Client name: abc
Status     : Enabled
  Primary server: abc.com
    Packets sent:
      Initialization request        : 1
      Initialization complete       : 1
      Register request              : 1
      Authentication information    : 1
      Address resolution request    : 9
      Network registration request  : 0
      Update request                : 0
      Logout request                : 0
      Hub information response      : 0
      Data flow information response: 0
      Keepalive                     : 35
      Error notification            : 0
    Packets received:
      Initialization response      : 1
      Initialization complete      : 1
      Authentication request       : 1
      Register response            : 1
      Address resolution response  : 9
      Network registration response: 0
```

```
    Update response              : 0
    Hub information request      : 0
    Data flow information request: 0
    Logout response              : 0
    Keepalive                    : 35
    Error notification           : 0
    Unknown                      : 0
Secondary server: 28.1.1.24
  Packets sent:
    Initialization request        : 15
    Initialization complete       : 0
    Register request              : 0
    Authentication information    : 0
    Address resolution request    : 0
    Network registration request  : 0
    Update request                : 0
    Logout request                : 0
    Hub information response      : 0
    Data flow information response: 0
    Keepalive                     : 0
    Error notification            : 0
  Packets received:
    Initialization response      : 0
    Initialization complete      : 0
    Register response            : 0
    Authentication request       : 0
    Address resolution response  : 0
    Network registration response: 0
    Update response              : 0
    Hub information request      : 0
    Data flow information request: 0
    Logout response              : 0
    Keepalive                    : 0
    Error notification           : 0
    Unknown                      : 0
```

Table 11 Command output

Field	Description
Status	VAM client status: **Enabled** or **Disabled**.
Primary server	Public address or domain name of the primary VAM server.
Secondary server	Public address or domain name of the secondary VAM server.

Related commands

reset vam client statistics

dumb-time

Use **dumb-time** to set the dumb timer for a VAM client.

Use **undo dumb-time** to restore the default.

Syntax

dumb-time *time-interval*

undo dumb-time

Default

The dumb timer for a VAM client is 120 seconds.

Views

VAM client view

Predefined user roles

network-admin

context-admin

Parameters

time-interval: Specifies the dumb timer in the range of 10 to 600 seconds.

Usage guidelines

A VAM client starts the dumb timer after the timeout timer expires. The client does not process any packets during the dumb time. When the dumb timer expires, the client sends a new connection request to the VAM server.

Examples

Set the dumb timer to 100 seconds.

```
<Sysname> system-view
[Sysname] vam client name abc
[Sysname-vam-client-abc] dumb-time 100
```

pre-shared-key (VAM client view)

Use **pre-shared-key** to configure a preshared key for a VAM client.

Use **undo pre-shared-key** to remove the configuration.

Syntax

pre-shared-key { **cipher** | **simple** } *string*

undo pre-shared-key

Default

No preshared key is configured for a VAM client.

Views

VAM client view

Predefined user roles

network-admin

context-admin

Parameters

cipher: Specifies a preshared key in encrypted form.

simple: Specifies a preshared key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the preshared key. Its plaintext form is a case-sensitive string of 1 to 31 characters. Its encrypted form is a case-sensitive string of 1 to 73 characters.

Usage guidelines

The preshared key is used to generate initial encryption and authentication keys during connection initialization. It is also used to generate encryption and authentication keys for subsequent packets if encryption and authentication are needed.

All VAM clients and the VAM server in an ADVPN domain must have the same preshared key.

Examples

Set the key to **123** in plaintext form for VAM client **abc**.

```
<Sysname> system-view
[Sysname] vam client name abc
[Sysname-vam-client-abc] pre-shared-key simple 123
```

Related commands

pre-shared-key (ADVPN domain view)

vam client name

reset vam client fsm

Use **reset vam client fsm** to reset FSMs for VAM clients.

Syntax

reset vam client fsm [**name** *client-name*]

Views

User view

Predefined user roles

network-admin

Parameters

name *client-name*: Resets the FSM for the specified VAM client. The *client-name* argument is a case-insensitive string of 1 to 63 characters that can include only letters, digits, and dots (.). If you do not specify this option, the command resets FSMs for all VAM clients.

Usage guidelines

CAUTION:

After you use the **reset vam client fsm** command to reset the FSM for a VAM client, the client will immediately try to come online.

Examples

Reset the FSM for VAM client **abc**.

```
<Sysname> reset vam client fsm name abc
```

Reset FSMs for all VAM clients.

```
<Sysname> reset vam client fsm
```

Related commands

display vam client fsm

reset vam client ipv6 fsm

Use **reset vam client ipv6 fsm** to reset FSMs for IPv6 VAM clients.

Syntax

reset vam client ipv6 fsm [**name** *client-name*]

Views

User view

Predefined user roles

network-admin

Parameters

name *client-name*: Resets the FSM for the specified IPv6 VAM client. The *client-name* argument is a case-insensitive string of 1 to 63 characters that can include only letters, digits, and dots (.). If you do not specify this option, the command resets FSMs for all IPv6 VAM clients.

Usage guidelines

CAUTION:

After you use the **reset vam client ipv6 fsm** command to reset the FSM for an IPv6 VAM client, the client will immediately try to come online.

Examples

Reset the FSM for IPv6 VAM client **abc**.

```
<Sysname> reset vam client ipv6 fsm name abc
```

Reset FSMs for all IPv6 VAM clients.

```
<Sysname> reset vam client ipv6 fsm
```

Related commands

display vam client fsm

reset vam client statistics

Use **reset vam client statistics** to clear VAM client statistics.

Syntax

reset vam client statistics [**name** *client-name*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

name *client-name*: Clears statistics for the specified VAM client. The *client-name* argument is a case-insensitive string of 1 to 63 characters that can include only letters, digits, and dots (.). If you do not specify this option, the command clears statistics for all VAM clients.

Examples

Clear statistics for VAM client **abc**.

```
<Sysname> reset vam client statistics name abc
```

Clear statistics for all VAM clients.

```
<Sysname> reset vam client statistics
```

Related commands

display vam client statistics

retry

Use **retry** to set the retry interval and retry number for a VAM client.

Use **undo retry** to restore the default.

Syntax

retry interval *interval* **count** *retries*

undo retry

Default

The retry interval is 5 seconds and the retry number is 3.

Views

VAM client view

Predefined user roles

network-admin

context-admin

Parameters

interval *interval*: Specifies the retry interval in the range of 3 to 30 seconds.

count *retries*: Specifies the number of retries, in the range of 1 to 6.

Usage guidelines

After a VAM client sends a request to the server, it resends the request if it does not receive any responses within the retry interval. If the client fails to receive a response after maximum attempts (retry times + 1), the client determines that the server is unreachable.

The *retry-times* setting does not apply to register and update requests. The client sends those requests at the retry interval until it goes offline.

Examples

Set the retry interval to 20 seconds and the retry number to 4 for VAM client **abc**.

```
<Sysname> system-view
[Sysname] vam client name abc
[Sysname-vam-client-abc] retry interval 20 count 4
```

server primary

Use **server primary** to specify a primary VAM server for a VAM client.

Use **undo server primary** to restore the default.

Syntax

server primary { **ip-address** *ipv4-address* | **ipv6-address** *ipv6-address* | **name** *host-name* } [**port** *port-number*]

undo server primary

Default

No primary VAM server is specified.

Views

VAM client view

Predefined user roles

network-admin

context-admin

Parameters

ip-address *ipv4-address*: Specifies a public IPv4 address for the primary VAM server. The address must be a unicast address.

ipv6-address *ipv6-address*: Specifies a public IPv6 address for the primary VAM server. The address must be a global unicast address.

name *host-name*: Specifies a domain name for the primary VAM server. It is a dot-separated, case-insensitive string that can include letters, digits, hyphens (-), and underscores (_). The domain name can include a maximum of 253 characters, and each separated string includes no more than 63 characters.

port *port-number*: Specifies a port number for the primary VAM server, in the range of 1025 to 65535. The default is 18000.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

The port number of a VAM server must be the same as the port number configured on the VAM server by using the **vam server listen-port** command.

If the specified primary and secondary VAM servers have the same address or name, only the primary VAM server takes effect.

Examples

Specify the domain name of the primary VAM server as **abc.com** and port number as **2000** for VAM client **abc**.

```
<Sysname> system-view
[Sysname] vam client name abc
[Sysname-vam-client-abc] server primary name abc.com port 2000
```

Specify the public IP address of the primary VAM server as **1.1.1.1** and port number as **2000** for VAM client **abc**.

```
<Sysname> system-view
[Sysname] vam client name abc
[Sysname-vam-client-abc] server primary ip-address 1.1.1.1 port 2000
```

Specify the public IPv6 address of the primary VAM server as **1001::1** and port number as **2000** for VAM client **abc**.

```
<Sysname> system-view
[Sysname] vam client name abc
[Sysname-vam-client-abc] server primary ipv6-address 1001::1 port 2000
```

Related commands

server secondary

server secondary

Use **server secondary** to specify a secondary VAM server for a VAM client.

Use **undo server secondary** to restore the default.

Syntax

server secondary { **ip-address** *ipv4-address* | **ipv6-address** *ipv6-address* | **name** *host-name* } [**port** *port-number*]

undo server secondary

Default

No secondary VAM server is specified.

Views

VAM client view

Predefined user roles

network-admin

context-admin

Parameters

ip-address *ipv4-address*: Specifies a public IPv4 address for the secondary VAM server. The address must be a unicast address.

ipv6-address *ipv6-address*: Specifies a public IPv6 address for the secondary VAM server. The address must be a global unicast address.

name *host-name*: Specifies a domain name of a secondary VAM server. It is a dot-separated, case-insensitive string that can include letters, digits, hyphens (-), and underscores (_). The domain name can include a maximum of 253 characters, and each separated string includes no more than 63 characters.

port *port-number*: Specifies a port number for the secondary VAM server, in the range of 1025 to 65535. The default is 18000.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

The port number of a VAM server must be the same as the port number configured on the VAM server by using the **vam server listen-port** command.

If the specified primary and secondary VAM servers have the same address or name, only the primary VAM server takes effect.

Examples

Specify the domain name of the secondary VAM server as **abc.com** and port number as **2000** for VAM client **abc**.

```
<Sysname> system-view
```

```
[Sysname] vam client name abc
[Sysname-vam-client-abc] server secondary name abc.com port 2000
```

Specify the public IP address of the secondary VAM server as **1.1.1.2** and port number as **3000** for VAM client **abc**.

```
<Sysname> system-view
[Sysname] vam client name abc
[Sysname-vam-client-abc] server secondary ip-address 1.1.1.2 port 3000
```

Specify the public IPv6 address of the primary VAM server as **1001::2** and port number as **3000** for VAM client **abc**.

```
<Sysname> system-view
[Sysname] vam client name abc
[Sysname-vam-client-abc] server secondary ipv6-address 1001::2 port 3000
```

Related commands

server primary

user

Use **user** to configure a username and password for a VAM client.

Use **undo user** to restore the default.

Syntax

user *username* **password** { **cipher** | **simple** } *string*

undo user

Default

No username or password is configured.

Views

VAM client view

Predefined user roles

network-admin

context-admin

Parameters

username: Specifies a username. The username is a case-sensitive string of 1 to 253 characters. It cannot include slashes (/), back slashes (\), colons (:), asterisks (*), question marks (?), left angle brackets (<), right angle brackets (>), quotation marks ("), vertical bars (|), and at signs (@).

password: Specifies a password.

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 63 characters. Its encrypted form is a case-sensitive string of 1 to 117 characters.

Usage guidelines

You can configure only one username for a VAM client.

Examples

Configure the username as **user** and password as **user** in plaintext form for VAM client **abc**.

```
<Sysname> system-view
[Sysname] vam client name abc
[Sysname-vam-client-abc] user user password simple user
```

vam client enable

Use **vam client enable** to enable VAM clients.

Use **undo vam client enable** to disable VAM clients.

Syntax

vam client enable [**name** *client-name*]

undo vam client enable [**name** *client-name*]

Default

The VAM client is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

name *client-name*: Enables the specified VAM client. The *client-name* argument is a case-insensitive string of 1 to 63 characters that can include only letters, digits, and dots (.). If you do not specify this option, the command enables all VAM clients.

Usage guidelines

You can also execute the **client enable** command in VAM client view to enable a VAM client.

Examples

Enable all VAM clients.

```
<Sysname> system-view
[Sysname] vam client enable
```

Enable VAM client **abc**.

```
<Sysname> system-view
[Sysname] vam client enable name abc
```

Related commands

client enable

vam client name

Use **vam client name** to create a VAM client and enter its view, or enter the view of an existing VAM client.

Use **undo vam client name** to remove a VAM client.

Syntax

vam client name *client-name*

undo vam client name *client-name*

Default

No VAM clients exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

client-name: Specifies a VAM client by its name. A VAM client name is a case-insensitive string of 1 to 63 characters that can include only letters, digits, and dots (.).

Examples

Create VAM client **abc** and enter its view.

```
<Sysname> system-view
[Sysname] vam client name abc
[Sysname-vam-client-abc]
```

ADVPN tunnel commands

advpn group

Use **advpn group** to configure an ADVPN group name.

Use **undo advpn group** to restore the default.

Syntax

advpn group *group-name*

undo advpn group

Default

No ADVPN group name is configured.

Views

Tunnel interface view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies the ADVPN group name. The group name is a case-insensitive string of 1 to 63 characters that can include only letters, digits, and dots (.).

Usage guidelines

This command must be used on the tunnel interface of a spoke. The spoke sends the ADVPN group name in a hub-spoke tunnel establishment request to a hub. The hub looks for an ADVPN group-to-QoS policy mapping that matches the ADVPN group name. If a matching mapping is found, the hub applies the QoS policy in the mapping to the hub-spoke tunnel. If no match is found, the hub does not apply a QoS policy to the hub-spoke tunnel.

If you modify the ADVPN group name after the tunnel is established, the spoke will inform the hub of the modification. The hub will look for an ADVPN group-to-QoS policy mapping that matches the new ADVPN group name and apply the QoS policy in the new mapping.

As a best practice, do not configure an ADVPN group name and apply a QoS policy on the same tunnel interface.

Examples

Configure **aaa** as the ADVPN group name.

```
<Sysname> system-view
[Sysname] interface tunnel1 mode advpn gre
[Sysname-Tunnel1] advpn group aaa
```

advpn ipv6 network

Use **advpn ipv6 network** to configure a private IPv6 network for an IPv6 ADVPN tunnel interface.

Use **undo advpn ipv6 network** to remove a private IPv6 network from an IPv6 ADVPN tunnel interface.

Syntax

advpn ipv6 network *prefix prefix-length* [**preference** *preference-value*]

undo advpn ipv6 network *prefix prefix-length*

Default

No private IPv6 network is configured.

Views

Tunnel interface view

Predefined user roles

network-admin

context-admin

Parameters

prefix prefix-length: Specifies the prefix and prefix length of the private IPv6 network address. The value range for *prefix-length* is 0 to 128.

preference *preference-value*: Specifies a preference for the route to the private network, in the range of 1 to 255. The default is 8.

Usage guidelines

This command is available only for IPv6 ADVPN tunnel interfaces.

Each VAM client registers the private networks for an ADVPN tunnel with the VAM server. If another VAM client receives a packet with the destination address resolved as a registered private address, the VAM server sends the registered VAM client information to the client.

This command takes effect on a tunnel interface that has been configured with an IPv6 address and bound to a VAM client by using the **vam ipv6 client** command.

You can configure multiple private IPv6 networks for a tunnel interface.

Set the preference of the private network route to be higher than other dynamic routing protocols, and lower than static routing. A higher preference value represents a lower priority.

Examples

Configure private IPv6 network 1001::/64 for Tunnel 1, and set the route preference to 20.

```
<Sysname> system-view
[Sysname] interface tunnel 1 mode advpn udp ipv6
[Sysname-Tunnel1] advpn ipv6 network 1001:: 64 preference 20
```

Related commands

vam ipv6 client

advpn logging enable

Use **advpn logging enable** to enable ADVPN logging.

Use **undo advpn logging enable** to disable ADVPN logging.

Syntax

advpn logging enable

undo advpn logging enable

Default

ADVPN logging is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command enables the device to generate logs for the ADVPN module and send the logs to the information center of the device. For the logs to be output correctly, you must also configure the information center on the device. For more information about information center configuration, see *Network Management and Monitoring Configuration Guide*.

Examples

Enable ADVPN logging.

```
<Sysname> system-view
[Sysname] advpn logging enable
```

advpn map group

Use **advpn map group** to configure a mapping between an ADVPN group and a QoS policy.

Use **undo advpn map group** to delete a mapping between an ADVPN group and a QoS policy.

Syntax

advpn map group *group-name* **qos-policy** *policy-name* **outbound**

undo advpn map group *group-name*

Default

No ADVPN group-to-QoS policy mappings are configured.

Views

Tunnel interface view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies the ADVPN group name. The group name is a case-insensitive string of 1 to 63 characters that can include only letters, digits, and dots (.).

qos-policy *policy-name*: Specifies the QoS policy name, a case-sensitive string of 1 to 31 characters.

outbound: Applies the QoS policy to the outbound direction.

Usage guidelines

This command must be used on the tunnel interface of a hub. After receiving a hub-spoke tunnel establishment request from a spoke, the hub looks for an ADVPN group-to-QoS policy mapping that matches the ADVPN group name carried in the request. If a matching mapping is found, the hub applies the QoS policy in the mapping to the hub-spoke tunnel.

You can configure multiple ADVPN group-to-QoS policy mappings on a tunnel interface.

You can map multiple ADVPN groups to a QoS policy. You can map an ADVPN group to only one QoS policy.

As a best practice, do not configure an ADVPN group-to-QoS policy mapping and apply a QoS policy on the same tunnel interface.

Examples

Configure a mapping between ADVPN group **aaa** and QoS policy **bbb** on **Tunnel1**.

```
<Sysname> system-view
[Sysname] interface Tunnel1 mode advpn gre
[Sysname-Tunnel1] advpn map group aaa qos-policy bbb outbound
```

advpn network

Use **advpn network** to configure a private IPv4 network for an IPv4 ADVPN tunnel interface.

Use **undo advpn network** to remove a private IPv4 network from an IPv4 ADVPN tunnel interface.

Syntax

advpn network *ip-address* { *mask-length* | *mask* } [**preference** *preference-value*]

undo advpn network *ip-address* { *mask-length* | *mask* }

Default

No private IPv4 network is configured.

Views

Tunnel interface view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the private IPv4 network address.

mask-length: Specifies the mask length of the private IPv4 network address, in the range of 0 to 32.

mask: Specifies the mask of the private IPv4 network address.

preference *preference-value*: Specifies a preference for the route to the private network, in the range of 1 to 255. The default is 8.

Usage guidelines

This command is available only for IPv4 ADVPN tunnel interfaces.

Each VAM client registers the private networks for an ADVPN tunnel with the VAM server. If another VAM client receives a packet with the destination address resolved as a registered private address, the VAM server sends the registered VAM client information to the client.

This command takes effect on a tunnel interface that has been configured with an IPv4 address and bound to a VAM client by using the **vam client** command.

You can configure multiple private IPv4 networks for a tunnel interface.

Set the preference of the private network route to be higher than other dynamic routing protocols, and lower than static routing. A higher preference value represents a lower priority.

Examples

Configure private IPv4 network 10.0.5.0 with mask 255.255.255.0 for Tunnel 1, and set the route preference to 20.

```
<Sysname> system-view
[Sysname] interface tunnel 1 mode advpn udp
[Sysname-Tunnel1] advpn network 10.0.5.0 255.255.255.0 preference 20
```

Related commands

vam client

advpn session dumb-time

Use **advpn session dumb-time** to set the dumb time for an ADVPN tunnel interface.

Use **undo advpn session dumb-time** to restore the default.

Syntax

advpn session dumb-time *time-interval*

undo advpn session dumb-time

Default

The dumb time is 120 seconds.

Views

Tunnel interface view

Predefined user roles

network-admin

context-admin

Parameters

time-interval: Specifies the dumb time in the range of 10 to 600 seconds.

Usage guidelines

This command is available only for ADVPN tunnel interfaces.

The new dumb time setting only applies to subsequently established tunnels.

Examples

Set the dumb time to 100 seconds.

```
<Sysname> system-view
[Sysname] interface tunnel 1 mode advpn udp
[Sysname-Tunnel1] advpn session dumb-time 100
```

advpn session idle-time

Use **advpn session idle-time** to set the idle timeout time for a spoke-spoke ADVPN tunnel.

Use **undo advpn session idle-time** to restore the default.

Syntax

advpn session idle-time *time-interval*

undo advpn session idle-time

Default

The idle timeout time is 600 seconds.

Views

Tunnel interface view

Predefined user roles

network-admin

context-admin

Parameters

time-interval: Specifies the idle timeout time in the range of 60 to 65535 seconds.

Usage guidelines

This command is available only for ADVPN tunnel interfaces.

The new idle timeout setting applies to both established and subsequently established spoke-spoke tunnels.

If no data is forwarded along a spoke-spoke tunnel during the idle timeout time, the tunnel will be removed automatically.

Examples

Set the idle timeout time to 800 seconds.

```
<Sysname> system-view
[Sysname] interface tunnel 1 mode advpn udp
[Sysname-tunnel1] advpn session idle-time 800
```

advpn source-port

Use **advpn source-port** to set the source UDP port number for ADVPN packets.

Use **undo advpn source-port** to restore the default.

Syntax

advpn source-port *port-number*

undo advpn source-port

Default

The source UDP port number is 18001.

Views

Tunnel interface view

Predefined user roles

network-admin

context-admin

Parameters

port-number: Specifies the UDP port number in the range of 1025 to 65535.

Usage guidelines

This command is available only for UDP-encapsulated ADVPN tunnels.

If the **vam client** command configured on the tunnel interface has the **compatible** keyword, the tunnel interface must have a different source UDP port number than other tunnel interfaces.

Examples

Set the source UDP port number to 6000.

```
<Sysname> system-view
[Sysname] interface tunnel 1 mode advpn udp
[Sysname-Tunnel1] advpn source-port 6000
```

Related commands

vam client

display advpn group-qos-map

Use **display advpn group-qos-map** to display ADVPN group-to-QoS policy mappings.

Syntax

display advpn group-qos-map [**interface tunnel** *number* [**group** *group-name*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface tunnel *number*: Specifies an ADVPN tunnel interface by its tunnel interface number. The value range for the *number* argument is 0 to 1023. If you do not specify a tunnel interface, this command displays ADVPN group-to-QoS policy mappings for all ADVPN tunnel interfaces.

group *group-name*: Specifies an ADVPN group by its name. If you do not specify an ADVPN group, this command displays ADVPN group-to-QoS policy mappings for all ADVPN groups.

Examples

Display ADVPN group-to-QoS policy mappings for all ADVPN tunnel interfaces.

```
<Sysname> display advpn group-qos-map
Interface: Tunnel1
  ADVPN group: group1
  QoS policy: policy1
  Session list:
     Private address         Public address
     10.0.0.3                 192.168.180.136
     10.0.1.4                 192.168.180.137

  ADVPN group: bb
  QoS policy: bb-policy
  No sessions match the ADVPN group-to-QoS policy mapping.

Interface: Tunnel2
  ADVPN group: group2
  QoS policy: policy2
  Session list:
    Private address         Public address
    20.0.0.3                 200::3
```

Table 12 Command output

Field	Description
Interface	ADVPN tunnel interface.
ADVPN group	ADVPN group name.
QoS policy	QoS policy to which the ADVPN group is mapped.
Session list	List of ADVPN tunnels that use the QoS policy on the tunnel interface.
Private address	Private address of the ADVPN tunnel peer.
Public address	Public address of the ADVPN tunnel peer.
No sessions match the ADVPN group-to-QoS policy mapping	No ADVPN tunnels match the ADVPN group-to-QoS policy mapping on the tunnel interface.

Related commands

advpn group

advpn map group

display advpn ipv6 session

Use **display advpn ipv6 session** to display IPv6 ADVPN tunnel information.

Syntax

display advpn ipv6 session [**interface tunnel** *number* [**private-address** *private-ipv6-address*]] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface tunnel *number*: Displays information about IPv6 ADVPN tunnels on an IPv6 ADVPN tunnel interface specified by the interface number. If you do not specify this option, the command displays information about all IPv6 ADVPN tunnels.

private-address *private-ipv6-address*: Displays information about the IPv6 ADVPN tunnel with the specified peer private IPv6 address. If you do not specify this option, the command displays information about the specified IPv6 ADVPN tunnel or all IPv6 ADVPN tunnels.

verbose: Displays detailed IPv6 ADVPN tunnel information. If you do not specify this keyword, the command displays brief IPv6 ADVPN tunnel information.

Examples

Display brief information about all IPv6 ADVPN tunnels.

```
<Sysname> display advpn ipv6 session
Interface         : Tunnel1
Number of sessions: 2
Private address       Public address        Port  Type  State      Holding time
1001::3               2000::180:136         1139  H-S   Success    5H 38M 8S
1001::4               2000::180:137         3546  H-S   Dumb       0H 0M 27S

Interface         : Tunnel2
Number of sessions: 1
Private address       Public address        Port  Type  State      Holding time
1002::4               202.0.180.137         --    S-H   Establish  0H 0M 2S

Interface         : Tunnel3
Number of sessions: 1
Private address       Public address        Port  Type  State      Holding time
1003::4               2003::180:137         2057  S-S   Success    1H 12M 26S

Interface         : Tunnel4
Number of sessions: 1
Private address       Public address        Port  Type  State      Holding time
1004::4               204.1.181:157         --    H-H   Success    10H 48M 19S
```

```
Interface         : Tunnel5
Number of sessions: 0
```

Display brief information about IPv6 ADVPN tunnels on Tunnel 1.

```
<Sysname> display advpn ipv6 session interface tunnel 1
Interface         : Tunnel1
Number of sessions: 2
Private address       Public address        Port  Type  State      Holding time
1001::3               2000::180:136         1139  H-S   Success    5H 38M 8S
1001::4               2000::180:137         3546  H-S   Dumb       0H 0M 27S
```

Display brief information about the IPv6 ADVPN tunnel with peer private IPv6 address 1001::3 on Tunnel 1.

```
<Sysname> display advpn ipv6 session interface tunnel 1 private-address 1001::3
Private address       Public address        Port  Type  State      Holding time
1001::3               2000::180:136         1139  H-S   Success    5H 38M 8S
```

Table 13 Command output

Field	Description
Interface	ADVPN tunnel interface.
Number of sessions	Number of ADVPN tunnels established on the tunnel interface.
Private address	Private address of the ADVPN tunnel peer.
Public address	Public address of the ADVPN tunnel peer.
Port	Port number of the ADVPN tunnel peer.
Type	ADVPN tunnel type: • **H-H**—Both the local end and the remote end are hubs. • **H-S**—The local end is a hub and the remote end is a spoke. • **S-H**—The local end is a spoke and the remote end is a hub. • **S-S**—Both the local end and the remote end are spokes.
State	ADVPN tunnel state: • **Success**—The tunnel has been successfully established. • **Establishing**—The tunnel is being established. • **Dumb**—The tunnel failed to be established and is now quiet.
Holding time	Duration time since the tunnel stayed in the current state, in the format of xH yM zS.

Display detailed information about all IPv6 ADVPN tunnels.

```
<Sysname> display advpn ipv6 session verbose
Interface         : Tunnel1
Client name       : vpn1
ADVPN domain name : 1
Link protocol     : UDP
Number of sessions: 2
  Private address: 1001::3
  Public address : 2000::180:136
  ADVPN port     : 1139
  Session type   : Hub-Spoke
  State          : Success
```

```
  Holding time   : 5H 38M 8S
  Input : 2201 packets, 2198 data packets, 3 control packets
          2191 multicasts, 0 errors
  Output: 2169 packets, 216 data packets, 1 control packets
          2163 multicasts, 0 errors

  Private address: 1001::4
  Public address : 2000::180:137
  ADVPN port     : 3546
  Session type   : Hub-Spoke
  State          : Dumb
  Holding time   : 0H 0M 27S
  Input : 1 packets, 0 data packets, 1 control packets
          0 multicasts, 0 errors
  Output: 16 packets, 0 data packets, 16 control packets
          0 multicasts, 0 errors

Interface         : Tunnel2
Client name       : vpn2
ADVPN domain name : 2
Link protocol     : GRE
Number of sessions: 1
  Private address: 1002::4
  Public address : 202.0.180.137
  Session type   : Spoke-Hub
  State          : Establish
  Holding time   : 0H 0M 2S
  Input:  0 packets, 0 data packets, 0 control packets
          0 multicasts, 0 errors
  Output: 1 packets, 0 data packets, 1 control packets
          0 multicasts, 0 errors

Interface         : Tunnel3
Client name       : vpn3
ADVPN domain name : 3
Link protocol     : IPsec-UDP
Number of sessions: 1
  Private address: 1003::4
  Public address : 2003::180:137
  ADVPN port     : 2057
  SA's SPI       :
    Inbound : 187199087 (0xb286e6f) [ESP]
    Outbound: 3562274487 (0xd453feb7) [ESP]
  Session type   : Spoke-Spoke
  State          : Establish
  Holding time   : 0H 0M 2S
  Input:  0 packets, 0 data packets, 0 control packets
          0 multicasts, 0 errors
```

```
  Output: 1 packets, 0 data packets, 1 control packets
          0 multicasts, 0 errors

Interface         : Tunnel4
Client name       : vpn4
ADVPN domain name : 4
Link protocol     : IPsec-GRE
Number of sessions: 1
  Private address: 1004::4
  Public address : 204.1.181:157
  SA's SPI       :
    Inbound:  187199087 (0xb286e6f) [ESP]
    Outbound: 3562274487 (0xd453feb7) [ESP]
  Session type   : Hub-Hub
  State          : Success
  Holding time   : 10H 48M 19S
  Input : 2201 packets, 2198 data packets, 3 control packets
          2191 multicasts, 0 errors
  Output: 2169 packets, 2168 data packets, 1 control packets
          2163 multicasts, 0 errors

Interface         : Tunnel5
Client name       : vpn5
ADVPN domain name : 5
Link protocol     : UDP
Number of sessions: 0
```

Display detailed information about IPv6 ADVPN tunnels on Tunnel 1.

```
<Sysname> display advpn ipv6 session interface tunnel 1 verbose
Interface         : Tunnel1
Client name       : vpn1
ADVPN domain name : 1
Link protocol     : UDP
Number of sessions: 2
  Private address: 1001::3
  Public address : 2000::180:136
  ADVPN port     : 1139
  Session type   : Hub-Spoke
  State          : Success
  Holding time   : 5H 38M 8S
  Input : 2201 packets, 2198 data packets, 3 control packets
          2191 multicasts, 0 errors
  Output: 2169 packets, 216 data packets, 1 control packets
          2163 multicasts, 0 errors

  Private address: 1001::4
  Public address : 2000::180:137
  ADVPN port     : 3546
  Session type   : Hub-Spoke
```

```
  State          : Dumb
  Holding time   : 0H 0M 27S
  Input : 1 packets, 0 data packets, 1 control packets
          0 multicasts, 0 errors
  Output: 16 packets, 0 data packets, 16 control packets
          0 multicasts, 0 errors
```

Display detailed information about the IPv6 ADVPN tunnel with peer private IPv6 address 1001::3 on Tunnel 1.

```
<Sysname> display advpn ipv6 session interface tunnel 1 private-address 1001::3 verbose
  Private address: 1001::3
  Public address : 2000::180:136
  ADVPN port     : 1139
  Session type   : Hub-Spoke
  State          : Success
  Holding time   : 5H 38M 8S
  Input : 2201 packets, 2198 data packets, 3 control packets
          2191 multicasts, 0 errors
  Output: 2169 packets, 216 data packets, 1 control packets
          2163 multicasts, 0 errors
```

Table 14 Command output

Field	Description
Interface	ADVPN tunnel interface.
Client name	Name of the VAM client bound to the tunnel interface.
Link protocol	Link layer protocol for the ADVPN tunnel: • **UDP**. • **GRE**. • **IPsec-UDP**. • **IPsec-GRE**.
Number of sessions	Number of ADVPN tunnels established on the tunnel interface.
Private address	Private address of the ADVPN tunnel peer.
Public address	Public address of the ADVPN tunnel peer.
ADVPN port	UDP port number for the ADVPN tunnel when the link layer protocol is **UDP** or **IPsec-UDP**.
SA's SPI	SPIs for the inbound and outbound SAs when link layer protocol is **IPsec-UDP** or **IPsec-GRE**.
Session type	ADVPN tunnel type: • **Hub-Hub**—Both the local end and the remote end are hubs. • **Hub-Spoke**—The local end is a hub and the remote end is a spoke. • **Spoke-Hub**—The local end is a spoke and the remote end is a hub. • **Spoke-Spoke**—Both the local end and the remote end are spokes.
State	ADVPN tunnel state: • **Success**—The tunnel has been successfully established. • **Establishing**—The tunnel is being established. • **Dumb**—The tunnel failed to be established and is now quiet.
Holding time	Duration time since the tunnel stayed in the current state, in the format of xH yM zS.

Field	Description
Input	Statistics for incoming packets, including the numbers of all packets, data packets, control packets, multicast packets, and erroneous packets.
Output	Statistics for outgoing packets, including the numbers of all packets, data packets, control packets, multicast packets, and erroneous packets.

Related commands

reset advpn ipv6 session

display advpn session

Use **display advpn session** to display IPv4 ADVPN tunnel information.

Syntax

display advpn session [**interface tunnel** *number* [**private-address** *private-ip-address*]] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface tunnel *number*: Displays information about IPv4 ADVPN tunnels on an IPv4 ADVPN tunnel interface specified by the interface number. If you do not specify this option, the command displays information about all IPv4 ADVPN tunnels.

private-address *private-ip-address*: Displays information about the IPv4 ADVPN tunnel with the specified peer private IPv4 address. If you do not specify this option, the command displays information about the specified IPv4 ADVPN tunnel or all IPv4 ADVPN tunnels.

verbose: Displays detailed IPv4 ADVPN tunnel information. If you do not specify this keyword, the command displays brief IPv4 ADVPN tunnel information.

Examples

Display brief information about all IPv4 ADVPN tunnels.

```
<Sysname> display advpn session
Interface         : Tunnel1
Number of sessions: 2
Private address  Public address             Port  Type  State      Holding time
10.0.0.3         192.168.180.136            1139  H-S   Success    5H 38M 8S
10.0.1.4         192.168.180.137            3546  H-S   Dumb       0H 0M 27S

Interface         : Tunnel2
Number of sessions: 1
Private address  Public address             Port  Type  State      Holding time
20.0.0.3         200::3                     --     S-H   Establish  0H 0M 2S
```

```
Interface         : Tunnel3
Number of sessions: 1
Private address  Public address              Port  Type  State      Holding time
30.0.0.3         192.168.200.22              2057  S-S   Success    1H 12M 26S

Interface         : Tunnel4
Number of sessions: 1
Private address  Public address              Port  Type  State      Holding time
40.0.0.3         4::4                        --    H-H   Success    10H 48M 19S

Interface         : Tunnel5
Number of sessions: 0
```

Display brief information about IPv4 ADVPN tunnels on Tunnel 1.

```
<Sysname> display advpn session interface tunnel 1
Interface         : Tunnel1
Number of sessions: 2
Private address  Public address              Port  Type  State      Holding time
10.0.0.3         192.168.180.136             1139  H-S   Success    5H 38M 8S
10.0.1.4         192.168.180.137             3546  H-S   Dumb       0H 0M 27S
```

Display brief information about the IPv4 ADVPN tunnel with peer private IP address 10.0.1.3 on Tunnel 1.

```
<Sysname> display advpn session interface tunnel 1 private-address 10.0.1.3
Private address  Public address              Port  Type  State      Holding time
10.0.0.3         192.168.180.136             1139  H-S   Success    5H 38M 8S
```

Table 15 Command output

Field	Description
Interface	ADVPN tunnel interface.
Number of sessions	Number of ADVPN tunnels established on the tunnel interface.
Private address	Private address of the ADVPN tunnel peer.
Public address	Public address of the ADVPN tunnel peer.
Port	Port number of the ADVPN tunnel peer.
Type	ADVPN tunnel type: • **H-H**—Both the local end and the remote end are hubs. • **H-S**—The local end is a hub and the remote end is a spoke. • **S-H**—The local end is a spoke and the remote end is a hub. • **S-S**—Both the local end and the remote end are spokes.
State	ADVPN tunnel state: • **Success**—The tunnel has been successfully established. • **Establishing**—The tunnel is being established. • **Dumb**—The tunnel failed to be established and is now quiet.
Holding time	Duration time since the tunnel stayed in the current state, in the format of xH yM zS.

Display detailed information about all IPv4 ADVPN tunnels.

```
<Sysname> display advpn session verbose
```

```
Interface         : Tunnel1
Client name       : vpn1
ADVPN domain name : 1
Link protocol     : UDP
Number of sessions: 2
  Private address: 10.0.1.3
  Public address : 192.168.180.136
  ADVPN port     : 1139
  Behind NAT     : No
  Session type   : Hub-Spoke
  State          : Success
  Holding time   : 5H 38M 8S
  Input : 2201 packets, 218 data packets, 3 control packets
          2191 multicasts, 0 errors
  Output: 2169 packets, 2168 data packets, 1 control packets
          2163 multicasts, 0 errors

  Private address: 10.0.1.4
  Public address : 192.168.180.137
  ADVPN port     : 3546
  Behind NAT     : No
  Session type   : Hub-Spoke
  State          : Dumb
  Holding time   : 0H 0M 27S
  ADVPN group      : group1
  Outbound QoS policy: policy1
  Input : 1 packets, 0 data packets, 1 control packets
          0 multicasts, 0 errors
  Output: 16 packets, 0 data packets, 16 control packets
          0 multicasts, 0 errors

Interface         : Tunnel2
Client name       : vpn2
ADVPN domain name : 2
Link protocol     : GRE
Number of sessions: 1
  Private address: 20.0.0.3
  Public address : 200::3
  Behind NAT     : No
  Session type   : Spoke-Hub
  State          : Establish
  Holding time   : 0H  0M 2S
  ADVPN group      : group1
  Outbound QoS policy: policy1
  Input:  0 packets, 0 data packets, 0 control packets
          0 multicasts, 0 errors
  Output: 1 packets, 0 data packets, 1 control packets
          0 multicasts, 0 errors
```

```
Interface         : Tunnel3
Client name       : vpn3
ADVPN domain name : 3
Link protocol     : IPsec-UDP
Number of sessions: 1
  Private address: 30.0.0.3
  Public address : 192.168.200.32
  ADVPN port     : 2057
  SA's SPI       :
    Inbound:  187199087 (0xb286e6f) [ESP]
    Outbound: 3562274487 (0xd453feb7) [ESP]
  Behind NAT     : No
  Session type   : Spoke-Spoke
  State          : Establish
  Holding time   : 0H  0M 2S
  Input:  0 packets, 0 data packets, 0 control packets
          0 multicasts, 0 errors
  Output: 1 packets, 0 data packets, 1 control packets
          0 multicasts, 0 errors

Interface         : Tunnel4
Client name       : vpn4
ADVPN domain name : 4
Link protocol     : IPsec-GRE
Number of sessions: 1
  Private address: 40.0.0.3
  Public address : 4::4
  SA's SPI       :
    Inbound:  187199087 (0xb286e6f) [ESP]
    Outbound: 3562274487 (0xd453feb7) [ESP]
  Behind NAT     : No
  Session type   : Hub-Hub
  State          : Success
  Holding time   : 10H 48M 19S
  ADVPN group      : group1
  Outbound QoS policy: policy1
  Input : 2201 packets, 2198 data packets, 3 control packets
          2191 multicasts, 0 errors
  Output: 2169 packets, 2168 data packets, 1 control packets
          2163 multicasts, 0 errors

Interface         : Tunnel5
Client name       : vpn5
ADVPN domain name : 5
Link protocol     : UDP
Number of sessions: 0
```

Display detailed information about IPv4 ADVPN tunnels on Tunnel 1.

```
<Sysname> display advpn session interface tunnel 1 verbose
Interface         : Tunnel1
Client name       : vpn1
ADVPN domain name : 1
Link protocol     : UDP
Number of sessions: 2
  Private address: 10.0.1.3
  Public address : 192.168.180.136
  ADVPN port     : 1139
  Behind NAT     : No
  Session type   : Hub-Spoke
  State          : Success
  Holding time   : 5H 38M 8S
  ADVPN group      : group1
  Outbound QoS policy: policy1
  Input : 2201 packets, 218 data packets, 3 control packets
          2191 multicasts, 0 errors
  Output: 2169 packets, 2168 data packets, 1 control packets
          2163 multicasts, 0 errors

  Private address: 10.0.1.4
  Public address : 192.168.180.137
  ADVPN port     : 3546
  Behind NAT     : No
  Session type   : Hub-Spoke
  State          : Dumb
  Holding time   : 0H 0M 27S
  ADVPN group      : group1
  Outbound QoS policy: policy1
  Input : 1 packets, 0 data packets, 1 control packets
          0 multicasts, 0 errors
  Output: 16 packets, 0 data packets, 16 control packets
          0 multicasts, 0 errors
```

Display detailed information about the IPv4 ADVPN tunnel with peer private IP address 10.0.1.3 on Tunnel 1.

```
<Sysname> display advpn session verbose interface tunnel 1 private-address 10.0.1.3
  Private address: 10.0.1.3
  Public address : 192.168.180.136
  ADVPN port     : 1139
  Behind NAT     : No
  Session type   : Hub-Spoke
  State          : Success
  Holding time   : 5H 38M 8S
  ADVPN group      : group1
  Outbound QoS policy: policy1
  Input : 2201 packets, 218 data packets, 3 control packets
          2191 multicasts, 0 errors
  Output: 2169 packets, 2168 data packets, 1 control packets
```

```
          2163 multicasts, 0 errors
```

Table 16 Command output

Field	Description
Interface	ADVPN tunnel interface.
Client name	Name of the VAM client bound to the tunnel interface.
Link protocol	Link layer protocol for the ADVPN tunnel: • **UDP**. • **GRE**. • **IPsec-UDP**. • **IPsec-GRE**.
Number of sessions	Number of ADVPN tunnels established on the tunnel interface.
Private address	Private address of the ADVPN tunnel peer.
Public address	Public address of the ADVPN tunnel peer.
ADVPN port	UDP port number for the ADVPN tunnel when the link layer protocol is **UDP** or **IPsec-UDP**.
SA's SPI	SPIs for the inbound and outbound SAs when link layer protocol is **IPsec-UDP** or **IPsec-GRE**.
Behind NAT	Whether NAT traversal is used.
Session type	ADVPN tunnel type: • **Hub-Hub**—Both the local end and the remote end are hubs. • **Hub-Spoke**—The local end is a hub and the remote end is a spoke. • **Spoke-Hub**—The local end is a spoke and the remote end is a hub. • **Spoke-Spoke**—Both the local end and the remote end are spokes.
State	ADVPN tunnel state: • **Success**—The tunnel has been successfully established. • **Establishing**—The tunnel is being established. • **Dumb**—The tunnel failed to be established and is now quiet.
Holding time	Duration time since the tunnel stayed in the current state, in the format of xH yM zS.
ADVPN group	ADVPN group name.
Outbound QoS policy	QoS policy to which the ADVPN group is mapped.
Input	Statistics for incoming packets, including the numbers of all packets, data packets, control packets, multicast packets, and erroneous packets.
Output	Statistics for outgoing packets, including the numbers of all packets, data packets, control packets, multicast packets, and erroneous packets.

Related commands

`reset advpn session`

display advpn session count

Use **`display advpn session count`** to display the number of ADVPN sessions in different states.

Syntax

display advpn session count

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display the number of ADVPN sessions in different states.

```
<Sysname> display advpn session count
Total ADVPN sessions: 7
IPv4 sessions: 3
  Success: 3
  Establishing: 0
  Dumb: 0
IPv6 sessions: 4
  Success: 4
  Establishing: 0
  Dumb: 0
```

Table 17 Command output

Field	Description
IPv4 sessions:	Number of ADVPN sessions in IPv4 private networks.
IPv6 sessions:	Number of ADVPN sessions in IPv6 private networks.
Success	Number of ADVPN sessions that have been successfully established.
Establishing	Number of ADVPN sessions that are being established.
Dumb	Number of ADVPN sessions that failed to be established and are now quiet.

keepalive

Use **keepalive** to set the keepalive interval and the maximum number of keepalive attempts for an ADVPN tunnel interface.

Use **undo keepalive** to restore the default.

Syntax

keepalive interval *interval* **retry** *retries*

undo keepalive

Default

The keepalive interval is 180 seconds, and the maximum number of keepalive attempts is 3.

Views

Tunnel interface view

Predefined user roles

network-admin

context-admin

Parameters

interval *interval*: Sets the keepalive interval in the range of 1 to 32767 seconds.

retry *retries*: Sets the maximum number of keepalive attempts, in the range of 1 to 255.

Usage guidelines

This command is available only for ADVPN tunnel interfaces.

If no keepalives is received before the timeout timer (product of the keepalive interval and keepalive attempts) expires, the tunnel will be removed automatically.

The keepalive interval and the maximum number of keepalive attempts must be the same on the tunnel interfaces in an ADVPN domain.

After this command is executed, the keepalive timer does not start immediately. It starts until the ADVPN tunnel is established.

Examples

Set the keepalive interval to 20 seconds and the maximum number of keepalive attempts to 5.

```
<Sysname> system-view
[Sysname] interface tunnel 1 mode advpn udp
[Sysname-Tunnel1] keepalive interval 20 retry 5
```

reset advpn ipv6 session

Use **reset advpn ipv6 session** to delete IPv6 ADVPN tunnels.

Syntax

reset advpn ipv6 session [**interface tunnel** *number* [**private-address** *private-ipv6-address*]]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

interface tunnel *number*: Deletes IPv6 ADVPN tunnels on an IPv6 ADVPN tunnel interface specified by the interface number. If you do not specify this option, the command deletes all IPv6 ADVPN tunnels.

private-address *private-ipv6-address*: Deletes the IPv6 ADVPN tunnel with the specified peer private IPv6 address. If you do not specify this option, the command deletes the specified IPv6 ADVPN tunnel or all IPv6 ADVPN tunnels.

Usage guidelines

If the remote tunnel end is a hub in the same group as the local end, the tunnel will be re-established after it is deleted.

Examples

Delete all IPv6 ADVPN tunnels.

```
<Sysname> reset advpn ipv6 session
```

Delete IPv6 ADVPN tunnels on Tunnel 1.

```
<Sysname> reset advpn ipv6 session interface tunnel 1
```

Delete the IPv6 ADVPN tunnel with peer private IPv6 address 1000::1 on Tunnel 1.

```
<Sysname> reset advpn ipv6 session interface tunnel 1 private-address 1000::1
```

Related commands

display advpn ipv6 session

reset advpn ipv6 session statistics

Use **reset advpn ipv6 session statistics** to clear statistics for IPv6 ADVPN tunnels.

Syntax

reset advpn ipv6 session statistics [**interface tunnel** *number* [**private-address** *private-ipv6-address*]]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

interface tunnel *number*: Clears statistics for IPv6 ADVPN tunnels on an IPv6 ADVPN tunnel interface specified by the interface number. If you do not specify this option, the command clears statistics for all IPv6 ADVPN tunnels.

private-address *private-ipv6-address*: Clears statistics for the IPv6 ADVPN tunnel with the specified peer private IPv6 address. If you do not specify this option, the command clears statistics for the specified IPv6 ADVPN tunnel or all IPv6 ADVPN tunnels.

Examples

Clear statistics for all IPv6 ADVPN tunnels.

```
<Sysname> reset advpn ipv6 session statistics
```

Clear statistics for IPv6 ADVPN tunnels on Tunnel 1.

```
<Sysname> reset advpn ipv6 session statistics interface tunnel 1
```

Clear statistics for the IPv6 ADVPN tunnel with peer private IPv6 address 1::1 on Tunnel 1.

```
<Sysname> reset advpn ipv6 session statistics interface tunnel 1 private-address 1::1
```

reset advpn session

Use **reset advpn session** to delete IPv4 ADVPN tunnels.

Syntax

reset advpn session [**interface tunnel** *number* [**private-address** *private-ip-address*]]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

interface tunnel *number*: Deletes IPv4 ADVPN tunnels on an IPv4 ADVPN tunnel interface specified by the interface number. If you do not specify this option, the command deletes all IPv4 ADVPN tunnels.

private-address *private-ip-address*: Deletes the IPv4 ADVPN tunnel with the specified peer private IPv4 address. If you do not specify this option, the command deletes the specified IPv4 ADVPN tunnel or all IPv4 ADVPN tunnels.

Usage guidelines

If the remote tunnel end is a hub in the same group as the local end, the tunnel will be re-established after it is deleted.

Examples

Delete all IPv4 ADVPN tunnels.

```
<Sysname> reset advpn session
```

Delete IPv4 ADVPN tunnels on Tunnel 1.

```
<Sysname> reset advpn session interface tunnel 1
```

Delete the IPv4 ADVPN tunnel with peer private IPv4 address 169.254.0.1 on Tunnel 1.

```
<Sysname> reset advpn session interface tunnel 1 private-address 169.254.0.1
```

Related commands

display advpn session

reset advpn session statistics

Use **reset advpn session statistics** to clear statistics for IPv4 ADVPN tunnels.

Syntax

reset advpn session statistics [**interface tunnel** *number* [**private-address** *private-ip-address*]]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

interface tunnel *number*: Clears statistics for IPv4 ADVPN tunnels on an IPv4 ADVPN tunnel interface specified by the interface number. If you do not specify this option, the command clears statistics for all IPv4 ADVPN tunnels.

private-address *private-ip-address*: Clears statistics for the IPv4 ADVPN tunnel with the specified peer private IPv4 address. If you do not specify this option, the command clears statistics for the specified IPv4 ADVPN tunnel or all IPv4 ADVPN tunnels.

Examples

Clear statistics for all IPv4 ADVPN tunnels.

```
<Sysname> reset advpn session statistics
```

Clear statistics for IPv4 ADVPN tunnels on Tunnel 1.

```
<Sysname> reset advpn session statistics interface tunnel 1
```

Clear statistics for the IPv4 ADVPN tunnel with peer private IPv4 address 169.254.0.1 on Tunnel 1.

```
<Sysname> reset advpn session statistics interface tunnel 1 private-address 169.254.0.1
```

vam client

Use **vam client** to bind a VAM client to an IPv4 ADVPN tunnel interface.

Use **undo vam client** to remove the binding.

Syntax

vam client *client-name* [**compatible advpn0**]

undo vam client

Default

No VAM client is bound to an IPv4 ADVPN tunnel interface.

Views

Tunnel interface view

Predefined user roles

network-admin

context-admin

Parameters

client-name: Specifies a VAM client by its name. A VAM client name is a case-insensitive string of 1 to 63 characters that can include only letters, digits, and dots (.).

compatible advpn0: Specifies ADVPN V0 packet format. If you do not specify this keyword, packets are not compatible with ADVPN V0 format.

Usage guidelines

This command is available only for IPv4 ADVPN tunnel interfaces.

After a VAM client is bound to an IPv4 ADVPN tunnel interface, the client registers IPv4 private networks for the tunnel interface with the VAM server.

A VAM client can be bound to only one IPv4 ADVPN tunnel interface.

The **compatible** keyword is required if a device that supports only ADVPN V0 packet format exists in the hub group for the bound VAM client. After the **compatible** keyword is specified, make sure the tunnel interface has a unique source UDP port number on the device.

Examples

Bind VAM client **abc** to IPv4 ADVPN tunnel interface Tunnel 1.

```
<Sysname> system-view
[Sysname] interface tunnel 1 mode advpn udp
[Sysname-Tunnel1] vam client abc
```

Related commands

advpn source-port

vam ipv6 client

vam ipv6 client

Use **vam ipv6 client** to bind a VAM client to an IPv6 ADVPN tunnel interface.

Use **undo vam ipv6 client** to remove the binding.

Syntax

vam ipv6 client *client-name*

undo vam ipv6 client

Default

No VAM client is bound to an IPv6 ADVPN tunnel interface.

Views

Tunnel interface view

Predefined user roles

network-admin

context-admin

Parameters

client-name: Specifies a VAM client by its name. A VAM client name is a case-insensitive string of 1 to 63 characters that can include only letters, digits, and dots (.).

Usage guidelines

This command is available only for IPv6 ADVPN tunnel interfaces.

After a VAM client is bound to an IPv6 ADVPN tunnel interface, the client registers IPv6 private networks for the tunnel interface with the VAM server.

A VAM client can be bound to only one IPv6 ADVPN tunnel interface.

Examples

Bind VAM client **abc** to IPv6 ADVPN tunnel interface Tunnel 1.

```
<Sysname> system-view
[Sysname] interface tunnel 1 mode advpn udp ipv6
[Sysname-Tunnel1] vam ipv6 client abc
```

Related commands

vam client

Contents

Tunneling commands

bandwidth

Use **bandwidth** to set the expected bandwidth for an interface.

Use **undo bandwidth** to restore the default.

Syntax

bandwidth *bandwidth-value*

undo bandwidth

Default

The expected bandwidth (in kbps) is the interface maximum rate divided by 1000.

Views

Tunnel interface view

Predefined user roles

network-admin

context-admin

Parameters

bandwidth-value: Specifies the expected bandwidth, in the range of 1 to 400000000 kbps.

Usage guidelines

The expected bandwidth for an interface affects the link costs.

For more information, see OSPF, OSPFv3, and IS-IS in *Layer 3—IP Routing Configuration Guide*.

Examples

Set the expected bandwidth for Tunnel 1 to 100 kbps.

```
<Sysname> system-view
[Sysname] interface tunnel 1
[Sysname-Tunnel1] bandwidth 100
```

default

Use **default** to restore the default settings for a tunnel interface.

Syntax

default

Views

Tunnel interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

CAUTION:

The **default** command might interrupt ongoing network services. Make sure you are fully aware of the impact of this command when you use it on a live network.

This command might fail to restore the default settings for some commands for reasons such as command dependencies or system restrictions. Use the **display this** command in interface view to identify these commands. Use their **undo** forms or follow the command reference to restore their default settings. If your restoration attempt still fails, follow the error message instructions to resolve the problem.

Examples

Restore the default settings of Tunnel 1.

```
<Sysname> system-view
[Sysname] interface tunnel 1
[Sysname-Tunnel1] default
```

description

Use **description** to configure the description of an interface.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

The description of a tunnel interface is **Tunnel***number* **Interface**, for example, **Tunnel1 Interface**.

Views

Tunnel interface view

Predefined user roles

network-admin

context-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 255 characters.

Usage guidelines

Configure descriptions for different interfaces for identification and management purposes.

You can use the **display interface** command to display the configured interface description.

Examples

Configure the description of Tunnel 1 as **tunnel1**.

```
<Sysname> system-view
[Sysname] interface tunnel 1
[Sysname-Tunnel1] description tunnel1
```

Related commands

display interface tunnel

destination

Use **destination** to specify the destination address of a tunnel.

Use **undo destination** to restore the default.

Syntax

destination { *ipv4-address* | *ipv6-address* | **dhcp-alloc** *interface-type interface-number* }

undo destination

Default

No tunnel destination address is configured.

Views

Tunnel interface view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-address: Specifies the tunnel destination IPv4 address.

ipv6-address: Specifies the tunnel destination IPv6 address.

dhcp-alloc *interface-type interface-number*: Specifies an interface by its type and number to obtain AFTR's IPv6 address from DHCPv6 packets.

Usage guidelines

For a manual tunnel, you must configure the destination address. For an automatic tunnel, you do not need to configure the destination address.

The tunnel destination address must be the address of the receiving interface on the tunnel peer. It is used as the destination address of tunneled packets.

The destination address of a tunnel at the local end must be the source address of the tunnel at the peer end. The source address of the tunnel at the local end must be the destination address of the tunnel at the peer end.

Do not specify the same tunnel source and destination addresses for different tunnels on the same device.

For a B4 router to automatically establish a DS-Lite tunnel with an AFTR, configure DHCPv6 client, IPv6 DNS client, and the **destination dhcp-alloc** command on the B4 router. In addition, make sure a DHCPv6 server and an IPv6 DNS server (for dynamic DNS) exist in the network.

After receiving a DHCPv6 packet from the interface specified by the **destination dhcp-alloc** command, the B4 router performs the following operations:

1. Obtains the domain name of the AFTR from the packet.
2. Sends a name query to the IPv6 DNS server to obtain the AFTR's IPv6 address.

   The server resolves the domain name to the IPv6 address of AFTR.

For more information about DHCPv6 server, DHCPv6 client, and IPv6 DNS, see *Layer 3—IP Services Configuration Guide*.

Examples

Interface GigabitEthernet 1/0/1 on Sysname 1 uses IP address 193.101.1.1 and interface GigabitEthernet 1/0/1 on Sysname 2 uses IP address 192.100.1.1. Configure the tunnel source address as 193.101.1.1 and tunnel destination address as 192.100.1.1 for tunnel 1 on Sysname 1.

```
<Sysname1> system-view
[Sysname1] interface tunnel 1 mode gre
[Sysname1-Tunnel1] source 193.101.1.1
[Sysname1-Tunnel1] destination 192.100.1.1
```

Configure the tunnel source address as 192.100.1.1 and tunnel destination address as 193.101.1.1 for tunnel 1 on Sysname 2.

```
<Sysname2> system-view
[Sysname2] interface tunnel 1 mode gre
[Sysname2-Tunnel1] source 192.100.1.1
[Sysname2-Tunnel1] destination 193.101.1.1
```

Related commands

display interface tunnel

interface tunnel

ipv6 address dhcp-alloc

source

display 6rd

Use **display 6rd** to display 6RD tunnel interface information.

Syntax

display 6rd [**interface tunnel** *number*]

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	No
NFNX3-HDB680, NFNX3-HDB1080	Yes

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface tunnel *number*: Specifies an existing tunnel interface by its number. If you do not specify a 6RD tunnel interface, this command displays information about all existing 6RD tunnel interfaces.

Examples

Display information about 6RD tunnel interface Tunnel 1.

```
<Sysname> display 6rd interface tunnel 1
Interface           : Tunnel1
  Tunnel source     : 10.11.12.13
  6RD status        : Operational
    IPv6 prefix     : 2001:1000::/32
    IPv4 prefix     : 10.0.0.0/8
    IPv4 suffix     : 0.0.0.0/0
    BR address      : 10.11.12.1
    Delegated prefix: 2001:1000:B0C:D00::/56
```

Display information about all 6RD tunnel interfaces.

```
<Sysname> display 6rd
Interface           : Tunnel0
  Tunnel source     : 0.0.0.0
  6RD status        : Not operational
    IPv6 prefix     : 2002:1000::/32

Interface           : Tunnel1
  Tunnel source     : 10.11.12.13
  6RD status        : Operational
    IPv6 prefix     : 2001:1000::/32
    IPv4 prefix     : 10.0.0.0/8
    IPv4 suffix     : 0.0.0.0/0
    BR address      : 10.11.12.1
    Delegated prefix: 2001:1000:B0C:D00::/56
```

Table 1 Command output

Field	Description
Interface	Tunnel interface.
Tunnel source	Source address of the tunnel. If a source interface is specified, this field displays the IP address of the source interface. If no source address or source interface is specified, or the specified source interface has no IP address, this field displays **0.0.0.0**.
6RD status	6RD configuration status: • **Operational**—6RD configuration is available. • **Not operational**—6RD configuration is not available. This field displays **Operational** when the tunnel source address and 6RD prefix are configured.
IPv6 prefix	6RD prefix and its length. If no 6RD prefix is configured, this field displays **Not configured**.
IPv4 prefix	IPv4 prefix and its length. If the prefix length is not configured, this field displays **0.0.0.0/0**.
IPv4 suffix	IPv4 suffix and its length. If the suffix length is not configured, this field displays **0.0.0.0/0**.

Field	Description
BR address	IP address of the BR router. If no BR address is configured, this field displays **Not configured**.
Delegated prefix	6RD delegated prefix calculated based on the 6RD configuration. This field is empty if the 6RD status is **Not operational**.

Related commands

tunnel 6rd br

tunnel 6rd ipv4

tunnel 6rd prefix

display 6rd destination

Use **display 6rd destination** to display a 6RD tunnel destination address.

Syntax

display 6rd destination prefix *ipv6-prefix* **interface tunnel** *number*

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	No
NFNX3-HDB680, NFNX3-HDB1080	Yes

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

prefix *ipv6-prefix*: Specifies a 6RD delegated prefix.

interface tunnel *number*: Specifies an existing tunnel interface by its number.

Usage guidelines

After this command is executed, the system displays the 6RD tunnel destination address calculated by the specified 6RD delegated prefix and 6RD configuration on the tunnel interface. The 6RD configuration includes the 6RD prefix/prefix length, IPv4 prefix/prefix length, and IPv4 suffix/suffix length.

Examples

Display the 6RD tunnel destination address calculated by the 6RD delegated prefix 2001:1000:0101:0100:: and 6RD configuration on Tunnel 1.

```
<Sysname> display 6rd destination prefix 2001:1000:0101:0100:: interface tunnel 1
Interface       : Tunnel1
```

```
Delegated prefix: 2001:1000:101:100::
Destination     : 10.1.1.1
```

Table 2 Command output

Field	Description
Interface	Tunnel interface.
Delegated prefix	6RD delegated prefix.
Destination	Tunnel destination address.

Related commands

display 6rd prefix

display 6rd prefix

Use **display 6rd prefix** to display a 6RD delegated prefix.

Syntax

display 6rd prefix destination *ipv4-address* **interface tunnel** *number*

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	No
NFNX3-HDB680, NFNX3-HDB1080	Yes

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

destination *ipv4-address*: Specifies a 6RD tunnel destination address.

interface tunnel *number*: Specifies an existing tunnel interface by its number.

Usage guidelines

After this command is executed, the system displays the 6RD delegated prefix calculated by the specified 6RD tunnel destination address and 6RD configuration on the tunnel interface. The 6RD configuration includes the 6RD prefix/prefix length, IPv4 prefix/prefix length, and IPv4 suffix/suffix length. The 6RD delegated prefix calculated on the peer tunnel interface must be the same as the 6RD delegated prefix configured on the local device.

Examples

Display the 6RD delegated prefix calculated by the 6RD tunnel destination address 10.1.1.1 and 6RD configuration on Tunnel 1.

```
<Sysname> display 6rd prefix destination 10.1.1.1 interface tunnel 1
Interface       : Tunnel1
Destination     : 10.1.1.1
Delegated Prefix: 2001:1000:101:100::
```

Table 3 Command output

Field	Description
Interface	Tunnel interface.
Destination	6RD tunnel destination address.
Delegated Prefix	6RD delegated prefix.

Related commands

`display 6rd destination`

display ds-lite b4 information

Use **`display ds-lite b4 information`** to display information about the connected B4 routers on the AFTR, including the IPv6 addresses of the B4 routers, and the assigned tunnel IDs.

Syntax

`display ds-lite b4 information`

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display information about the connected B4 routers.

```
<Sysname> display ds-lite b4 information
Slot 0 Cpu 0:
 B4 address                                 Tunnel ID  Tunnel interface  Idle time
 1234:5678:1234:5678:abcd:abcd:efff:1234    0x00000023       1              12
 2000::100:1                                0x80000013       2              13
 3000::2                                    0x00000015       3              2
 3001::2                                    0x00000032       --             --
Total B4 addresses: 4

Slot 1 Cpu 0:
 B4 address                                 Tunnel ID  Tunnel interface  Idle time
 1234:5678:1234:5678:abcd:abcd:efff:ffff    0x00000125       1              12
 5000::100:1                                0x80000010       5              13
Total B4 addresses: 2
```

Table 4 Command output

Field	Description
B4 address	IPv6 address of the B4 router.
Tunnel ID	Tunnel ID that the IPv6 address of the B4 router maps to.
Tunnel interface	ID of the tunnel interface on the DS-Lite tunnel to which the mapping belongs. When the tunnel to which the mapping belongs is removed or a tunnel with the same ID but different mode is created, this field displays hyphens (--).
Idle time	Remaining time in minutes for the mapping between the IPv6 address of the B4 router and tunnel ID. When the mapping ages out but is still used by a session, this field displays hyphens (--).
Total B4 addresses	Number of IPv6 addresses of the B4 routers.

display interface tunnel

Use **display interface tunnel** to display tunnel interface information.

Syntax

display interface [**tunnel** [*number*]] [**brief** [**description** | **down**]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

tunnel [*number*]: Specifies a tunnel interface. The *number* argument specifies the tunnel interface number. The specified tunnel interface must have been created. If you do not specify the **tunnel** keyword, this command displays information about all interfaces on the device. If you specify the **tunnel** keyword without the *number* argument, this command displays information about all existing tunnel interfaces.

brief: Displays brief interface information. If you do not specify this keyword, the command displays detailed interface information.

description: Displays complete interface descriptions. If you do not specify this keyword, the command displays only the first 27 characters of interface descriptions.

down: Displays information about interfaces in the physical state of DOWN and the causes. If you do not specify this keyword, the command displays information about interfaces in all states.

Examples

Display detailed information about Tunnel 1.

```
<Sysname> display interface tunnel 1
Tunnel1
```

```
Current state: UP
Line protocol state: UP
Description: Tunnel1 Interface
Bandwidth: 64kbps
Maximum transmission unit: 1476
Internet address: 10.1.2.1/24 (primary)
Tunnel source 1.1.1.1, destination 2.2.2.2
Tunnel keepalive enabled, Period(100 s), Retries(254)
Tunnel TOS 0xC8, Tunnel TTL 255
Tunnel protocol/transport GRE/IP
    GRE key disabled
    Checksumming of GRE packets disabled
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

Table 5 Command output

Field	Description
Tunnel1	Information about the tunnel interface Tunnel 1.
Current state	Physical link state of the tunnel interface: • **Administratively DOWN**—The interface has been shut down by using the **shutdown** command. • **DOWN**—The interface is administratively up, but its physical state is down (possibly because no physical link exists or the link has failed). • **UP**—The interface is both administratively and physically up.
Line protocol state	Data link layer state of the interface. The state is determined through automatic parameter negotiation at the data link layer. • **UP**—The data link layer protocol is up. • **UP (spoofing)**—The data link layer protocol is up, but the link is an on-demand link or does not exist. This attribute is typical of null interfaces and loopback interfaces. • **DOWN**—The data link layer protocol is down.
Description	Description of the tunnel interface.
Bandwidth	Expected bandwidth of the tunnel interface.
Maximum transmission unit	MTU of the tunnel interface.
Internet protocol processing: Disabled	The tunnel interface is not assigned an IP address and cannot process IP packets.

Field	Description
Internet address: *ip-address*/*mask-length* (*Type*)	IP address of the interface and type of the address in parentheses. Possible IP address types include: • **Primary**—Manually configured primary IP address. • **Sub**—Manually configured secondary IP address. If the interface has both primary and secondary IP addresses, the primary IP address is displayed. If the interface has only secondary IP addresses, the lowest secondary IP address is displayed. • **DHCP-allocated**—DHCP allocated IP address. For more information, see DHCP client configuration in *Layer 3—IP Services Configuration Guide*. • **BOOTP-allocated**—BOOTP allocated IP address. For more information, see BOOTP client configuration in *Layer 3—IP Services Configuration Guide*. • **PPP-negotiated**—IP address assigned by a PPP server during PPP negotiation. For more information, see PPP configuration in *Layer 2—WAN Access Configuration Guide*. • **Unnumbered**—IP address borrowed from another interface. • **MAD**—IP address assigned to an IRF member device for MAD on the interface. For more information, see IRF configuration in *Virtual Technologies Configuration Guide*.
Tunnel source	Source address of the tunnel. If a source interface is specified, this field also displays the source interface in parentheses.
destination	Destination address of the tunnel.
Tunnel keepalive enabled, Period(50 s), Retries(3)	GRE keepalive is enabled. In this example, the keepalive interval is 50 seconds and the keepalive number is 3.
Tunnel TOS	ToS of tunneled packets.
Tunnel TTL	TTL of tunneled packets.
Tunnel protocol/transport	Tunnel mode and transport protocol: • **GRE/IP**—GRE/IPv4 tunnel mode. • **GRE/IPv6**—GRE/IPv6 tunnel mode. • **GRE P2MP**—GRE/IPv4 P2MP tunnel mode. • **GRE P2MP/IPv6**—GRE/IPv6 P2MP tunnel mode. • **GRE_ADVPN/IP**—GRE-encapsulated IPv4 ADVPN tunnel mode. • **GRE_ADVPN/IPv6**—GRE-encapsulated IPv6 ADVPN tunnel mode. • **UDP_ADVPN/IP**—UDP-encapsulated IPv4 ADVPN tunnel mode. • **UDP_ADVPN/IPv6**—UDP-encapsulated IPv6 ADVPN tunnel mode. • **IP/IP**—IPv4 over IPv4 tunnel mode. • **IPv6**—IPv6 tunnel mode. • **IPv6/IP**—IPv6 over IPv4 manual tunnel mode. • **IPv6/IP 6to4**—IPv6 over IPv4 6to4 tunnel mode. • **IPv6/IP auto-tunnel**—Automatic IPv6 over IPv4 tunnel mode. • **IPv6/IP ISATAP**—IPv6 over IPv4 ISATAP tunnel mode. • **DSLITE**—DS-Lite tunnel mode on the AFTR.
GRE key disabled	No GRE tunnel interface key is configured.
Checksumming of GRE packets disabled	The GRE packet checksum feature is disabled.

Field	Description
Source port number is 18001	The source port number is 18001 in ADVPN packets sent by the UDP-encapsulated ADVPN tunnel interface.
Last clearing of counters	Last time when counters were cleared.
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec	Average input rate in the last 300 seconds.
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec	Average output rate in the last 300 seconds.
Input: 0 packets, 0 bytes, 0 drops	Total input packets, total input bytes, and total input packets dropped. Input packets are counted after hardware or software de-encapsulation.
Output: 0 packets, 0 bytes, 0 drops	Total output packets, total output bytes, and total output packets dropped. Output packets are counted before hardware or software encapsulation.

Display brief information about Tunnel 1.

```
<Sysname> display interface tunnel 1 brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP     Description
Tun1                 UP   UP       1.1.1.1        Tunnel1
```

Display brief information about Tunnel 1, including the complete interface description.

```
<Sysname> display interface tunnel 1 brief description
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP     Description
Tun1                 UP    UP      1.1.1.1        Tunnel1
```

Display information about interfaces in DOWN state and the causes.

```
<Sysname> display interface tunnel brief down
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Interface            Link Cause
Tun0                  DOWN Not connected
Tun1                  DOWN Not connected
```

Table 6 Command output

Field	Description
Interface	Abbreviated interface name.

Field	Description
Link	Physical link state of the interface: • **UP**—The interface is physically up. • **DOWN**—The interface is physically down. • **ADM**—The interface has been shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command. • **Stby**—The interface is a backup interface in standby state. To see the primary interface, use the **display interface-backup state** command.
Protocol	Data link layer protocol state of the interface: • **UP**—The data link layer protocol of the interface is up. • **DOWN**—The data link layer protocol of the interface is down. • **UP(s)**—The data link layer protocol of the interface is up, but the link is an on-demand link or does not exist. The **(s)** attribute represents the spoofing flag. This value is typical of null interfaces and loopback interfaces.
Primary IP	Primary IP address of the interface. This field displays two hyphens (**--**) if the interface does not have an IP address.
Description	Description of the interface.
Cause	Cause for the physical link state of an interface to be **DOWN**: • **Administratively**—The interface has been manually shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command. • **Not connected**—The tunnel is not established.

Related commands

destination

interface tunnel

source

ds-lite enable

Use **ds-lite enable** to enable DS-Lite tunneling on an interface.

Use **undo ds-lite enable** to disable DS-Lite tunneling on an interface.

Syntax

ds-lite enable

undo ds-lite enable

Default

DS-Lite tunneling is disabled on an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

Use this command on the AFTR's interface connected to the public IPv4 network, so the AFTR can forward IPv4 packets to the B4 router through the DS-Lite tunnel.

You cannot enable DS-Lite tunneling on a DS-Lite tunnel interface on the AFTR.

Examples

Enable DS-Lite tunneling on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ds-lite enable
```

interface tunnel

Use **interface tunnel** to create a tunnel interface, specify the tunnel mode, and enter tunnel interface view, or enter the view of an existing tunnel interface.

Use **undo interface tunnel** to delete a tunnel interface.

Syntax

interface tunnel *number* [**mode** { **advpn** { **gre** | **udp** } [**ipv6**] | **ds-lite-aftr** | **gre** [**ipv6**] | **gre-p2mp** [**ipv6**] | **ipsec** [**ipv6**] | **ipv4-ipv4** | **ipv6** | **ipv6-ipv4** [**6rd** | **6to4** | **auto-tunnel** | **isatap**] }]

undo interface tunnel *number*

Default

No tunnel interfaces exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

number: Specifies the number of the tunnel interface. The value range is 0 to 1023. The number of tunnel interfaces that can be created is restricted by the total number of interfaces and the memory.

mode advpn gre: Specifies the GRE-encapsulated IPv4 ADVPN tunnel mode.

The following compatibility matrixes show the support of hardware platforms for the **mode advpn gre** parameter:

Models	Parameter compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB1180, NFNX3-HDB1480	No

mode advpn udp: Specifies the UDP-encapsulated IPv4 ADVPN tunnel mode.

The following compatibility matrixes show the support of hardware platforms for the **mode advpn udp** parameter:

Models	Parameter compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB1180, NFNX3-HDB1480	No

`mode advpn gre ipv6`: Specifies the GRE-encapsulated IPv6 ADVPN tunnel mode.

The following compatibility matrixes show the support of hardware platforms for the **`mode advpn gre ipv6`** parameter:

Models	Parameter compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB1180, NFNX3-HDB1480	No

`mode advpn udp ipv6`: Specifies the UDP-encapsulated IPv6 ADVPN tunnel mode.

The following compatibility matrixes show the support of hardware platforms for the **`mode advpn udp ipv6`** parameter:

Models	Parameter compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB1180, NFNX3-HDB1480	No

`mode ds-lite-aftr`: Specifies the DS-Lite tunnel mode on the AFTR.

`mode gre`: Specifies the GRE/IPv4 tunnel mode.

`mode gre ipv6`: Specifies the GRE/IPv6 tunnel mode.

`mode gre-p2mp`: Specifies the GRE/IPv4 P2MP tunnel mode.

The following compatibility matrixes show the support of hardware platforms for the **`mode gre-p2mp`** parameter:

Models	Parameter compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080	Yes
NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	No

`mode gre-p2mp ipv6`: Specifies the GRE/IPv6 P2MP tunnel mode.

The following compatibility matrixes show the support of hardware platforms for the **`mode gre-p2mp ipv6`** parameter:

Models	Parameter compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080	Yes

NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	No

mode ipsec: Specifies the IPsec/IPv4 tunnel mode.

The following compatibility matrixes show the support of hardware platforms for the **mode ipsec** parameter:

Models	Parameter compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB1180, NFNX3-HDB1480	No

mode ipsec ipv6: Specifies the IPsec/IPv6 tunnel mode.

The following compatibility matrixes show the support of hardware platforms for the **mode ipsec ipv6** parameter:

Models	Parameter compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB1180, NFNX3-HDB1480	No

mode ipv4-ipv4: Specifies the IPv4 over IPv4 tunnel mode.

mode ipv6: Specifies the IPv6 tunnel mode. Set this mode for IPv4 over IPv6 manual and IPv6 over IPv6 tunnels.

mode ipv6-ipv4: Specifies the IPv6 over IPv4 manual tunnel mode.

mode ipv6-ipv4 6rd: Specifies the 6RD tunnel mode.

The following compatibility matrixes show the support of hardware platforms for the 6RD tunnel mode parameter:

Models	Parameter compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	No
NFNX3-HDB680, NFNX3-HDB1080	Yes

mode ipv6-ipv4 6to4: Specifies the 6to4 tunnel mode.

mode ipv6-ipv4 auto-tunnel: Specifies the IPv4-compatible IPv6 automatic tunnel mode.

mode ipv6-ipv4 isatap: Specifies the ISATAP tunnel mode.

Usage guidelines

To create a new tunnel interface, you must specify the tunnel mode in this command. To enter the view of an existing tunnel interface, you do not need to specify the tunnel mode.

A tunnel interface number is locally significant. The tunnel interfaces on the two ends of a tunnel can use the same or different interface numbers.

On IPv4 and IPv6 VXLAN tunnel interfaces and VXLAN-DCI tunnel interfaces, IP addresses (assigned by **ip address** and **ipv6 address** commands) are meaningless. As a best practice, do not assign IP addresses to those types of tunnel interfaces.

Examples

Create GRE/IPv4 tunnel interface Tunnel 1 and enter tunnel interface view.

```
<Sysname> system-view
[Sysname] interface tunnel 1 mode gre
[Sysname-Tunnel1]
```

Related commands

destination

display interface tunnel

source

mtu

Use **mtu** to set the MTU on a tunnel interface.

Use **undo mtu** to restore the default.

Syntax

mtu *size*

undo mtu

Default

If the tunnel interface has never been up, the MTU is 64000 bytes.

If the tunnel interface is up, its MTU is identical to the outgoing interface's MTU minus the length of the tunnel headers. The outgoing interface is automatically obtained through routing table lookup based on the tunnel destination address.

Views

Tunnel interface view

Predefined user roles

network-admin

context-admin

Parameters

size: Specifies the MTU, in the range of 100 to 64000 bytes.

Usage guidelines

After you configure an MTU for a tunnel interface, the configured MTU applies regardless of the tunnel interface status (up/down) and the outgoing interface MTU.

To avoid fragmentation after tunnel encapsulation, set the tunnel interface MTU no greater than the value of the outgoing interface MTU minus the length of the tunnel headers.

Examples

Set the MTU on Tunnel 1 to 1000 bytes.

```
<Sysname> system-view
[Sysname] interface tunnel 1
[Sysname-Tunnel1] mtu 1000
```

Related commands

display interface tunnel

reset counters interface tunnel

Use **reset counters interface tunnel** to clear tunnel interface statistics.

Syntax

reset counters interface [**tunnel** [*number*]]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

tunnel [*number*]: Specifies a tunnel interface. The *number* argument specifies the tunnel interface number. If you do not specify the **tunnel** keyword, this command clears statistics for all interfaces. If you specify the **tunnel** keyword without the *number* argument, this command clears statistics for all tunnel interfaces.

Usage guidelines

Use this command to clear old statistics so you can observe new traffic statistics on a tunnel interface.

Examples

Clear statistics for Tunnel 1.

```
<Sysname> reset counters interface tunnel 1
```

Related commands

display interface tunnel

shutdown

Use **shutdown** to shut down a tunnel interface.

Use **undo shutdown** to bring up a tunnel interface.

Syntax

shutdown

undo shutdown

Default

A tunnel interface is not administratively down.

Views

Tunnel interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command disconnects all links set up on the interface. Make sure you fully understand the impact of the command on your network.

Examples

Shut down Tunnel 1.

```
<Sysname> system-view
[Sysname] interface tunnel 1
[Sysname-Tunnel1] shutdown
```

Related commands

display interface tunnel

source

Use **source** to specify the source address or source interface of a tunnel.

Use **undo source** to restore the default.

Syntax

source { *ipv4-address* | *ipv6-address* | *interface-type interface-number* }

undo source

Default

No source address or source interface is specified for a tunnel.

Views

Tunnel interface view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-address: Specifies the tunnel source IPv4 address.

ipv6-address: Specifies the tunnel source IPv6 address.

interface-type interface-number: Specifies the source interface by its type and number. The interface must be up and must have an IP address.

Usage guidelines

The specified source address or the address of the specified source interface is used as the source address of tunneled packets. To display the configured tunnel source address, use the **display interface tunnel** command.

Do not specify the same tunnel source and destination addresses for different tunnels on the same device.

The destination address of a tunnel at the local end must be the source address of the tunnel at the peer end. The source address of the tunnel at the local end must be the destination address of the tunnel at the peer end.

If you execute this command multiple times, the most recent configuration takes effect.

You cannot specify the tunnel interface of the DS-Lite tunnel on the AFTR as the source interface.

Examples

Specify GigabitEthernet 1/0/1 as the source interface of Tunnel 1.

```
<Sysname> system-view
[Sysname] interface tunnel 1 mode gre
[Sysname-Tunnel1] source gigabitethernet 1/0/1
```

Specify 192.100.1.1 as the source address of Tunnel 1.

```
<Sysname> system-view
[Sysname] interface tunnel 1 mode gre
[Sysname-Tunnel1] source 192.100.1.1
```

Related commands

`destination`

`display interface tunnel`

`interface tunnel`

tunnel 6rd br

Use **`tunnel 6rd br`** to specify a BR address for a 6RD tunnel.

Use **`undo tunnel 6rd br`** to restore the default.

Syntax

`tunnel 6rd br` *`ipv4-address`*

`undo tunnel 6rd br`

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	No
NFNX3-HDB680, NFNX3-HDB1080	Yes

Default

No BR address is specified for a 6RD tunnel.

Views

Tunnel interface view

Predefined user roles

network-admin

context-admin

Parameters

`ipv4-address`: Specifies the BR address (IPv4 address of a 6RD BR router), in dotted decimal notation.

Usage guidelines

Use this command on a 6RD CE. For a 6RD network to communicate with a non-6RD network over a 6RD tunnel, you must specify the BR address on the 6RD CE.

All the 6RD CEs and 6RD BR routers in a 6RD network must have the same IPv4 prefix and suffix. Make sure the BR address and the tunnel source address have the same IPv4 prefix and suffix.

Examples

Specify the BR address as 10.11.12.13 on Tunnel 1.

```
<Sysname> system-view
[Sysname] interface tunnel 1 mode ipv6-ipv4 6rd
[Sysname-Tunnel1] tunnel 6rd br 10.11.12.13
```

Related commands

display 6rd

tunnel 6rd ipv4

Use **tunnel 6rd ipv4** to specify a prefix length and a suffix length for a 6RD tunnel source address.

Use **undo tunnel 6rd ipv4** to restore the default.

Syntax

tunnel 6rd ipv4 { **prefix-length** *length* | **suffix-length** *length* } *

undo tunnel 6rd ipv4

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	No
NFNX3-HDB680, NFNX3-HDB1080	Yes

Default

All 32 bits of the IPv4 tunnel source address are used to create the 6RD delegated prefix.

Views

Tunnel interface view

Predefined user roles

network-admin

context-admin

Parameters

prefix-length *length*: Specifies the prefix length in the range of 0 to 31.

suffix-length *length*: Specifies the suffix length in the range of 0 to 31.

Usage guidelines

All 6RD tunnel interfaces in a 6RD network must be configured with the same IPv4 prefix length and suffix length.

You can specify a prefix length, a suffix length, both prefix and suffix lengths, or neither. The device will remove the prefix and suffix bits from the tunnel source address and embed the left bits of the address to the 6RD delegated prefix. If neither a prefix length nor a suffix length is specified, all 32 bits of the IPv4 tunnel source address will be embedded in the 6RD delegated prefix.

Examples

Specify both the prefix length and suffix length as 8 on Tunnel 1.

```
<Sysname> system-view
[Sysname] interface tunnel 1 mode ipv6-ipv4 6rd
[Sysname-Tunnel1] tunnel 6rd ipv4 prefix-length 8 suffix-length 8
```

Related commands

display 6rd

display 6rd destination

display 6rd prefix

tunnel 6rd prefix

Use **tunnel 6rd prefix** to configure the 6RD prefix for a 6RD tunnel.

Use **undo tunnel 6rd prefix** to restore the default.

Syntax

tunnel 6rd prefix *ipv6-prefix/prefix-length*

undo tunnel 6rd prefix

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	No
NFNX3-HDB680, NFNX3-HDB1080	Yes

Default

No 6RD prefix is configured for a 6RD tunnel.

Views

Tunnel interface view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-prefix/prefix-length: Specifies the IPv6 prefix and its length. The value range for the prefix length is 1 to 127.

Usage guidelines

A 6RD delegated prefix contains a 6RD prefix and all or part of the bits in the IPv4 tunnel source address.

All tunnels in a 6RD network must have the same 6RD prefix.

Examples

Configure the 6RD prefix as 2001:1000::/32 on Tunnel 1.

```
<Sysname> system-view
[Sysname] interface tunnel 1 mode ipv6-ipv4 6rd
```

```
[Sysname-Tunnel1] tunnel 6rd prefix 2001:1000::/32
```

Related commands

display 6rd

display 6rd destination

display 6rd prefix

tunnel dfbit enable

Use **tunnel dfbit enable** to set the Don't Fragment (DF) bit for tunneled packets.

Use **undo tunnel dfbit enable** to restore the default.

Syntax

tunnel dfbit enable

undo tunnel dfbit enable

Default

The DF bit is not set for tunneled packets.

Views

Tunnel interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

To avoid fragmentation and delay, set the DF bit for tunneled packets. Make sure the path MTU is larger than the tunneled packet length. To avoid discarding tunneled packets whose length is larger than the path MTU, do not set the DF bit.

This command is not supported on a GRE/IPv6 tunnel interface and an IPv6 tunnel interface.

Examples

Set the DF bit for tunneled packets on Tunnel 1.

```
<Sysname> system-view
[Sysname] interface tunnel 1 mode gre
[Sysname-Tunnel1] tunnel dfbit enable
```

tunnel discard ipv4-compatible-packet

Use **tunnel discard ipv4-compatible-packet** to enable dropping IPv6 packets that use IPv4-compatible IPv6 addresses.

Use **undo tunnel discard ipv4-compatible-packet** to restore the default.

Syntax

tunnel discard ipv4-compatible-packet

undo tunnel discard ipv4-compatible-packet

Default

IPv6 packets that use IPv4-compatible IPv6 addresses are not dropped.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command enables the device to check the source and destination IPv6 addresses of the de-encapsulated IPv6 packets from a tunnel. If a packet uses an IPv4-compatible IPv6 address as the source or destination address, the device discards the packet.

Examples

Enable dropping IPv6 packets that use IPv4-compatible IPv6 addresses.

```
<Sysname> system-view
[Sysname] tunnel discard ipv4-compatible-packet
```

tunnel tos

Use **tunnel tos** to set the ToS of tunneled packets.

Use **undo tunnel tos** to restore the default.

Syntax

tunnel tos { **copy-inner-tos** | *tos-value* }

undo tunnel tos

Default

For VXLAN tunneled packets, the ToS is 0.

For non-VXLAN tunneled packets, the ToS is the same as the ToS of the original packets.

Views

Tunnel interface view

Predefined user roles

network-admin

context-admin

Parameters

copy-inner-tos: Configures tunneled packets to use the ToS of the original packets. This keyword is supported only by VXLAN tunnels.

tos-value: Specifies the ToS of tunneled packets, in the range of 0 to 255.

Usage guidelines

After you execute this command, all the tunneled packets of different services sent on the tunnel interface will use the same configured ToS. For more information about ToS, see *ACL and QoS Configuration Guide*.

Examples

Set the ToS of tunneled packets to 20 on Tunnel 1.

```
<Sysname> system-view
[Sysname] interface tunnel 1 mode gre
[Sysname-Tunnel1] tunnel tos 20
```

Configure VXLAN tunnel interface Tunnel 2 to use the ToS of the original packets as the ToS of tunneled packets.

```
<Sysname> system-view
[Sysname] interface tunnel 2 mode vxlan
[Sysname-Tunnel2] tunnel tos copy-inner-tos
```

Related commands

display interface tunnel

tunnel ttl

Use **tunnel ttl** to set the Time to Live (TTL) of tunneled packets.

Use **undo tunnel ttl** to restore the default.

Syntax

tunnel ttl *ttl-value*

undo tunnel ttl

Default

The TTL of tunneled packets is 255.

Views

Tunnel interface view

Predefined user roles

network-admin

context-admin

Parameters

ttl-value: Specifies the TTL of tunneled packets, in the range of 1 to 255.

Usage guidelines

The TTL determines the maximum number of hops that the tunneled packets can pass. When the TTL expires, the tunneled packets are discarded to avoid loops.

Examples

Set the TTL of tunneled packets to 100 on Tunnel 1.

```
<Sysname> system-view
[Sysname] interface tunnel 1 mode gre
[Sysname-Tunnel1] tunnel ttl 100
```

Related commands

display interface tunnel

tunnel vpn-instance

Use **tunnel vpn-instance** to specify a VPN instance for the destination address of a tunnel interface.

Use **undo tunnel vpn-instance** to restore the default.

Syntax

tunnel vpn-instance *vpn-instance-name*

undo tunnel vpn-instance

Default

The destination address of a tunnel interface belongs to the public network.

Views

Tunnel interface view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance-name: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

After this command is executed, the device looks up the routing table of the specified VPN instance to forward tunneled packets on the tunnel interface.

For a tunnel interface to come up, the tunnel source and destination must belong to the same VPN instance. To specify a VPN instance for the tunnel source, use the **ip binding vpn-instance** command on the tunnel source interface.

Examples

Specify VPN instance **vpn10** for the tunnel destination on Tunnel 1.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn10
[Sysname-vpn-instance-vpn10] route-distinguisher 1:1
[Sysname-vpn-instance-vpn10] vpn-target 1:1
[Sysname-vpn-instance-vpn10] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip binding vpn-instance vpn10
[Sysname-GigabitEthernet1/0/1] ip address 1.1.1.1 24
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] interface tunnel 1 mode gre
[Sysname-Tunnel1] source gigabitethernet 1/0/1
[Sysname-Tunnel1] destination 1.1.1.2
[Sysname-Tunnel1] tunnel vpn-instance vpn10
```

Related commands

ip binding vpn-instance (*VPN Instance Command Reference*)

Contents

GRE commands

display gre p2mp tunnel-table interface tunnel

Use **display gre p2mp tunnel-table interface tunnel** to display dynamic tunnel entry information for a GRE P2MP tunnel interface.

Syntax

display gre p2mp tunnel-table interface tunnel *number* [**ipv4** | **ipv6**]

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080	Yes
NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	No

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

number: Specifies an existing GRE P2MP tunnel interface by its interface number.

ipv4: Specifies dynamic IPv4 tunnel entries.

ipv6: Specifies dynamic IPv6 tunnel entries.

Usage guidelines

If you do not specify the **ipv4** keyword or the **ipv6** keyword, this command displays all dynamic tunnel entries for a GRE P2MP tunnel interface.

Examples

Display all dynamic tunnel entries for GRE P2MP tunnel interface **Tunnel 0**.

```
<Sysname> display gre p2mp tunnel-table interface tunnel 0
Total number:2
Dest Addr               Mask/Prefix Len Tunnel Dest Addr        Gre Key   Aging
10.0.0.1                255.255.255.255 20.0.0.1                          10
10::1                   64              20.0.0.2                          5
```

Display dynamic IPv4 tunnel entries for GRE P2MP tunnel interface **Tunnel 0**.

```
<Sysname> display gre p2mp tunnel-table interface tunnel 0 ipv4
Total number:1
Dest Addr               Mask/Prefix Len Tunnel Dest Addr        Gre Key   Aging
100.0.0.1               255.255.255.255  20.0.0.1                         9
```

Display dynamic IPv6 tunnel entries for GRE P2MP tunnel interface **Tunnel 0**.

```
<Sysname> display gre p2mp tunnel-table interface tunnel 0 ipv6
Total number:1
Dest Addr             Mask/Prefix Len Tunnel Dest Addr        Gre Key   Aging
100::1                128                   20::2                       3
```

Table 1 Command output

Field	Description
Total number	Total number of GRE P2MP dynamic tunnel entries.
Dest Addr	Network address of the branch network.
Mask/Prefix Len	Address mask or prefix length of the branch network.
Tunnel Dest Addr	Destination address of the tunnel.
Gre Key	GRE key, which indicates the priority of the dynamic tunnel entry. This field does not display anything if the tunnel destination end does not have a GRE key.
Aging	Remaining lifetime of the entry, in seconds.

display gre p2mp tunnel-table statistics

Use **display gre p2mp tunnel-table statistics** to display packet statistics of static tunnel entries for a GRE P2MP tunnel interface.

Syntax

display gre p2mp tunnel-table statistics interface tunnel *number* [**vpn-instance** *vpn-instance-name*] [**branch-network-address** *branch-network-address* { *mask* | *mask-length* }]

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080	Yes
NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	No

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface tunnel *number*: Specifies an existing GRE P2MP tunnel interface by its interface number.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays packet statistics of static tunnel entries on the public network for the specified GRE P2MP tunnel interface.

branch-network-address *branch-network-address*: Specifies an IPv4 branch network address. If you do not specify this option, the command displays packets statistics of static tunnel entries for all IPv4 branch networks of the specified scope.

mask: Specifies the mask of the branch network address, in dotted decimal notation.

mask-length: Specifies the mask length of the branch network address, in the range of 0 to 32.

Usage guidelines

If you do not specify any parameters, this command displays packet statistics of all static tunnel entries on the public network for the specified GRE P2MP tunnel interface.

Examples

Display packet statistics of all static tunnel entries on the public network for GRE P2MP tunnel interface **Tunnel 1**.

```
<Sysname> display gre p2mp tunnel-table statistics interface tunnel 1

VPN-instance name: -       Map entries: 2

Branch network address    : 192.168.11.1/32
Tunnel destination address: 11.1.1.1
Checksum value            : 192.168.20.1
  Input:
    0 packets, 0 bytes, 0 drops
  Output:
    0 packets, 0 bytes, 0 drops

Branch network address    : 192.168.12.1/32
Tunnel destination address: 11.1.1.1
Checksum value            : 192.168.20.2
  Input:
    0 packets, 0 bytes, 0 drops
  Output:
    0 packets, 0 bytes, 0 drops
```

Table 2 Command output

Field	Description
VPN-instance name	VPN instance of the branch networks. If the branch networks belong to the public network, this field displays a hyphen (-).
Map entries	Total number of GRE P2MP tunnel mapping entries.
Branch network address	IPv4 address and mask of a branch network.
Tunnel destination address	A destination address of the tunnel.
Checksum value	Value to fill in the **checksum** field. The system does not display the **Checksum value** field if no value is specified to fill in the **checksum** field.

Field	Description
Input: 0 packets, 0 bytes, 0 drops	Incoming traffic statistics: • Number of incoming packets. • Number of incoming bytes. • Number of dropped packets.
Output: 0 packets, 0 bytes, 0 drops	Outgoing traffic statistics: • Number of outgoing packets. • Number of outgoing bytes. • Number of dropped packets.

gre checksum

Use **gre checksum** to enable GRE checksum.

Use **undo gre checksum** to disable GRE checksum.

Syntax

gre checksum

undo gre checksum

Default

GRE checksum is disabled.

Views

Tunnel interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

GRE checksum verifies packet integrity.

You can enable or disable GRE checksum at each end of a tunnel as needed. After GRE checksum is enabled, the sender does the following:

- Calculates the checksum for the GRE header and the payload.
- Sends the packet containing the checksum information to the peer.

The receiver calculates the checksum for the received packet and compares it with that carried in the packet. If the checksums are the same, the receiver processes the packet. If the checksums are different, the receiver discards the packet.

If a packet carries a GRE checksum, the receiver checks the checksum whether or not the receiver is enabled with GRE checksum.

Examples

Enable GRE checksum.

```
<Sysname> system-view
[Sysname] interface tunnel 2 mode gre
[Sysname-Tunnel2] gre checksum
```

gre key

Use **gre key** to configure a key for a GRE tunnel interface.

Use **undo gre key** to restore the default.

Syntax

gre key *key*

undo gre key

Default

No key is configured for a GRE tunnel interface.

Views

Tunnel interface view

Predefined user roles

network-admin

context-admin

Parameters

key: Specifies the key for the GRE tunnel interface, in the range of 0 to 4294967295.

Usage guidelines

Both ends of a GRE point-to-point tunnel must have the same key or no key.

Do not configure any GRE key on a GRE P2MP tunnel interface. You can configure GRE keys on the point-to-point tunnel interfaces in the branch networks. The GRE keys not only check for the validity of packets received on the tunnel interfaces but also indicate the priorities of dynamic tunnels. The GRE P2MP tunnel end prefers the branch tunnel that has the highest priority to forward traffic.

Do not use this command together with the **gre vpc enable** command on the same tunnel interface.

Examples

Configure the GRE key as 123 for the GRE tunnel interface Tunnel 2.

```
<Sysname> system-view
[Sysname] interface tunnel 2 mode gre
[Sysname-Tunnel2] gre key 123
```

gre p2mp aging-time

Use **gre p2mp aging-time** to specify an aging timer for dynamic tunnel entries of a GRE P2MP tunnel interface.

Use **undo gre p2mp aging-time** to restore the default.

Syntax

gre p2mp aging-time *aging-time*

undo gre p2mp aging-time

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280,	Yes

Models	Command compatibility
NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080	
NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	No

Default

The aging timer is 5 seconds.

Views

Tunnel interface view

Predefined user roles

network-admin

context-admin

Parameters

aging-time: Specifies an aging timer in the range of 1 to 86400 seconds.

Usage guidelines

This command is applicable only to GRE P2MP tunnel interfaces.

If the headquarters gateway does not receive any packets from a branch when the aging timer expires, it deletes the dynamic tunnel entry of that branch.

Set an appropriate aging timer depending on the network condition. A shorter timer might cause forwarding failure to an actual reachable network. A longer timer cannot quickly update dynamic tunnel entries.

Examples

Set the aging timer to 10 seconds for dynamic tunnel entry on GRE P2MP tunnel interface **Tunnel 0**.

```
<Sysname> system-view
[Sysname] interface tunnel 0 mode gre-p2mp
[Sysname-Tunnel0] gre p2mp aging-time 10
```

gre p2mp backup-interface

Use **gre p2mp backup-interface** to specify a backup interface for a GRE P2MP tunnel interface.

Use **undo gre p2mp backup-interface** to restore the default.

Syntax

gre p2mp backup-interface tunnel *number*

undo gre p2mp backup-interface

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080	Yes
NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	No

Default

No backup interface is configured for a GRE P2MP tunnel interface.

Views

Tunnel interface view

Predefined user roles

network-admin

context-admin

Parameters

tunnel *number*: Specifies a tunnel interface by its interface number. The tunnel interface must exist on the device and must be a GRE/IPv4 or GRE/IPv6 tunnel interface.

Usage guidelines

This command is applicable only to GRE P2MP tunnel interfaces.

When the device cannot find a matching GRE P2MP dynamic tunnel entry to forward traffic, it forwards the traffic to the backup gateway through the backup interface. Services (for example, NetStream and NAT) on the backup interface do not take effect on the traffic. The service configuration on the primary GRE P2MP tunnel interface is used for the traffic.

Examples

Specify tunnel interface **Tunnel 100** as the backup interface of GRE P2MP tunnel interface **Tunnel 0**.

```
<Sysname> system-view
[Sysname] interface tunnel 0 mode gre-p2mp
[Sysname-Tunnel0] gre p2mp backup-interface tunnel 100
```

gre p2mp branch-network-mask

Use **gre p2mp branch-network-mask** to specify the network mask or mask length for IPv4 branch networks or specify the prefix length for IPv6 branch networks on a GRE P2MP tunnel interface.

Use **undo gre p2mp branch-network-mask** to restore the default.

Syntax

gre p2mp branch-network-mask { *mask* | *mask-length* | **ipv6** *prefix-length* }

undo gre p2mp branch-network-mask [**ipv6**]

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080	Yes
NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	No

Default

The IPv4 address mask is 255.255.255.255 (the mask length is 32) and the IPv6 address prefix length is 128 for branch networks.

Views

Tunnel interface view

Predefined user roles

network-admin

context-admin

Parameters

mask: Specifies the IPv4 address mask, in dotted decimal notation.

mask-length: Specifies the IPv4 address mask length, in the range of 0 to 32.

ipv6 *prefix-length*: Specifies the IPv6 address prefix length, in the range of 0 to 128.

Usage guidelines

This command is applicable only to GRE P2MP tunnel interfaces.

This command enables a GRE P2MP tunnel interface to use the same network mask or prefix length to create dynamic tunnel entries for branch networks. One branch has only one dynamic tunnel entry.

To ensure successful packet forwarding, make sure all branch networks have the same network mask or prefix length, which is the same as that specified by this command.

Examples

Specify the IPv4 branch network mask as 255.255.255.0 for GRE P2MP dynamic tunnel entries on tunnel interface **Tunnel 0**.

```
<Sysname> system-view
[Sysname] interface tunnel 0 mode gre-p2mp
[Sysname-Tunnel0] gre p2mp branch-network-mask 255.255.255.0
```

gre p2mp nexthop-learning

Use **gre p2mp nexthop-learning** to enable next hop host route learning.

Use **undo gre p2mp nexthop-learning** to disable next hop host route learning.

Syntax

gre p2mp nexthop-learning

undo gre p2mp nexthop-learning

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080	Yes
NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	No

Default

Next hop host route learning is disabled.

Views

Tunnel interface view.

Predefined user roles

network-admin

context-admin

Usage guidelines

This command is supported only on GRE/IPv4 P2MP tunnel interfaces.

The headquarters gateway uses the same branch network mask to create tunnel entries for all branch networks. If some branch network addresses are in the same subnet, the headquarters gateway will learn the same destination address for these branch networks in the tunnel entries. In this case, the headquarters cannot establish BGP neighbors with these branches.

To resolve this issue, enable next hop host route learning on the headquarters gateway. This feature enables the gateway to learn destination addresses with the 32-bit mask when it establishes a BGP neighbor relationship with peers that are in the same subnet.

Examples

Enable next hop host route learning on GRE/IPv4 P2MP tunnel interface **Tunnel 0**.

```
<Sysname> system-view
[Sysname] interface tunnel 0 mode gre-p2mp
[Sysname-Tunnel0] gre p2mp nexthop-learning
```

Related commands

gre p2mp branch-network-mask

gre p2mp-template (system view)

Use **gre p2mp-template** to create a GRE P2MP tunnel template and enter its view, or enter the view of an existing GRE P2MP tunnel template.

Use **undo gre p2mp-template** to delete a GRE P2MP tunnel template.

Syntax

gre p2mp-template *template-name*

undo gre p2mp-template *template-name*

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080	Yes
NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	No

Default

No GRE P2MP tunnel templates exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

template-name: Specifies a name for the GRE P2MP tunnel template, a case-sensitive string of 1 to 31 characters.

Examples

Create a GRE P2MP tunnel template named **aa** and enter its view.

```
<Sysname> system-view
[Sysname] gre p2mp-template aa
[Sysname-p2mp-template-aa]
```

Related commands

map

gre p2mp-template (tunnel interface view)

Use **gre p2mp-template** to apply a GRE P2MP tunnel template to a GRE P2MP tunnel interface.

Use **undo gre p2mp-template** to restore the default.

Syntax

gre p2mp-template *template-name*

undo gre p2mp-template

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080	Yes
NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	No

Default

No GRE P2MP tunnel template is applied to a GRE P2MP tunnel interface.

Views

Tunnel interface view

Predefined user roles

network-admin

context-admin

Parameters

template-name: Specifies a GRE P2MP tunnel template by its name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

A GRE P2MP tunnel interface can use only one GRE P2MP tunnel template. If you execute this command multiple times, the most recent configuration takes effect.

Examples

Apply GRE P2MP tunnel template **aa** to GRE P2MP tunnel interface **Tunnel 1**.

```
<Sysname> system-view
[Sysname] interface tunnel 1 mode gre-p2mp
```

```
[Sysname-Tunnel1] gre p2mp-template aa
```

Related commands

gre p2mp-template (system view)

keepalive

Use **keepalive** to enable GRE keepalive and set the keepalive interval and the keepalive number.

Use **undo keepalive** to disable GRE keepalive.

Syntax

keepalive [*interval* [*times*]]

undo keepalive

Default

GRE keepalive is disabled.

Views

Tunnel interface view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies the keepalive interval, in the range of 1 to 32767 seconds. The default value is 10.

times: Specifies the keepalive number, in the range of 1 to 255. The default value is 3.

Usage guidelines

This command enables the tunnel interface to send keepalive packets at the specified interval. If the device receives no response from the peer within the timeout time, it shuts down the local tunnel interface. The device brings the local tunnel interface up if it receives a keepalive acknowledgment packet from the peer. The timeout time is the result of multiplying the keepalive interval by the keepalive number.

The device always acknowledges the keepalive packets it receives whether or not GRE keepalive is enabled.

GRE/IPv6 mode tunnel interfaces do not support this command.

Examples

Enable GRE keepalive, set the keepalive interval to 20 seconds, and set the keepalive number to 5.

```
<Sysname> system-view
[Sysname] interface tunnel 2 mode gre
[Sysname-Tunnel2] keepalive 20 5
```

map

Use **map** to configure a tunnel mapping entry in a GRE P2MP tunnel template.

Use **undo map** to delete a tunnel mapping entry from a GRE P2MP tunnel template.

Syntax

map [**vpn-instance** *vpn-instance-name*] **branch-network-address** *branch-network-address* { *mask* | *mask-length* } **tunnel-destination** *tunnel-dest-address* [**checksum-fill** *checksum-value*]

undo map [**vpn-instance** *vpn-instance-name*] **branch-network-address** *branch-network-address* { *mask* | *mask-length* } [**tunnel-destination** *tunnel-dest-address*]

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080	Yes
NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	No

Default

No tunnel mapping entries are configured in a GRE P2MP tunnel template.

Views

GRE P2MP tunnel template view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the branch network address belongs to a private network, you must specify this option. If the branch network address belongs to the public network, do not specify this option.

branch-network-address *branch-network-address*: Specifies an IPv4 branch network address.

mask: Specifies the mask of the branch network IPv4 address, in dotted decimal notation.

mask-length: Specifies the mask length of the branch network IPv4 address, in the range of 0 to 32.

tunnel-destination *tunnel-dest-address*: Specifies the tunnel destination IPv4 address.

checksum-fill *checksum-value*: Specifies an IPv4 address to fill in the **checksum** field of the GRE header. The IPv4 address is in dotted decimal notation. If you do not specify this option, the device does not fill in the **checksum** field of the GRE header.

Usage guidelines

The tunnel mapping entries in the tunnel template are static tunnel entries.

You can repeat this command to configure multiple tunnel mapping entries for a GRE P2MP tunnel template. Each entry defines a mapping between a branch network address and a tunnel destination address. One branch network address can be mapped to only one tunnel destination address.

If a branch network contains VMs that have multiple users, fill the IPv4 address of the destination VM to the **checksum** field for correct forwarding of a GRE packet. Specify the **checksum-fill**

checksum-value option depending on your network. Incorrect usage of the option will cause GRE checksum failures.

Examples

In GRE P2MP tunnel template **aa**, configure a tunnel mapping entry. The branch network address is 192.168.0.11 and the mask length is 32, the tunnel destination address is 10.108.113.71, and the IPv4 address to fill in the **checksum** field is 192.168.20.1.

```
<Sysname> system-view
[Sysname] gre p2mp-template aa
[Sysname-p2mp-template-aa] map branch-network-address 192.168.0.11 32 tunnel-destination
10.108.113.71 checksum-fill 192.168.20.1
```

Related commands

gre p2mp-template (system view)

reset gre p2mp tunnel-table

Use **reset gre p2mp tunnel-table** to clear dynamic tunnel entry information for a GRE P2MP tunnel interface.

Syntax

reset gre p2mp tunnel-table interface tunnel *number* [**destination** { *dest-address* | **ipv6** *dest-ipv6-address* } **tunnel-destination** { *tunnel-dest-address* | **ipv6** *tunnel-dest-address* }]

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080	Yes
NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	No

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

interface tunnel *number*: Specifies a GRE P2MP tunnel interface by its interface number.

destination { *dest-address* | **ipv6** *dest-ipv6-address* }: Specifies an IPv4 or IPv6 branch network address of the specified GRE P2MP tunnel interface.

tunnel-destination { *tunnel-dest-address* | **ipv6** *tunnel-dest-address* }: Specifies a tunnel destination IPv4 or IPv6 address.

Usage guidelines

If you do not specify a branch network address or a tunnel destination address, this command clears all dynamic tunnel entries for the specified GRE P2MP tunnel interface.

Examples

Clear all dynamic tunnel entries for GRE P2MP tunnel interface **Tunnel 0**.

```
<Sysname> reset gre p2mp tunnel-table interface tunnel 0
```

Clear a dynamic tunnel entry of which the branch network is 10.0.0.1 and the tunnel destination is 20.0.0.1 on GRE P2MP tunnel interface **Tunnel 0**.

```
<Sysname> reset gre p2mp tunnel-table interface tunnel 0 destination 10.0.0.1
tunnel-destination 20.0.0.1
```

Related commands

display gre p2mp tunnel-table interface tunnel

reset gre p2mp tunnel-table statistics

Use **reset gre p2mp tunnel-table statistics** to clear packet statistics of static tunnel entries for a GRE P2MP tunnel interface.

Syntax

reset gre p2mp tunnel-table statistics interface tunnel *number* [**vpn-instance** *vpn-instance-name*] [**branch-network-address** *branch-network-address* { *mask* | *mask-length* }]

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080	Yes
NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	No

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

interface tunnel *number*: Specifies an existing GRE P2MP tunnel interface by its interface number.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears packet statistics of static tunnel entries on the public network for the specified GRE P2MP tunnel interface.

branch-network-address *branch-network-address*: Specifies a branch network IPv4 address. If you do not specify this option, the command clears packet statistics of static tunnel entries for all IPv4 branch networks of the specified scope.

mask: Specifies the mask of the branch network address, in dotted decimal notation.

mask-length: Specifies the mask length of the branch network address, in the range of 0 to 32.

Usage guidelines

If you do not specify any parameters, this command clears packet statistics of all static tunnel entries on the public network for the specified GRE P2MP tunnel interface.

Examples

Clear packet statistics of all static tunnel entries on the public network for GRE P2MP tunnel interface **Tunnel 1**.

```
<Sysname> reset gre p2mp tunnel-table statistics interface tunnel 1
```

Related commands

display gre p2mp tunnel-table statistics

tunnel route-static

Use **tunnel route-static** to configure the preference of static routes for a GRE P2MP tunnel interface.

Use **undo tunnel route-static** to restore the default.

Syntax

tunnel route-static [**preference** *preference-value*]

undo tunnel route-static

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080	Yes
NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	No

Default

The preference of static routes is 60 for a GRE P2MP tunnel interface.

Views

Tunnel interface view

Predefined user roles

network-admin

context-admin

Parameters

preference *preference-value*: Specifies a preference value in the range of 1 to 255. The default value is 60, which is not affected by the **ip route-static default-preference** command.

Usage guidelines

A GRE P2MP tunnel interface automatically issues reachable static routes according to the tunnel mapping entries configured in the GRE P2MP tunnel template applied to the interface. This command takes effect on these static routes.

Examples

Set the preference of static routes to 3 for GRE P2MP tunnel interface **Tunnel 1**.

```
<Sysname> system-view
[Sysname] interface tunnel 1 mode gre-p2mp
[Sysname-Tunnel1] tunnel route-static preference 3
```

Related commands

`display ip routing-table protocol` (*Layer 3—IP Routing Command Reference*)

Contents

L2TP commands

allow l2tp

Use **allow l2tp** to configure an L2TP network server (LNS) to accept Layer 2 Tunneling Protocol (L2TP) tunneling requests from an L2TP access concentrator (LAC), and to specify a VT interface for tunnel setup.

Use **undo allow** to restore the default.

Syntax

allow l2tp virtual-template *virtual-template-number* [**remote** *remote-name*]

undo allow

Default

An LNS denies L2TP tunneling requests from any LACs.

Views

L2TP group view

Predefined user roles

network-admin

context-admin

Parameters

virtual-template *virtual-template-number*: Specifies a VT interface by its number. The value range for the *virtual-template-number* argument is 1 to 1024. An LNS dynamically creates virtual access (VA) interfaces based on the configuration of a VT interface. Each VA interface is used to carry data for a different L2TP session.

remote *remote-name*: Specifies the name of the tunnel peer (LAC) initiating tunneling requests, a case-sensitive string of 1 to 31 characters.

Usage guidelines

The **allow l2tp** command is available only on L2TP groups in LNS mode.

Make sure the specified name of the tunnel peer is consistent with the local name configured on the LAC.

If you execute this command multiple times for an L2TP group, the most recent configuration takes effect.

For L2TP group 1, if you do not specify the **remote** *remote-name* option, an LNS accepts tunneling requests from any LACs. In this case, L2TP group 1 acts as the default L2TP group. For L2TP groups other than L2TP group 1, the **remote** *remote-name* option must be configured.

The **allow l2tp** command is available only on LNSs.

- When an LAC that initiates a tunneling request is the tunnel peer configured in an L2TP group, the LNS uses the tunnel parameters configured in this group for tunnel setup.
- When the LAC is not the tunnel peer configured in any L2TP group, the LNS performs one of the following operations:
  - Uses the tunnel parameters for the default L2TP group if it exists.
  - Fails to set up a tunnel with the LAC if the default L2TP group does not exist.

As a best practice, configure a default L2TP group on the LNS in the following cases:

- LACs (such as hosts with Windows 2000 Beta 2 installed) include blank local names in their tunneling requests.
- The LNS sets up tunnels with multiple LACs by using the same tunnel parameters.

Examples

Specify L2TP group 1 as the default L2TP group, and specify Virtual-Template 1 for tunnel setup. For L2TP group 2, configure the LNS to accept the L2TP tunneling request initiated by the peer (LAC) named **aaa**, and specify Virtual-Template 2 for tunnel setup.

```
<Sysname> system-view
[Sysname] l2tp-group 1 mode lns
[Sysname-l2tp1] allow l2tp virtual-template 1
[Sysname-l2tp1] quit
[Sysname] l2tp-group 2 mode lns
[Sysname-l2tp2] allow l2tp virtual-template 2 remote aaa
```

Related commands

tunnel name

bandwidth

Use **bandwidth** to set the expected bandwidth for an interface.

Use **undo bandwidth** to restore the default.

Syntax

bandwidth *bandwidth-value*

undo bandwidth

Default

The expected bandwidth (in kbps) is interface baudrate divided by 1000.

Views

Virtual PPP interface view

Predefined user roles

network-admin

context-admin

Parameters

bandwidth-value: Specifies the expected bandwidth in the range of 1 to 400000000 kbps.

Usage guidelines

The expected bandwidth of an interface affects the link costs in OSPF, OSPFv3, and IS-IS. For more information, see *Layer 3—IP Routing Configuration Guide*.

Examples

Set the expected bandwidth of Virtual-PPP 10 to 100 kbps.

```
<Sysname> system-view
[Sysname] interface virtual-ppp 10
[Sysname-Virtual-PPP10] bandwidth 100
```

default

Use **default** to restore the default settings for a virtual PPP interface.

Syntax

default

Views

Virtual PPP interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

CAUTION:
The **default** command might interrupt ongoing network services. Make sure you are fully aware of the impact of this command when you execute it on a live network.

This command might fail to restore the default settings for some commands for reasons such as command dependencies or system restrictions. Use the **display this** command in interface view to identify these commands. Use the **undo** forms of these commands or follow the command reference to individually restore their default settings. If your restoration attempt still fails, follow the error message instructions to resolve the problem.

Examples

Restore the default settings for Virtual-PPP 10.

```
<Sysname> system-view
[Sysname] interface virtual-ppp 10
[Sysname-Virtual-PPP10] default
```

description

Use **description** to configure the description of an interface.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

The description of an interface is the *interface-name* plus **Interface**. For example, the default description of Virtual-PPP254 is **Virtual-PPP254 Interface**.

Views

Virtual PPP interface view

Predefined user roles

network-admin

context-admin

Parameters

text: Specifies the interface description, a case-sensitive string of 1 to 255 characters.

Examples

Set the description of Virtual-PPP 10 to **virtual-interface**.

```
<Sysname> system-view
[Sysname] interface virtual-ppp 10
[Sysname-Virtual-PPP10] description virtual-interface
```

display interface virtual-ppp

Use **display interface virtual-ppp** to display information about virtual PPP interfaces.

Syntax

display interface [**virtual-ppp** [*interface-number*]] [**brief** [**description** | **down**]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

virtual-ppp [*interface-number*]: Specifies an existing virtual PPP interface by its number in the range of 0 to 255. If you do not specify the **virtual-ppp** keyword, this command displays information about all interfaces. If you specify the **virtual-ppp** keyword but you do not specify an interface, this command displays information about all virtual PPP interfaces.

brief: Displays brief interface information. If you do not specify this keyword, the command displays detailed interface information.

description: Displays complete interface descriptions. If you do not specify this keyword, the command displays only the first 27 characters of each interface description.

down: Displays information about the interfaces in physically down state and the causes. If you do not specify this keyword, the command displays information about interfaces in any state.

Examples

Display detailed information about Virtual-PPP 10.

```
<Sysname> display interface virtual-ppp 10
Virtual-PPP10
Current state: Administratively DOWN
Line protocol state: DOWN
Description: Virtual-PPP10 Interface
Bandwidth: 100000kbps
Maximum transmission unit: 1500
Hold timer: 10 seconds, retry times: 5
Internet address: 10.0.0.1/24 (primary)
Link layer protocol: PPP
```

```
LCP: initial
Physical: L2TP, baudrate: 100000000 bps
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 154 packets, 1880 bytes, 0 drops
Output: 155 packets, 1875 bytes, 0 drops
```

Table 1 Command output

Field	Description
Current state	Physical link state of the interface: • **Administratively DOWN**—The interface has been shut down by using the **shutdown** command. • **DOWN**—The interface is administratively up, but its physical state is down (possibly because no physical link exists or the link has failed). • **UP**—The interface is up both administratively and physically.
Line protocol state	Data link layer state of the interface. The state is determined through automatic parameter negotiation at the data link layer. • **UP**—The data link layer protocol is up. • **UP (spoofing)**—The data link layer protocol is up, but the link is an on-demand link or does not exist. This attribute is typical of null interfaces and loopback interfaces. • **DOWN**—The data link layer protocol is down.
Bandwidth	Expected bandwidth of the interface.
Hold timer	Interval in seconds for the interface to send keepalive packets.
retry times	Maximum number of keepalive retransmission attempts. A link is removed after the maximum number of retransmission attempts is reached.
Internet protocol processing: Disabled	The interface is not assigned an IP address and cannot process IP packets.

Field	Description
Internet address: *ip-address*/*mask-length* (*Type*)	IP address of the interface and type of the address in parentheses. Possible IP address types include: • **Primary**—Manually configured primary IP address. • **Sub**—Manually configured secondary IP address. If the interface has both primary and secondary IP addresses, the primary IP address is displayed. If the interface has only secondary IP addresses, the lowest secondary IP address is displayed. • **DHCP-allocated**—DHCP allocated IP address. For more information, see DHCP client configuration in *Layer 3—IP Services Configuration Guide*. • **BOOTP-allocated**—BOOTP allocated IP address. For more information, see BOOTP client configuration in *Layer 3—IP Services Configuration Guide*. • **PPP-negotiated**—IP address assigned by a PPP server during PPP negotiation. For more information, see PPP configuration in *Layer 2—WAN Access Configuration Guide*. • **Unnumbered**—IP address borrowed from another interface. • **MAD**—IP address assigned to an IRF member device for MAD on the interface. For more information, see IRF configuration in *Virtual Technologies Configuration Guide*.
Link layer protocol	Link layer protocol of the interface: PPP.
Physical	Physical type of the interface: L2TP.
baudrate	Baud rate of the interface.
Last clearing of counters	Time when the **reset counters interface** command was last used to clear the interface statistics. This field displays **Never** if the **reset counters interface** command has never been used on the interface since device startup.
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec	Average rate of inbound traffic in the last 300 seconds.
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec	Average rate of outbound traffic in the last 300 seconds.
Input: 154 packets, 1880 bytes, 0 drops	Total number of inbound packets, total number of inbound bytes, and total number of dropped inbound packets.
Output: 155 packets, 1875 bytes, 0 drops	Total number of outbound packets, total number of outbound bytes, and total number of dropped outbound packets.

Display summary information about virtual PPP interface Virtual-PPP 10.

```
<Sysname> display interface virtual-ppp 10 brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP         Description
VPPP10               ADM  DOWN     10.0.0.1
```

Display information about the virtual PPP interfaces in physically down state and the causes.

```
<Sysname> display interface virtual-ppp brief down
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
```

```
Interface            Link Cause
VPPP9                ADM  Administratively
VPPP10               ADM  Administratively
VPPP12               ADM  Administratively
```

Display summary information about virtual PPP interface Virtual-PPP 10, including the complete interface description.

```
<Sysname> display interface Virtual-PPP 10 brief description
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP         Description
VPPP10               ADM  DOWN     10.0.0.1
```

Table 2 Command output

Field	Description
Brief information on interfaces in route mode	Summary information about Layer 3 interfaces.
Interface	Abbreviated interface name.
Link	Physical link state of the interface: • **UP**—The interface is physically up. • **DOWN**—The interface is physically down. • **ADM**—The interface has been shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command. • **Stby**—The interface is a backup interface in standby state. To see the primary interface, use the **display interface-backup state** command.
Protocol	Data link layer protocol state of the interface: • **UP**—The data link layer protocol of the interface is up. • **DOWN**—The data link layer protocol of the interface is down. • **UP(s)**—The data link layer protocol of the interface is up, but the link is an on-demand link or does not exist. The **(s)** attribute represents the spoofing flag. This value is typical of null interfaces and loopback interfaces.
Primary IP	Primary IP address of the interface. This field displays two hyphens (**--**) if the interface does not have an IP address.
Description	Description of the interface.
Cause	Cause for the physical link state of an interface to be **DOWN**: • **Administratively**—The interface has been manually shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command. • **Not connected**—No physical connection exists (possibly because the network cable is disconnected or faulty).

display l2tp session

Use **display l2tp session** to display information about L2TP sessions.

Syntax

display l2tp session [**statistics**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

`statistics`: Displays statistics for L2TP sessions.

Examples

Display statistics for L2TP sessions.

```
<Sysname> display l2tp session statistics
Total number of sessions: 1
```

Display information about L2TP sessions.

```
<Sysname> display l2tp session
LocalSID      RemoteSID      LocalTID      State
89            36245          10878         Established
```

Table 3 Command output

Field	Description
LocalSID	Local session ID.
RemoteSID	Remote session ID.
LocalTID	Local tunnel ID.
State	Session state: • **Idle**. • **Wait-tunnel**—Waits for the tunnel to be established. • **Wait-reply**—Waits for an Incoming-Call-Reply (ICRP) message indicating the call is accepted. • **Wait-connect**—Waits for an Incoming-Call-Connected (ICCN) message. • **Established**.

display l2tp session temporary

Use **`display l2tp session temporary`** to display information about temporary L2TP sessions.

Syntax

`display l2tp session temporary`

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display information about temporary L2TP sessions.

```
<Sysname> display l2tp session temporary
Total number of temporary sessions: 6
LocalSID    RemoteSID    LocalTID    State
2298        0            19699       Wait-tunnel
42805       0            19699       Wait-tunnel
17777       0            19699       Wait-tunnel
58284       0            19699       Wait-tunnel
33256       0            19699       Wait-tunnel
8228        0            19699       Wait-tunnel
```

Table 4 Command output

Field	Description
LocalSID	Local session ID.
RemoteSID	Remote session ID.
LocalTID	Local tunnel ID.
State	Session state: • **Idle**. • **Wait-tunnel**—Waits for the tunnel to be established. • **Wait-reply**—Waits for an ICRP message indicating the call is accepted. • **Wait-connect**—Waits for an ICCN message.

display l2tp tunnel

Use **`display l2tp tunnel`** to display information about L2TP tunnels.

Syntax

`display l2tp tunnel` [**`statistics`**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

`statistics`: Displays statistics for L2TP tunnels.

Examples

Display statistics for L2TP tunnels.

```
<Sysname> display l2tp tunnel statistics
Total number of tunnels: 1
```

Display information about L2TP tunnels.

```
<Sysname> display l2tp tunnel
LocalTID RemoteTID State         Sessions RemoteAddress    RemotePort RemoteName
10878    21        Established   1        20.1.1.2         1701       lns
```

Table 5 Command output

Field	Description
LocalTID	Local tunnel ID.
RemoteTID	Remote tunnel ID.
State	Tunnel state: • **Idle**. • **Wait-reply**. • **Wait-connect**. • **Established**. • **Stopping**.
Sessions	Number of sessions within the tunnel.
RemoteAddress	IP address of the peer.
RemotePort	UDP port number of the peer.
RemoteName	Name of the tunnel peer.

Related commands

`reset l2tp tunnel`

display l2tp va-pool

Use **`display l2tp va-pool`** to display information about L2TP VA pools.

Syntax

`display l2tp va-pool` [**`dynamic`**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

`dynamic`: Displays information about dynamic L2TP VA pools. If you do not specify this keyword, this command displays information about static L2TP VA pools.

Examples

Display information about static L2TP VA pools.

```
<Sysname> display l2tp va-pool
VT interface          Size      Unused      State
Virtual-Template1     1000      900         Normal
```

Display information about dynamic L2TP VA pools.

```
<Sysname> display l2tp va-pool dynamic
VT interface          Size      Unused      State
Virtual-Template1     128       96          Normal
```

Table 6 Command output

Field	Description
VT interface	VT interface that uses the VA pool.
Size	VA pool capacity set for L2TP users.
Unused	VA pool capacity available for L2TP users.
State	Current state of the VA pool: • **Creating**—The VA pool is being created. • **Destroying**—The VA pool is being removed. • **Normal**—The VA pool has been created.

Related commands

`l2tp virtual-template va-pool`

interface virtual-ppp

Use **`interface virtual-ppp`** to create a virtual PPP interface and enter its view, or enter the view of an existing virtual PPP interface.

Use **`undo interface virtual-ppp`** to delete a virtual PPP interface.

Syntax

`interface virtual-ppp` *`interface-number`*

`undo interface virtual-ppp` *`interface-number`*

Default

No virtual PPP interface exists.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

`interface-number`: Specifies a virtual PPP interface by its number in the range of 0 to 255.

Usage guidelines

A virtual PPP interface is required on the LAC for establishing an LAC-auto-initiated L2TP tunnel.

Examples

Create Virtual-PPP 10 and enter its view.

```
<Sysname> system-view
[Sysname] interface virtual-ppp 10
[Sysname-Virtual-PPP10]
```

ip dscp

Use **ip dscp** to set the DSCP value of L2TP packets.

Use **undo ip dscp** to restore the default.

Syntax

ip dscp *dscp-value*

undo ip dscp

Default

The DSCP value of L2TP packets is 0.

Views

L2TP group view

Predefined user roles

network-admin

context-admin

Parameters

dscp-value: Specifies the DSCP value of L2TP packets, in the range of 0 to 63.

Usage guidelines

The DSCP field is the IP ToS byte. This field marks the priority of IP packets for forwarding. This command sets the DSCP value for the IP packet when L2TP encapsulates a PPP frame into an IP packet.

Examples

Set the DSCP value of L2TP packets to 50.

```
<Sysname> system-view
[Sysname] l2tp-group 1 mode lac
[Sysname-l2tp1] ip dscp 50
```

l2tp enable

Use **l2tp enable** to enable L2TP.

Use **undo l2tp enable** to disable L2TP.

Syntax

l2tp enable

undo l2tp enable

Default

L2TP is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

For L2TP configurations to take effect, you must enable L2TP.

Examples

Enable L2TP.

```
<Sysname> system-view
[Sysname] l2tp enable
```

l2tp icrq-limit

Use **l2tp icrq-limit** to set the maximum number of incoming call request (ICRQ) packets that the LNS can process per second.

Use **undo l2tp icrq-limit** to restore the default.

Syntax

l2tp icrq-limit *number*

undo l2tp icrq-limit

Default

The maximum number of ICRQ packets that the LNS can process per second is not limited.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

number: Specifies the ICRQ packet processing limit in the range of 1 to 1000.

Usage guidelines

To avoid device performance degradation and make sure the LNS can process ICRQ requests correctly, use this command to adjust the ICRQ packet processing rate limit.

Examples

Set the maximum number of ICRQ packets that the LNS can process per second to 200.

```
<Sysname> system-view
[Sysname] l2tp icrq-limit 200
```

l2tp tsa-id

Use **l2tp tsa-id** to set the TSA ID for the L2TP tunnel switching (LTS) device and enable L2TP loop detection on the LTS device.

Use **undo l2tp tsa-id** to restore the default.

Syntax

l2tp tsa-id *tsa-id*

undo l2tp tsa-id

Default

The TSA ID of the LTS device is not set, and L2TP loop detection is disabled on the LTS device.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

tsa-id: Specifies a TSA ID that uniquely identifies the LTS device. This argument is a case-sensitive string of 1 to 64 characters.

Usage guidelines

The LTS device compares the configured TSA ID with each TSA ID Attribute Value Pair (AVP) in a received ICRQ packet for loop detection.

- If a match is found, a loop exists. The LTS immediately tears down the session.
- If no match is found, the LTS performs the following operations:
  a. Encapsulates the configured TSA ID into a new TSA ID AVP.
  b. Appends the new TSA ID AVP to the packet.
  c. Sends the packet to the next hop LTS.

To avoid loop detection errors, make sure the TSA ID of each LTS device is unique.

Examples

Set the TSA ID of the LTS device to **lts0**, and enable L2TP loop detection on the LTS device.

```
<Sysname> system-view
[Sysname] l2tp tsa-id lts0
```

l2tp user-ip-conflict offline

Use **l2tp user-ip-conflict offline** to allow a new L2TP user to come online and log out an old L2TP user when the IP addresses of the two user conflict.

Use **undo l2tp user-ip-conflict** to restore the default.

Syntax

l2tp user-ip-conflict offline

undo l2tp user-ip-conflict

Default

A new L2TP user cannot come online and an old L2TP user keeps online when the IP addresses of the two user conflict.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

When the IP addresses of a new L2TP user and an old L2TP user conflict, you can select to forbid the new user from coming online or log out the old user.

This command takes effect only on IPv4 L2TP users on LNSs.

Examples

Allow a new L2TP user to come online and log out an old L2TP user when the IP addresses of the two user conflict.

```
<Sysname> system-view
[Sysname] l2tp user-ip-conflict offline
```

l2tp virtual-template va-pool

Use **l2tp virtual-template va-pool** to create a static VA pool.

Use **undo l2tp virtual-template va-pool** to delete a static VA pool.

Syntax

l2tp virtual-template *template-number* **va-pool** *va-volume*

undo l2tp virtual-template *template-number* **va-pool**

Default

No static VA pool exists.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

virtual-template *template-number*: Specifies an existing VT interface by its number to use the static VA pool.

va-pool *va-volume*: Specifies the maximum number of VA interfaces contained in the static VA pool, in the range of 1 to 65534.

Usage guidelines

The LNS creates a VA interface for an L2TP session to exchange packets with the LAC, and it deletes the VA interface when the user goes offline. Creating and deleting VA interfaces take time. If a large number of users are coming online or going offline, the performance of L2TP connection establishment and termination will be degraded.

You can configure a VA pool to improve the performance. A VA pool contains a group of VA interfaces. The LNS selects a VA interface from the pool for a requesting user and places the interface back to the VA pool when the user goes offline. This mechanism speeds up the establishment and termination of L2TP connections.

L2TP supports the following types of VA pools:

- **Static VA pool**—VA pool manually created by using the **l2tp virtual-template va-pool** command.
- **Dynamic VA pool**—VA pool automatically created by the device.

When an L2TP user comes online, the device select a VA interface for the user in the following order:

1. VA interfaces in the static VA pool.
2. VA interfaces in the dynamic VA pool.

If no static VA pool is configured for a VT interface or the static VA pool configured for a VT interface is exhausted, the following rules apply when a new L2TP user comes online:

- If no dynamic VA pool is created for the VT interface, the device first creates a dynamic VA pool containing 128 VA interfaces for the VT interface. Then, the device allocates a VA interface in the dynamic VA pool to the user.
- If a dynamic VA pool with more than 64 available VA interfaces exists for the VT interface, the device will allocate a VA interface in the dynamic VA pool to the user.
- If a dynamic VA pool with less than 64 available VA interfaces exists for the VT interface, the device adds 128 VA interfaces to the dynamic VA pool. Then, the device allocates a VA interface in the dynamic VA pool to the user.

The VA pool occupies certain memory resources. When the device memory is large or the user scale is stable, as a best practice, create a static VA pool of a suitable capacity. When the device memory is small or the user scale is uncertain, as a best practice, use a dynamic VA pool. In this case, the device can automatically create a dynamic VA pool with the number of VA interfaces at the step of 128 according to the network user scale.

For a VA pool, follow these restrictions and guidelines:

- Static VA pool
  - A VT interface can be associated with only one static VA pool. To change the capacity of a static VA pool, delete the previous configuration, and reconfigure the static VA pool.
  - Creating or deleting a static VA pool takes time. During the process of creating or deleting a static VA pool, users can come online or go offline, but the static VA pool does not take effect.
  - The system might create a static VA pool that contains VA interfaces less than the specified number because of insufficient resources. In this case, you can use the **display l2tp va-pool** command to view the number of available VA interfaces and current state of the static VA pool.
  - Create a static VA pool with an appropriate capacity, because a static VA pool occupies much system memory.
  - Deleting a static VA pool does not log off the users who are using VA interfaces in the static VA pool.
- Dynamic VA pool
  - A dynamic VA pool is automatically created by the device. It cannot be manually configured, modified, or deleted.
  - The device automatically deletes VA interfaces that are not used for a long period of time from the dynamic VA pool to release the memory resources.

Examples

Create a static VA pool with a capacity of 1000 VA interfaces for Virtual-template 2.

```
<Sysname> system-view
[Sysname] l2tp virtual-template 2 va-pool 1000
```

Related commands

display l2tp va-pool

l2tp-auto-client

Use **l2tp-auto-client** to trigger an LAC to automatically establish an L2TP tunnel.

Use **undo l2tp-auto-client** to delete the automatically established L2TP tunnel.

Syntax

l2tp-auto-client l2tp-group *group-number*

undo l2tp-auto-client

Default

An LAC does not automatically establish an L2TP tunnel.

Views

Virtual PPP interface view

Predefined user roles

network-admin

context-admin

Parameters

l2tp-group *group-number*: Specifies an L2TP group by its number in the range of 1 to 65535. The LAC uses tunnel parameters of the L2TP group to establish the tunnel.

Usage guidelines

For this command to take effect, the L2TP group specified in this command must be an existing one in LAC mode.

An L2TP tunnel automatically established in LAC-auto-initiated mode exists until you delete the tunnel by using the **undo l2tp-auto-client** or **undo l2tp-group** *group-number* command.

Examples

Trigger the LAC to automatically establish an L2TP tunnel by using the tunnel parameters of L2TP group 10.

```
<Sysname> system-view
[Sysname] interface virtual-ppp 1
[Sysname-Virtual-PPP1] l2tp-auto-client l2tp-group 10
```

Related commands

l2tp-group

l2tp-group

Use **l2tp-group** to create an L2TP group and enter its view, or enter the view of an existing L2TP group.

Use **undo l2tp-group** to delete an L2TP group.

Syntax

l2tp-group *group-number* [**mode** { **lac** | **lns** }]

undo l2tp-group *group-number*

Default

No L2TP group exists.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

group-number: Specifies an L2TP group by its number in the range of 1 to 65535.

mode: Specifies a mode for the L2TP group.

lac: Specifies the LAC mode.

lns: Specifies the LNS mode.

Usage guidelines

To create a new L2TP group, you must specify the **mode** keyword. To enter the view of an existing L2TP group, you do not need to specify this keyword.

In L2TP group view, you can configure L2TP tunnel parameters, such as tunnel authentication and flow control.

A device can have L2TP groups in both LAC and LNS modes at the same time.

Examples

Create L2TP group 2 in LAC mode, and enter its view.

```
<Sysname> system-view
[Sysname] l2tp-group 2 mode lac
[Sysname-l2tp2]
```

Related commands

allow l2tp

lns-ip

user

lns-ip

Use **lns-ip** to specify LNS IP addresses or domain names on an LAC.

Use **undo lns-ip** to remove the specified LNS IP addresses or domain names on an LAC.

Syntax

lns-ip { *ip-address* | **host-name** *name* }&<1-5>

undo lns-ip

Default

No LNS IP addresses or domain names are specified on an LAC.

Views

L2TP group view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies LNS IP addresses.

host-name *name*: Specifies LNS host names (domain names). A domain name is a dot (.) separated list of strings, for example, example.com. Each string cannot exceed 63 characters. A domain name cannot exceed 253 characters, including dots (.). A domain name is case-insensitive, and each string can contain letters, digits, hyphens (-), underscores (_), and dots (.).

&<1-5> indicates that you can enter a maximum of five IP addresses or domain names.

Usage guidelines

When the IP address of an LNS is fixed, you can specify the LNS IP address by using the **lns-ip** *ip-address* command. When the IP address of an LNS is not fixed, you can specify the LNS domain name by using the **lns-ip host-name** command. In this case, the LAC will deliver the domain name to the DNS module for processing. Then, the LAC can initiate an L2TP tunneling request to the LNS according to the returned IP address. For more information about DNS, see *Layer 3—IP Services Configuration Guide*.

The LAC initiates an L2TP tunneling request to its specified LNSs consecutively in their configuration order until it receives an acknowledgment from an LNS. The LNS then becomes the tunnel peer.

The **lns-ip** command is available only on L2TP groups in LAC mode.

If you execute this command multiple times for an L2TP group, the most recent configuration takes effect.

Examples

Specify the LNS IP address as 202.1.1.1.

```
<Sysname> system-view
[Sysname] l2tp-group 1 mode lac
[Sysname-l2tp1] lns-ip 202.1.1.1
```

Specify the LNS domain name as example.com.

```
<Sysname> system-view
[Sysname] l2tp-group 1 mode lac
[Sysname-l2tp1] lns-ip host-name example.com
```

mandatory-chap

Use **mandatory-chap** to force the LNS to perform CHAP authentication for users.

Use **undo mandatory-chap** to restore the default.

Syntax

mandatory-chap

undo mandatory-chap

Default

An LNS does not perform CHAP authentication for users.

Views

L2TP group view

Predefined user roles

network-admin

context-admin

Usage guidelines

The LNS uses the LAC as an authentication proxy. The LAC sends the LNS all user authentication information from users and the authentication method configured on the LAC itself. The LNS then checks the user validity according to the received information and the locally configured authentication method.

When mandatory CHAP authentication is configured, a user who depends on an LAC to initiate tunneling requests is authenticated by both the LAC and the LNS for increased security. Some users might not support the authentication on the LNS. In this situation, do not configure this command, because CHAP authentication on the LNS will fail.

This command is available only on L2TP groups in LNS mode.

This command takes effect only on NAS-initiated L2TP tunnels.

The **mandatory-lcp** command takes precedence over this command. If both commands are configured for an L2TP group, the LNS performs LCP renegotiation with the user.

Examples

Force the LNS to perform CHAP authentication for users.

```
<Sysname> system-view
[Sysname] l2tp-group 1 mode lns
[Sysname-l2tp1] mandatory-chap
```

Related commands

mandatory-lcp

mandatory-lcp

Use **mandatory-lcp** to force an LNS to perform LCP negotiation with users.

Use **undo mandatory-lcp** to restore the default.

Syntax

mandatory-lcp

undo mandatory-lcp

Default

An LNS does not perform LCP negotiation with users.

Views

L2TP group view

Predefined user roles

network-admin

context-admin

Usage guidelines

By default, to establish a NAS-initiated tunnel, the user performs LCP negotiation with the LAC. If the negotiation succeeds, the LAC initiates a tunneling request and sends the negotiation results (including authentication information) to the LNS. Then, the LNS determines whether the user is valid based on the information received instead of performing LCP renegotiation with the user.

If you do not expect the LNS to accept LCP negotiation parameters, configure this command to perform an LCP negotiation between the LNS and the user. In this case, the information sent by the LAC will be ignored.

Some users might not support LCP negotiation. In this case, do not configure this command because LCP negotiation will fail.

This command is available only on L2TP groups in LNS mode.

This command takes effect only on NAS-initiated L2TP tunnels.

This command takes precedence over the **mandatory-chap** command. If both commands are configured for an L2TP group, the LNS performs LCP negotiation with the user.

Examples

Force an LNS to perform LCP negotiation with users.

```
<Sysname> system-view
```

```
[Sysname] l2tp-group 1 mode lns
[Sysname-l2tp1] mandatory-lcp
```

Related commands

mandatory-chap

mtu

Use **mtu** to set the MTU size of an interface.

Use **undo mtu** to restore the default.

Syntax

mtu *size*

undo mtu

Default

The MTU size of a virtual PPP interface is 1500 bytes.

Views

Virtual PPP interface view

Predefined user roles

network-admin

context-admin

Parameters

size: Specifies the MTU size in bytes. The value range is 128 to 1500.

Usage guidelines

The MTU size of an interface affects the fragmentation and reassembly of IP packets on the interface.

For the configured MTU size to take effect, you must execute the **shutdown** command and then the **undo shutdown** command on the interface.

Examples

Set the MTU size of Virtual-PPP 10 to 1400 bytes.

```
<Sysname> system-view
[Sysname] interface virtual-ppp 10
[Sysname-Virtual-PPP10] mtu 1400
```

reset counters interface virtual-ppp

Use **reset counters interface virtual-ppp** to clear the statistics for virtual PPP interfaces.

Syntax

reset counters interface [**virtual-ppp** [*interface-number*]]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

virtual-ppp [*interface-number*]: Specifies a virtual PPP interface by its number in the range of 0 to 255. If you specify neither **virtual-ppp** nor *interface-number*, this command clears the statistics for all interfaces. If you specify **virtual-ppp** but not *interface-number*, this command clears the statistics for all virtual PPP interfaces. If you specify both **virtual-ppp** and *interface-number*, this command clears the statistics for the specified virtual PPP interface.

Usage guidelines

Use this command to clear history statistics if you want to collect traffic statistics for a specific time period.

Examples

Clear the statistics for Virtual-PPP 10.

```
<Sysname> reset counters interface virtual-ppp 10
```

reset l2tp tunnel

Use **reset l2tp tunnel** to disconnect tunnels and all sessions within the tunnels.

Syntax

reset l2tp tunnel { **id** *tunnel-id* | **name** *remote-name* }

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

id *tunnel-id*: Specifies a tunnel by its local ID in the range of 1 to 65535.

name *remote-name*: Specifies L2TP tunnels by the tunnel peer name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

When the number of user connections is 0 or a network fault occurs, you can disconnect the L2TP tunnel by using this command on either the LAC or LNS. After the tunnel is disconnected, all sessions within it are disconnected.

If you specify a tunnel peer name, all tunnels with the tunnel peer name will be disconnected. If no tunnel with the tunnel peer name exists, nothing happens.

A tunnel disconnected by force can be re-established when a client makes a call.

Examples

Disconnect all tunnels with the tunnel peer name of **aaa**.

```
<Sysname> reset l2tp tunnel name aaa
```

Related commands

display l2tp tunnel

shutdown

Use **shutdown** to shut down a virtual PPP interface.

Use **undo shutdown** to bring up a virtual PPP interface.

Syntax

shutdown

undo shutdown

Default

A virtual PPP interface is up.

Views

Virtual PPP interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

Executing this command to shut down an interface will make L2TP based on this interface become unavailable. As a best practice, make sure you fully understand the impact before executing this command.

Examples

Shut down Virtual-PPP 10.

```
<Sysname> system-view
[Sysname] interface virtual-ppp 10
[Sysname-Virtual-PPP10] shutdown
```

source-ip

Use **source-ip** to configure the source IP address of L2TP tunnel packets.

Use **undo source-ip** to restore the default.

Syntax

source-ip *ip-address*

undo source-ip

Default

The source IP address of L2TP tunnel packets is the IP address of the egress interface.

Views

L2TP group view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the source IP address of L2TP tunnel packets.

Usage guidelines

This command is available only on an L2TP group in LAC mode.

For high availability, as a best practice, use the IP address of a loopback interface as the source IP address of L2TP tunnel packets.

Examples

Configure the source IP address of L2TP tunnel packets as **2.2.2.2**.

```
<Sysname> system-view
[Sysname] l2tp-group 1 mode lac
[Sysname-l2tp1] source-ip 2.2.2.2
```

timer-hold

Use **timer-hold** to set the keepalive interval.

Use **undo timer-hold** to restore the default.

Syntax

timer-hold *seconds*

undo timer-hold

Default

The keepalive interval is 10 seconds.

Views

Virtual PPP interface view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies the interval at which the LAC or the LNS sends keepalive packets, in the range of 0 to 32767 seconds.

Usage guidelines

A virtual PPP interface sends keepalive packets at keepalive intervals to detect the availability of the peer. If the interface fails to receive keepalive packets when the keepalive retry limit is reached, it determines that the link fails and reports a link layer down event.

To set the keepalive retry limit, use the **timer-hold retry** command.

On a slow link, increase the keepalive interval to prevent false shutdown of the interface. This situation might occur when keepalive packets are delayed because a large packet is being transmitted on the link.

Examples

Set the keepalive interval to 20 seconds for Virtual-PPP 10.

```
<Sysname> system-view
[Sysname] interface virtual-ppp 10
[Sysname-Virtual-PPP10] timer-hold 20
```

Related commands

timer-hold retry

timer-hold retry

Use **timer-hold retry** to set the keepalive retry limit.

Use **undo timer-hold retry** to restore the default.

Syntax

timer-hold retry *retries*

undo timer-hold retry

Default

The keepalive retry limit is 5.

Views

Virtual PPP interface view

Predefined user roles

network-admin

context-admin

Parameters

retries: Specifies the maximum number of keepalive attempts in the range of 1 to 255.

Usage guidelines

A virtual PPP interface sends keepalive packets at keepalive intervals to detect the availability of the peer. If the interface fails to receive keepalive packets when the keepalive retry limit is reached, it determines that the link fails and reports a link layer down event.

To set the keepalive interval, use the **timer-hold** command.

On a slow link, increase the keepalive retry limit to prevent false shutdown of the interface. This situation might occur when keepalive packets are delayed because a large packet is being transmitted on the link.

Examples

Set the keepalive retry limit to 10 for Virtual-PPP 10.

```
<Sysname> system-view
[Sysname] interface virtual-ppp 10
[Sysname-Virtual-PPP10] timer-hold retry 10
```

Related commands

timer-hold

tunnel authentication

Use **tunnel authentication** to enable L2TP tunnel authentication.

Use **undo tunnel authentication** to disable L2TP tunnel authentication.

Syntax

tunnel authentication

undo tunnel authentication

Default

L2TP tunnel authentication is enabled.

Views

L2TP group view

Predefined user roles

network-admin

context-admin

Usage guidelines

Tunnel authentication prevents the local end from establishing L2TP tunnels with illegal remote ends.

You can enable tunnel authentication on both sides or either side.

To ensure a successful tunnel establishment when tunnel authentication is enabled on both sides or either side, set the same non-null key on the LAC and the LNS. To set the tunnel authentication key, use the **tunnel password** command.

When neither side is enabled with tunnel authentication, the key settings of the LAC and the LNS do not affect the tunnel establishment.

For tunnel security, enable tunnel authentication.

Examples

Enable L2TP tunnel authentication.

```
<Sysname> system-view
[Sysname] l2tp-group 1 mode lns
[Sysname-l2tp1] tunnel authentication
```

Related commands

tunnel password

tunnel avp-hidden

Use **tunnel avp-hidden** to enable transferring AVP data in hidden mode.

Use **undo tunnel avp-hidden** to restore the default.

Syntax

tunnel avp-hidden

undo tunnel avp-hidden

Default

AVP data is transferred over the tunnel in plaintext mode.

Views

L2TP group view

Predefined user roles

network-admin

context-admin

Usage guidelines

L2TP uses AVPs to transmit tunnel negotiation parameters, session negotiation parameters, and user authentication information. This feature can hide sensitive AVP data, such as user passwords. This feature encrypts AVP data with the key configured by using the **tunnel password** command before transmission.

The **tunnel avp-hidden** command can be configured for L2TP groups in both LAC and LNS modes. However, it does not take effect on L2TP groups in LNS mode.

For this command to take effect, you must enable tunnel authentication by using the **tunnel authentication** command.

Examples

Enable transferring AVP data in hidden mode.

```
<Sysname> system-view
[Sysname] l2tp-group 1 mode lac
[Sysname-l2tp1] tunnel avp-hidden
```

Related commands

tunnel authentication

tunnel password

tunnel flow-control

Use **tunnel flow-control** to enable L2TP session flow control.

Use **undo tunnel flow-control** to disable L2TP session flow control.

Syntax

tunnel flow-control

undo tunnel flow-control

Default

L2TP session flow control is disabled.

Views

L2TP group view

Predefined user roles

network-admin

context-admin

Usage guidelines

This feature adds sequence numbers to transmitted packets and uses them to reorder packets arriving out of order and to detect lost packets.

This feature takes effect on both sent and received L2TP data messages. The L2TP sessions support this feature if either the LAC or LNS is enabled with this feature.

When the device acts as an LAC, a change in the flow control status on the LNS causes the same change in the flow control status of L2TP sessions. When the device acts as an LNS, a change in the flow control status on the LAC does not affect the flow control status of L2TP sessions.

Examples

Enable L2TP session flow control.

```
<Sysname> system-view
[Sysname] l2tp-group 1 mode lac
[Sysname-l2tp1] tunnel flow-control
```

tunnel name

Use **tunnel name** to specify the local tunnel name.

Use **undo tunnel name** to restore the default.

Syntax

tunnel name *name*

undo tunnel name

Default

The local tunnel name is the device name. For more information about the device name, see *Fundamentals Configuration Guide*.

Views

L2TP group view

Predefined user roles

network-admin

context-admin

Parameters

name: Specifies the local tunnel name, a case-sensitive string of 1 to 31 characters.

Examples

Specify the local tunnel name as **itsme**.

```
<Sysname> system-view
[Sysname] l2tp-group 1 mode lns
[Sysname-l2tp1] tunnel name itsme
```

Related commands

sysname (*Fundamentals Command Reference*)

tunnel password

Use **tunnel password** to configure the key for tunnel authentication.

Use **undo tunnel password** to restore the default.

Syntax

tunnel password { **cipher** | **simple** } *string*

undo tunnel password

Default

No key is configured for tunnel authentication.

Views

L2TP group view

Predefined user roles

network-admin

context-admin

Parameters

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 16 characters. Its encrypted form is a case-sensitive string of 1 to 53 characters.

Usage guidelines

For this command to take effect, you must enable tunnel authentication by using the **tunnel authentication** command.

For the tunnel authentication key change to take effect, change the tunnel authentication key before tunnel negotiation is performed.

Examples

Configure the key for tunnel authentication to a plaintext key **yougotit**.

```
<Sysname> system-view
[Sysname] l2tp-group 1 mode lac
[Sysname-l2tp1] tunnel password simple yougotit
```

Related commands

tunnel authentication

tunnel timer hello

Use **tunnel timer hello** to set the Hello interval.

Use **undo tunnel timer hello** to restore the default.

Syntax

tunnel timer hello *hello-interval*

undo tunnel timer hello

Default

The Hello interval is 60 seconds.

Views

L2TP group view

Predefined user roles

network-admin

context-admin

Parameters

hello-interval: Specifies the interval at which the LAC or the LNS sends Hello packets, in the range of 60 to 1000 seconds.

Usage guidelines

The device sends Hello packets at the set interval. This prevents the L2TP tunnels and sessions from being removed due to timeouts.

You can set different Hello intervals for the LNS and LAC.

Examples

Set the Hello interval to 90 seconds.

```
<Sysname> system-view
[Sysname] l2tp-group 1 mode lac
[Sysname-l2tp1] tunnel timer hello 90
```

tunnel window receive

Use **tunnel window receive** to set the receiving window size for an L2TP tunnel.

Use **undo tunnel window receive** to restore the default.

Syntax

tunnel window receive *size*

undo tunnel window receive

Default

The receiving window size for an L2TP tunnel is 1024.

Views

L2TP group view

Predefined user roles

network-admin

context-admin

Parameters

size: Specifies the receiving window size in the range of 1 to 5000. It is the number of packets that can be buffered at the local end.

Usage guidelines

To enable the device to process a larger number of disordered packets, use this command to enlarge the receiving window size for an L2TP tunnel.

The device uses a receiving window to reorder disordered packets based on packet sequence numbers.

If the sequence number of a packet is within the receiving window but does not equal the minimum value of the window, the device performs the following operations:

3. The device buffers the packet.
4. The minimum value and maximum value of the receiving window increment by one.
5. The device continues to check the next arriving packet.

If the sequence number of a packet equals the minimum value of the receiving window, the device performs the following operations:

1. The device processes the packet.
2. The minimum value and maximum value of the receiving window increment by one.
3. The device checks buffered packets for a packet with the sequence number equal to the new minimum value of the receiving window.
4. If no required packet is found, the device checks the next arriving packet.

If the sequence number of a packet is not within the receiving window, the device drops the packet.

In the L2TP tunnel establishment process, the device uses the value specified in L2TP group view as the receiving window size.

Changing the receiving window size after an L2TP tunnel is established does not affect the established L2TP tunnel.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the receiving window size for L2TP group 1 to 128.

```
<Sysname> system-view
[Sysname] l2tp-group 1 mode lac
[Sysname-l2tp1] tunnel window receive 128
```

Related commands

tunnel window send

tunnel window send

Use **tunnel window send** to set the sending window size for an L2TP tunnel.

Use **undo tunnel window send** to restore the default.

Syntax

tunnel window send *size*

undo tunnel window send

Default

The sending window size for an L2TP tunnel is 0, which means using the value of the receiving window size carried in messages sent by the peer end in the tunnel establishment process.

Views

L2TP group view

Predefined user roles

network-admin

context-admin

Parameters

size: Specifies the sending window size for an L2TP tunnel, in the range of 0 to 1024. It is the maximum number of packets the device can send to a peer end when the device receives no response from the peer end. If the messages from the peer end carry no receiving window size in the tunnel establishment process, the sending window size for the device is 4.

Usage guidelines

The packet processing capability of a peer end might mismatch the receiving window size of the peer end in some networks. For example, the actual packet processing capability of the peer end is 10, but the receiving window size of the peer end is 20. To ensure stable L2TP services, you can adjust the sending window size for the device to match the actual packet processing capability of the peer end.

The sending window size set in L2TP group view is obtained in the L2TP tunnel establishment process.

- If the sending window size is 0, the device uses the default sending window size.
- If the sending window size is not 0, the device uses the specified value as the sending window size.

Changing the sending window size after an L2TP tunnel is established does not affect the established L2TP tunnel.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the sending window size for L2TP group 1 to 128.

```
<Sysname> system-view
[Sysname] l2tp-group 1 mode lac
[Sysname-l2tp1] tunnel window send 128
```

Related commands

tunnel window receive

user

Use **user** to configure the condition for the LAC to initiate tunneling requests.

Use **undo user** to restore the default.

Syntax

user { **domain** *domain-name* | **fullusername** *user-name* }

undo user

Default

No condition is configured for the LAC to initiate tunneling requests.

Views

L2TP group view

Predefined user roles

network-admin

context-admin

Parameters

domain *domain-name*: Configures the LAC to initiate tunneling requests to the LNS when the domain name of a user matches a configured domain name. The *domain-name* argument represents the domain name of the user and is a case-insensitive string of 1 to 24 characters.

fullusername *user-name*: Configures the LAC to initiate tunneling requests to the LNS when the username of a user matches a configured full username. The *domain-name* argument represents the username of the user and is a case-sensitive string of 1 to 255 characters.

Usage guidelines

The LAC initiates tunneling requests to the LNS only when the domain name or the username of a user matches a configured domain name or a configured full username.

This command is available only on L2TP groups in LAC mode.

If you execute this command multiple times for an L2TP group, the most recent configuration takes effect.

Examples

Configure the LAC to initiate tunneling requests to the LNS when the username of the user is **test@dm1**.

```
<Sysname> system-view
[Sysname] l2tp-group 1 mode lac
[Sysname-l2tp1] user fullusername test@dm1
```

vpn-instance

Use **vpn-instance** to assign a tunnel peer to a VPN.

Use **undo vpn-instance** to restore the default.

Syntax

vpn-instance *vpn-instance-name*

undo vpn-instance

Default

A tunnel peer belongs to the public network.

Views

L2TP group view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance-name: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

This command enables the device to transmit L2TP control messages and data messages in the specified VPN by searching the routing table in that VPN.

When one L2TP endpoint is in a VPN, assign the peer endpoint to the VPN for correct packet forwarding between the two endpoints.

The tunnel peer and the physical port connecting to the tunnel peer should belong to the same VPN. The VPN to which this physical port belongs is configured by using the **ip binding vpn-instance** command.

The specified VPN must already exist.

Examples

Assign the tunnel peer to VPN **vpn1**.

```
<Sysname>system-view
[Sysname] l2tp-group 1 mode lac
[Sysname-l2tp1] vpn-instance vpn1
```

Related commands

ip vpn-instance (*VPN Instance Command Reference*)

ip binding vpn-instance (*VPN Instance Command Reference*)

NSFOCUS Firewall Series

NF Internet Access Behavior Management

Command Reference

NSFOCUS Technologies, Inc.

Document version: 6W600-20230221

Preface

This command reference describes the commands for configuring Internet access behavior management features, including:bandwidth management, application audit and management and NetShare control.

This preface includes the following topics about the documentation:

- Audience.
- Conventions.

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators.

Conventions

The following information describes the conventions used in the documentation.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select a minimum of one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
CAUTION:	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Contents

Bandwidth management commands

action

Use **action** to specify an action for a traffic rule.

Use **undo action** to restore the default.

Syntax

action { **deny** | **none** | **qos profile** *profile-name* }

undo action

Default

The action for a traffic rule is **none**.

Views

Traffic rule view

Predefined user roles

network-admin

context-admin

Parameters

deny: Drops matching packets.

none: Allows matching packets to pass through without bandwidth management.

qos profile *profile-name*: Specifies a traffic profile by its name to limit the rate of matching packets. The profile name is a case-insensitive string of 1 to 63 characters.

Usage guidelines

If a packet matches a traffic rule, the device performs the action specified in the traffic rule on the packet.

Examples

Create a traffic rule named **rule1**, and apply traffic profile **profile1** to the traffic rule.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name rule1
[Sysname-traffic-policy-rule-rule1] action qos profile profile1
```

Related commands

profile name

rule name

all-traffic-control enable

Use **all-traffic-control enable** to enable bandwidth management for traffic flows of the IP layer and upper layers.

Use **undo all-traffic-control enable** to restore the default.

Syntax

all-traffic-control enable

undo all-traffic-control enable

Default

Bandwidth management is performed only for traffic flows of Layer 4 and upper layers.

Views

Traffic policy view

Predefined user roles

network-admin

context-admin

Usage guidelines

Use this command when there is a large number of IP traffic flows in the network.

Examples

Enable bandwidth management for traffic flows of the IP layer and upper layers.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] all-traffic-control enable
```

application

Use **application** to configure application or application group as a match criterion.

Use **undo application** to delete an application or application group match criterion.

Syntax

application { **app** *application-name* | **app-group** *application-group-name* }

undo application { **app** *application-name* | **app-group** *application-group-name* }

Default

No application or application group is used as a match criterion.

Views

Traffic rule view

Predefined user roles

network-admin

context-admin

Parameters

app *application-name*: Specifies an application by its name, a case-insensitive string of 1 to 63 characters.

app-group *application-group-name*: Specifies an application group by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

You can configure multiple applications or application groups for a traffic rule to match packets.

This command enables the device to manage bandwidth by application type, such as email, P2P, IM, and web browsing.

If you specify a user-defined application that uses DCCP, SCTP, or UDP-Lite as the transport layer protocol, the application is not limited by bandwidth management. For information about user-defined applications, see *Security Configuration Guide*.

Examples

Configure **P2P_General_TCP_Communications** as a match criterion for traffic rule **rule1**.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name rule1
[Sysname-traffic-policy-rule-rule1] application app P2P_General_TCP_Communications
```

Related commands

app-group (*Security Command Reference*)

nbar application (*Security Command Reference*)

port-mapping (*Security Command Reference*)

bandwidth

Use **bandwidth** to set the total guaranteed bandwidth or maximum bandwidth in a traffic profile.

Use **undo bandwidth** to delete the total guaranteed bandwidth or maximum bandwidth setting of a traffic profile.

Syntax

bandwidth { **downstream** | **total** | **upstream** } { **guaranteed** | **maximum** } *bandwidth-value*

undo bandwidth { **downstream** | **total** | **upstream** } { **guaranteed** | **maximum** }

Default

The total guaranteed bandwidth and maximum bandwidth are not set in a traffic profile.

Views

Traffic profile view

Predefined user roles

network-admin

context-admin

Parameters

downstream: Specifies downstream traffic (traffic from a server to a client).

total: Specifies both downstream traffic and upstream traffic.

upstream: Specifies upstream traffic (traffic from a client to a server).

guaranteed: Specifies the guaranteed bandwidth.

maximum: Specifies the maximum bandwidth. The maximum bandwidth must be greater than or equal to the guaranteed bandwidth.

bandwidth-value: Specifies the bandwidth value in the range of 8 to 100000000 kbps.

Usage guidelines

When you specify traffic profiles for parent and child traffic rules, following these restrictions and guidelines:

- The maximum bandwidth for the child traffic rule must be smaller than or equal to that for the parent traffic rule.
- The guaranteed bandwidth for a child traffic rule must be smaller than or equal to that for the parent traffic rule.
- The traffic profiles cannot be the same for the child and parent traffic rules.

An interface with small default expected bandwidth might experience traffic loss if the following conditions exist:

- There is a large amount of traffic on the interface.
- The interface uses the default expected bandwidth.

To avoid traffic loss, implicitly set the expected bandwidth to a large value for such an interface. For example, you can set the expected bandwidth of a tunnel interface to a value greater than 64 kbps (the default) if there is a large amount of traffic on the interface.

Examples

In traffic profile **profile1**, set both upstream and downstream maximum bandwidth to 10000 kbps, and set both upstream and downstream guaranteed bandwidth to 5000 kbps.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] profile name profile1
[Sysname-traffic-policy-profile-profile1] bandwidth upstream maximum 10000
[Sysname-traffic-policy-profile-profile1] bandwidth downstream maximum 10000
[Sysname-traffic-policy-profile-profile1] bandwidth upstream guaranteed 5000
[Sysname-traffic-policy-profile-profile1] bandwidth downstream guaranteed 5000
```

bandwidth average enable

Use **bandwidth average enable** to enable dynamic and even allocation for maximum bandwidth.

Use **undo bandwidth average enable** to disable dynamic and even allocation for maximum bandwidth.

Syntax

bandwidth average enable

undo bandwidth average enable

Default

Dynamic and even allocation for maximum bandwidth is disabled.

Views

Traffic profile view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command allows the device to dynamically and evenly allocate the total maximum bandwidth among all online IP addresses.

This command can be enabled only after you set the total maximum bandwidth.

Examples

Enable dynamic and even allocation for maximum bandwidth in traffic profile **profile1**.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] profile name profile1
[Sysname-traffic-policy-profile-profile1] bandwidth total maximum 10000
[Sysname-traffic-policy-profile-profile1] bandwidth average enable
```

Related commands

bandwidth { **downstream** | **total** | **upstream** } **maximum**

bandwidth { per-ip | per-user }

Use **bandwidth** { **per-ip** | **per-user** } to set the per-IP or per-user maximum or guaranteed bandwidth for a traffic profile.

Use **undo bandwidth** { **per-ip** | **per-user** } to delete the per-IP or per-user maximum or guaranteed bandwidth setting of a traffic profile.

Syntax

bandwidth { **downstream** | **total** | **upstream** } { **guaranteed** | **maximum** } { **per-ip** | **per-user** } *bandwidth-value*

undo bandwidth { **downstream** | **total** | **upstream** } { **guaranteed** | **maximum** } { **per-ip** | **per-user** }

Default

The per-IP or per-user maximum bandwidth and guaranteed bandwidth are not set in a traffic profile.

Views

Traffic profile view

Predefined user roles

network-admin

context-admin

Parameters

downstream: Specifies downstream traffic (traffic from a server to a client).

total: Specifies both downstream traffic and upstream traffic.

upstream: Specifies upstream traffic (traffic from a client to a server).

guaranteed: Sets the guaranteed bandwidth.

maximum: Sets the maximum bandwidth.

per-ip: Sets the per-IP bandwidth.

per-user: Sets the per-user bandwidth.

bandwidth-value: Specifies the bandwidth value in the range of 8 to 100000000 kbps.

Usage guidelines

This command allows you to manage bandwidth at finer granularity.

The per-IP or per-user maximum bandwidth cannot be greater than the total maximum bandwidth.

The per-IP or per-user guaranteed bandwidth cannot be greater than the total guaranteed bandwidth.

The per-IP or per-user guaranteed bandwidth cannot be greater than the per-IP or per-user maximum bandwidth.

Examples

In traffic profile **profile1**, set both upstream and downstream per-IP maximum bandwidth to 10000 kbps.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] profile name profile1
[Sysname-traffic-policy-profile-profile1] bandwidth upstream maximum per-ip 10000
[Sysname-traffic-policy-profile-profile1] bandwidth downstream maximum per-ip 10000
```

per-ip total traffic-quota per-ip monthly

Use **per-ip total traffic-quota per-ip monthly** to set the per-IP monthly traffic quota.

Use **undo total traffic-quota per-ip monthly** to restore the default.

Syntax

bandwidth total traffic-quota per-ip monthly *quota-value*

undo bandwidth total traffic-quota per-ip monthly

Default

The amount of traffic used by an IP address per month is not limited.

Views

Traffic profile view

Predefined user roles

network-admin

context-admin

Parameters

quota-value: Specifies the per-IP monthly traffic quota in the range of 1 to 1000000000 KB.

Usage guidelines

This command limits the total amount traffic (uplink and downlink) used by an IP address per month. When the traffic used by an IP address reaches the traffic quota, the device drops packets from the IP address.

Examples

In traffic profile **prof1**, set the per-IP monthly traffic quota to 5000 KB.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] profile name prof1
[Sysname-traffic-policy-profile-prof1] bandwidth total traffic-quota per-ip monthly 5000
```

connection-limit count

Use **connection-limit count** to set the connection count limit for a traffic profile.

Use **undo connection-limit count** to delete the connection count limit setting of a traffic profile.

Syntax

connection-limit count { **per-rule** | **per-ip** | **per-user** } *connection-number*

undo connection-limit count { **per-rule** | **per-ip** | **per-user** }

Default

No connection count limit is set for a traffic profile.

Views

Traffic profile view

Predefined user roles

network-admin

context-admin

Parameters

per-rule: Specifies the total connection count limit (count limit for the traffic rule associated with the traffic profile).

per-ip: Specifies the per-IP connection count limit.

per-user: Specifies the per-user connection count limit.

connection-number: Specifies the maximum number of connections allowed, in the range of 1 to 12000000.

Usage guidelines

The per-IP or per-user connection count limit cannot be greater than the total connection count limit.

You cannot set both per-IP and per-user connection count limits for one traffic profile.

Examples

In traffic profile **profile1**, set the total connection count limit to 1000.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] profile name profile1
[Sysname-traffic-policy-profile-profile1] connection-limit count per-rule 1000
```

In traffic profile **profile1**, set the per-IP connection count limit to 500.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] profile name profile1
[Sysname-traffic-policy-profile-profile1] connection-limit count per-ip 500
```

connection-limit rate

Use **connection-limit rate** to set the connection rate limit for a traffic profile.

Use **undo connection-limit rate** to delete the connection rate limit setting of a traffic profile.

Syntax

connection-limit rate { **per-rule** | **per-ip** | **per-user** } *connection-rate*

undo connection-limit rate { **per-rule** | **per-ip** | **per-user** }

Default

No connection rate limit is set for a traffic profile.

Views

Traffic profile view

Predefined user roles

network-admin

context-admin

Parameters

per-rule: Specifies the total connection rate limit (rate limit for the traffic rule associated with the traffic profile).

per-ip: Specifies the per-IP connection rate limit.

per-user: Specifies the per-user connection rate limit.

connection- rate: Specifies the maximum connection rate in the range of 1 to 12000000 connections per second.

Usage guidelines

The per-IP or per-user connection rate limit cannot be greater than the total connection rate limit.

You cannot set both per-IP and per-user connection rate limits for one traffic profile.

Examples

In traffic profile **profile1**, set the total connection rate limit to 1000 connections per second.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] profile name profile1
[Sysname-traffic-policy-profile-profile1] connection-limit rate per-rule 1000
```

In traffic profile **profile1**, set the per-IP connection rate limit to 500 connections per second.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] profile name profile1
[Sysname-traffic-policy-profile-profile1] connection-limit rate per-user 500
```

destination-address

Use **destination-address** to configure a destination IP address object group as a match criterion.

Use **undo destination-address** to remove a destination IP address object group as a match criterion.

Syntax

destination-address address-set *object-group-name*

undo destination-address address-set *object-group-name*

Default

No destination IP address object group is used as a match criterion.

Views

Traffic rule view

Predefined user roles

network-admin

context-admin

Parameters

object-group-name: Specifies an IPv4 or IPv6 address object group by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

This command is used to match the packets with the destination IP addresses in the specified address object group. You can specify multiple address object groups for a traffic rule to match destination IP addresses of packets.

Before rolling back configuration by using the **configuration replace file** *filename* command, check the address object group configuration in the traffic rule in the configuration file. The address object group configuration fails to be rolled back if two address object groups have the same name but are of different types (IPv4/IPv6).

Examples

Configure IPv4 address object group **obgroup2** for traffic rule **rule1** to match destination IPv4 addresses of packets.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name rule1
[Sysname-traffic-policy-rule-rule1] destination-address address-set obgroup2
```

Related commands

object-group (*Security Command Reference*)

destination-zone

Use **destination-zone** to configure a destination security zone as a match criterion.

Use **undo destination-zone** to delete a destination security zone match criterion.

Syntax

destination-zone *destination-zone-name*

undo destination-zone *destination-zone-name*

Default

No destination security zone is used as a match criterion.

Views

Traffic rule view

Predefined user roles

network-admin

context-admin

Parameters

destination-zone-name: Specifies a destination zone by its name, a case-insensitive string of 1 to 31 characters.

Examples

Configure destination security zone **zone2** as a match criterion for traffic rule **rule1**.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name rule1
[Sysname-traffic-policy-rule-rule1] destination-zone zone2
```

Related commands

security-zone name (*Security Command Reference*)

disable

Use **disable** to disable a traffic rule.

Use **undo disable** to enable a traffic rule.

Syntax

disable

undo disable

Default

A traffic rule is enabled.

Views

Traffic rule view

Predefined user roles

network-admin

context-admin

Usage guidelines

If a traffic rule is not used, use this command to disable it. A disabled traffic rule does not participate in traffic matching. You can copy, rename, and move a disabled traffic rule.

Examples

Disable traffic rule **rule1**.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name rule1
[Sysname-traffic-policy-rule-rule1] disable
```

display traffic-policy statistics bandwidth

Use **display traffic-policy statistics bandwidth** to display traffic statistics for traffic rules.

Syntax

display traffic-policy statistics bandwidth { **downstream** | **total** | **upstream** } { **per-ip** { **ipv4** [*ipv4-address*] | **ipv6** [*ipv6-address*] } **rule** *rule-name* | **per-rule** [**name** *rule-name*] | **per-user** [**user** *user-name*] **rule** *rule-name* } [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

downstream: Displays downstream traffic statistics.

total: Displays the sum of downstream traffic statistics and upstream traffic statistics.

upstream: Displays upstream traffic statistics.

per-ip: Displays per-IP traffic statistics.

ipv4: Displays per-IP traffic statistics for IPv4 addresses.

ipv4-address: Specifies an IPv4 address. If you do not specify an IPv4 address, this command displays per-IP traffic statistics for all IPv4 addresses of the specified traffic rule.

ipv6: Displays per-IP traffic statistics for IPv6 addresses. Non-default vSystems do not support this parameter.

ipv6-address: Specifies an IPv6 address. If you do not specify an IPv6 address, this command displays per-IP traffic statistics for all IPv6 addresses of the specified traffic rule.

rule *rule-name*: Specifies a traffic rule by its name, a case-insensitive string of 1 to 63 characters.

per-rule: Displays per-rule traffic statistics.

name *rule-name*: Specifies a traffic rule by its name, a case-insensitive string of 1 to 63 characters. If you do not specify a traffic rule, this command displays per-rule traffic statistics for all traffic rules.

per-user: Displays per-user traffic statistics.

user *user-name*: Specifies a user by its name, a case-insensitive string of 1 to 55 characters. If you do not specify a user, this command displays per-user traffic statistics for all users of the specified traffic rule.

rule *rule-name*: Specifies a traffic rule by its name, a case-insensitive string of 1 to 63 characters.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays traffic statistics for all member devices.

Usage guidelines

You can identify whether a traffic rule works as configured by displaying the traffic statistics for the traffic rule.

Examples

Display per-rule upstream traffic statistics for traffic rule **traffic-rule**.

```
<Sysname> display traffic-policy statistics bandwidth upstream per-rule name traffic-rule
Slot 1:
Codes: PP(Passed Packets), PB(Passed Bytes), DP(Dropped Packets), DB(Dropped Bytes),
PR(Passed Rate:kbps), DR(Drop Rate:kbps), FPP(Final Passed Packets), FPB(Final Passed
Bytes), FPR(Final Passed Rate:kbps)
-------------------------------------------------------------------------------
---
Rule name     State    Profile name    PP   PB     DP   DB    PR   DR    FPP  FPB    FPR
```

```
-------------------------------------------------------------------------------
---
traffic-rule  Enabled  profile1        726   7550   4    2961  703  497   595  6632   664.1
-------------------------------------------------------------------------------
---

-------------------------------------------------------------------------------
```

Display per-IP upstream traffic statistics for all IPv4 addresses in traffic rule **traffic-rule**.

```
<Sysname> display traffic-policy statistics bandwidth upstream per-ip ipv4 rule
traffic-rule
Slot 1:
Codes: PP(Passed Packets), PB(Passed Bytes), DP(Dropped Packets), DB(Dropped Bytes),
PR(Passed Rate:kbps), DR(Drop Rate:kbps), FPP(Final Passed Packets), FPB(Final Passed
Bytes), FPR(Final Passed Rate:kbps)
-------------------------------------------------------------------------------
---
Rule name      State    IP       PP    PB       DP   DB    PR     DR   FPP      FPB      FPR
-------------------------------------------------------------------------------
---
traffic-rule   Enabled  1.1.1.1  726   75502    4    2961  703.3  497  595      6632     664.1
-------------------------------------------------------------------------------
---
traffic-rule2  Enabled  1.1.1.5  756   74502    4    2901  712    488  595      6632     664.1
-------------------------------------------------------------------------------
---
traffic-rule3  Enabled  1.1.1.8  756   74502    4    2951  712    488  595      6632     664.1
-------------------------------------------------------------------------------
---
-------------------------------------------------------------------------------
---
```

Table 1 Command output

Field	Description
Codes	Acronyms for fields: • **PP(Passed Packets)**—Number of packets permitted by the traffic rule. • **PB(Passed Bytes)**—Number of bytes permitted by the traffic rule. • **DP(Dropped Packets)**—Number of packets dropped by the traffic rule. • **DB(Dropped Bytes)**—Number of bytes dropped by the traffic rule. • **PR(Passed Rate:kbps)**—Rate of packets permitted by the traffic rule, in kbps. • **DR(Drop Rate:kbps)**—Rate of packets dropped by the traffic rule, in kbps. • **FPP(Final Passed Packets)**—Number of packets permitted by both the traffic rule and interface bandwidth. • **FPB(Final Passed Bytes)**—Number of bytes permitted by both the traffic rule and interface bandwidth. • **FPR(Final Passed Rate:kbps)**—Rate of packets permitted by both the traffic rule and interface bandwidth, in kbps. In the case of rule nesting, the actual values of the **FPP**, **FPB**, and

Field	Description
	FPR fields are displayed only if you specify the lowest-level traffic rule in the **display traffic-policy statistics bandwidth** command. If you specify a non-lowest-level traffic rule, the value 0 is displayed for these fields.

display traffic-policy statistics connection-limit

Use **display traffic-policy statistics connection-limit** to display connection limit statistics.

Syntax

display traffic-policy statistics connection-limit { **per-ip** { **ipv4** [*ipv4-address*] | **ipv6** [*ipv6-address*] } **rule** *rule-name* | **per-rule** [**name** *rule-name*] | **per-user** [**user** *user-name*] **rule** *rule-name* } } [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

per-ip: Displays per-IP connection limit statistics.

ipv4: Displays per-IP connection limit statistics for IPv4 addresses.

ipv4-address: Specifies an IPv4 address. If you do not specify an IPv4 address, this command displays connection limit statistics for all IPv4 addresses of the specified traffic rule.

ipv6: Displays per-IP connection limit statistics for IPv6 addresses.

ipv6-address: Specifies an IPv6 address. If you do not specify an IPv6 address, this command displays connection limit statistics for all IPv6 addresses of the specified traffic rule.

rule *rule-name*: Specifies a traffic rule by its name, a case-insensitive string of 1 to 63 characters.

per-rule: Displays per-rule connection limit statistics.

name *rule-name*: Specifies a traffic rule by its name, a case-insensitive string of 1 to 63 characters. If you do not specify a traffic rule, this command displays per-rule connection limit statistics for all traffic rules.

per-user: Displays per-user connection limit statistics.

user *user-name*: Specifies a user by its name, a case-insensitive string of 1 to 55 characters. If you do not specify a user, this command displays per-user connection limit statistics for all users of the specified traffic rule.

rule *rule-name*: Specifies a traffic rule by its name, a case-insensitive string of 1 to 63 characters.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays connection limit statistics for all member devices.

Usage guidelines

You can identify whether a traffic rule works as configured by displaying the connection limit statistics for the traffic rule.

Examples

Display per-rule connection limit statistics for traffic rule **traffic-rule**.

```
<Sysname> display traffic-policy statistics connection-limit per-rule name traffic-rule
Slot 1:
Codes: CC(Current Connection), RC(Rejective Connection), CL(Current Limit), RRC(Rate
Rejective Connection), RR(Rejective Rate), PR(Pass Rate)
-------------------------------------------------------------------------------------
---
Rule name     State     Profile name   CC        RC        CL      RRC       RR      PR
-------------------------------------------------------------------------------------
---
traffic-rule   Enabled    profile1     200       300       200     200       300     200
-------------------------------------------------------------------------------------
---
-------------------------------------------------------------------------------------
---
```

Display per-user connection limit statistics for all users of traffic rule **traffic-rule**.

```
<Sysname> display traffic-policy statistics connection-limit per-user rule traffic-rule
Slot 1:
Codes: CC(Current Connection), RC(Rejective Connection), CL(Current Limit), RRC(Rate
Rejective Connection), RR(Rejective Rate), PR(Pass Rate)
-------------------------------------------------------------------------------------
---
Rule name       State     Profile name   User ID   User name  CC   RC    CL    RRC    RR
PR
-------------------------------------------------------------------------------------
---
traffic-rule   Enabled    profile1      0x3d     user1     200  300   200   200    300
200
-------------------------------------------------------------------------------------
---
-------------------------------------------------------------------------------------
---
```

Table 2 Command output

Field	Description
Codes	Acronyms for fields: • **CC (current connections)**—Number of current connections. • **RC (rejected connections)**—Number of connections rejected after the number of current connections reached the limit. • **CL (connection limit)**—Maximum number of connections allowed. • **RRC(Rate Rejective Connection)**—Number of connections rejected after the connection establishment rate reached the limit. • **RR(Rejective Rate)**—Rate of connections rejected, in connections per second.

Field	Description
	• **PR(Pass Rate)**—Rate of connections established, in connections per second.

display traffic-policy statistics rule-hit

Use **display traffic-policy statistics rule-hit** to display rule-hit statistics.

Syntax

display traffic-policy statistics rule-hit [**rule** *rule-name*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

rule *rule-name*: Specifies a traffic rule by its name, a case-insensitive string of 1 to 63 characters. If you do not specify a traffic rule, this command displays rule-hit statistics for all traffic rules.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays rule-hit statistics for all member devices.

Examples

Display rule-hit statistics for all traffic rules.

```
<Sysname> display traffic-policy statistics rule-hit
Slot 1:
-------------------------------------------------------------------------------
---
Rule ID  Rule name       State       Profile ID    Profile name  Hit
-------------------------------------------------------------------------------
---
201      traffic-rule    Enabled     21            profile1     11111
-------------------------------------------------------------------------------
---
202      traffic-rule1   Enabled     22            profile2     11112
-------------------------------------------------------------------------------
---
203      traffic-rule2   Enabled     23            profile1     11565
-------------------------------------------------------------------------------
---
-------------------------------------------------------------------------------
---
```

Table 3 Command output

Field	Description
Hit	Number of times that a rule is matched.

dscp

Use **dscp** to configure a DSCP priority as a match criterion.

Use **undo dscp** to remove all DSCP priority match criteria.

Syntax

dscp *dscp-value*

undo dscp *dscp-value*

Default

No DSCP priority is used as a match criterion.

Views

Traffic rule view

Predefined user roles

network-admin

context-admin

Parameters

dscp-value: Specifies a DSCP priority, which can only be a keyword in Table 4.

Table 4 Keyword-value map

Keyword	DSCP value (binary)	DSCP value (decimal)
default	000000	0
af11	001010	10
af12	001100	12
af13	001110	14
af21	010010	18
af22	010100	20
af23	010110	22
af31	011010	26
af32	011100	28
af33	011110	30
af41	100010	34
af42	100100	36
af43	100110	38
cs1	001000	8
cs2	010000	16

Keyword	DSCP value (binary)	DSCP value (decimal)
cs3	011000	24
cs4	100000	32
cs5	101000	40
cs6	110000	48
cs7	111000	56
ef	101110	46

Examples

Configure DSCP priority **af11** as a match criterion in traffic rule **rule1**.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name rule1
[Sysname-traffic-policy-rule-rule1] dscp af11
```

ipv6 extension-header

Use **ipv6 extension-header** to configure the IPv6 extension header attribute as a match criterion.

Use **undo ipv6 extension-header** to delete an extension header match criterion.

Syntax

ipv6 extension-header { **authentication** | **destination** | **encapsulating** | **fragment** | **hop-by-hop** | **routing** }

undo ipv6 extension-header

Default

The IPv6 extension header attribute is not used as a match criterion.

Views

Traffic rule view

Predefined user roles

network-admin

context-admin

Parameters

nonzero: Specifies the Authentication header.

destination: Specifies the Destination Options header.

encapsulating: Specifies the Encapsulating Security Payload header.

fragment: Specifies the Fragment header.

hop-by-hop: Specifies the Hop-by-Hop Options header.

routing: Specifies the Routing header.

Usage guidelines

This command enables the device to perform bandwidth management on the IPv6 packets with the specified extension header. For more information about extension headers, see RFC 2460.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure the Destination Options header as a match criterion in traffic rule **rule1**.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name rule1
[Sysname-traffic-policy-rule-rule1] ipv6 extension-header destination
```

Related commands

ipv6 flow-label

ipv6 flow-label

Use **ipv6 flow-label** to configure the IPv6 flow label attribute as a match criterion.

Use **undo ipv6 flow-label** to delete a flow label match criterion.

Syntax

ipv6 flow-label { **nonzero** | **zero** }

undo ipv6 flow-label

Default

The IPv6 flow label attribute is not used as a match criterion.

Views

Traffic rule view

Predefined user roles

network-admin

context-admin

Parameters

nonzero: Specifies non-zero IPv6 flow labels.

zero: Specifies the zero IPv6 flow label.

Usage guidelines

The **Flow Label** field in IPv6 packet headers is used to identify packets of a flow. This command enables the device to perform bandwidth management on the IPv6 packets with the specified flow label value. For more information about the **Flow Label** field, see RFC 2460.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure a flow label value of zero as a match criterion in traffic rule **rule1**.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name rule1
[Sysname-traffic-policy-rule-rule1] ipv6 flow-label zero
```

Related commands

ipv6 extension-header

per-ip bandwidth-threshold max-value

Use **per-ip bandwidth-threshold max-value** to set the per-IP static maximum bandwidth threshold.

Use **undo per-ip bandwidth-threshold max-value** to restore the default.

Syntax

per-ip bandwidth-threshold max-value *max-value*

undo per-ip bandwidth-threshold max-value

Default

The per-IP static maximum bandwidth threshold is not set.

Views

Traffic profile view

Predefined user roles

network-admin

context-admin

Parameters

max-value: Specifies the maximum bandwidth threshold in the range of 8 to 1000000000 kbps.

Usage guidelines

When the device detects that the traffic rate of an IP address exceeds the maximum bandwidth threshold, it sends logs to the log host by using the fast log output feature.

If you configure both the per-IP static maximum bandwidth threshold and the per-IP dynamic threshold learning feature, the following rules apply:

- Before the device learns the average traffic rate, it uses the static maximum bandwidth threshold.
- After the device learns the average traffic rate, it uses the average traffic rate multiplied by the maximum tolerance value as the maximum bandwidth threshold.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

In traffic profile **news**, set the per-IP static maximum bandwidth threshold to 50000 kbps.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] profile name news
[Sysname-traffic-policy-profile-news] per-ip bandwidth-threshold max-value 50000
```

Related commands

per-ip bandwidth-threshold min-value

per-ip bandwidth-threshold min-value

Use **per-ip bandwidth-threshold min-value** to set the per-IP static minimum bandwidth threshold.

Use **undo per-ip bandwidth-threshold min-value** to restore the default.

Syntax

per-ip bandwidth-threshold min-value *min-value*

undo per-ip bandwidth-threshold min-value

Default

The per-IP static minimum bandwidth threshold is not set.

Views

Traffic profile view

Predefined user roles

network-admin

context-admin

Parameters

min-value: Specifies the minimum bandwidth threshold in the range of 8 to 100000000 kbps.

Usage guidelines

When the device detects that the traffic rate of an IP address falls below the minimum bandwidth threshold, it sends logs to the log host by using the fast log output feature.

If you configure both the per-IP static minimum bandwidth threshold and the per-IP dynamic threshold learning feature, the following rules apply:

- Before the device learns the average traffic rate, it uses the static minimum bandwidth threshold.
- After the device learns the average traffic rate, it uses the average traffic rate multiplied by the minimum tolerance value as the minimum bandwidth threshold.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

In traffic profile **news**, set the per-IP static minimum bandwidth threshold to 500 kbps.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] profile name news
[Sysname-traffic-policy-profile-news] per-ip bandwidth-threshold min-value 500
```

Related commands

per-ip bandwidth-threshold max-value

per-ip bandwidth-threshold-detect enable

Use **per-ip bandwidth-threshold-detect enable** to enable per-IP bandwidth threshold detection.

Use **undo per-ip bandwidth-threshold-detect enable** to disable per-IP bandwidth threshold detection.

Syntax

per-ip bandwidth-threshold-detect enable

undo per-ip bandwidth-threshold-detect enable

Default

Per-IP bandwidth threshold detection is disabled.

Views

Traffic profile view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command enables the device to monitor the traffic rates based on source IP addresses in real time to identify the maximum rate and minimum rate of each IP address.

Examples

In traffic profile **news**, enable per-IP bandwidth threshold detection.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] profile name news
[Sysname-traffic-policy-profile-news] per-ip bandwidth-threshold-detect enable
```

per-ip bandwidth-threshold-learn duration

Use **per-ip bandwidth-threshold-learn duration** to set the learning duration for per-IP dynamic threshold learning.

Use **undo per-ip bandwidth-threshold-learn duration** to restore the default.

Syntax

per-ip bandwidth-threshold-learn duration *duration-value*

undo per-ip bandwidth-threshold-learn duration

Default

The learning duration is 1440 minutes.

Views

Traffic profile view

Predefined user roles

network-admin

context-admin

Parameters

duration-value: Specifies the learning duration in the range of 8 to 10080 minutes.

Usage guidelines

After per-IP bandwidth threshold detection is enabled, the device measures the traffic rates over a user-configured duration and calculates an average rate. As a best practice, set the learning duration to be longer than 1440 minutes for the device to learn the traffic for no less than a whole day. After a learning duration ends, for the device to learn traffic again, disable and then re-enable dynamic threshold learning. The device will clear the previous learning results and perform a new learning process based on the same duration.

If you modify the duration during the learning process, the device starts a new learning process with the new duration.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

In traffic profile **news**, set the learning duration for per-IP dynamic threshold learning to 2880 minutes.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] profile name news
[Sysname-traffic-policy-profile-news] per-ip bandwidth-threshold-learn duration 2880
```

Related commands

per-ip bandwidth-threshold-learn enable

per-ip bandwidth-threshold-learn enable

Use **per-ip bandwidth-threshold-learn enable** to enable per-IP dynamic bandwidth threshold learning.

Use **undo per-ip bandwidth-threshold-learn enable** to disable per-IP dynamic bandwidth threshold learning.

Syntax

per-ip bandwidth-threshold-learn enable

undo per-ip bandwidth-threshold-learn enable

Default

Per-IP dynamic bandwidth threshold learning is disabled.

Views

Traffic profile view

Predefined user roles

network-admin

context-admin

Usage guidelines

Dynamic bandwidth threshold learning is useful if you do not know the traffic patterns in a network and cannot determine appropriate bandwidth thresholds. With this feature enabled, the device measures the traffic rates over a user-configured duration and calculates an average rate. Then, the device obtains the minimum and maximum bandwidth thresholds by using the average rate multiplied by the minimum and maximum tolerance values.

If you configure both static bandwidth thresholds and the dynamic threshold learning feature for a traffic profile, the following rules apply:

- Before the device learns the average traffic rate, it uses the static bandwidth thresholds.
- After the device learns the average traffic rate, it uses the dynamic bandwidth thresholds.

Examples

In traffic profile **news**, enable per-IP dynamic bandwidth threshold learning.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] profile name news
[Sysname-traffic-policy-profile-news] per-ip bandwidth-threshold-learn enable
```

Related commands

per-ip bandwidth-threshold max-value

per-ip bandwidth-threshold min-value
per-ip bandwidth-threshold-learn tolerance max-value
per-ip bandwidth-threshold-learn tolerance min-value

per-ip bandwidth-threshold-learn tolerance max-value

Use **per-ip bandwidth-threshold-learn tolerance max-value** to set the maximum tolerance value for per-IP dynamic bandwidth threshold learning.

Use **undo per-ip bandwidth-threshold-learn tolerance max-value** to restore the default.

Syntax

per-ip bandwidth-threshold-learn tolerance max-value *max-value*

undo per-ip bandwidth-threshold-learn tolerance max-value

Default

The maximum tolerance value is not set.

Views

Traffic profile view

Predefined user roles

network-admin

context-admin

Parameters

max-value: Specifies the maximum tolerance value in the range of 1 to 4000, in percentage.

Usage guidelines

The per-IP dynamic threshold learning feature uses the learned average traffic rate to multiply the maximum tolerance value to obtain the maximum bandwidth threshold. If you also configure a static maximum bandwidth threshold for the traffic profile, the dynamic maximum bandwidth threshold is used after the average traffic rate is learned.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

In traffic profile **news**, set the maximum tolerance value for per-IP dynamic bandwidth threshold learning to 200.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] profile name news
[Sysname-traffic-policy-profile-news] per-ip bandwidth-threshold-learn tolerance
max-value 200
```

Related commands

per-ip bandwidth-threshold-learn tolerance min-value

per-ip bandwidth-threshold-learn tolerance min-value

Use **per-ip bandwidth-threshold-learn tolerance min-value** to set the minimum tolerance value for per-IP dynamic bandwidth threshold learning.

Use **undo per-ip bandwidth-threshold-learn tolerance min-value** to restore the default.

Syntax

per-ip bandwidth-threshold-learn tolerance min-value *min-value*

undo per-ip bandwidth-threshold-learn tolerance min-value

Default

The minimum tolerance value is not set.

Views

Traffic profile view

Predefined user roles

network-admin

context-admin

Parameters

min-value: Specifies the minimum tolerance value in the range of 1 to 4000, in percentage.

Usage guidelines

The per-IP dynamic threshold learning feature uses the learned average traffic rate to multiply the minimum tolerance value to obtain the minimum bandwidth threshold. If you also configure a static minimum bandwidth threshold for the traffic profile, the dynamic minimum bandwidth threshold is used after the average traffic rate is learned.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

In traffic profile **news**, set the minimum tolerance value for per-IP dynamic bandwidth threshold learning to 50.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] profile name news
[Sysname-traffic-policy-profile-news] per-ip bandwidth-threshold-learn tolerance
min-value 50
```

Related commands

per-ip bandwidth-threshold-learn tolerance max-value

profile name

Use **profile name** to create a traffic profile and enter its view, or enter the view of an existing traffic profile.

Use **undo profile name** to delete a traffic profile.

Syntax

profile name *profile-name*

undo profile name *profile-name*

Default

No traffic profile exists.

Views

Traffic policy view

Predefined user roles

network-admin

context-admin

Parameters

profile-name: Specifies a name for the traffic profile, a case-insensitive string of 1 to 63 characters.

Usage guidelines

A traffic profile defines the bandwidth resources that can be used and takes effect after it is specified for a traffic rule.

Examples

Create a traffic profile named **profile1** and enter traffic profile view.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] profile name profile1
[Sysname-traffic-policy-profile-profile1]
```

Related commands

action

profile reference-mode

Use **profile reference-mode** to set the reference mode for a traffic profile.

Use **undo profile reference-mode** to restore the default.

Syntax

profile reference-mode { **per-rule** | **rule-shared** }

undo profile reference-mode

Default

The reference mode for a traffic profile is **per-rule**.

Views

Traffic profile view

Predefined user roles

network-admin

context-admin

Parameters

per-rule: Specifies that each traffic rule that uses the traffic profile can reach the bandwidth limits and connection limits specified in the profile.

rule-shared: Specifies that all traffic rules that use the traffic profile share the bandwidth limits and connection limits specified in the profile.

Usage guidelines

After a traffic profile is specified for a traffic rule, the bandwidth limits and connection limits in the profile take effect. The reference mode for a traffic profile can be **per-rule** or **rule-shared**.

Examples

Set the reference mode to **rule-shared** for traffic profile **profile1**.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] profile name profile1
[Sysname-traffic-policy-profile-profile1] profile reference-mode rule-shared
```

profile rename

Use **profile rename** to rename a traffic profile.

Syntax

profile rename *old-name new-name*

Views

Traffic policy view

Predefined user roles

network-admin

context-admin

Parameters

old-name: Specifies the old name of the traffic profile, a case-insensitive string of 1 to 63 characters.

new-name: Specifies a new name for the traffic profile, a case-insensitive string of 1 to 63 characters. The new name cannot be an existing traffic profile name.

Examples

Create a traffic profile named **profile1**, and rename traffic profile **profile1** as **profile2**.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] profile name profile1
[Sysname-traffic-policy-profile-profile1] quit
[Sysname-traffic-policy] profile rename profile1 profile2
```

remark dscp

Use **remark dscp** to mark the DSCP priority for packets of a traffic profile.

Use **undo remark dscp** to restore the default.

Syntax

remark dscp *dscp-value*

undo remark dscp

Default

The DSCP priority for packets of a traffic profile is not marked.

Views

Traffic profile view

Predefined user roles

network-admin

context-admin

Parameters

dscp-value: Specifies a DSCP priority, which can only be a keyword in Table 4.

Usage guidelines

Network devices can classify traffic by using DSCP priorities and provide different treatment for packets with different DSCP priorities.

Examples

Mark DSCP priority **af22** for packets of traffic profile **profile1**.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] profile name profile1
[Sysname-traffic-policy-profile-profile1] remark dscp af22
```

Related commands

profile name

reset traffic-policy statistics bandwidth

Use **reset traffic-policy statistics bandwidth** to clear traffic statistics for traffic rules.

Syntax

reset traffic-policy statistics bandwidth { **downstream** | **total** | **upstream** } { **per-ip** { **ipv4** [*ipv4-address*] | **ipv6** [*ipv6-address*] } **rule** *rule-name* | **per-rule** [**name** *rule-name*] | **per-user** [**user** *user-name*] **rule** *rule-name* } [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

downstream: Specifies downstream traffic.

total: Specifies both downstream traffic and upstream traffic.

upstream: Specifies upstream traffic.

per-ip: Clears per-IP traffic statistics.

ipv4: Clears per-IP traffic statistics for IPv4 addresses.

ipv4-address: Specifies an IPv4 address. If you do not specify an IPv4 address, this command clears per-IP traffic statistics for all IPv4 addresses of the specified traffic rule.

ipv6: Clears per-IP traffic statistics for IPv6 addresses. Non-default vSystems do not support this parameter.

ipv6-address: Specifies an IPv6 address. If you do not specify an IPv6 address, this command clears per-IP traffic statistics for all IPv6 addresses of the specified traffic rule.

rule *rule-name*: Specifies a traffic rule by its name, a case-insensitive string of 1 to 63 characters.

per-rule: Clears per-rule traffic statistics.

name *rule-name*: Specifies a traffic rule by its name, a case-insensitive string of 1 to 63 characters. If you do not specify a traffic rule, this command clears per-rule traffic statistics for all traffic rules.

per-user: Clears per-user traffic statistics.

user *user-name*: Specifies a user by its name, a case-insensitive string of 1 to 55 characters. If you do not specify a user, this command clears per-user traffic statistics for all users of the specified traffic rule.

rule *rule-name*: Specifies a traffic rule by its name, a case-insensitive string of 1 to 63 characters.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears traffic statistics for all member devices.

Examples

Clear per-rule upstream traffic statistics for traffic rule **traffic-rule** on a slot.

```
<Sysname> reset traffic-policy statistics bandwidth upstream per-rule name traffic-rule
slot 1
```

reset traffic-policy statistics connection-limit

Use **reset traffic-policy statistics connection-limit** to clear connection limit statistics.

Syntax

reset traffic-policy statistics connection-limit { **per-ip** { **ipv4** [*ipv4-address*] | **ipv6** [*ipv6-address*] } **rule** *rule-name* | **per-rule** [**name** *rule-name*] | **per-user** [**user** *user-name*] **rule** *rule-name* } } [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

per-ip: Clears per-IP connection limit statistics.

ipv4: Clears per-IP connection limit statistics for IPv4 addresses.

ipv4-address: Specifies an IPv4 address. If you do not specify an IPv4 address, this command clears connection limit statistics for all IPv4 addresses of the specified traffic rule.

ipv6: Clears per-IP connection limit statistics for IPv6 addresses.

ipv6-address: Specifies an IPv6 address. If you do not specify an IPv6 address, this command clears connection limit statistics for all IPv6 addresses of the specified traffic rule.

rule *rule-name*: Specifies a traffic rule by its name, a case-insensitive string of 1 to 63 characters.

per-rule: Clears per-rule connection limit statistics.

name *rule-name*: Specifies a traffic rule by its name, a case-insensitive string of 1 to 63 characters. If you do not specify a traffic rule, this command clears per-rule connection limit statistics for all traffic rules.

per-user: Clears per-user connection limit statistics.

user *user-name*: Specifies a user by its name, a case-insensitive string of 1 to 55 characters. If you do not specify a user, this command clears per-user connection limit statistics for all users of the specified traffic rule.

rule *rule-name*: Specifies a traffic rule by its name, a case-insensitive string of 1 to 63 characters.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears connection limit statistics for all member devices.

Examples

Clear per-rule connection limit statistics for traffic rule **traffic-rule** on a slot.

```
<Sysname> reset traffic-policy statistics connection-limit per-rule name traffic-rule
slot 1
```

reset traffic-policy statistics rule-hit

Use **reset traffic-policy statistics rule-hit** to clear rule-hit statistics.

Syntax

reset traffic-policy statistics rule-hit [**rule** *rule-name*] [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

rule *rule-name*: Specifies a traffic rule by its name, a case-insensitive string of 1 to 63 characters. If you do not specify a traffic rule, this command clears rule-hit statistics for all traffic rules.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears rule-hit statistics for all member devices.

Examples

Clear rule-hit statistics for traffic rule **traffic-rule** on a slot.

```
<Sysname> reset traffic-policy statistics rule-hit rule traffic-rule slot 1
```

rule

Use **rule** to create a traffic rule and enter its view, or enter the view of an existing traffic rule.

Use **undo rule** to delete a traffic rule.

Syntax

rule *rule-id*

rule [*rule-id*] **name** *rule-name* [**parent** *parent-rule-name*]

undo rule { *rule-id* | **name** *rule-name* }

Default

No traffic rule exists.

Views

Traffic policy view

Predefined user roles

network-admin

context-admin

Parameters

rule-id: Specifies an ID for the traffic rule, in the range of 1 to 65534. If you do not specify a rule ID, the system assigns the unused ID next to the ID used last time. If the rule ID to be assigned is greater than 65534, the system assigns the smallest available rule ID.

rule-name: Specifies a name for the traffic rule, a case-insensitive string of 1 to 63 characters. You must specify a rule name when creating a traffic rule.

parent *parent-rule-name*: Specifies a parent traffic rule by its name, a case-insensitive string of 1 to 63 characters. To successfully create the traffic rule, make sure the parent traffic rule already exists.

Usage guidelines

You can configure multiple traffic rules in the traffic policy. For a traffic rule, you can configure match criteria to match packets and specify the traffic profile to apply to matching packets. The device matches traffic rules in their order of appearance on the device. When a traffic rule is matched, the matching process ends and the device applies the traffic profile for the traffic rule to the traffic. If no traffic rule is matched, the device forwards the traffic.

For a new traffic rule to inherit the match criteria of an existing traffic rule, specify the existing traffic rule as the parent of the new traffic rule.

A level-4 rule cannot act as a parent rule

You can specify a parent traffic rule only when creating a traffic rule. You cannot add or modify a parent traffic rule for an existing traffic rule.

Examples

Create a traffic rule with ID 111 and name **rule1** and enter traffic rule view.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule 111 name rule1
[Sysname-traffic-policy-rule-111-rule1]
```

rule copy

Use **rule copy** to copy a traffic rule.

Syntax

rule copy *rule-name new-rule-name*

Views

Traffic policy view

Predefined user roles

network-admin

context-admin

Parameters

rule-name: Specifies a traffic rule to be copied by its name, a case-insensitive string of 1 to 63 characters.

new-rule-name: Specifies a name for the new traffic rule, a case-insensitive string of 1 to 63 characters. The new name cannot be an existing traffic profile name.

Usage guidelines

If a traffic rule to be created is similar to an existing traffic rule, create the traffic rule by copying the existing traffic rule and then modify it. The new traffic rule is placed next to the copied traffic rule.

If a traffic rule to be copied has child traffic rules, only the parent traffic rule is copied.

Examples

Create a traffic rule named **rule2** by copying traffic rule **rule1**.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule copy rule1 rule2
```

rule move

Use **rule move** to move a traffic rule to a new position.

Syntax

rule move *rule-name1* { **after** *rule-name2* | **before** [*rule-name2*] }

Views

Traffic policy view

Predefined user roles

network-admin

context-admin

Parameters

rule-name1: Specifies a traffic rule to be moved by its name, a case-insensitive string of 1 to 63 characters. The traffic rule can be a parent or child traffic rule.

after: Moves the specified traffic rule to the position after a target traffic rule.

before: Moves the specified traffic rule to the position before a target traffic rule. If you do not specify the *rule-name2* argument, the specified traffic rule is moved to the front of the traffic policy.

rule-name2: Specifies the target traffic rule by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

The device matches traffic with traffic rules in their order of appearance on the device. When a traffic rule is matched, the matching process ends and the device applies the traffic profile specified for the traffic rule to the traffic. If no traffic rule is matched, the device forwards the traffic.

To ensure reasonable, precise bandwidth management, configure traffic rules in ascending order of granularity. If the traffic rules are not in ascending order of granularity, you can use the **rule move** command to change the position of them.

You can move child traffic rules only within their parent traffic rule.

Examples

Create two traffic rules named **rule1** and **rule2**, and move **rule1** to the position after **rule2**.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name rule1
[Sysname-traffic-policy-rule-rule1] quit
[Sysname-traffic-policy] rule name rule2
[Sysname-traffic-policy-rule-rule2] quit
[Sysname-traffic-policy] rule move rule1 after rule2
```

rule rename

Use **rule rename** to rename a traffic rule.

Syntax

rule rename *old-rule-name new-rule-name*

Views

Traffic policy view

Predefined user roles

network-admin

context-admin

Parameters

old-rule-name: Specifies the old name of the traffic rule, a case-insensitive string of 1 to 63 characters.

new-rule-name: Specifies a new name for the traffic rule, a case-insensitive string of 1 to 63 characters. The new name cannot be an existing traffic profile name.

Examples

Create a traffic rule named **rule1**, and rename traffic rule **rule1** as **rule2**.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name rule1
[Sysname-traffic-policy-rule-rule1] quit
[Sysname-traffic-policy] rule rename rule1 rule2
```

service

Use **service** to configure a service object group as a match criterion.

Use **undo service** to delete a service object group match criterion.

Syntax

service *object-group-name*

undo service [*object-group-name*]

Default

No service object group is used as a match criterion.

Views

Traffic rule view

Predefined user roles

network-admin

context-admin

Parameters

object-group-name: Specifies a service object group by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

You can specify multiple service object groups for a traffic rule to match packets.

The **undo service** command removes all service object groups from match criteria if you do not specify a service object group or specify the system-defined service object group **any**.

Examples

Specify predefined service object group **ftp** for traffic rule **rule1** to match packets.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name rule1
[Sysname-traffic-policy-rule-rule1] service ftp
```

Related commands

object-group (*Security Command Reference*)

source-address

Use **source-address** to configure a source IP address object group as a match criterion.

Use **undo source-address** to delete a source IP address object group as a match criterion.

Syntax

source-address address-set *object-group-name*

undo source-address address-set *object-group-name*

Default

No source IP address object group is used as a match criterion.

Views

Traffic rule view

Predefined user roles

network-admin

context-admin

Parameters

object-group-name: Specifies an IPv4 or IPv6 address object group by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

This command is used to match the packets with the source IP addresses in the specified address object group. You can specify multiple address object groups for a traffic rule to match source IP addresses of packets.

Before rolling back configuration by using the **configuration replace file** *filename* command, check the address object group configuration in the traffic rule in the configuration file. The address object group configuration fails to be rolled back if two address object groups have the same name but are of different types (IPv4/IPv6).

Examples

Specify IPv4 address object group **obgroup1** for traffic rule **rule1** to match source IPv4 addresses of packets.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name rule1
[Sysname-traffic-policy-rule-rule1] source-address address-set obgroup1
```

Related commands

object-group (*Security Command Reference*)

source-zone

Use **source-zone** to configure a source security zone as a match criterion.

Use **undo source-zone** to delete a source security zone match criterion.

Syntax

source-zone *source-zone-name*

undo source-zone *source-zone-name*

Default

No source security zone is used as a match criterion.

Views

Traffic rule view

Predefined user roles

network-admin

context-admin

Parameters

source-zone-name: Specifies a source zone by its name, a case-insensitive string of 1 to 31 characters.

Examples

Configure source security zone **zone1** as a match criterion in traffic rule **rule1**.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name rule1
[Sysname-traffic-policy-rule-rule1] source-zone zone1
```

Related commands

security-zone name (*Security Command Reference*)

statistics bandwidth enable

Use **statistics bandwidth enable** to enable traffic statistics collection.

Use **undo statistics bandwidth enable** to disable traffic statistics collection.

Syntax

statistics bandwidth enable

undo statistics bandwidth enable

Default

Traffic statistics collection is disabled.

Views

Traffic policy view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command enables the device to collect statistics about matching traffic. To view the statistics, use the **display traffic-policy statistics bandwidth** command.

This command affects device performance. As a best practice, configure this command only if you need to view statistics.

Examples

Enable traffic statistics collection.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] statistics bandwidth enable
```

Related commands

display traffic-policy statistics bandwidth

statistics connection-limit enable

Use **statistics connection-limit enable** to enable connection limit statistics collection.

Use **undo statistics connection-limit enable** to disable connection limit statistics collection.

Syntax

statistics connection-limit enable

undo statistics connection-limit enable

Default

Connection limit statistics collection is disabled.

Views

Traffic policy view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command enables the device to collect statistics about matching connections. To view the statistics, use the **display traffic-policy statistics connection-limit** command.

This command affects device performance. As a best practice, configure this command only if you need to view statistics.

Examples

Enable connection limit statistics collection.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] statistics connection-limit enable
```

Related commands

display traffic-policy statistics connection-limit

statistics rule-hit enable

Use **statistics rule-hit enable** to enable rule-hit statistics collection.

Use **undo statistics rule-hit enable** to disable rule-hit statistics collection.

Syntax

statistics rule-hit enable

undo statistics rule-hit enable

Default

Rule-hit statistics collection is disabled.

Views

Traffic policy view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command enables the device to collect rule-hit statistics. To view the statistics, use the **display traffic-policy statistics rule-hit** command.

This command affects device performance. As a best practice, configure this command only if you need to view statistics.

Examples

Enable rule-hit statistics collection.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] statistics rule-hit enable
```

Related commands

display traffic-policy statistics rule-hit

tcp mss

Use **tcp mss** to set the TCP maximum segment size (MSS).

Use **undo tcp mss** to restore the default.

Syntax

tcp mss *mss-value*

undo tcp mss

Default

The TCP MSS is not set.

Views

Traffic profile view

Predefined user roles

network-admin

context-admin

Parameters

mss-value: Specifies the TCP MSS in the range of 128 to 9158 bytes.

Usage guidelines

The MSS specifies the maximum size of TCP segments that the peer device can send to the local device. It is negotiated during TCP connection establishment. When establishing a TCP connection, the local device advertises the MSS to the peer device. The peer device does not send TCP packets greater than the MSS. For TCP packets that exceed the MSS, the peer device fragments them before sending them.

This command takes effect only on new TCP connections and does not take effect on existing TCP connections.

This command takes effect only on IP packets. If MPLS is configured, do not set the MSS.

If you configure the MSS in both traffic profile view and interface view, the smaller MSS value takes effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the TCP MSS to 128 bytes for traffic profile **profile1**.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] profile name profile1
[Sysname-traffic-policy-profile–profile1] tcp mss 128
```

Related commands

tcp mss (*Layer 3—IP Services Command Reference*)

terminal

Use **terminal** to configure a terminal as a match criterion.

Use **undo terminal** to delete a terminal match criterion.

Syntax

terminal *terminal-name*

undo terminal *terminal-name*

Default

No terminal is used as a match criterion.

Views

Traffic rule view

Predefined terminal roles

network-admin

context-admin

Parameters

terminal-name: Specifies a terminal by its name, a case-insensitive string of 1 to 63 characters. The names **invalid** and **other** are not supported.

Usage guidelines

You can execute this command multiple times to specify multiple terminals for a traffic rule to match packets.

Examples

Configure terminal **terminaltest** as a match criterion in traffic rule **news**.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name news
[Sysname-traffic-policy-rule-news] terminal terminaltest
```

Related commands

terminal-group

terminal-group

Use **terminal-group** to configure a terminal group as a match criterion.

Use **undo terminal-group** to delete a terminal group match criterion.

Syntax

terminal-group *group-name*

undo terminal-group *group-name*

Default

No terminal group is used as a match criterion.

Views

Traffic rule view

Predefined terminal-group roles

network-admin

context-admin

Parameters

group-name: Specifies a terminal group by its name, a case-insensitive string of 1 to 63 characters. The names **invalid** and **other** are not supported.

Usage guidelines

You can execute this command multiple times to specify multiple terminal groups for a traffic rule to match packets.

Examples

Configure terminal group **terminalgrouptest** as a match criterion in traffic rule **news**.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name news
[Sysname-traffic-policy-rule-news] terminal-group terminalgrouptest
```

Related commands

terminal

time-range

Use **time-range** to specify a time range during which a traffic rule is in effect.

Use **undo time-range** to restore the default.

Syntax

time-range *time-range-name*

undo time-range

Default

A traffic rule is in effect at any time.

Views

Traffic rule view

Predefined user roles

network-admin

context-admin

Parameters

time-range-name: Specifies a time range by its name, a case-insensitive string of 1 to 32 characters.

Examples

Specify time range **work-time** for traffic rule **rule1**.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name rule1
[Sysname-traffic-policy-rule-rule1] time-range work-time
```

Related commands

time-range (*ACL and QoS Command Reference*)

traffic-policy

Use **traffic-policy** to enter traffic policy view.

Use **undo traffic-policy** to remove all traffic policy settings.

Syntax

traffic-policy

undo traffic-policy

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

In traffic policy view, you can create and manage traffic rules.

Examples

Enter traffic policy view.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy]
```

traffic-priority

Use **traffic-priority** to set the traffic priority for a traffic profile.

Use **undo traffic-priority** to restore the default.

Syntax

traffic-priority *priority-value*

undo traffic-priority

Default

The traffic priority is 1 for a traffic profile.

Views

Traffic profile view

Predefined user roles

network-admin

context-admin

Parameters

priority-value: Specifies the priority value in the range of 1 to 7. The larger the priority value, the higher the priority.

Usage guidelines

When an interface is congested with packets of multiple traffic profiles, packets with higher priority are sent first. Packets with the same priority have the same chance of being forwarded.

Examples

Set the traffic priority to 7 for traffic profile **profile1**.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] profile name profile1
[Sysname-traffic-policy-profile-profile1] traffic-priority 7
```

Related commands

profile name

user

Use **user** to configure a username as a match criterion.

Use **undo user** to delete a username match criterion.

Syntax

user *user-name* [**domain** *domain-name*]

undo user *user-name* [**domain** *domain-name*]

Default

No username is used as a match criterion.

Views

Traffic rule view

Predefined user roles

network-admin

context-admin

Parameters

user-name: Specifies a username, a case-insensitive string of 1 to 55 characters. The username cannot be **a**, **al**, or **all**, and cannot contain the following special characters: backslashes (\), vertical bars (|), slash (/), colon (:), asterisks (*), question marks (?), left angle brackets (<), right angle brackets (>), and at signs (@).

domain *domain-name*: Matches the user in an identity domain. The *domain-name* argument represents the identity domain name, a case-insensitive string of 1 to 255 characters. The identity domain name cannot contain the following special characters: backslashes (\), vertical bars (|), slash (/), colon (:), asterisks (*), question marks (?), left angle brackets (<), right angle brackets (>), and at signs (@). If you do not specify this option, the system matches the user among users that do not belong to any identity domain. For more information about identity domains, see user identification in *Security Configuration Guide*.

Usage guidelines

A username corresponds to changing IP addresses. This command implements per-user bandwidth management and facilitates bandwidth management for mobile Internet users whose IP addresses change.

Examples

Configure username **managers** as a match criterion in traffic rule **rule1**.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name rule1
```

```
[Sysname-traffic-policy-rule-rule1] user managers
```

Configure username **user1** in identity domain **dpi** as a match criterion in traffic rule **myrule**.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name myrule
[Sysname-traffic-policy-rule-myrule] user user1 domain dpi
```

Related commands

`local-user` (*Security Command Reference*)

`user-identity enable` (*Security Command Reference*)

`user-identity static-user` (*Security Command Reference*)

user-group

Use **`user-group`** to configure a user group as a match criterion.

Use **`undo user-group`** to delete a user group match criterion.

Syntax

`user-group` *`user-group-name`* [**`domain`** *`domain-name`*]

`undo user-group` *`user-group-name`* [**`domain`** *`domain-name`*]

Default

No user group is used as a match criterion.

Views

Traffic rule view

Predefined user roles

network-admin

context-admin

Parameters

`user-group-name`: Specifies a user group by its name, a case-insensitive string of 1 to 200 characters.

`domain` *`domain-name`*: Matches the user group in an identity domain. The *`domain-name`* argument represents the identity domain name, a case-insensitive string of 1 to 255 characters. The identity domain name cannot contain the following special characters: backslashes (\), vertical bars (|), slash (/), colon (:), asterisks (*), question marks (?), left angle brackets (<), right angle brackets (>), and at signs (@). If you do not specify this option, the system matches the user group among user groups that do not belong to any identity domain. For more information about identity domains, see user identification in *Security Configuration Guide*.

Usage guidelines

A user group corresponds to changing IP addresses. This command implements per-user-group bandwidth management and facilitates bandwidth management for mobile Internet users whose IP addresses change.

Examples

Configure user group **mak** as a match criterion in traffic rule **rule1**.

```
<Sysname> system-view
[Sysname] traffic-policy
```

```
[Sysname-traffic-policy] rule name rule1
[Sysname-traffic-policy-rule-rule1] user-group mak
```

Configure user group **usergroup1** in identity domain **dpi** as a match criterion in traffic rule **myrule**.

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name myrule
[Sysname-traffic-policy-rule-myrule] user-group usergroup1 domain dpi
```

Related commands

user-group (*Security Command Reference*)

user-identity enable (*Security Command Reference*)

Contents

Application audit and management commands

This feature parses personal information from user packets and must be used for legitimate purposes.

application

Use **application** to configure an application or application group as a match criterion for an application audit and management policy.

Use **undo application** to delete an application or application group match criterion from an application audit and management policy.

Syntax

application { **app** *application-name* | **app-group** *application-group-name* }

undo application { **app** *application-name* | **app-group** *application-group-name* }

Default

No application or application group is used as a match criterion.

Views

Application audit and management policy view

Predefined user roles

network-admin

context-admin

Parameters

app *application-name*: Specifies an application by its name, a case-insensitive string of 1 to 63 characters.

app-group *application-group-name*: Specifies an application group by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

You can configure this command only in an audit-free policy or deny policy.

You can configure this command multiple times to specify multiple applications or application groups.

Examples

Specify applications **app1** and **app2** and application groups **group1** and **group2** for policy **mypolicy2** to match packets.

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy name mypolicy2 deny
[Sysname-uapp-control-policy-mypolicy2] application app app1
[Sysname-uapp-control-policy-mypolicy2] application app app2
[Sysname-uapp-control-policy-mypolicy2] application app-group group1
[Sysname-uapp-control-policy-mypolicy2] application app-group group2
```

Related commands

app-group (*Security Command Reference*)

nbar application (*Security Command Reference*)

port-mapping (*Security Command Reference*)

description

Use **description** to set a description for a keyword group.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

No description exists for a keyword group.

Views

Keyword group view

Predefined user roles

network-admin

context-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 255 characters.

Examples

Set the description to **account limit** for keyword group **mykeywordgroup**.

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] keyword-group name mykeywordgroup
[Sysname-uapp-control-keyword-group-mykeywordgroup] description account limit
```

destination-address

Use **destination-address** to configure a destination IP address object group as a match criterion for an application audit and management policy.

Use **undo destination-address** to remove a destination IP address object group as a match criterion from an application audit and management policy.

Syntax

destination-address { **ipv4** | **ipv6** } *object-group-name*

undo destination-address { **ipv4** | **ipv6** } *object-group-name*

Default

No destination IP address object group is used as a match criterion.

Views

Application audit and management policy view

Predefined user roles

network-admin

context-admin

Parameters

ipv4: Specifies an IPv4 address object group.

ipv6: Specifies an IPv6 address object group.

object-group-name: Specifies an existing address object group by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

You can configure this command multiple times to specify multiple IPv4 or IPv6 address object groups.

Examples

Specify IPv4 address object groups **obgroup3** and **obgroup4** for policy **mypolicy1** to match destination IPv4 addresses of packets.

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy name mypolicy1 audit
[Sysname-uapp-control-policy-mypolicy1] destination-address ipv4 obgroup3
[Sysname-uapp-control-policy-mypolicy1] destination-address ipv4 obgroup4
```

Related commands

object-group (*Security Command Reference*)

destination-zone

Use **destination-zone** to configure a destination security zone as a match criterion for an application audit and management policy.

Use **undo destination-zone** to delete a destination security zone match criterion from an application audit and management policy.

Syntax

destination-zone *destination-zone-name*

undo destination-zone *destination-zone-name*

Default

No destination security zone is used as a match criterion.

Views

Application audit and management policy view

Predefined user roles

network-admin

context-admin

Parameters

destination-zone-name: Specifies a destination security zone by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

You can configure this command multiple times to specify multiple destination security zones.

Examples

Specify destination security zones **zone3** and **zone4** for policy **mypolicy1** to match packets.

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy name mypolicy1 audit
[Sysname-uapp-control-policy-mypolicy1] destination-zone zone3
[Sysname-uapp-control-policy-mypolicy1] destination-zone zone4
```

Related commands

security-zone name (*Security Command Reference*)

disable

Use **disable** to disable an application audit and management policy.

Use **undo disable** to enable an application audit and management policy.

Syntax

disable

undo disable

Default

An application audit and management policy is enabled.

Views

Application audit and management policy view

Predefined user roles

network-admin

context-admin

Usage guidelines

If an application audit and management policy is not used, use this command to disable it. A disabled policy does not participate in traffic matching. You can copy, rename, and move a disabled policy.

Examples

Disable application audit and management policy **mypolicy1**.

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy name mypolicy1
[Sysname-uapp-control-policy-mypolicy1] disable
```

keyword

Use **keyword** to add a keyword to a keyword group.

Use **undo keyword** to delete a keyword from a keyword group.

Syntax

keyword *keyword-value*

undo keyword *keyword-value*

Default

No keywords exist in a keyword group.

Views

Keyword group view

Predefined user roles

network-admin

context-admin

Parameters

keyword-value: Specifies a keyword, a case-sensitive string of 1 to 63 characters.

Examples

Add keyword **keywordname** to keyword group **mykeywordgroup**.

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] keyword-group name mykeywordgroup
[Sysname-uapp-control-keyword-group-mykeywordgroup] keyword keywordname
```

keyword-group name

Use **keyword-group name** to create a keyword group and enter its view, or enter the view of an existing keyword group.

Use **undo keyword-group name** to delete a keyword group.

Syntax

keyword-group name *keyword-group-name*

undo keyword-group name *keyword-group-name*

Default

No keyword groups exist.

Views

Application audit and management view

Predefined user roles

network-admin

context-admin

Parameters

keyword-group-name: Specifies a keyword group by its name, a case-insensitive string of 1 to 63 characters.

Examples

Create a keyword group named **mykeywordgroup** and enter its view.

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] keyword-group name mykeywordgroup
[Sysname-uapp-control-keyword-group-mykeywordgroup]
```

policy copy

Use **policy copy** to copy an application audit and management policy.

Syntax

policy copy *policy-name new-policy-name*

Default

No application audit and management policies exist.

Views

Application audit and management view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies an application audit and management policy to be copied by its name, a case-insensitive string of 1 to 63 characters.

new-policy-name: Specifies a name for the new application audit and management policy, a case-insensitive string of 1 to 63 characters.

Usage guidelines

If an application audit and management policy to be created is similar to an existing policy, create the policy by copying the existing policy and then modify it.

Examples

Create an application audit and management policy named **policy2** by copying policy **policy1**.

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy copy policy1 policy2
```

policy default-action

Use **policy default-action** to configure the default action for application audit and management policies.

Syntax

policy default-action { **deny** | **permit** }

Default

The default action for application audit and management policies is **permit**.

Views

Application audit and management view

Predefined user roles

network-admin

context-admin

Parameters

deny: Drops packets.

permit: Allows packets to pass.

Usage guidelines

If a packet does not match any application audit and management policy, the device applies the default action to the packet.

Examples

Configure the default action as **deny** for application audit and management policies.

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy default-action deny
```

policy move

Use **policy move** to move an application audit and management policy to a new position.

Syntax

policy move *policy-name1* { **after** *policy-name2* | **before** [*policy-name2*] }

Views

Application audit and management view

Predefined user roles

network-admin

context-admin

Parameters

policy-name1: Specifies an application audit and management policy to be moved by its name, a case-insensitive string of 1 to 63 characters. The traffic rule can be a parent or child traffic rule.

after: Moves the specified policy to the position after a target policy.

before: Moves the specified policy to the position before a target policy. If you do not specify the *policy-name2* argument, the specified policy is moved before all policies.

policy-name2: Specifies the target policy by its name, a case-insensitive string of 1 to 63 characters.

Examples

Create two application audit and management policies named **policy1** and **policy2**, and move **policy1** to the position after **policy2**.

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy name policy1 audit
[Sysname-uapp-control-policy-policy1] quit
[Sysname-uapp-control] policy name policy2 audit
[Sysname-uapp-control-policy-policy2] quit
[Sysname-uapp-control] policy move policy1 after policy2
```

policy name

Use **policy name** to create an application audit and management policy and enter its view, or enter the view of an existing policy.

Use **undo policy name** to delete an application audit and management policy.

Syntax

policy name *policy-name* [**audit** | **deny** | **noaudit**]

undo policy name *policy-name*

Default

No application audit and management policies exist.

Views

Application audit and management view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies a name for the application audit and management policy, a case-insensitive string of 1 to 63 characters. The name must be globally unique.

audit: Creates an audit policy.

deny: Creates a deny policy.

noaudit: Creates an audit-free policy.

Usage guidelines

You must specify the policy type when creating a policy. Application audit and management policies have the following types:

- **Audit policy**—Audits packets that meet match criteria in the policy.
- **Audit-free policy**—Does not audit packets that meet match criteria in the policy.
- **Deny policy**—Drops packets that meet match criteria in the policy.

The **application** command can be configured only in an audit-free policy or deny policy.

The following commands can be configured only in an audit policy:

- **rule**.
- **rule default-action**.
- **rule match-method**.

Examples

Create an application audit and management policy named **mypolicy1** and enter its view.

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy name mypolicy1 audit
[Sysname-uapp-control-policy-mypolicy1]
```

policy rename

Use **policy rename** to rename an application audit and management policy.

Syntax

policy rename *old-policy-name new-policy-name*

Views

Application audit and management view

Predefined user roles

network-admin

context-admin

Parameters

old-policy-name: Specifies the old name of the policy, a case-insensitive string of 1 to 63 characters.

new-policy-name: Specifies a new name for the policy, a case-insensitive string of 1 to 63 characters.

Examples

Create an application audit and management policy named **policy1**, and rename the policy as **policy2**.

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy name policy1 audit
[Sysname-uapp-control-policy-policy1] quit
[Sysname-uapp-control] policy rename policy1 policy2
```

rule

Use **rule** to configure an audit rule.

Use **undo rule** to delete an audit rule.

Syntax

rule *rule-id* { **app** *app-name* | **app-category** *app-category-name* | **any** } **behavior** { *behavior-name* | **any** } **bhcontent** { *bhcontent-name* | **any** } { **keyword** { **equal** | **exclude** | **include** | **unequal** } { *keyword-group-name* | **any** } | **integer** { **equal** | **greater** | **greater-equal** | **less** | **less-equal** | **unequal** } { *number* } } **action** { **deny** | **permit** } [**audit-logging**]

rule *rule-id* { **email-bomb-defense** [**interval** *interval* **max-number** *email-number*] | **email-send-restriction** } * **action** { **deny** | **permit** } [**audit-logging**]

undo rule *rule-id*

Default

No audit rules exist.

Views

Application audit and management policy view

Predefined user roles

network-admin

context-admin

Parameters

rule-id: Specifies a rule ID in the range of 1 to 64.

app *app-name*: Audits an application specified by its name.

app-category *app-category-name*: Audits an application category specified by its name.

any: Audits all applications and application categories.

behavior *behavior-name*: Audits a behavior specified by its name.

behavior any: Audits all behaviors.

bhcontent *bhcontent-name*: Audits a behavior content specified by its name.

bhcontent any: Audits all behavior contents.

keyword: Matches behavior contents by a string-type keyword.

- **equal**: Matches behavior contents that are the same as the keyword.
- **exclude**: Matches behavior contents that do not include the keyword.
- **include**: Matches behavior contents that include the keyword.
- **unequal**: Matches behavior contents that are different from the keyword.

keyword-group-name: Specifies a keyword group by its name.

any: Audits all behavior contents of an application or application category.

integer: Matches behavior contents by a number.

- **equal**: Matches behavior contents that are equal to the number.
- **greater**: Matches behavior contents that are greater than the number.
- **greater-equal**: Matches behavior contents that are greater than or equal to the number.
- **less**: Matches behavior contents that are smaller than the number.
- **less-equal**: Matches behavior contents that are smaller than or equal to the number.
- **unequal**: Matches behavior contents that are not equal to the number.

number: Specifies a number in the range of 0 to 4294967295.

action: Specifies the action to take on packets that match the audit rule.

- **deny**: Denies matching packets.
- **permit**: Allows matching packets to pass.

audit-logging: Generates audit logs for packets that match the audit rule. If you do not specify this keyword, audit logs are not generated for packets that match the audit rule.

email-bomb-defense: Configures email bomb prevention.

interval *interval*: Specifies the detection time in the range of 1 to 5 minutes. The default is 1 minute.

max-number *email-number*: Specifies the maximum number of emails that can be received from the same user during the detection time.

email-send-restriction: Enables preventing users from sending emails to users of a different domain.

Usage guidelines

After a packet matches all match criteria in an application audit and management policy, the device performs a finer audit on the packet.

- If a packet matches all items in an audit rule, the action in the audit rule is taken on the packet.
- If a packet matches only the specified application or application category in an audit rule, the packet is allowed to pass through.
- If a packet does not match the specified application or application category in an audit rule, the default action for audit rules is taken on the packet.

This command can be configured only in an audit policy.

For WeChat and QQ, specific messages cannot be audited.

An audit rule provices the following functions:

- **General auditing**—Performs granular control on user behaviors.
- **Email protection**—Detects incoming emails, counts emails based on recipients, and protects recipients from attacks. Specifically, you can configure the following functions:
  - **Limit email sending**—Prevents users from sending emails to users of a different domain. For example, the user at user1@abc.com cannot receive emails from the user at user2@123.com.
  - **Prevent email bombing**—Protects recipients from being overwhelmed by large numbers of emails from the same sender during a short period of time.

Examples

Create an application audit and management policy named **mypolicy1**.

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy name mypolicy1 audit
```

Create an audit rule that allows login packets from accounts that include keyword 0 in the IM application group, generating audit logs.

```
[Sysname-uapp-control-policy-mypolicy1] rule 1 app-category IM behavior Login bhcontent
Account keyword include mykeywd2 action deny audit-logging
```

Create an audit rule that enables email bombing prevention, with the permit action and logging action specified.

```
[Sysname-uapp-control-policy-mypolicy1] rule 2 email-bomb-defense interval 1 max-number
5 action permit audit-logging
```

Create an audit rule that enables email sending limitation, with the permit action and logging action specified.

```
[Sysname-uapp-control-policy-mypolicy1] rule 3 email-send-restriction action permit
audit-logging
```

Related commands

keyword

keyword-group name

rule default-action

Use **rule default-action** to configure the default action for audit rules in an application audit and management policy.

Syntax

rule default-action { **deny** | **permit** }

Default

The default action for audit rules is **permit**.

Views

Application audit and management policy view

Predefined user roles

network-admin

context-admin

Parameters

deny: Drops packets.

permit: Allows packets to pass.

Usage guidelines

If a packet does not match the application or application category in any audit rule, the device applies the default action to the packet.

Examples

Configure the default action as **deny** for audit rules in policy **mypolicy1**.

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy name mypolicy1 audit
[Sysname-uapp-control-policy-mypolicy1] rule default-action deny
```

rule match-method

Use **rule match-method** to configure the match mode for audit rules in an application audit and management policy.

Syntax

rule match-method { **all** | **in-order** }

Default

The match mode for audit rules is **in-order**.

Views

Application audit and management policy view

Predefined user roles

network-admin

context-admin

Parameters

all: Specifies the **all** match mode.

in-order: Specifies the **in-order** match mode.

Usage guidelines

In the **in-order** match mode, the device compares packets with audit rules in ascending order of rule ID. When a packet matches a rule, the device stops the match process and performs the action defined in the rule.

In the **all** match mode, the device compares packets with audit rules in ascending order of rule ID.

- If a packet matches a rule with the permit action, all subsequent rules continue to be matched.

  The device takes the action with higher priority on matching packets. The deny action has higher priority than the permit action.
- If a packet matches a rule with the deny action, the device stops the match process and performs the deny action.

Examples

Configure the match mode as **all** for audit rules in policy **mypolicy1**.

```
<Sysname> system-view
```

```
[Sysname] uapp-control
[Sysname-uapp-control] policy name mypolicy1 audit
[Sysname-uapp-control-policy-mypolicy1] rule match-method all
```

service

Use **service** to configure a service object group as a match criterion for an application audit and management policy.

Use **undo service** to delete a service object group match criterion from an application audit and management policy.

Syntax

service *service-name*

undo service [*service-name*]

Default

No service object group is used as a match criterion.

Views

Application audit and management policy view

Predefined user roles

network-admin

context-admin

Parameters

service-name: Specifies an existing service object group by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

You can configure this command multiple times to specify multiple service object groups.

The **undo service** command removes all service object groups from match criteria if you do not specify a service object group or specify the system-defined service object group **any**.

Examples

Specify service object groups **dns-tcp** and **dns-udp** for policy **mypolicy1** to match packets.

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy name mypolicy1 audit
[Sysname-uapp-control-policy-mypolicy1] service dns-tcp
[Sysname-uapp-control-policy-mypolicy1] service dns-udp
```

Related commands

object-group (*Security Command Reference*)

source-address

Use **source-address** to configure a source IP address object group as a match criterion for an application audit and management policy.

Use **undo source-address** to remove a source IP address object group as a match criterion from an application audit and management policy.

Syntax

source-address { **ipv4** | **ipv6** } *object-group-name*

undo source-address { **ipv4** | **ipv6** } *object-group-name*

Default

No source IP address object group is used as a match criterion.

Views

Application audit and management policy view

Predefined user roles

network-admin

context-admin

Parameters

ipv4: Specifies an IPv4 address object group.

ipv6: Specifies an IPv6 address object group.

object-group-name: Specifies an existing address object group by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

You can configure this command multiple times to specify multiple IPv4 or IPv6 address object groups.

Examples

Specify IPv4 address object groups **obgroup1** and **obgroup2** for policy **mypolicy1** to match source IPv4 addresses of packets.

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy name mypolicy audit
[Sysname-uapp-control-policy-mypolicy] source-address ipv4 obgroup1
[Sysname-uapp-control-policy-mypolicy] source-address ipv4 obgroup2
```

Related commands

object-group (*Security Command Reference*)

source-zone

Use **source-zone** to configure a source security zone as a match criterion for an application audit and management policy.

Use **undo source-zone** to delete a source security zone match criterion from an application audit and management policy.

Syntax

source-zone *source-zone-name*

undo source-zone *source-zone-name*

Default

No source security zone is used as a match criterion.

Views

Application audit and management policy view

Predefined user roles

network-admin

context-admin

Parameters

source-zone-name: Specifies a source security zone by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

You can configure this command multiple times to specify multiple source security zones.

Examples

Specify source security zones **zone1** and **zone2** for policy **mypolicy1** to match packets.

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy name mypolicy1 audit
[Sysname-uapp-control-policy-mypolicy1] source-zone zone1
[Sysname-uapp-control-policy-mypolicy1] source-zone zone2
```

Related commands

security-zone name (*Security Command Reference*)

time-range

Use **time-range** to specify a time range during which an application audit and management policy is in effect.

Use **undo time-range** to restore the default.

Syntax

time-range *time-range-name*

undo time-range

Default

An application audit and management policy is in effect at any time.

Views

Application audit and management policy view

Predefined user roles

network-admin

context-admin

Parameters

time-range-name: Specifies a time range by its name, a case-insensitive string of 1 to 32 characters.

Examples

Specify time range **work-time** for policy **mypolicy1**.

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy name mypolicy1 audit
[Sysname-uapp-control-policy-mypolicy1] time-range work-time
```

Related commands

time-range (*ACL and QoS Command Reference*)

uapp-control

Use **uapp-control** to enter application audit and management view.

Use **undo uapp-control** to remove all application audit and management policy settings.

Syntax

uapp-control

undo uapp-control

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

In application audit and management view, you can create, copy, move, and rename application audit and management policies. You can also create keyword groups in this view.

Application audit and management policies have the following types:

- Audit policy.
- Audit-free policy.
- Deny policy.

Audit-free policies and deny policies provide application audit and management at a coarse level of granularity. Audit policies provide more granular application audit and management.

Examples

Enter application audit and management view.

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control]
```

user

Use **user** to configure a user as a match criterion for an application audit and management policy.

Use **undo user** to delete a user match criterion from an application audit and management policy.

Syntax

user *user-name* [**domain** *domain-name*]

undo user *user-name* [**domain** *domain-name*]

Default

No user is used as a match criterion.

Views

Application audit and management policy view

Predefined user roles

network-admin

context-admin

Parameters

user-name: Specifies an identity user by its name, a case-sensitive string of 1 to 55 characters. The username cannot be **a**, **al**, or **all**, and cannot contain the following special characters: \ | / : * ? < > @.

domain *domain-name*: Matches the user in an identity domain. The *domain-name* argument represents the identity domain name, a case-insensitive string of 1 to 255 characters. The domain name cannot contain the following special characters: \ | / : * ? < > @. If you do not specify this option, the system matches the user among users that do not belong to any identity domain. For more information about identity domains, see user identification in *Security Configuration Guide*.

Usage guidelines

You can configure this command multiple times to specify multiple users.

Examples

Specify users **managers1** and **managers2** for policy **mypolicy1** to match packets.

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy name mypolicy1 audit
[Sysname-uapp-control-policy-mypolicy1] user managers1
[Sysname-uapp-control-policy-mypolicy1] user managers2
```

Configure user **managers1** in identity domain **dpi** for policy **mypolicy1** to match packets.

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy name mypolicy1 audit
[Sysname-uapp-control-policy-mypolicy1] user managers1 domain dpi
```

Related commands

user-identity enable (*Security Command Reference*)

user-group

Use **user-group** to configure a user group as a match criterion for an application audit and management policy.

Use **undo user-group** to delete a user group match criterion from an application audit and management policy.

Syntax

user-group *user-group-name* [**domain** *domain-name*]

undo user-group *user-group-name* [**domain** *domain-name*]

Default

No user group is used as a match criterion.

Views

Application audit and management policy view

Predefined user roles

network-admin

context-admin

Parameters

user-group-name: Specifies an identity user group by its name, a case-insensitive string of 1 to 200 characters.

domain *domain-name*: Matches the user group in an identity domain. The *domain-name* argument represents the identity domain name, a case-insensitive string of 1 to 255 characters. The domain name cannot contain the following special characters: \ | / : * ? < > @.If you do not specify this option, the system matches the user group among user groups that do not belong to any identity domain. For more information about identity domains, see user identification in *Security Configuration Guide*.

Usage guidelines

You can configure this command multiple times to specify multiple user groups.

Examples

Specify user groups **group1** and **group2** for policy **mypolicy1** to match packets.

```
<Sysname> system-view
[Sysname-uapp-control] policy name mypolicy1 audit
[Sysname-uapp-control-policy-mypolicy1] user-group group1
[Sysname-uapp-control-policy-mypolicy1] user-group group2
```

Configure user group **group1** in identity domain **dpi** for policy **mypolicy1** to match packets.

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy name mypolicy1 audit
[Sysname-uapp-control-policy-mypolicy1] user-group group1 domain dpi
```

Related commands

user-identity enable (*Security Command Reference*)

Contents

NetShare control commands

action

Use **action** to specify the NetShare control action to take when the number of terminals sharing an IP address exceeds the limit.

Use **undo action** to restore the default.

Syntax

action { **freeze** *freeze-time* | **permit** } [**logging**]

undo action

Default

A NetShare control policy uses the **permit** action.

Views

NetShare control policy view

Predefined user roles

network-admin

context-admin

Parameters

freeze: Freezes the shared IP address so all packets sourced from the IP address will be dropped.

freeze-time: Specifies the time period that an IP address will be frozen, in minutes. The value range for this argument is 2 to 720.

permit: Permits the packets sourced from the IP address to pass through.

logging: Logs the NetShare control event.

Usage guidelines

A NetShare control policy analyzes packets to track the number of terminals sharing the same source IP address. If the number of terminals sharing an IP address exceeds the limit set by using the **per-ip-shared max-terminals** command, the device will take the NetShare control action in the policy.

Examples

Specify the **freeze** action and set the freezing time to 10 minutes in NetShare control policy **abc**.

```
<Sysname> system-view
[Sysname] netshare-control
[Sysname-netshare-control] policy name abc
[Sysname-netshare-control-policy-abc] action freeze 10
```

Related commands

per-ip-shared max-terminals

application-inspect enable

Use **application-inspect enable** to enable APR-based detection.

Use **undo application-inspect enable** to disable APR-based detection.

Syntax

application-inspect enable

undo application-inspect enable

Default

APR-based detection is enabled.

Views

NetShare control policy view

Predefined user roles

network-admin

context-admin

Usage guidelines

APR-based NetShare detection uses the APR signature library to inspect only specific applications, such as QQ and WeChat. If an application is encrypted, APR-based NetShare detection cannot inspect it. As a best practice, enable APR-based detection only when explicitly required, because the detection might degrade the device performance.

You can enable both APR-based detection and IPID trail tracking to detect NetShare behaviors.

Examples

Enable APR-based detection in NetShare control policy **share**.

```
<Sysname> system-view
[Sysname] netshare-control
[Sysname-netshare-control] policy name share
[Sysname-netshare-control-policy-share] application-inspect enable
```

Related commands

ipid-trail enable

description

Use **description** to configure a description for a NetShare control policy.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

No description is configured for a NetShare control policy.

Views

NetShare control policy view

Predefined user roles

network-admin

context-admin

Parameters

text: Configures a description, a case-sensitive string of 1 to 127 characters.

Examples

Configure a description for NetShare control policy **abc**.

```
<Sysname> system-view
[Sysname] netshare-control
[Sysname-netshare-control] policy name abc
[Sysname-netshare-control-policy-abc] description The Netshare Management
```

destination-address

Use **destination-address** to set a destination address filtering criterion in a NetShare control policy.

Use **undo destination-address** to remove a destination address filtering criterion from a NetShare control policy.

Syntax

destination-address { **ipv4** | **ipv6** } *object-group-name*

undo destination-address { **ipv4** | **ipv6** } *object-group-name*

Default

A NetShare control policy does not contain any destination address filtering criterion.

Views

NetShare control policy view

Predefined user roles

network-admin

context-admin

Parameters

ipv4: Specifies an IPv4 address object group.

ipv6: Specifies an IPv6 address object group.

object-group-name: Specifies an address object group by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

You can execute this command multiple times in a NetShare control policy to set multiple destination address filtering criteria. A packet passes the destination address filtering if it matches any of the configured destination address filtering criteria.

Examples

Set IPv4 address object group **obgroup2** as a destination address filtering criterion in NetShare control policy **abc**.

```
<Sysname> system-view
[Sysname] netshare-control
[Sysname-netshare-control] policy name abc
[Sysname-netshare-control-policy-abc] destination-address ipv4 obgroup2
```

Related commands

object-group (*Security Command Reference*)

destination-zone

Use **destination-zone** to set a destination security zone filtering criterion in a NetShare control policy.

Use **undo destination-zone** to remove a destination security zone filtering criterion from a NetShare control policy.

Syntax

destination-zone *destination-zone-name*

undo destination-zone *destination-zone-name*

Default

A NetShare control policy does not contain any destination security zone filtering criterion.

Views

NetShare control policy view

Predefined user roles

network-admin

context-admin

Parameters

destination-zone-name: Specifies a destination security zone by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

You can execute this command multiple times in a NetShare control policy to set multiple destination security zone filtering criteria. A packet passes the destination security zone filtering if it matches any of the configured destination security zone filtering criteria.

Examples

Set security zone **zone2** as a destination security zone filtering criterion in NetShare control policy **abc**.

```
<Sysname> system-view
[Sysname] netshare-control
[sysname-netshare-control] policy name abc
[sysname-netshare-control-policy-abc] destination-zone zone2
```

Related commands

security-zone name (*Security Command Reference*)

disable

Use **disable** to disable a NetShare control policy.

Use **undo disable** to enable a NetShare control policy.

Syntax

disable

undo disable

Default

A NetShare control policy is enabled.

Views

NetShare control policy view

Predefined user roles

network-admin

context-admin

Usage guidelines

The device supports only one NetShare control policy.

After you disable the NetShare control policy, the NetShare control feature becomes invalid.

Examples

Disable NetShare control policy **abc**.

```
<Sysname> system-view
[Sysname] netshare-control
[Sysname-netshare-control] policy name abc
[Sysname-netshare-control-policy-abc] disable
```

display netshare-control

Use **display netshare-control** to display NetShare control information about shared IP addresses.

Syntax

display netshare-control [{ **ipv4** | **ipv6** } *ip-address* | **status** { **frozen** | **unfrozen** }] [**slot** *slot-number*]

Views

Any

Predefined user roles

network-admin

context-admin

Parameters

ipv4: Specifies the IPv4 address type.

ipv6: Specifies the IPv6 address type.

ip-address: Displays NetShare control information about the specified IP address.

status: Specifies the status of the IP addresses to be displayed.

frozen: Displays NetShare control information about frozen IP addresses.

unfrozen: Displays NetShare control information about unfrozen IP addresses.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all member devices.

Usage guidelines

This command displays information about detected IP addresses that are shared by multiple terminals.

Examples

Displays all shared IP addresses in frozen state.

```
<Sysname> display netshare-control status frozen
Slot 1:
  Total frozen shared IP addresses: 2

  IP address     VPN instance  Policy   Terminals   Status    Remaining time  User
  192.168.1.18   vpn1          P1       3           Frozen    20 min          abc
  12.12.12.1     -             P1       4           Frozen    10 min          kwq123
```

Table 1 Command output

Field	Description
Total frozen shared IP addresses	Total number of shared IP address in frozen state.
IP address	Shared IP address.
VPN instance	VPN instance to which the IP address belongs. This field displays a hyphen (-) if the IP address is on the public network.
Policy	Name of the NetShare control policy.
Terminals	Number of terminals sharing the IP address.
Status	Status of the shared IP address: **frozen** or **unfrozen**.
Remaining time	Remaining time before the IP address will be released from the frozen IP address list.
User	User name.

freeze

Use **freeze** to manually freeze an IP address.

Syntax

freeze { **ipv4** | **ipv6** } *ip-address* [**vpn-instance** *vpn-instance-name*] **time** *freeze-time*

Views

NetShare control configuration view

Predefined user roles

network-admin

context-admin

Parameters

ipv4: Specifies the IPv4 address type.

ipv6: Specifies the IPv6 address type.

ip-address: Specifies the IP address to freeze.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If the IP address is on the public network, do not specify this option.

freeze-time: Specifies the time period that the IP address will be frozen, in minutes. The value range is 5 to 720.

Usage guidelines

Use this command to manually freeze an IP address that is shared by terminals. This command is not available for IP addresses that are already on frozen IP address list.

To view the shared IP addresses that can be manually frozen, use the **display netshare-control** command.

Examples

Manually freeze IP address 12.12.12.1 for 15 minutes.

```
<Sysname> system-view
[Sysname] netshare-control
[Sysname-netshare-control] freeze ipv4 12.12.12.1 time 15
```

Related commands

display netshare-control

unfreeze

ipid-trail enable

Use **ipid-trail enable** to enable IPID trail tracking.

Use **undo ipid-trail enable** to disable IPID trail tracking.

Syntax

ipid-trail enable

undo ipid-trail enable

Default

IPID trail tracking is disabled.

Views

NetShare control policy view

Predefined user roles

network-admin

context-admin

Usage guidelines

By default, the device uses the Application Recognition (APR) feature to detect NetShare behaviors. APR-based detection applies only to a limited set of applications in the APR signature library. You can enable IPID trail tracking to meet the NetShare control requirements of various application scenarios.

IPID trail tracking tracks the values of the IPID fields in packets to detect NetShare behaviors. Packets sent by the same host contain incremented IPID values of a unique sequential pattern that starts at a random number. NetShare control tracks the IPID values of packets sourced from the same IP address. In a time period, if the IPID values in the packets belong to the same unique sequential pattern, only one terminal is using the IP address. If the IPID values belong to different sequential patterns, the source IP address is shared by multiple terminals.

You can enable both APR-based detection and IPID trail tracking to detect NetShare behaviors.

IPID trail tracking might degrade the device performance. Enable it only when explicitly required.

IPID trail tracking supports detecting the terminals that are running the Windows system, and detecting packets in which values of the IPID fields change regularly. Mobile terminals are not supported.

IPID trail tracking supports detecting IPv4 packets.

Examples

Enable IPID trail tracking in NetShare control policy **abc**.

```
<Sysname> system-view
[Sysname] netshare-control
[Sysname-netshare-control] policy name abc
[Sysname-netshare-control-policy-abc] ipid-trail enable
```

Related commands

`application-inspect enable`

netshare-control

Use **`netshare-control`** to enter NetShare control configuration view.

Syntax

`netshare-control`

Views

System view

Predefined user roles

network-admin

context-admin

Examples

Enter NetShare control configuration view.

```
<Sysname> system-view
[Sysname] netshare-control
[Sysname-netshare-control]
```

per-ip-shared max-terminals

Use **`per-ip-shared max-terminals`** to set the maximum number of terminals that can share an IP address.

Use **`undo per-ip-shared max-terminals`** to restore the default.

Syntax

`per-ip-shared max-terminals` *number*

`undo per-ip-shared max-terminals`

Default

The number of terminals that can share an IP address is not limited.

Views

NetShare control policy view

Predefined user roles

network-admin

context-admin

Parameters

number: Sets the maximum number of terminals that can share an IP address. The value range is 1 to 15. If you set the value to 1, one IP address can be used by only one terminal.

Usage guidelines

If the number of terminals sharing an IP address exceeds the limit, the device will take the NetShare control action set by using the **action** command in the NetShare control policy.

Examples

Set the maximum number of terminals that can share an IP address to 3 in NetShare control policy **abc**.

```
<sysname> system-view
[sysname] netshare-control
[sysname-netshare-control] policy name abc
[sysname-netshare-control-policy-abc] per-ip-shared max-terminals 3
```

Related commands

action

policy name

Use **policy name** to create a NetShare control policy and enter its view, or enter the view of an existing NetShare control policy.

Use **undo policy name** to delete a NetShare control policy.

Syntax

policy name *policy-name*

undo policy name *policy-name*

Default

No NetShare control policy exists.

Views

NetShare control configuration view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specify a name for the NetShare control policy, a case-insensitive string of 1 to 63 characters.

Usage guidelines

The device supports only one NetShare control policy.

In the NetShare control policy, you can configure the following items:

- The following types of criteria to filter the packets to be analyzed by the NetShare control policy:
  - Source IP address.
  - Destination IP address.
  - Source security zone.

    - Destination security zone.
    - User.
    - User group.
- Maximum number of terminals that can share an IP address.
- Action to take when the number of terminals sharing an IP address exceeds the limit.

Examples

Create NetShare control policy **abc** and enter its view.

```
<Sysname> system-view
[Sysname] netshare-control
[Sysname-netshare-control] policy name abc
[Sysname-netshare-control-policy-abc]
```

source-address

Use **source-address** to set a source address filtering criterion in a NetShare control policy.

Use **undo source-address** to remove a source address filtering criterion from a NetShare control policy.

Syntax

source-address { **ipv4** | **ipv6** } *object-group-name*

undo source-address { **ipv4** | **ipv6** } *object-group-name*

Default

A NetShare control policy does not contain any source address filtering criterion.

Views

NetShare control policy view

Predefined user roles

network-admin

context-admin

Parameters

ipv4: Specifies an IPv4 address object group.

ipv6: Specifies an IPv6 address object group.

object-group-name: Specifies an address object group by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

You can execute this command multiple times in a NetShare control policy to set multiple source address filtering criteria. A packet passes the source address filtering if it matches any of the configured source address filtering criteria.

Examples

Set IPv4 address object group **obgroup1** as a source address filtering criterion in NetShare control policy **abc**.

```
<Sysname> system-view
[Sysname] netshare-control
[Sysname-netshare-control] policy name abc
[Sysname-netshare-control-policy-abc] source-address ipv4 obgroup1
```

Related commands

object-group (*Security Command Reference*)

source-zone

Use **source zone** to set a source security zone filtering criterion in a NetShare control policy.

Use **undo source zone** to remove a source security zone filtering criterion from a NetShare control policy.

Syntax

source-zone *source-zone-name*

undo source-zone *source-zone-name*

Default

A NetShare control policy does not contain any source security zone filtering criterion.

Views

NetShare control policy view

Predefined user roles

network-admin

context-admin

Parameters

source-zone-name: Specifies a source security zone by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

You can execute this command multiple times in a NetShare control policy to set multiple source security zone filtering criteria. A packet passes the source security zone filtering if it matches any of the configured source security zone filtering criteria.

Examples

Set security zone **zone1** as a source security zone filtering criterion in NetShare control policy **abc**.

```
<Sysname> system-view
[Sysname] netshare-control
[Sysname-netshare-control] policy name abc
[Sysname-netshare-control-policy-abc] source-zone zone1
```

Related commands

security-zone name (*Security Command Reference*)

unfreeze

Use **freeze** to manually unfreeze an IP address.

Syntax

unfreeze { **ipv4** | **ipv6** } *ip-address* [**vpn-instance** *vpn-instance-name*]

Views

NetShare control configuration view

Predefined user roles

network-admin

context-admin

Parameters

ipv4: Specifies the IPv4 address type.

ipv6: Specifies the IPv6 address type.

ip-address: Specifies the IP address to unfreeze.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If the IP address is on the public network, do not specify this option.

Usage guidelines

Use this command to manually unfreeze a frozen IP address.

To view the available frozen IP addresses, use the **display netshare-control** command.

Examples

Manually unfreeze IP address 12.12.12.1.

```
<Sysname> system-view
[Sysname] netshare-control
[Sysname-netshare-control] unfreeze ipv4 12.12.12.1
```

Related commands

display netshare-control

user

Use **user** to set a user filtering criterion in a NetShare control policy.

Use **undo user** to remove a user filtering criterion from a NetShare control policy.

Syntax

user *username* [**domain** *domain-name*]

undo user *username* [**domain** *domain-name*]

Default

A NetShare control policy does not contain any user filtering criteria.

Views

NetShare control policy view

Predefined user roles

network-admin

context-admin

Parameters

username: Specify a user name, a case-sensitive string of 1 to 55 characters.

domain *domain-name*: Specifies the name of the identity domain to which the user belongs. The identity domain name is a case-insensitive string of 1 to 255 characters which cannot contain question marks (?). If the user name does not belong to any identity domains, do not specify this

option. For more information about identity domains, see user identification configuration in *Security Configuration Guide*.

Usage guidelines

You can execute this command multiple times in a NetShare control policy to set multiple user filtering criteria. A packet passes the user filtering if it matches any of the configured user filtering criteria.

Examples

Set user **managers** as a user filtering criterion in NetShare control policy **abc**.

```
<sysname> system-view
[sysname] netshare-control
[sysname-netshare-control] policy name abc
[sysname-netshare-control-policy-abc] user managers
```

Related commands

user-identity enable (*Security Command Reference*)

user-group

Use **user-group** to set a user group filtering criterion in a NetShare control policy.

Use **undo user-group** to remove a user group filtering criterion from a NetShare control policy.

Syntax

user-group *user-group-name* [**domain** *domain-name*]

undo user-group *user-group-name* [**domain** *domain-name*]

Default

A NetShare control policy does not contain any user group filtering criteria.

Views

NetShare control policy view

Predefined user roles

network-admin

context-admin

Parameters

user-group-name: Specify a user group by its name, a case-sensitive string of 1 to 32 characters.

domain *domain-name*: Specifies the name of the identity domain to which the user group belongs. The identity domain name is a case-insensitive string of 1 to 255 characters which cannot contain question marks (?). If the user group does not belong to any identity domains, do not specify this option. For more information about identity domains, see user identification configuration in *Security Configuration Guide*.

Usage guidelines

You can execute this command multiple times in a NetShare control policy to set multiple user group filtering criteria. A packet passes the user group filtering if it matches any of the configured user group filtering criteria.

Examples

Set user group **group1** as a user group filtering criterion in NetShare control policy **abc**.

```
<sysname> system-view
[sysname] netshare-control
[sysname-netshare-control] policy name abc
[sysname-netshare-control-policy-abc] user-group group1
```

Related commands

identity-group (*Security Command Reference*)

NSFOCUS Firewall Series

NF Load Balancing

Command Reference

NSFOCUS Technologies, Inc.

Document version: 6W600-20230221

Preface

This command reference describes the commands for configuring load balancing.

This preface includes the following topics about the documentation:

- Audience.
- Conventions.

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators.

Conventions

The following information describes the conventions used in the documentation.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select a minimum of one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
CAUTION:	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Contents

Load balancing commands

The following compatibility matrixes show the support of hardware platforms for server load balancing:

Models	Server load balancing compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	Yes
NFNX3-HDB680, NFNX3-HDB1080	No

activate (link group view)

Use **activate** to set the criteria to determine whether a link group is available.

Use **undo activate** to restore the default.

Syntax

activate lower *lower-percentage* **upper** *upper-percentage*

undo activate

Default

A link group is available when a minimum of one link is available.

Views

Link group view

Predefined user roles

network-admin

context-admin

Parameters

lower *lower-percentage*: Specifies the lower percentage value in the range of 1 to 99.

upper *upper-percentage*: Specifies the upper percentage value in the range of 1 to 99. The upper percentage value must be greater than or equal to the lower percentage value.

Usage guidelines

When the percentage of available links in a primary link group is smaller than the lower percentage value, the primary link group becomes unavailable. Then the backup link group takes over. When the percentage of available links in a primary link group is greater than the upper percentage value, the primary link group becomes available again to process services.

If no backup link group is configured on the virtual server, this configuration does not take effect.

Examples

Set the lower percentage value to 20 and upper percentage value to 80 for the link group **lg**.

```
<Sysname> system-view
[Sysname] loadbalance link-group lg
[Sysname-lb-lgroup-lg] activate lower 20 upper 80
```

activate (server farm view)

Use **activate** to set the criteria to determine whether a server farm is available.

Use **undo activate** to restore the default.

Syntax

activate lower *lower-percentage* **upper** *upper-percentage*

undo activate

Default

A server farm is available when a minimum of one real server is available.

Views

Server farm view

Predefined user roles

network-admin

context-admin

Parameters

lower *lower-percentage*: Specifies the lower percentage value in the range of 1 to 99. When the percentage of available real servers in the primary server farm is lower than the lower percentage value, the primary server farm becomes unavailable. Then the backup server farm takes over.

upper *upper-percentage*: Specifies the upper percentage value in the range of 1 to 99. The upper percentage value must be higher than or equal to the lower percentage value. When the percentage of available real servers in the primary server farm is higher than the upper percentage value, the primary server farm becomes available again to process services.

Usage guidelines

If no backup server farm is configured on the virtual server, this configuration does not take effect.

Examples

Set the lower percentage value to 20 and upper percentage value to 80 for the server farm **sf**.

```
<Sysname> system-view
[Sysname] server-farm sf
[Sysname-sfarm-sf] activate lower 20 upper 80
```

Related commands

default server-farm

application-mode enable

Use **application-mode enable** to configure a TCP virtual server to operate at Layer 7.

Use **undo application-mode enable** to restore the default.

Syntax

application-mode enable

undo application-mode enable

Default

A TCP virtual server operates at Layer 4.

Views

TCP virtual server view

Predefined user roles

network-admin

context-admin

Examples

Configure TCP virtual server **vs** to operate at Layer 7.

```
<Sysname> system-view
[Sysname] virtual-server vs type tcp
[Sysname-vs-tcp-vs] application-mode enable
```

argument

Use **argument** to configure user-defined information for a custom-monitoring LB probe template.

Use **undo argument** to restore the default.

Syntax

argument *text*

undo argument

Default

No user-defined information is configured for a custom-monitoring LB probe template.

Views

Custom-monitoring LB probe template view

Predefined user roles

network-admin

context-admin

Parameters

text: Specifies an information text, a case-sensitive string of 1 to 255 characters. The string can contain spaces and cannot contain quotation marks (").

Usage guidelines

When executing the script file used for custom monitoring, the device transfers the information text to the script file as a parameter.

You can configure multiple arguments separated by spaces as the user-defined information.

Examples

In custom-monitoring LB probe template **test_external**, configure user-defined information as **abc 123 456**.

```
<Sysname> system-view
[Sysname] loadbalance probe-template external-monitor test_external
[Sysname-lbpt-external-monitor-test_external] argument abc 123 456
```

arp-nd interface (SNAT address pool view)

Use **arp-nd interface** to specify an interface for sending gratuitous ARP packets and ND packets.

Use **undo arp-nd interface** to disable an interface from sending gratuitous ARP packets and ND packets.

Syntax

arp-nd interface *interface-type interface-number*

undo arp-nd interface *interface-type interface-number*

Default

No interface is specified for sending gratuitous ARP packets and ND packets. No interface can send gratuitous ARP packets or ND packets.

Views

SNAT address pool view

Predefined user roles

network-admin

context-admin

Parameters

*interface-type interface-numbe*r: Specifies an interface by its type and number.

Usage guidelines

You can execute this command multiple times to specify multiple interfaces for one SNAT address pool.

Examples

For SNAT address pool **lbsp**, specify GigabitEthernet 1/0/1 as the interface for sending gratuitous ARP packets and ND packets.

```
<Sysname> system-view
[Sysname] loadbalance snat-pool lbsp
[Sysname-lbsnat-pool-lbsp] arp-nd interface gigabitethernet 1/0/1
```

arp-nd interface (virtual server view)

Use **arp-nd interface** to specify an interface for sending gratuitous ARP packets and ND packets.

Use **undo arp-nd interface** to disable an interface from sending gratuitous ARP packets and ND packets.

Syntax

arp-nd interface *interface-type interface-number*

undo arp-nd interface *interface-type interface-number*

Default

No interface is specified for sending gratuitous ARP packets and ND packets. No interface can send gratuitous ARP packets or ND packets.

Views

Virtual server view

Predefined user roles

network-admin

context-admin

Parameters

*interface-type interface-numbe*r: Specifies an interface by its type and number.

Usage guidelines

You can execute this command multiple times to specify multiple interfaces for one virtual server.

Examples

For virtual server **vs3**, specify GigabitEthernet 1/0/1 as the interface for sending gratuitous ARP packets and ND packets.

```
<Sysname> system-view
[Sysname] virtual-server vs3 type ip
[Sysname-vs-ip-vs3] arp-nd interface gigabitethernet 1/0/1
```

auto-alloc address

Use **auto-alloc address** to enable the device to automatically obtain the IP address of a DNS server.

Use **undo auto-alloc address** to disable the device from automatically obtaining the IP address of a DNS server.

Syntax

auto-alloc address

undo auto-alloc address

Default

The device is disabled from automatically obtaining the IP address of a DNS server.

Views

DNS server view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command is mutually exclusive with the **ip address** and **ipv6 address** commands.

Before configuring this command, you must configure the **router interface** command. Otherwise, the IP address of the DNS server cannot be obtained.

If the device obtains multiple DNS server IP addresses, it uses the smallest available IP address.

Examples

Enable the device to automatically obtain the IP address of DNS server **ds1**.

```
<Sysname> system-view
[Sysname] loadbalance dns-server ds1
[Sysname-lb-ds-ds1] auto-alloc address
```

Related commands

display loadbalance dns-server

auto-shutdown recovery-time

Use **auto-shutdown recovery-time** to set the automatic recovery time for intelligent monitoring.

Use **undo auto-shutdown recovery-time** to restore the default.

Syntax

auto-shutdown recovery-time *recovery-time*

undo auto-shutdown recovery-time

Default

The automatic recovery time is 0 minutes.

Views

Server farm view

Predefined user roles

network-admin

context-admin

Parameters

recovery-time: Specifies the automatic recovery time in the range of 0 to 15300 minutes. The value of 0 means that a server farm member placed in Auto shutdown state does not automatically recover.

Usage guidelines

Use this command to enable automatic recovery for a real server that is shut down by intelligent monitoring.

If health monitoring is not configured, a recovered real server is set to Unknown state.

If health monitoring is configured and succeeds, a recovered real server is set to Active state. If health monitoring fails, a recovered real server is set to Probe-failed state.

Examples

Set the automatic recovery time to 5 minutes for server farm **sf**.

```
<Sysname> system-view
[Sysname] server-farm sf
[Sysname-sfarm-sf] auto-shutdown recovery-time 5
```

bandwidth busy-protection enable (transparent DNS proxy view)

Use **bandwidth busy-protection enable** to enable the link protection feature for a transparent DNS proxy.

Use **undo bandwidth busy-protection enable** to disable the link protection feature for a transparent DNS proxy.

Syntax

bandwidth busy-protection enable

undo bandwidth busy-protection enable

Default

The link protection feature is disabled for a transparent DNS proxy.

Views

Transparent DNS proxy view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command enables a transparent DNS proxy to select a DNS server from the DNS server pool based on the link bandwidth ratio. If the bandwidth ratio of a link exceeds the specified value, the corresponding DNS server is not selected.

If the link bandwidth ratio of all DNS servers in the DNS server pool exceeds the specified value, the link protection feature is automatically disabled. If the link bandwidth ratio of any DNS server drops below the specified value, the link protection feature is automatically enabled, and the corresponding DNS server is selected.

Examples

Enable the link protection feature for transparent DNS proxy **dns-proxy1**.

```
<Sysname> system-view
[Sysname] loadbalance dns-proxy dns-proxy1
[Sysname-lb-dp-udp-dns-proxy1] bandwidth busy-protection enable
```

Related commands

bandwidth busy-rate (link view)

bandwidth busy-protection enable (virtual server pool view)

Use **bandwidth busy-protection enable** to enable the link protection feature for a virtual server pool.

Use **undo bandwidth busy-protection enable** to disable the link protection feature for a virtual server pool.

Syntax

bandwidth busy-protection enable

undo bandwidth busy-protection enable

Default

The link protection feature is disabled for a virtual server pool.

Views

Virtual server pool view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command enables a virtual server pool to select a virtual server based on the link bandwidth ratio. If the bandwidth ratio of a link is exceeded, the virtual server is not selected.

Examples

Enable the link protection feature for the virtual server pool **local-pool**.

```
<Sysname> system-view
[Sysname] loadbalance virtual-server-pool local-pool
[Sysname-lb-vspool-local-pool] bandwidth busy-protection enable
```

Related commands

bandwidth busy-rate (link view)

bandwidth busy-protection enable (virtual server view)

Use **bandwidth busy-protection enable** to enable the link protection feature.

Use **undo bandwidth busy-protection enable** to disable the link protection feature.

Syntax

bandwidth busy-protection enable

undo bandwidth busy-protection enable

Default

The link protection feature is disabled.

Views

Virtual server view

Predefined user roles

network-admin

context-admin

Usage guidelines

The link protection feature limits packets that exceed the bandwidth busy rate in the inbound or outbound direction of a link. When a link is busy in only the outbound direction, new traffic (traffic that does not match any sticky entry) is not distributed to the link. However, existing traffic is still distributed to the link. When a link is busy in only the inbound direction, new traffic can be distributed to the link.

When a link becomes busy in at least one direction, the link state becomes busy. When a link is not busy in both directions, the link sate is normal.

The link protection feature takes effect only when bandwidth statistics collection by interfaces is enabled.

Examples

Enable the link protection feature for the IP-type virtual server **vs3**.

```
<Sysname>system-view
[Sysname] virtual-server vs3 type ip
[Sysname-vs-ip-vs3] bandwidth busy-protection enable
```

Related commands

bandwidth interface statistics enable

bandwidth busy-rate

Use **bandwidth busy-rate** to set the bandwidth ratio for an LB link.

Use **undo bandwidth busy-rate** to restore the default.

Syntax

bandwidth [**inbound** | **outbound**] **busy-rate** *busy-rate-number* [**recovery** *recovery-rate-number*]

undo bandwidth [**inbound** | **outbound**] **busy-rate**

Default

The bandwidth ratio is 70.

Views

LB link view

Predefined user roles

network-admin

context-admin

Parameters

inbound: Specifies the inbound bandwidth ratio.

outbound: Specifies the outbound bandwidth ratio.

busy-rate-number: Specifies bandwidth ratio in the range of 1 to 100.

recovery *recovery-rate-number*: Specifies bandwidth recovery ratio in the range of 1 to 100. By default, if the bandwidth ratio is greater than 10, the bandwidth recovery ratio equals the bandwidth ratio minus 10; if the bandwidth ratio is smaller than or equal to 10, the bandwidth recovery ratio equals the bandwidth ratio.

Usage guidelines

If the bandwidth of an LB link exceeds the maximum expected bandwidth multiplied by the bandwidth ratio, the LB link is busy and will not be selected. If the bandwidth of the LB link drops below the maximum expected bandwidth multiplied by the bandwidth recovery ratio, the LB link participates in scheduling again.

If you do not specify the **inbound** or **outbound** keyword, this command sets the total bandwidth ratio.

The bandwidth ratio equals the current bandwidth divided by the maximum bandwidth of the LB link. If the maximum bandwidth is not limited, the supported maximum bandwidth is used for calculating the bandwidth ratio.

The bandwidth recovery ratio must be smaller than or equal to the bandwidth ratio of an LB link.

This command takes effect only on new sessions and does not take effect on existing sessions.

Examples

Set the total bandwidth ratio and bandwidth recovery ratio for the LB link **lk1** to 90 and 85.

```
<Sysname> system-view
[Sysname] loadbalance link lk1
[Sysname-lb-link-link1] bandwidth busy-rate 90 recovery 85
```

Related commands

display loadbalance link

max-bandwidth (link view)

bandwidth interface statistics enable

Use **bandwidth interface statistics enable** to enable bandwidth statistics collection by interfaces.

Use **undo bandwidth interface statistics enable** to disable bandwidth statistics collection by interfaces.

Syntax

bandwidth interface statistics enable

undo bandwidth interface statistics enable

Default

Bandwidth statistics collection by interfaces is disabled.

Views

Virtual server view

Predefined user roles

network-admin

context-admin

Examples

Enable bandwidth statistics collection by interfaces for the IP-type virtual server **vs3**.

```
<Sysname> system-view
[Sysname] virtual-server vs3 type ip
[Sysname-vs-ip-vs3] bandwidth interface statistics enable
```

bandwidth weight

Use **bandwidth weight** to set the bandwidth weight for proximity calculation.

Use **undo bandwidth weight** to restore the default.

Syntax

bandwidth { **inbound** | **outbound** } **weight** *bandwidth-weight*

undo bandwidth { **inbound** | **outbound** } **weight**

Default

The inbound or outbound bandwidth weight for proximity calculation is 100.

Views

Proximity view

Predefined user roles

network-admin

context-admin

Parameters

inbound: Specifies the inbound bandwidth weight.

outbound: Specifies the outbound bandwidth weight.

bandwidth-weight: Specifies the bandwidth weight for proximity calculation, in the range of 0 to 255. A larger value indicates a higher bandwidth weight.

Examples

Set the inbound bandwidth weight for proximity calculation to 200.

```
<Sysname> system-view
[Sysname] loadbalance proximity
[Sysname-lb-proximity] bandwidth inbound weight 200
```

Set the outbound bandwidth weight for proximity calculation to 200.

```
<Sysname> system-view
[Sysname] loadbalance proximity
[Sysname-lb-proximity] bandwidth outbound weight 200
```

busy-action

Use **busy-action** to configure the action to take when a server farm is busy.

Use **undo busy-action** to restore the default.

Syntax

busy-action { **drop** | **enqueue length** *length* **timeout** *timeout-value* | **force** }

undo busy-action

Default

The default action is **drop**.

Views

Server farm view

Predefined user roles

network-admin

context-admin

Parameters

drop: Stops assigning client requests to the server farm.

enqueue: Assigns new client requests to a wait queue.

length *length*: Specifies the maximum number of client requests allowed in the wait queue, in the range of 1 to 100000. When the queue is full, new client requests are dropped.

timeout *timeout-value*: Specifies the aging time for the wait queue, in the range of 1 to 60 seconds.

force: Forcibly assigns client requests to all real servers in the server farm.

Usage guidelines

For the **drop** action, if the LB policy for the server farm contains the action of matching the next rule, the device compares client requests with the next rule. Otherwise, the device drops the client requests.

Examples

Configure the action to take when a server farm is busy as **force**.

```
<Sysname> system-view
[Sysname] server-farm sf
```

```
[Sysname-sfarm-sf] busy-action force
```

busy-action continue

Use **busy-action continue** to configure the action of matching the next rule when all links or DNS servers are busy.

Use **undo busy-action** to restore the default.

Syntax

busy-action continue

undo busy-action

Default

The device assigns packets to links or DNS servers regardless of whether they are busy.

Views

Link-generic LB action view

DNS server LB action view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command enables the device to match the next rule when all links or DNS servers are busy.

Examples

Configure link-generic LB action **a1** to match the next rule when all links or DNS servers are busy.

```
<Sysname> system-view
[Sysname] loadbalance action a1 type link-generic
[Sysname-lba-link-generic-a1] busy-action continue
```

case-insensitive

Use **case-insensitive** to disable case sensitivity for matching character strings.

Use **undo case-insensitive** to restore the default.

Syntax

case-insensitive

undo case-insensitive

Default

Case sensitivity is enabled for matching character strings.

Views

HTTP parameter profile view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command affects the following content:

- HTTP header value, HTTP cookie name and value, and URL for matching classes.
- Header value, URL, and key value used for generating sticky entries for the HTTP header sticky method.
- Cookie name and value and key value used for generating sticky entries for the cookie get sticky method.

Examples

Disable case sensitivity for the HTTP-type parameter profile **pp1**.

```
<Sysname> system-view
[Sysname] parameter-profile pp1 type http
[Sysname-para-http-pp1] case-insensitive
```

check all-packet

Use **check all-packet** to enable checking for all packets.

Use **undo check all-packet** to restore the default.

Syntax

check all-packet

undo check all-packet

Default

Checking for all packets is disabled.

Views

HTTP cookie sticky group view

HTTP passive sticky group view

Predefined user roles

network-admin

context-admin

Usage guidelines

If the sticky method is cookie get, use this command to get cookies from all HTTP response packets. If this command is not executed, the device gets only the Set-Cookie from the first response packet of a connection.

If the sticky method is cookie rewrite, use this command to rewrite cookies in all HTTP response packets. If this command is not executed, the device rewrites only the Set-Cookie in the first response packet of a connection.

If the sticky method is cookie insert, use this command to insert cookies to all HTTP response packets. If this command is not executed, the device inserts only the Set-Cookie to the first response packet of a connection.

If the sticky method is HTTP passive, use this command to generate sticky entries from all HTTP response packets. If this command is not executed, the device generates sticky entries only from the first response packet of a connection.

Examples

Enable checking for all packets in the HTTP cookie sticky group **sg3**.

```
<Sysname> system-view
```

```
[Sysname] sticky-group sg3 type http-cookie
[Sysname-sticky-http-cookie-sg3] check all-packet
```

check-url

Use **check-url** to configure a URL regular expression to match URLs for an HTTP passive LB probe template.

Use **undo check-url** to remove the URL regular expression configuration.

Syntax

check-url *url*

undo check-url *url*

Default

No URL regular expression is configured.

Views

HTTP passive LB probe template view

Predefined user roles

network-admin

context-admin

Parameters

url: Specifies a URL regular expression, a case-insensitive string of 1 to 255 characters. The string cannot contain question marks (?).

Usage guidelines

If an HTTP request carries one of the specified URLs, the device examines whether a URL error occurs in the HTTP response.

You can configure a maximum of 10 URL regular expressions for one HTTP passive LB probe template.

Examples

Configure **www.abc.com** as a matching URL for HTTP passive LB probe template **tplt**.

```
<Sysname> system-view
[Sysname] loadbalance probe-template http-passive tplt
[Sysname-lbpt-http-passive-tplt] check-url www.abc.com
```

class

Use **class** to specify an LB action for the specified LB class.

Use **undo class** to delete an LB class.

Syntax

class *class-name* [**insert-before** *before-class-name* | **insert-after** [*after-class-name*]] **action** *action-name*

undo class *class-name*

Default

No LB action is specified for the LB class.

Views

LB policy view

Predefined user roles

network-admin

context-admin

Parameters

class-name: Specifies an LB class by its name, a case-insensitive string of 1 to 63 characters.

insert-before: Inserts the target class before an LB class (which must already be referenced by the current LB policy).

before-class-name: Specifies an LB class by its name, a case-insensitive string of 1 to 63 characters.

insert-after: Inserts the target class after an LB class (which must already be referenced by the current LB policy).

after-class-name: Specifies an LB class by its name, a case-insensitive string of 1 to 63 characters.

action-name: Specifies an LB action by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

This command sets an LB action for packets matching the specified LB class.

If you specify both the **insert-before** and **insert-after** keywords, the command inserts the target LB class after all LB classes.

You can specify an LB action for different LB classes.

A DNS LB policy can reference DNS LB actions only; a generic LB policy can reference generic LB classes and generic LB actions only. This rule does not apply to HTTP LB policies.

Examples

Specify the LB action **lba1** for the LB class **lbc1** in the generic LB policy **lbp1**, and insert **lbc1** before the LB class **lbc0**.

```
<Sysname> system-view
[Sysname] loadbalance policy lbp1 type generic
[Sysname-lbp-generic-lbp1] class lbc1 insert-before lbc0 action lba1
```

compression level

Use **compression level** to set the compression level for response packets.

Use **undo compression level** to restore the default.

Syntax

compression level *level*

undo compression level

Default

The compression level for response packets is 1.

Views

HTTP-compression parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

level: Specifies the compression level in the range of 1 to 9. A larger value indicates a lower compression speed and a higher compression ratio.

Examples

Create the HTTP-compression parameter profile **pa1**, and set the compression level to 6.

```
<Sysname> system-view
[Sysname] parameter-profile pa1 type http-compress
[Sysname-para-http-compress-pa1] compression level 6
```

connection-limit max (link group member view)

Use **connection-limit max** to set the maximum number of connections of a link group member.

Use **undo connection-limit max** to restore the default.

Syntax

connection-limit max *max-number*

undo connection-limit max

Default

The maximum number of connections of a link is 0, which means the number is not limited.

Views

Link group member view

Predefined user roles

network-admin

context-admin

Parameters

max-number: Specifies the maximum number of connections, in the range of 0 to 4294967295. If the value of this argument takes 0, the number is not limited.

Examples

Set the maximum number of connections of the link group member **lk1** to 10000.

```
<Sysname> system-view
[Sysname] loadbalance link-group lg
[Sysname-lb-lgroup-lg] link lk1
[Sysname-lb-lgroup-lg-#member#-lk1] connection-limit max 10000
```

connection-limit max (link view)

Use **connection-limit max** to set the maximum number of connections of a link.

Use **undo connection-limit max** to restore the default.

Syntax

connection-limit max *max-number*

undo connection-limit max

Default

The maximum number of connections of a link is 0, which means the number is not limited.

Views

Link view

Predefined user roles

network-admin

context-admin

Parameters

max-number: Specifies the maximum number of connections, in the range of 0 to 4294967295. If the value of this argument takes 0, the number is not limited.

Usage guidelines

This command takes effect only on new sessions and does not take effect on existing sessions.

Examples

Set the maximum number of connections of the link **lk** to 10000.

```
<Sysname> system-view
[Sysname] loadbalance link lk
[Sysname-lb-link-lk] connection-limit max 10000
```

connection-limit max (real server view)

Use **connection-limit max** to set the maximum number of connections of a real server.

Use **undo connection-limit max** to restore the default.

Syntax

connection-limit max *max-number*

undo connection-limit max

Default

The maximum number of connections of a real server is 0, which means the number is not limited.

Views

Real server view

Predefined user roles

network-admin

context-admin

Parameters

max-number: Specifies the maximum number of connections, in the range of 0 to 4294967295. If the value of this argument takes 0, the number is not limited.

Usage guidelines

This command takes effect only on new sessions and does not take effect on existing sessions.

Examples

Set the maximum number of connections of the real server **rs** to 10000.

```
<Sysname> system-view
[Sysname] real-server rs
[Sysname-rserver-rs] connection-limit max 10000
```

connection-limit max (server farm member view)

Use **connection-limit max** to set the maximum number of connections of a server farm member.

Use **undo connection-limit max** to restore the default.

Syntax

connection-limit max *max-number*

undo connection-limit max

Default

The maximum number of connections of a link is 0, which means the number is not limited.

Views

Server farm member view

Predefined user roles

network-admin

context-admin

Parameters

max-number: Specifies the maximum number of connections, in the range of 0 to 4294967295. If the value of this argument takes 0, the number is not limited.

Examples

Set the maximum number of connections of the server farm member **rs1** to 10000.

```
<Sysname> system-view
[Sysname] server-farm sf
[Sysname-sfarm-sf] real-server rs1 port 80
[Sysname -sfarm-sf-#member#-rs1-port-80] connection-limit max 10000
```

connection-limit max (virtual server view)

Use **connection-limit max** to set the maximum number of connections of a virtual server.

Use **undo connection-limit max** to restore the default.

Syntax

connection-limit max *max-number*

undo connection-limit max

Default

The maximum number of connections of a virtual server is 0, which means the number is not limited.

Views

Virtual server view

Predefined user roles

network-admin

context-admin

Parameters

max-number: Specifies the maximum number of connections, in the range of 0 to 4294967295. If the value of this argument takes 0, the number is not limited.

Usage guidelines

This command takes effect only on new sessions and does not take effect on existing sessions.

Examples

Set the maximum number of connections for the IP-type virtual server **vs3** to 10000.

```
<Sysname> system-view
[Sysname] virtual-server vs3 type ip
[Sysname-vs-ip-vs3] connection-limit max 10000
```

connection-sync enable (transparent DNS proxy view)

Use **connection-sync enable** to enable session extension information synchronization for a transparent DNS proxy.

Use **undo connection-sync enable** to disable session extension information synchronization for a transparent DNS proxy.

Syntax

connection-sync enable

undo connection-sync enable

Default

Session extension information synchronization is disabled for a transparent DNS proxy.

Views

Transparent DNS proxy view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command can back up session information to ensure service continuity during a master and backup switchover in hot backup mode.

Examples

Enable session extension information synchronization for the transparent DNS proxy **dns_proxy1**.

```
<Sysname>system-view
[Sysname] loadbalance dns-proxy dns-proxy1
[Sysname-lb-dp-udp-dns-proxy1] connection-sync enable
```

connection-sync enable (virtual server view)

Use **connection-sync enable** to enable session extension information synchronization for a virtual server.

Use **undo connection-sync enable** to disable session extension information synchronization for a virtual server.

Syntax

connection-sync enable

undo connection-sync enable

Default

Session extension information synchronization is disabled for a virtual server.

Views

Virtual server view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command is not supported by the virtual servers of the HTTP type.

Examples

Enable session extension information synchronization for the IP-type virtual server **vs3**.

```
<Sysname>system-view
[Sysname] virtual-server vs3 type ip
[Sysname-vs-ip-vs3] connection-sync enable
```

content (HTTP content sticky group view)

Use **content** to configure the HTTP entity sticky method.

Use **undo content** to delete the HTTP entity sticky method.

Syntax

content [**offset** *offset*] [**start** *start-string*] [**end** *end-string* | **length** *length*]

undo content

Default

No sticky methods exist.

Views

HTTP entity sticky group view

Predefined user roles

network-admin

context-admin

Parameters

offset *offset*: Specifies the offset value of the entity based on the start of the HTTP packet, in the range of 0 to 1000 bytes. The default is 0.

start *start-string*: Specifies the regular expression that marks the start of the entity, a case-sensitive string of 1 to 127 characters starting from the *offset* value. The string cannot contain question marks (?).

end *end-string*: Specifies the regular expression that marks the end of the entity, a case-sensitive string of 1 to 127 characters starting from the *start-string* value. The string cannot contain question marks (?).

length *length*: Specifies the length of the entity, in the range of 0 to 1000 bytes. The default is 0, which indicates all lengths.

Usage guidelines

Use this command to obtain the HTTP entity information used to generate sticky entries based on the *offset*, *start-string*, *end-string*, and *length* values. The *start-string* and *end-string* values are not included in the sticky entry information.

The HTTP entity sticky method applies only to contents within the entity. The HTTP entity sticky method does not apply to chunk and multipart entity content.

The HTTP entity sticky method is not supported by the virtual servers of the fast HTTP type.

Examples

Configure the HTTP entity sticky method for the HTTP entity sticky group **sg2**: Starting from the 30th byte of start of the HTTP packet, use the 20-byte HTTP entity with **abc** as the start string to generate sticky entries.

```
<Sysname> system-view
[Sysname] sticky-group sg2 type http-content
[Sysname-sticky-http-content-sg2] content offset 30 start abc length 20
```

content (HTTP passive sticky group view)

Use **content** to configure the HTTP passive entity sticky method.

Use **undo content** to delete the HTTP passive entity sticky method.

Syntax

content { **get** | **match** } *id* **start** *start-string* { **end** *end-string* | **length** *length* }

undo content { **get** | **match** } *id*

Default

No sticky methods exist.

Views

HTTP passive sticky group view

Predefined user roles

network-admin

context-admin

Parameters

get: Obtains the specified string in the HTTP response entity, which is used to generate a sticky entry.

match: Obtains the specified string in the HTTP request entity, which is used to match a sticky entry.

id: Specifies the string ID in the range of 1 to 4.

start *start-string*: Specifies the regular expression that marks the start of the entity, a case-sensitive string of 1 to 127 characters. The string cannot contain question marks (?).

end *end-string*: Specifies the regular expression that marks the end of the entity, a case-sensitive string of 1 to 127 characters starting from the *start-string* value. The string cannot contain question marks (?).

length *length*: Specifies the length of the entity, in the range of 0 to 1000 bytes. The default is 0, which indicates all lengths.

Usage guidelines

The *start-string* and *end-string* values are not included in the sticky entry information.

Both the **content get** and **content match** commands are required for an HTTP passive sticky method.

The device obtains the content information of an incoming HTTP request based on the **content match** command and obtains the content information of an incoming HTTP response based on the **content get** command. If the content information of the HTTP request matches the content information of the HTTP response, the device generates a sticky entry based on the content information of the HTTP response. Subsequent HTTP requests that match the sticky entry are forwarded according to the sticky entry.

The following rules apply to use of the **content match** and **content get** commands:

- You can execute a maximum of four **content get** commands and four **content match** commands for one HTTP passive sticky method.
- A number of *n* strings that are obtained based on *n* **content get** commands generates 2^n-1 strings in ascending order of string IDs. If the string obtained based on the **content match** command matches any one of these generated strings, the match is successful.
- A number of *n* strings that are obtained based on *n* **content match** commands combine as one string in ascending order of string IDs.

For example, three **content get** commands are executed with string IDs 1, 2, and 3. The device obtains three strings a, b, and c in the HTTP response header, generates seven strings a, b, c, ab, ac, bc, and abc, and generates seven sticky entries. Then, three **content match** commands are executed with string IDs 2, 3, and 4. The device obtains three strings a, b, and c in the HTTP request header and generates one string abc. If the string matches one of the seven strings, the device generates a sticky entry based on the string abc. Subsequent HTTP requests that match the sticky entry are forwarded according to the sticky entry.

Examples

Configure the HTTP passive sticky method for the HTTP passive sticky group **sg2**: Obtain the 20-byte HTTP entity string starting with **abc** in the HTTP response. If the string matches the 20-byte HTTP entity string starting with **xxx** in the HTTP request, the device generates a sticky entry based on the string obtained from the HTTP response.

```
<Sysname> system-view
[Sysname] sticky-group sg2 type http-passive
[Sysname-sticky-http-passive-sg2] content get 1 start abc length 20
[Sysname-sticky-http-passive-sg2] content match 1 start xxx length 20
```

Related commands

display sticky-group

header (HTTP passive sticky group view)

content length-threshold

Use **content length-threshold** to set the minimum length of HTTP response content for compression.

Use **undo content length-threshold** to restore the default.

Syntax

content length-threshold *length*

undo content length-threshold

Default

The minimum length of HTTP response content for compression is 1024 bytes.

Views

HTTP-compression parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

length: Specifies the minimum length of HTTP response content for compression, in the range of 0 to 4294967295 bytes.

Usage guidelines

If an HTTP response packet contains the Content-Length header, the packet content is compressed only when its length reaches the minimum length of HTTP response content for compression. If the HTTP response packet does not contain the Content-Length header, the configuration does not take effect. The packet content is compressed regardless of its length.

Examples

Create the HTTP-compression parameter profile **http1**, and set the minimum length of HTTP response content for compression to 2000 bytes.

```
<Sysname> system-view
[Sysname] parameter-profile http1 type http-compression
[Sysname-para-http-compression-http1] content length-threshold 2000
```

content maxparse-length

Use **content maxparse-length** to set the maximum length of HTTP entities that can be parsed.

Use **undo content maxparse-length** to restore the default.

Syntax

content maxparse-length *length*

undo content maxparse-length

Default

The maximum length of HTTP entities that can be parsed is 4096.

Views

HTTP parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

length: Specifies the maximum length of HTTP entities that can be parsed, in the range of 1 to 65535 bytes.

Usage guidelines

This command is not supported by the virtual servers of the fast HTTP type.

Examples

Set the maximum length of HTTP entities that can be parsed to 8192 for the HTTP parameter profile **pp1**.

```
<Sysname> system-view
[Sysname] parameter-profile pp1 type http
[Sysname-para-http-pp1] content maxparse-length 8192
```

content request-max-length

Use **content request-max-length** to set the maximum size of the HTTP content.

Use **undo content request-max-length** to restore the default.

Syntax

content request-max-length *length*

undo content request-max-length

Default

The size of the HTTP content is not limited.

Views

HTTP parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

length: Specifies the maximum size of the HTTP content, in the range of 1 to 4294967295 bytes.

Usage guidelines

If the size of the HTTP content in an HTTP request exceeds the specified maximum size, the device discards the HTTP request.

Examples

Set the maximum size of the HTTP content to 1000 for the HTTP parameter profile **h1**.

```
<Sysname> system-view
[Sysname] parameter h1 type http
[Sysname-para-http-h1] content request-max-length 1000
```

content rewrite

Use **content rewrite** to rewrite the content of HTTP responses.

Use **undo content rewrite** to restore the default.

Syntax

content rewrite value *value* **replace** *replace-string*

undo content rewrite

Default

The content of HTTP responses is not rewritten.

Views

HTTP LB action view

Predefined user roles

network-admin

context-admin

Parameters

value *value*: Specifies the HTTP packet content to be rewritten, a case-sensitive string of 1 to 127 characters. The string cannot contain question marks (?).

replace *replace-string*: Specifies the content after rewrite, a case-sensitive string of 1 to 127 characters.

Usage guidelines

This command applies only to the HTTP response packets in the format of text/*.

The rewrite operation is not performed in either of the following situations:

- A regular expression is used to match the content before rewrite, and the content before rewrite exceeds 4096 bytes in size.
- The content after rewrite exceeds 4096 bytes in size.

If you specify the *replace-string* argument as %[1-9], the matching packet content *value* will be replaced by the content in the corresponding pair of brackets. For example, if you execute the **content rewrite value** (Wel)(co)(me) **replace** %2 command, the content **Welcome** will be replaced by the content **co** in the second pair of brackets.

If you execute the **content rewrite** command multiple times, the most recent configuration takes effect.

Examples

Create the HTTP LB action named **replace**, and replace the content **2000::1** in HTTP response packets with **2.3.4.5**.

```
<Sysname> system-view
[Sysname] loadbalance action replace type http
[Sysname-lba-http-replace] content rewrite value 2000::1 replace 2.3.4.5
```

cookie (protection rule view)

Use **cookie** to configure a cookie-based protection threshold.

Use **undo cookie** to restore the default.

Syntax

cookie *cookie-name* **request-threshold** *threshold*

undo cookie

Default

No cookie-based protection threshold is configured.

Views

Protection rule view

Predefined user roles

network-admin

context-admin

Parameters

cookie-name: Specifies an HTTP cookie by its name, a case-sensitive string of 1 to 63 characters. The cookie name cannot contain brackets ({ }, ( ), [ ], < >), at sign (@), comma (,), semicolon (;), colon (:), backslash (\), quotation mark ("), slash (/), question mark (?), equal sign (=), space character (SP), and horizontal tab (HT). Additionally, the cookie name cannot contain ASCII codes that are less than or equal to 31 and greater than or equal to 127.

request-threshold *threshold*: Specifies a request threshold in the range of 1 to 4294967295.

Usage guidelines

If the number of times that a user accesses a protected URL exceeds the request threshold during the protection period, the protection action is taken. The device determines whether requests belong to the same user based on the following elements:

- **Cookie**—Requests with the same cookie value for the cookie specified in this command belong to the same user.
- **Source IP address**—Requests with the same source IP address belong to the same user.

If you configure both a cookie-based request threshold and a source-IP-based request threshold, the protection action is taken when either threshold is exceeded.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

In protection rule 5, configure the cookie name as **jsessionid** and the request threshold as 2.

```
<Sysname> system-view
[Sysname] loadbalance protection-policy p1
[Sysname-lbpp-http-p1] rule 5
[Sysname-lbpp-http-p1-rule-5] cookie jsessionid request-threshold 2
```

Related commands

protected-url

protection-action

protection-period

source-ip

cookie (sticky group view)

Use **cookie** to configure the HTTP cookie sticky method.

Use **undo cookie** to restore the default.

Syntax

cookie { **get name** *cookie-name* [**offset** *offset*] [**start** *start-string*] [**end** *end-string* | **length** *length*] | { **insert** [**domain** *domain-name*] [**path** *path*] [**httponly**] [**secure**] | **rewrite** } [**name** *cookie-name*] [**httponly**] [**secure**] }

undo cookie { **get** | **insert** | **rewrite** }

Default

No HTTP cookie sticky methods exist.

Views

HTTP cookie sticky group view

Predefined user roles

network-admin

context-admin

Parameters

get: Specifies the cookie get sticky method that gets the Set-Cookie field in the HTTP response packets sent by the server.

cookie-name: Specifies an HTTP cookie by its name, a case-sensitive string of 1 to 63 characters.

offset *offset*: Specifies the offset value based on the start of the cookie value, in the range of 0 to 1000 bytes. The default is 0.

start *start-string*: Specifies the regular expression that marks the start of the cookie, a case-sensitive string of 1 to 127 characters starting from the *offset* value. The string cannot contain question marks (?).

end *end-string*: Specifies the regular expression that marks the end of the cookie, a case-sensitive string of 1 to 127 characters starting from the *start-string* value. The string cannot contain question marks (?).

length *length*: Specifies the length of the cookie, in the range of 0 to 1000 bytes. The default is 0, which indicates all lengths.

insert: Specifies the cookie insert sticky method that inserts the Set-Cookie field to the HTTP response packets sent by the server.

rewrite: Specifies the cookie rewrite sticky method that rewrites the Set-Cookie field in the HTTP response packets sent by the server.

name *cookie-name*: Specifies an HTTP cookie by its name, a case-sensitive string of 1 to 63 characters. The default name is X-LB.

domain *domain-name*: Specifies a domain name indicating the hosts to which the cookie will be sent, a case-sensitive string of 1 to 255 characters. If you do not specify this option, the cookie will be sent to only the host where it is created.

path *path*: Specifies a path indicating the paths to which the cookie will be sent, a case-sensitive string of 1 to 255 characters. If you do not specify this option, the cookie will be sent to every path (the root directory **/** applies).

httponly: Specifies that the cookie cannot be accessed by scripts. If you do not specify this keyword, the cookie can be accessed by scripts.

secure: Specifies that the cookie can be transmitted over only HTTPS connections. If you do not specify this keyword, the cookie can be transmitted over any connections.

Usage guidelines

Use the **cookie get** command to obtain the HTTP cookie information used to generate sticky entries based on the *offset*, *start-string*, *end-string*, and *length* values. The *start-string* and *end-string* values are not included in the sticky entry information.

If the sticky method is cookie rewrite, the Set-Cookie field of the specified cookie must be available in the HTTP response packets sent by the server. The system modifies only the cookie name and value in the Set-Cookie field without modifying other attributes such as Expires.

If the sticky method is cookie insert or cookie rewrite and the timeout timer for sticky entries is 0, the system adds the Expires field after the inserted or rewritten value. If the HTTP response packets sent by the server carry this attribute, the load balancing module does not modify the attribute. Instead, it adds the user-configured Expires information after the value. As a best practice, do not carry any timeout attribute in the Set-Cookie header on the server when you configure the cookie rewrite sticky method.

The **domain** *domain-name* option specifies the hosts to which the cookie will be sent. Suppose a client can visit hosts **example.com**, **www.example.com**, and **www.corp.example.com**. If you specify **example.com** for the **domain** *domain-name* option, the client includes the cookie when sending HTTP requests to any one of the three hosts. If you specify **www.corp.example.com** for the **domain** *domain-name* option, the client includes the cookie only when sending HTTP requests to **www.corp.example.com**.

The **path** *path* option limits the scope of the cookie to a set of paths. Suppose a client can visit folders **www.example.com/a** and **www.example.com/b**. If you specify **www.example.com** for the **domain** *domain-name* option and **/a** for the **path** *path* option, the client includes the cookie only when sending HTTP requests to **www.example.com/a**.

The **httponly** option prevents attackers from obtaining cookie information by using scripts.

The **secure** option makes sure the cookie is transmitted over an HTTPS connection. For an HTTP connection, the cookie is not transmitted.

Examples

Configure the cookie get sticky method for the HTTP cookie sticky group **sg3**: Starting from the 10th byte of start of the HTTP packet, use the 32-byte HTTP cookie named **user** to generate sticky entries.

```
<Sysname> system-view
[Sysname] sticky-group sg3 type http-cookie
[Sysname-sticky-http-cookie-sg3] cookie get name user offset 10 length 32
```

Configure the cookie insert sticky method for the HTTP cookie sticky group **sg3**.

```
<Sysname> system-view
[Sysname] sticky-group sg3 type http-cookie
[Sysname-sticky-http-cookie-sg3] cookie insert
```

cookie secondary name

Use **cookie secondary name** to specify the name of the secondary cookie to be searched in the URI.

Use **undo cookie secondary name** to restore the default.

Syntax

cookie secondary name *value*

undo cookie secondary name

Default

The name of the secondary cookie to be searched in the URI is not specified.

Views

HTTP cookie sticky group view

Predefined user roles

network-admin

context-admin

Parameters

value: Specifies the name of the secondary cookie, a case-sensitive token string of 1 to 63 characters excluding brackets ({ }, ( ),[ ], < >), at sign (@), comma (,), semicolon (;), colon (:), backslash (\), quotation mark ("), slash (/), question mark (?), equal sign (=), space character (SP), and horizontal tab (HT). The character string also excludes ASCII codes that are less than or equal to 31 and greater than or equal to 127.

Usage guidelines

This command applies only to the cookie get sticky method. Executing this command enables the system to locate the secondary cookie in the URI when it fails to locate the specified cookie in the HTTP request packet header.

Examples

Specify the name of the secondary cookie to be searched in the URI as **sid** for the HTTP cookie sticky group **sg3**.

```
<Sysname> system-view
[Sysname] sticky-group sg3 type http-cookie
[Sysname-sticky-http-cookie-sg3] cookie secondary name sid
```

cost

Use **cost** to set the link cost for proximity calculation.

Use **undo cost** to restore the default.

Syntax

cost *cost-value*

undo cost

Default

The link cost for proximity calculation is 0.

Views

Link view

Predefined user roles

network-admin

context-admin

Parameters

cost-value: Specifies the link cost for proximity calculation, in the range of 0 to 10240.

Examples

Set the link cost for proximity calculation to 200 for the link **lk1**.

```
<Sysname> system-view
[Sysname] loadbalance link lk1
[Sysname-lb-link-lk1] cost 200
```

cost weight

Use **cost weight** to set the cost weight for proximity calculation.

Use **undo cost weight** to restore the default.

Syntax

cost weight *cost-weight*

undo cost weight

Default

The cost weight for proximity calculation is 100.

Views

Proximity view

Predefined user roles

network-admin

context-admin

Parameters

cost-weight: Specifies the cost weight for proximity calculation, in the range of 0 to 255. A larger value indicates a higher cost weight.

Examples

Set the cost weight for proximity calculation to 200.

```
<Sysname> system-view
[Sysname] loadbalance proximity
[Sysname-lb-proximity] cost weight 200
```

customlog content

Use **customlog content** to configure the content to be output by using the fast log output feature.

Use **undo customlog content** to restore the default.

Syntax

customlog content *content-value*

undo customlog content

Default

No content is output by using the fast log output feature.

Views

HTTP virtual server view

Predefined user roles

network-admin

context-admin

Parameters

content-value: Specifies the log content to be output, a case-sensitive string of 1 to 255 characters. To enter multiple variables, separate them by semicolons. The device supports the following variables:

- **%{is}**—Source IP address in HTTP requests.
- **%{ps}**—Source port number in HTTP requests.
- **%{id}**—Destination IP address in HTTP requests.
- **%{pd}**—Destination port number in HTTP requests.
- **%{sis}**—Source IP address in HTTP responses.
- **%{sps}**—Source port number in HTTP responses.
- **%{sid}**—Destination IP address in HTTP responses.
- **%{spd}**—Destination port number in HTTP responses.
- **%{vsn}**—Virtual server name.
- **%{sfn}**—Server farm name.
- **%{reqtmstamp}**—HTTP request timestamp.
- **%{uri}**—HTTP URI.
- **%{ver}**—HTTP version number.
- **%{args}**—HTTP access parameters.
- **%{method}**—HTTP request method.
- **%{xff}**—IP address of XFF (X-Forwarded-For).
- **%{ctype}**—Content-Type field in HTTP requests.
- **%{clen}**—Content-Length field in HTTP requests.
- **%{ref}**—Referer header field in HTTP requests.
- **%{ua}**—User-Agent header field in HTTP requests.
- **%{host}**—Host header field in HTTP requests.
- **%{path}**—Path in HTTP requests.
- **%{reqsz}**—HTTP request size in bytes.
- **%{reqtm}**—HTTP request duration in milliseconds. The duration is from time when the device receives an HTTP request to the time when the device receives the HTTP response.
- **%{rspclen}**—Content-Type field in HTTP responses.
- **%{reqsz}**—HTTP response size in bytes.
- **%{rsptm}**—HTTP response duration in milliseconds. The duration is from the time when the device receives an HTTP response to the time when the device finishes sending out the HTTP response.
- **%{stscode}**—HTTP response status code.
- **%{reqbsz}**—Body size of HTTP requests, in bytes.
- **%{rspbsz}**—Body size of HTTP responses received by the device from the server, in bytes.
- **%{rspsntbsz}**—Body size of HTTP responses sent from the device to the client, in bytes.
- **%{cookie_***cookie-name*—HTTP cookie. The cookie name cannot contain brackets ({ }, ( ), [ ], < >), at sign (@), comma (,), semicolon (;), colon (:), backslash (\), quotation mark ("), slash (/), question mark (?), equal sign (=), space character (SP), and horizontal tab (HT).

Additionally, the cookie name cannot contain ASCII codes that are less than or equal to 31 and greater than or equal to 127. You can specify multiple cookies.

Usage guidelines

After you execute this command, the device sends the specified content to the log host by using the fast log output feature.

Before executing this command, you must enable fast log output for load balancing and configure fast log output parameters.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

For HTTP virtual server **vs**, output the source IP address and source port number in HTTP requests by using the fast log output feature.

```
<Sysname> system-view
[Sysname] virtual-server vs type http
[Sysname-vs-http-vs] customlog content %{is};%{ps}
```

Related commands

customlog format (*Network Management and Monitoring Command Reference*)

customlog host (*Network Management and Monitoring Command Reference*)

default dns-server-pool

Use **default dns-server-pool** to specify the default (primary) DNS server pool for a transparent DNS proxy.

Use **undo default dns-server-pool** to restore the default.

Syntax

default dns-server-pool *pool-name* [**sticky** *sticky-name*]

undo default dns-server-pool

Default

No default DNS server pool is specified for a transparent DNS proxy.

Views

Transparent DNS proxy view

Predefined user roles

network-admin

context-admin

Parameters

pool-name: Specifies a primary DNS server pool by its name, a case-insensitive string of 1 to 63 characters.

sticky *sticky-name*: Specifies a sticky group by its name, a case-insensitive string of 1 to 63 characters. If you do not specify a sticky group, the DNS server pool does not correspond to any sticky group.

Usage guidelines

If you execute the **default dns-server-pool** command multiple times, the most recent configuration takes effect.

Examples

Specify the primary DNS server pool **dns-pool1** and the sticky group **st1** for the transparent DNS proxy **dns-proxy1**.

```
<Sysname> system-view
[Sysname] loadbalance dns-proxy dns-proxy1
[Sysname-lb-dp-udp-dns-proxy1] default dns-server-pool dns-pool1 sticky st1
```

default link-group

Use **default link-group** to specify the default (primary) link group.

Use **undo default link-group** to restore the default.

Syntax

default link-group *link-group-name* [**backup** *backup-link-group-name*] [**sticky** *sticky-name*]

undo default link-group

Default

No default link group is specified.

Views

Link-IP virtual server view

Predefined user roles

network-admin

context-admin

Parameters

link-group-name: Specifies a primary link group by its name, a case-insensitive string of 1 to 63 characters.

backup *backup-link-group-name*: Specifies a backup link group by its name, a case-insensitive string of 1 to 63 characters.

sticky *sticky-name*: Specifies a sticky group by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

When the primary link group is available (contains links), the virtual server forwards packets through the primary link group. When the primary link group is not available, the virtual server forwards packets through the backup link group.

Examples

Specify the primary link group **link1**, the backup link group **link2**, and the sticky group **sg1** for the link-IP-type virtual server **vs3**.

```
<Sysname> system-view
[Sysname] virtual-server vs3 type link-ip
[Sysname-vs-link-ip-vs3] default link-group link1 backup link2 sticky sg1
```

default server-farm

Use **default server-farm** to specify the default (primary) server farm.

Use **undo default server-farm** to restore the default.

Syntax

default server-farm *server-farm-name* [**backup** *backup-server-farm-name*] [**sticky** *sticky-name* [**backup** *backup-sticky-name*]]

undo default server-farm

Default

No default server farm is specified.

Views

Fast HTTP virtual server view

HTTP virtual server view

IP virtual server view

TCP virtual server view

UDP virtual server view

Predefined user roles

network-admin

context-admin

Parameters

server-farm-name: Specifies a primary server farm by its name, a case-insensitive string of 1 to 63 characters.

backup *backup-server-farm-name*: Specifies a backup server farm by its name, a case-insensitive string of 1 to 63 characters.

sticky *sticky-name*: Specifies a primary sticky group by its name, a case-insensitive string of 1 to 63 characters.

backup *backup-sticky-name*: Specifies a backup sticky group by its name, a case-insensitive string of 1 to 63 characters. This option is supported only by HTTP virtual servers and RADIUS virtual servers.

Usage guidelines

When the primary server farm is available (contains real servers), the virtual server forwards packets through the primary server farm. When the primary server farm is not available, the virtual server forwards packets through the backup server farm.

If you specify both a primary sticky group and a backup sticky group, the device generates both primary sticky entries and backup sticky entries. If packets do not match primary sticky entries, backup sticky entries will apply.

The device generates backup sticky entries for only the following sticky group combinations:

- RADIUS-type primary sticky group and port-address-type backup sticky group.
- HTTP cookie-type primary sticky group and port-address-type backup sticky group.
- HTTP cookie-type primary sticky group and HTTP passive-type backup sticky group.

Examples

Specify the primary server farm **sf**, the backup server farm **sfb**, and the sticky group **sg1** for the IP-type virtual server **vs3**.

```
<Sysname> system-view
[Sysname] virtual-server vs3 type ip
[Sysname-vs-ip-vs3] default server-farm sf backup sfb sticky sg1
```

default-class action

Use **default-class action** to specify the default LB action.

Use **undo default-class** to restore the default.

Syntax

default-class action *action-name*

undo default-class

Default

No default LB action is specified.

Views

LB policy view

Predefined user roles

network-admin

context-admin

Parameters

action-name: Specifies an LB action by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

This command sets the default LB action for packets that fail to match any LB class.

A DNS LB policy can reference DNS LB actions only; a generic LB policy can reference generic LB actions only. This rule does not apply to HTTP LB policies.

Examples

Specify the default LB action **lba1** for the generic LB policy **lbp1**.

```
<Sysname> system-view
[Sysname] loadbalance policy lbp1 type generic
[Sysname-lbp-generic-lbp1] default-class action lba1
```

description

Use **description** to configure a description.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

No description is configured.

Views

ISP view

LB action view

LB class view

LB policy view

LB connection limit policy view

Parameter profile view

Protection policy view

Real server view

Server farm member view

Server farm view

SNAT address pool view

SNAT global policy view

Sticky group view

Virtual server view

Link group view

Link group member view

Link view

DNS server pool view

DNS server pool member view

DNS server view

Statistics node view

Predefined user roles

network-admin

context-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 127 characters.

Examples

Configure the description **LB action LBA1** for the generic LB action **lba1**.

```
<Sysname> system-view
[Sysname] loadbalance action lba1 type generic
[Sysname-lba-generic-lba1] description LB action LBA1
```

destination-ip object-group

Use **destination-ip object-group** to specify a destination IP address object group for address translation.

Use **undo destination-ip object-group** to restore the default.

Syntax

destination-ip object-group *object-group-name*

undo destination-ip object-group

Default

All packets matching a virtual server are translated.

Views

SNAT global policy view

Predefined user roles

network-admin

context-admin

Parameters

object-group-name: Specifies a destination IP address object group by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

If you specify a destination IP address object group, the device performs SNAT on only packets with a matching destination IP address. For information about configuring an IP address object group, see object group configuration in *Security Configuration Guide*.

Examples

Specify destination IP address object group **obj1** for SNAT global policy **sn1**.

```
<Sysname> system-view
[Sysname] loadbalance snat-global-policy sn1
[Sysname-lb-snat-gp-sn1] destination-ip object-group obj1
```

Related commands

object-group (*Security Command Reference*)

display loadbalance action

Use **display loadbalance action** to display LB action information.

Syntax

display loadbalance action [**name** *action-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

name *action-name*: Specifies an LB action by its name, a case-insensitive string of 1 to 63 characters. If you do not specify this option, the command displays information about all LB actions.

Examples

Display information about all LB actions.

```
<Sysname> display loadbalance action
LB action: lba1
  Description:
  Type: Generic
  State: Inactive
  Forward type: Drop
  IP ToS:
  Fallback-action: Disabled
```

```
  Busy-action: Force
  TCP payload rewrite:
    Value: QMGR.S01
    Replacement: QMGR.S01%[variable]
    Direction: Request
  TCP payload rewrite:
    Value: QMGR.S01_1
    Replacement: QMGR.S01_2
    Direction: Response
  TCP payload rewrite:
    Value: QMGR.S02_2
    Replacement: QMGR.S01_2
    Direction: Response

LB action: lba2
  Description:
  Type: HTTP
  State: Active
  Forward type: Server farm
  Server farm: sf (in use)
  Backup server farm: sfb
  Sticky: sg3
  Backup sticky: sg4
  IP ToS: 20
  Fallback-action: Disabled
  SSL client policy:
  Content rewrite:
    Value:
    Replacement:
  Redirect relocation:
  Redirect return-code: 302
  External-link proxy: Disabled
  Header delete:
    Name: ww
    Direction: Request
  Header insert:
    Name: aa
    Value: 12345678901234567890123456789012345678901234567890123456789012345678901234567890
    Direction: Both
  Header insert:
    Name: cc
    Value: dd
    Direction: Request
  Header rewrite:
    Name: ee
    Value: dd
    Replacement: ff
    Direction: Response
```

```
  SSL URL rewrite:
    Value: 12
    Clear port: 12
    SSL port: 123

LB action: lba3
  Description: sina
  Type: Link-generic
  State: Active
  Forward type: link group
  Link group: lg1 (in use)
  Backup link group: lg2
  Sticky:
  IP ToS:
  Fallback-action: None

LB action: lba4
  Description: xx
  Type: DNS
  State: Active
  Forward type: DNS server pool
  DNS server pool: dsp1
  Sticky: st
  IP ToS:
  Fallback-action: Disabled
  Busy-action: Force

LB action: lba5
  Description:
  Type: HTTP
  State: Active
  Forward type: Redirect
  IP ToS:
  Fallback-action: Continue
  SSL client policy:
  Content rewrite:
    Value:
    Replacement:
  Redirect relocation: www.nsfocus.com.cn
  Redirect return-code: 302
  External-link proxy: Disabled

LB action: lba6
  Description:
  Type: HTTP
  State: Active
  Forward type: Response
  IP ToS:
```

```
Fallback-action: Response
  Raw file name: 301.raw
SSL client policy:
Content rewrite:
  Value:
  Replacement:
Redirect relocation:
Redirect return-code: 302
External-link proxy: Disabled
Response file:
  File: index.html
  URL: /index/css
Response file:
  File name: subsys_intf.js
  URL: /index/subsys
Response file:
  File name: subsys.js
  URL: /subsys.js
Response zip file:
  Zip file name: subsys.zip
  Working path: /
```

Table 1 Command output

Field	Description
LB action	LB action name.
Description	Description for the LB action.
Type	LB action type: • DNS. • Generic. • HTTP. • Link-generic. • RADIUS.
State	LB action state: • Active. • Inactive.
Forward type	Packet forwarding mode of the LB action: • **Drop**—Discards packets. • **Drop(FIN-close)**—Closes TCP connections by sending FIN packets (applicable to generic and HTTP LB actions). • **Drop(RST-close)**—Closes TCP connections by sending RST packets (applicable to generic and HTTP LB actions). • **Forward**—Forwards packets. • **Server farm**—Forwards packets through the server farm (applicable to generic, HTTP, and RADIUS LB actions). • **Link group**—Forwards packets through the link group (applicable to link-generic LB actions). • **DNS server pool**—Forwards packets through the DNS server pool (applicable to DNS LB actions). • **Skip current DNS proxy** (applicable to DNS LB actions).

Field	Description
	• **Redirect**—Redirects packets. • **Response**—Responds to client requests by using a file.
Server farm	Primary server farm name. **(in use)** indicates the server farm is in use. This field is displayed only when the packet forwarding mode is **server farm**.
Backup server farm	Backup server farm name. **(in use)** indicates the server farm is in use. This field is displayed only when the packet forwarding mode is **server farm**.
Link group	Default link group name. **(in use)** indicates the link group is in use.
Backup link group	Backup link group name. **(in use)** indicates the link group is in use.
Sticky	Primary sticky group name. This field is displayed only when the packet forwarding mode is **server farm** or **DNS server pool**.
Backup sticky	Backup sticky group name. This field is displayed only when the packet forwarding mode is **server farm** and the LB action type is **HTTP** or **RADIUS**.
IP ToS	ToS field value of IP packets.
Fallback-action	Action taken upon load balancing failure: • **None**—Does not take any action. • **Continue**—Matches the next rule. • **Response**—Responds to client requests by using a file. • **Drop(FIN-close)**—Closes TCP connections by sending FIN packets (applicable to generic and HTTP LB actions). • **Drop(RST-close)**—Closes TCP connections by sending RST packets (applicable to generic and HTTP LB actions).
Busy-action	Action taken upon busyness: • **Continue**—Matches the next rule. • **Force**—Assigns packets to links or DNS servers regardless of whether they are busy.
SSL client policy	SSL client policy name. This field is displayed for HTTP LB actions only.
Content rewrite	HTTP content rewrite configuration: • **Value**—Specifies the HTTP packet content to be rewritten. • **Replacement**—Specifies the content after rewrite. This field is displayed only for an HTTP-type LB action.
Redirect relocation	Redirection URL. This field is displayed only for HTTP-type LB actions.
Redirect return-code	Status code in the redirection packets. This field is displayed only for HTTP-type LB actions.
Header delete	Deletes the HTTP header. • **Name**—Name of the HTTP packet header. • **Direction**—Specifies HTTP requests, HTTP responses, or both. This field is displayed only when the **`header delete`** command is configured.
Header insert	Inserts the HTTP header. • **Name**—Name of the HTTP packet header. • **Value**—Content of the HTTP packet header. • **Direction**—Specifies HTTP requests, HTTP responses, or both. This field is displayed only when the **`header insert`** command is configured.
Header rewrite	Rewrites the HTTP header. • **Name**—Name of the HTTP packet header. • **Value**—Content of the HTTP packet header to be rewritten.

Field	Description
	• **Replacement**—Content after rewrite. • **Direction**—Specifies HTTP requests, HTTP responses, or both. This field is displayed only when the **header rewrite** command is configured.
SSL URL rewrite	Rewrites the URL in the Location header of HTTP response packets sent by the server. • **Value**—Regular expression for the location header URL. • **Clear port**—HTTP port number to be rewritten. • **SSL port**—SSL port number after rewrite. This field is displayed only when the **ssl url rewrite** command is configured.
DNS server pool	DNS server pool name. This field is displayed only when the packet forwarding mode is **DNS server pool**.
Response file	Responds to client requests by using an uncompressed file.
File name	Name of the uncompressed file.
URL	URL path used to match client requests.
Response zip file	Responds to client requests by using a compressed file.
Zip file name	Name of the compressed file.
Working path	Working path used to match client requests.
Raw file name	Response file used upon load balancing failure.
TCP payload rewrite	Rewrite the TCP payload: • **Value**—Content of the TCP packet header to be rewritten. • **Replacement**—Content after rewrite. • **Direction**—Specifies TCP requests, TCP responses, or both. This field is displayed only when the **payload rewrite** command is configured.

display loadbalance alg

Use **display loadbalance alg** to display the ALG status for all protocols.

Syntax

display loadbalance alg

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display the ALG status for all protocols.

```
<Sysname> display loadbalance alg
LB ALG:
  DNS         : Enable
```

```
  FTP          : Enable
  H323         : Disabled
  ICMP-ERROR   : Enable
  ILS          : Disabled
  MGCP         : Disabled
  NBT          : Disabled
  PPTP         : Enable
  RSH          : Disabled
  RTSP         : Enable
  SCCP         : Disabled
  SIP          : Disabled
  SQLNET       : Disabled
  TFTP         : Disabled
  XDMCP        : Disabled
```

display loadbalance class

Use **display loadbalance class** to display LB class information.

Syntax

display loadbalance class [**name** *class-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

name *class-name*: Specifies an LB class by its name, a case-insensitive string of 1 to 63 characters. If you do not specify this option, the command displays information about all LB classes.

Examples

Display information about all LB classes.

```
<Sysname> display loadbalance class
LB class: lbc1
  Description:
  Type: HTTP
  Match type: Match-all
  Match rule:
    match 1 source ip address 1.2.3.0 24
    match 2 source ipv6 address 1::2
    match 3 cookie abc value 123
    match 4 header def value 12
    match 5 method ext xde
    match 6 method rfc CONNECT
    match 7 class cla2
```

```
    match 8 url 2q3
    match 9 acl ipv4 number 2000
    match 10 acl ipv6 number 2001
    match 11 acl ipv4 name aaa
    match 12 acl ipv6 name bbb
    match 13 isp name isp1

LB class: lbc2
  Description:
  Type: Generic
  Match type: Match-any
  Match rule:
    match 1 class cla2
    match 2 source ip address 1.2.23.0 24
    match 3 source ipv6 address 1::12
    match 4 acl ipv4 number 3000
    match 5 acl ipv6 number 3001
    match 6 acl ipv4 name ccc
    match 7 acl ipv6 name ddd
    match 8 isp name isp2
    match 9 payload orcl

LB class: lbc3
  Description:
  Type: Link-generic
  Match type: Match-any
  Match rule:
    match 1 class cla3
    match 2 source ip address 1.2.3.0 24
    match 3 source ipv6 address 1::12
    match 4 acl ipv4 number 3002
    match 5 acl ipv6 number 3003
    match 6 acl ipv4 name ccc
    match 7 acl ipv6 name ddd
    match 8 isp name isp2
    match 9 user u1
    match 10 user-group lb-group
    match 11 interface GE1/0/1

LB class: lbc4
  Description:
  Type: DNS
  Match type: Match-any
  Match rule:
    match 1 class cla2
    match 2 source ip address 1.2.3.0 24
    match 3 source ipv6 address 1::12
    match 4 acl ipv4 number 3002
```

```
    match 5 acl ipv6 number 3003
    match 6 acl ipv4 name ccc
    match 7 acl ipv6 name ddd
    match 8 destination ip address 1.2.3.0 24
    match 9 destination ipv6 address 1::12
    match 10 domain-name www.nsfocus.com.cn

LB class: lbc5
  Description:
  Type: MySQL
  Match type: Match-any
  Match rule:
    match 1 class cla2
    match 2 source ip address 1.2.3.0 24
    match 3 source ipv6 address 1::12
    match 4 acl ipv4 number 3002
    match 5 acl ipv6 number 3003
    match 6 acl ipv4 name ccc
    match 7 acl ipv6 name ddd
    match 8 sql select
```

Table 2 Command output

Field	Description
LB class	LB class name.
Description	Description for the LB class.
Type	LB class type: • DNS. • Generic. • HTTP. • Link-generic. • MySQL. • RADIUS.
Match type	Match type for the LB class: • **Match-all**—Requires matching all rules of the LB class. • **Match-any**—Requires matching any rule of the LB class.
Match rule	Match rules for the LB class.

display loadbalance connections

Use **display loadbalance connections** to display information about Layer 7 LB TCP connections.

Syntax

display loadbalance connections [**client-side**{ **ipv4** | **ipv6** } [**cs-client-ip** *ip-address* [**cs-client-port** *port-number*]] [**cs-server-ip** *ip-address* [**cs-server-port** *port-number*]] [**state** { **closed** | **close_wait** | **closing** | **established** | **fin_wait_1** | **fin_wait_2** | **last_ack** | **listening** | **syn_received** | **syn_sent** | **time_wait** }]] [**server-side** { **ipv4** | **ipv6** }

[**ss-client-ip** *ip-address* [**ss-client-port** *port-number*]] [**ss-server-ip** *ip-address* [**ss-server-port** *port-number*]] [**state** { **closed** | **close_wait** | **closing** | **established** | **fin_wait_1** | **fin_wait_2** | **last_ack** | **listening** | **syn_received** | **syn_sent** | **time_wait** }]] [**slot** *slot-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

client-side: Displays client-side connections.

server-side: Displays server-side connections.

ipv4: Specifies IPv4 connections.

ipv6: Specifies IPv6 connections.

cs-client-ip *ip-address*: Specifies a client by its IP address on the client side.

cs-client-port *port-number*: Specifies the port number of the client on the client side, in the range of 0 to 65535. 0 means any port number.

ss-client-ip *ip-address*: Specifies a client by its IP address on the server side.

ss-client-port *port-number*: Specifies the port number of the client on the server side, in the range of 0 to 65535. 0 means any port number.

cs-server-ip *ip-address*: Specifies a server by its IP address on the client side.

cs-server-port *port-number*: Specifies the port number of the server on the client side, in the range of 0 to 65535. 0 means any port number.

ss-server-ip *ip-address*: Specifies a server by its IP address on the server side.

ss-server-port *port-number*: Specifies the port number of the server on the server side, in the range of 0 to 65535. 0 means any port number.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about Layer 7 LB TCP connections for all member devices.

state { **closed** | **close_wait** | **closing** | **established** | **fin_wait_1** | **fin_wait_2** | **last_ack** | **listening** | **syn_received** | **syn_sent** | **time_wait** }: Specifies TCP connections by connection state. If you do not specify this parameter, the command displays information about TCP connections in each state.

verbose: Displays detailed information about TCP connections. If you do not specify this keyword, the command displays brief information.

Usage guidelines

If you do not specify any parameters, this command displays information about all Layer 7 LB TCP connections.

Examples

Display brief information about all Layer 7 LB TCP connections.

```
<Sysname> display loadbalance connections
```

```
Client side:                        State        Server side:                       State
192.168.56.1    <--> 8.8.8.8/80    ESTAB        192.168.56.1   <--> 2.2.2.2/80   ESTB
/50168                                          /1026
Any             <-->Any            CLOSED       192.168.56.1   <--> 2.2.2.2/80   TIMEWT
                                                /1027
Total sessions: 3
```

Display detailed information about all Layer 7 LB TCP connections.

```
<Sysname> display loadbalance connections verbose
Slot 1:
--------------------------------------------------------------------------------
                Client side                     Server side
Client address  12.12.12.12/3032                12.12.12.12/54649
Server address  4.4.44.4/80                     5.5.5.5/80
State           ESTABLISHED                     ESTABLISHED
VPN name        --                              --
Idle time       0 sec
Idle timeout    20 sec
Start time      2018-05-30 16:54:13

--------------------------------------------------------------------------------
                Client side                     Server side
Client address  12.12.12.12/2996                Any
Server address  4.4.44.4/80                     Any
State           TIME_WAIT                       N/A
VPN name        --                              --
Idle time       1 sec
Idle timeout    20 sec
Start time      2018-05-30 16:54:12

--------------------------------------------------------------------------------
                Client side                     Server side
Client address  12.12.12.12/3251                12.12.12.12/54341
Server address  4.4.44.4/80                     5.5.5.5/80
State           ESTABLISHED                     ESTABLISHED
VPN name        --                              --
Idle time       0 sec
Idle timeout    20 sec
Start time      2018-05-30 16:54:14
Total sessions: 3
```

Table 3 Command output

Field	Description
State	TCP connection state: • **LISTEN**. • **SYNSNT**—SYN_SENT. • **SYNRCV**—SYN_RECEIVED. • **ESTB**—ESTABLISHED. • **FINWT1**—FIN_WAIT_1.

Field	Description
	• **FINWT2**—FIN_WAIT_2. • **CLOWAT**—CLOSE_WAIT. • **CLOSING**. • **LASACK**—LAST_ACK. • **TIMEWT**—TIME_WAIT. • **CLOSED**. For more information about these states, see RFC 793.
Start time	Time when the TCP connection was established.

display loadbalance dns-cache

Use **display loadbalance dns-cache** to display DNS cache information.

Syntax

display loadbalance dns-cache [**vpn-instance** *vpn-instance-name*] [**domain-name** *domain-name*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays DNS cache information for the public network.

domain-name *domain-name*: Specifies a domain name, a case-insensitive string of 1 to 63 characters. If you do not specify this option, the command displays DNS cache information for all domain names.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays DNS cache information for all member devices.

Usage guidelines

DNS cache information records mappings between domain names and IP addresses.

Examples

Display all DNS cache information.

```
<Sysname> display loadbalance dns-cache
Slot 1:
Domain name: www.aaa.com
Aging time: 20 min
IPv4 addresses: 6.3.5.2
                4.5.6.3
                192.169.41.8
```

```
IPv6 addresses: 4:4:4::7

Domain name: www.bbb.com
Aging time: 20 min
IPv4 addresses: 5.5.5.5
                3.4.5.9
```

display loadbalance dns-listener

Use **display loadbalance dns-listener** to display DNS listener information.

Syntax

display loadbalance dns-listener [**name** *listener-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

name *listener-name*: Specifies a DNS listener by its name, a case-insensitive string of 1 to 63 characters. If you do not specify this option, the command displays information about all DNS listeners.

Usage guidelines

This command can display the service state, IPv4 address, port number, and fallback method.

Examples

Display information about the DNS listener **listener1**.

```
<Sysname> display loadbalance dns-listener name listener1
DNS listener name: listener1
  Service state: Enabled
  IPv4 address: 1.1.1.2
  Port: 53
  IPv6 address: --
  IPv6 Port: 53
  Fallback: Reject
  VPN instance:
```

Table 4 Command output

Field	Description
Service state	DNS listener state: • Enabled. • Disabled.
IPv4 address	IPv4 address of the DNS listener.
Port	Port number of the DNS listener.

Field	Description
IPv6 address	IPv6 address of the DNS listener.
IPv6 Port	IPv6 port number of the DNS listener.
Fallback	Processing method when the DNS listener fails to find the server to respond to the DNS request: • **dns-proxy**—Responds to the DNS request through the DNS proxy. • **No-response**—Does not respond to the DNS request. • **Reject**—Sends a DNS reject packet.
VPN instance	VPN instance to which the DNS listener belongs.

display loadbalance dns-listener statistics

Use **display loadbalance dns-listener statistics** to display DNS listener statistics.

Syntax

display loadbalance dns-listener statistics [**name** *dns-listener-name*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

name *dns-listener-name*: Specifies a DNS listener by its name, a case-insensitive string of 1 to 63 characters. If you do not specify this option, the command displays statistics for all DNS listeners.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays DNS listener statistics for all member devices.

Examples

Display statistics for the DNS listener **dl**.

```
<Sysname> display loadbalance dns-listener statistics name dl
DNS listener: dl
Total:
  Received requests: 100
  Received valid requests: 70
  Unresponded requests: 10
  Rejected requests: 20
  Proxy requests: 0
  ------------------------------------------------
  RCVR - Received requests, RVR - Received valid requests,
  UR - Unresponded requests, RJTR - Rejected requests, PR - Proxy requests
  Type        RCVR        RVR       UR          RJTR         PR
```

```
A           50          50          0           0           0
AAAA        0           0           0           0           0
MX          10          5           5           0           0
NS          20          5           5           10          0
CNAME       10          5           0           5           0
SOA         10          5           0           5           0
PTR         0           0           0           0           0
TXT         10          5           0           5           0
SRV         0           0           0           0           0
```

Table 5 Command output

Field	Description
Proxy requests	Number of responses to DNS requests through transparent DNS proxies.
Type	DNS request type: • **A**—IPv4 host address. • **AAAA**—IPv6 host address. • **CNAME**—Canonical name. • **MX**—Mail exchanger. • **NS**—Name server. • **PTR**—Pointer. • **SOA**—Start of authority. • **SRV**—Service. • **TXT**—Text.

display loadbalance dns-map

Use **display loadbalance dns-map** to display DNS mapping information.

Syntax

display loadbalance dns-map [**name** *dns-map-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

dns-map-name: Specifies a DNS mapping by its name, a case-insensitive string of 1 to 63 characters. If you do not specify this argument, the command displays information about all DNS mappings.

Usage guidelines

Use this command to view the service state, domain name, and virtual server pool for DNS mappings.

Examples

Display information about the DNS mapping **dm1**.

```
<Sysname> display loadbalance dns-map name dm1
DNS mapping name: dm1
  Service state: Enabled
  TTL: 3600s
  Domain name list: www.nsfocus.domain.com.cn
  Virtual server pool: pool1
```

Table 6 Command output

Field	Description
Service state	DNS mapping state: • Enabled. • Disabled.
TTL	TTL, in seconds, to cache DNS records for DNS responses.
Domain name list	Domain name of the DNS mapping.
Virtual server pool	Virtual server pool used by the DNS mapping.

display loadbalance dns-map statistics

Use **display loadbalance dns-map statistics** to display DNS mapping statistics.

Syntax

display loadbalance dns-map statistics [**name** *dns-map-name*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

name *dns-map-name*: Specifies a DNS mapping by its name, a case-insensitive string of 1 to 63 characters. If you do not specify this option, the command displays statistics for all DNS mappings.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays DNS mapping statistics for all member devices.

Examples

Display statistics for the DNS mapping **dm**.

```
<Sysname> display loadbalance dns-map statistics name dm
DNS map: dm
Matched DNS requests: 100
```

Table 7 Command output

Field	Description
DNS map	DNS mapping name.
Matched DNS requests	Number of DNS requests matching the DNS mapping.

display loadbalance dns-proxy

Use **display loadbalance dns-proxy** to display transparent DNS proxy information.

Syntax

display loadbalance dns-proxy [**brief** | **name** *dns-proxy-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

brief: Displays brief transparent DNS proxy information. If you do not specify this keyword, the command displays detailed transparent DNS proxy information.

name *dns-proxy-name*: Specifies a transparent DNS proxy by its name, a case-insensitive string of 1 to 63 characters. If you do not specify this option, the command displays information about all transparent DNS proxies.

Examples

Display brief information about all transparent DNS proxies.

```
<Sysname> display loadbalance dns-proxy brief
DNS proxy     State       Type    VPN instance    IP address     Port
dns-proxy1    Active      UDP                     1.2.3.0/24     53
dns-proxy2    Inactive    UDP                     --             5353
```

Display information about transparent DNS proxy **dns-proxy1**.

```
<Sysname> display loadbalance dns-proxy name dns-proxy1
DNS proxy: dns-proxy1
  Type: UDP
  State: Active
  Service state: Enabled
  VPN instance:
  IPv4 address: 1.2.3.0/24
  IPv6 address: --
  Port: 53
  DNS server pool: dns-pool1
  Sticky: st
```

```
LB policy: dns-policy1
Connection synchronization: Enabled
Sticky synchronization: Enabled
Bandwidth busy protection: Disabled
```

Table 8 Command output

Field	Description
DNS proxy	Transparent DNS proxy name.
Type	Transparent DNS proxy type. Only UDP is supported.
State	Transparent DNS proxy state: • **Active**—The transparent DNS proxy is available. • **Inactive**—The transparent DNS proxy is unavailable for any reason except that the transparent DNS proxy feature is disabled. • **Inactive (disabled)**—The transparent DNS proxy is unavailable because the transparent DNS proxy feature is disabled.
Service state	Transparent DNS proxy state: **Enabled** or **Disabled**.
DNS server pool	Default DNS server pool used by the transparent DNS proxy.
Sticky	Sticky group used by the transparent DNS proxy.
Connection synchronization	Session extension information synchronization state: **Enabled** or **Disabled**.
Sticky synchronization	Sticky entry synchronization state: **Enabled** or **Disabled**.
Bandwidth busy protection	Link protection state: **Enabled** or **Disabled**.

display loadbalance dns-proxy statistics

Use **display loadbalance dns-proxy statistics** to display transparent DNS proxy statistics.

Syntax

display loadbalance dns-proxy statistics [**name** *dns-proxy-name*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

name *dns-proxy-name*: Specifies a transparent DNS proxy by its name, a case-insensitive string of 1 to 63 characters. If you do not specify this option, the command displays statistics for all transparent DNS proxies.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays transparent DNS proxy statistics for all member devices.

Examples

Display statistics for the transparent DNS proxy **dns-proxy1**.

```
<Sysname> display loadbalance dns-proxy statistics name dns-proxy1
DNS proxy: dns-proxy1
Received requests: 100
Dropped requests: 2
Received responses: 98
Dropped responses: 0
```

Table 9 Command output

Field	Description
DNS proxy	Transparent DNS proxy name.
Received requests	Number of DNS requests received by the transparent DNS proxy.
Dropped requests	Number of DNS requests dropped by the transparent DNS proxy.
Received responses	Number of DNS responses received by the transparent DNS proxy.
Dropped responses	Number of DNS responses dropped by the transparent DNS proxy.

display loadbalance dns-query

Use **display loadbalance dns-query** to display information about the domain names queried by external link proxy.

Syntax

display loadbalance dns-query [**vpn-instance** *vpn-instance-name*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays domain name information for the public network.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays domain name information for all member devices.

Examples

Display information about the domain names queried by external link proxy.

```
<Sysname> display loadbalance dns-query
Slot 1:
```

```
VPN instance: vpn1
  Domain name      DNS server
  www.a.com        1.2.3.4
  www.b.com        2.2.3.4
Slot 2:
VPN instance: vpn2
  Domain name      DNS server
  www.c.com        3.2.3.4
  www.d.com        4.2.3.4
```

Table 10 Command output

Field	Description
Domain name	Domain name being queried.
DNS server	IP address of the DNS server.

display loadbalance dns-server

Use **display loadbalance dns-server** to display DNS server information or DNS server pool member information.

Syntax

display loadbalance dns-server [**brief** | **name** *dns-server-name*]

display loadbalance dns-server dns-server-pool *dns-server-pool-name* [**name** *dns-server-name* **port** *port-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

brief: Displays brief DNS server information. If you do not specify this keyword, the command displays detailed DNS server information.

name *dns-server-name*: Displays detailed information about a DNS server. The *dns-server-name* argument specifies a DNS server by its name, a case-insensitive string of 1 to 63 characters.

dns-server-pool *dns-server-pool-name*: Displays information about members of a DNS server pool. The *dns-server-pool-name* argument specifies a DNS server pool by its name, a case-insensitive string of 1 to 63 characters.

dns-server *dns-server-name* **port** *port-number*: Displays information about a DNS server pool member. The *dns-server-name* argument specifies a DNS server pool member by its name, a case-insensitive string of 1 to 63 characters. The *port-number* argument specifies the port number of the DNS server pool member, in the range of 0 to 65535. If you do not specify this option, the command displays information about all members of a DNS server pool.

Usage guidelines

If you do not specify any parameter, the command displays detailed information about all DNS servers.

If the device obtains multiple DNS server IP addresses, it uses the smallest available IP address.

If no health monitoring method is specified, the device determines that all obtained DNS server IP addresses are available. If a health monitoring method is specified, the device determines that only the DNS server IP addresses that pass health monitoring are available.

Examples

Display brief information about all DNS servers.

```
<Sysname> display loadbalance dns-server brief
(*) – Auto-alloc address using
DNS server   Address             Port    Link         State         DNS server pool
ds1          10.150.100.100(*)   0       link1        Active        dns_pool
ds2          20.150.100.100      5353    link2        Probe-failed  dns_pool
ds3          --                  0       link3        Inactive      dns_pool
ds4          --(*)               0       link3        Inactive      dns_pool
```

Display detailed information about DNS server **ds1**.

```
<Sysname> display loadbalance dns-server name ds1
(*) – Auto-alloc address using
dns-server: ds1
  Description:
  State: Active
  VPN instance: --
  Auto-alloc address: Enabled
  IPv4 address: 10.150.100.100(*)
                10.160.100.1
                10.154.60.2
  IPv6 address: --

  Port: 0 (port number in original packet)
  Link: link1
  DNS server pool: dns-pool
  Weight: 100
  Priority: 4
  Probe information:
    Probe success criteria: All
    Probe method      State
    t4                Succeeded
```

Display information about all members of DNS server pool **dsp1**.

```
<Sysname> display loadbalance dns-server dns-server-pool dsp1
DNS server pool: dsp1
  dns-server: ds1
    Description: DNS server 1
    Parent state: Inactive
    State: Inactive
    Port: 0 (port number in original packet)
    Weight: 2
```

```
  Priority: 2
  Probe success criteria: All
    Probe method                    State
    icmp                            Failed

dns-server: rs2
  Description: DNS server 2
  Parent state: Inactive
  State: Inactive
  Port: 53
  Weight: 100
  Priority: 4
  Probe information:
    Probe success criteria: All
    Probe method                    State
    DNS                             Failed
```

Table 11 Command output

Field	Description
DNS server	DNS server name.
Address	IP address of the DNS server. The asterisk (*) indicates that the IP address is automatically obtained and is being used. If all obtained IP addresses are unavailable, this field displays --(*). If no IP address is obtained and no IP address is manually configured, this field displays two hyphens (--).
Link	Link of the DNS server.
Parent state/State	DNS server state/DNS server pool member state: • **Active**—The DNS server is available. • **Busy**—The DNS server is busy. When the DNS server is in **Active** state and enabled with the link protection feature, this field displays **Busy** if the maximum expected bandwidth is reached. • **Inactive**—The DNS server is unavailable, because the configuration is not complete or the server is not referenced. • **Probe-failed**—Health monitoring has failed. • **Unknown**—Health monitoring is not configured.
Description	Description for the DNS server.
Auto-alloc address	Whether the device is enabled to automatically obtain the IP address of a DNS server: **Disabled** or **Enabled**.
IPv4 address	IPv4 address of the DNS server.
IPv6 address	IPv6 address of the DNS server.
Port	Port number of the DNS server. 0 means the port number in the packet is used.
Weight	Weight of the DNS server.
Priority	Priority of the DNS server.
Probe information	Detailed health monitoring information for the DNS server.
Probe success criteria	Health monitoring success criteria for the DNS server: • **All**—Health monitoring succeeds only when all the specified health monitoring methods succeed. • **At least**—Health monitoring succeeds when a specified minimum number of

Field	Description
	health monitoring methods succeed.
Probe method	Name of the NQA template used by the health monitoring method.
State	State of the health monitoring method: • **Failed**—Health monitoring has failed. • **In progress**—Health monitoring is in progress. • **Invalid**—Health monitoring is unavailable (because the configuration of the NQA template is not complete), or the DNS server is unavailable. • **Succeeded**—Health monitoring has succeeded.

display loadbalance dns-server statistics

Use **display loadbalance dns-server statistics** to display DNS server statistics or DNS server pool member statistics.

Syntax

display loadbalance dns-server statistics [**name** *dns-server-name*] [**slot** *slot-number*]

display loadbalance dns-server statistics dns-server-pool *dns-server-pool-name* [**name** *dns-server-name* **port** *port-number*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

name *dns-server-name*: Specifies a DNS server by its name, a case-insensitive string of 1 to 63 characters. If you do not specify this option, the command displays statistics for all DNS servers.

dns-server-pool *dns-server-pool-name*: Displays statistics for members of a DNS server pool. The *dns-server-pool-name* argument specifies a DNS server pool by its name, a case-insensitive string of 1 to 63 characters.

dns-server *dns-server-name* **port** *port-number*: Displays statistics for a DNS server pool member. The *dns-server-name* argument specifies a DNS server pool member by its name, a case-insensitive string of 1 to 63 characters. The *port-number* argument specifies the port number of the DNS server pool member, in the range of 0 to 65535. If you do not specify this option, the command displays statistics for all members of a DNS server pool.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays DNS server statistics for all member devices.

Examples

Display statistics for the DNS server **ds1**.

```
<Sysname> display loadbalance dns-server statistics name ds1
DNS server: ds1
```

```
Received requests: 100
Send requests: 98
Dropped requests: 2
Received responses: 98
Send responses: 98
Dropped responses: 0
```

Display statistics for all members of DNS server pool **dsp1**.

```
<Sysname> display loadbalance dns-server statistics dns-server-pool dsp1
DNS server pool: dsp1
DNS server (port: 20): ds1
Received requests: 100
Dropped requests: 2
Sent responses: 98
Dropped responses: 0

DNS server (port: 28): ds2
Received requests: 100
Dropped requests: 0
Sent responses: 100
Dropped responses: 0
```

Table 12 Command output

Field	Description
DNS server	DNS server name.
Received requests	Number of DNS requests received by the DNS server.
Send requests	Number of DNS requests sent by the DNS server.
Dropped requests	Number of DNS requests dropped by the DNS server.
Received responses	Number of DNS responses received by the DNS server.
Send responses	Number of DNS responses sent by the DNS server.
Dropped responses	Number of DNS responses dropped by the DNS server.

display loadbalance dns-server-pool

Use **display loadbalance dns-server-pool** to display DNS server pool information.

Syntax

display loadbalance dns-server-pool [**brief** | **name** *pool-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

brief: Displays brief DNS server pool information. If you do not specify this keyword, the command displays detailed DNS server pool information.

name *pool-name*: Displays detailed information about a DNS server pool. The *pool-name* argument specifies a DNS server pool by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

If you do not specify any parameter, the command displays detailed information about all DNS server pools.

Examples

Display brief information about all DNS server pools.

```
<Sysname> display loadbalance dns-server-pool brief
Predictor: RR - Round robin, RD - Random,
           BW - Bandwidth, MBW - Max bandwidth,
           IBW - Inbound bandwidth, OBW - Outbound bandwidth,
           MIBW - Max inbound bandwidth, MOBW - Max outbound bandwidth,
           HASH(SIP) - Hash address source IP,
           HASH(DIP) - Hash address destination IP,
           HASH(SIP-PORT) - Hash address source IP-port
DNS server pool    Predictor     Total    Active
dns-pool           RR            3        2
dns-pool1          RR            0        0
dns-pool2          RD            3        0
```

Display detailed information about DNS server pool **dns-pool**.

```
<Sysname> display loadbalance dns-server-pool name dns-pool
DNS server pool: dns-pool
Description:
Predictor: Round robin
Selected server: Enabled
Min servers: 3
  Max servers: 5
Probe information:
  Probe success criteria: At-least 2
  Probe method: t4
Total DNS servers: 3
Active DNS servers: 0
DNS server list:
Name        State         Address          port    Link        Weight   Priority
ds1         Active        10.150.100.100   0       link1       100      4
ds2         Probe-failed  20.150.100.100   5353    link2       100      4
ds3         Inactive      --               0       link3       100      4
```

Table 13 Command output

Field	Description
Predictor	Scheduling algorithm of the DNS server pool: • **RR**—Weighted round robin algorithm.

Field	Description
	• **RD**—Random algorithm. • **BW**—Bandwidth algorithm. • **IBW**—Inbound bandwidth algorithm. • **OBW**—Outbound bandwidth algorithm. • **MBW**—Maximum bandwidth algorithm. • **MIBW**—Maximum inbound bandwidth algorithm. • **MOBW**—Maximum outbound bandwidth algorithm. • **HASH(SIP)**—Hash algorithm based on source IP address. • **HASH(DIP)**—Hash algorithm based on destination IP address. • **HASH(SIP-PORT)**—Hash algorithm based on source IP address and port number.
DNS server pool	DNS server pool name.
Total	Total number of DNS servers.
Active	Number of active DNS servers.
Description	Description for the DNS server pool.
Selected server	State of DNS server limit to participate in scheduling: disabled or enabled. If the state is enabled, the following fields are displayed: • **Min servers**—Minimum number of DNS servers that can participate in scheduling. • **Max servers**—Maximum number of DNS servers that can participate in scheduling.
Probe information	Detailed health monitoring information for the DNS server pool.
Probe success criteria	Health monitoring success criteria for the DNS server pool: • **All**—Health monitoring succeeds only when all the specified health monitoring methods succeed. • **At least**—Health monitoring succeeds when a specified minimum number of health monitoring methods succeed.
Probe method	Name of the NQA template used by the health monitoring method.
Total DNS servers	Total number of DNS servers.
Active DNS servers	Number of active DNS servers.
Name	DNS server name.
State	DNS server state: • **Active**—The DNS server is available. • **Busy**—The DNS server is busy. When the DNS server is in **Active** or **Ramp** state and enabled with link protection, this field displays **Busy** if the maximum expected bandwidth is reached. • **Inactive**—The DNS server is unavailable, because the configuration is not complete or the server is not referenced. • **Probe-failed**—Health monitoring has failed.
Address	IP address of the DNS server. The asterisk (*) indicates that the IP address is automatically obtained and is being used. If all obtained IP addresses are unavailable, this field displays --(*). If no IP address is obtained and no IP address is manually configured, this field displays two hyphens (--).
Port	Port number of the DNS server.
Link	Name of the link corresponding to the DNS server.
Weight	Weight of the DNS server.

Field	Description
Priority	Priority of the DNS server.

display loadbalance external-monitor log

Use **display loadbalance external-monitor log** to display the log information for custom monitoring.

Syntax

display loadbalance external-monitor log

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display the log information for custom monitoring.

```
<Sysname> display loadbalance external-monitor log
The external monitor probe state of (server farm sf, real server rs, port: 3306) template
mysql-template changed to successful.
The external monitor probe state of (server farm sf2, real server rs2, port: 3306) template
mysql-template changed to failed.
```

display loadbalance hot-backup statistics

Use **display loadbalance hot-backup statistics** to display LB hot backup statistics.

Syntax

display loadbalance hot-backup statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays LB hot backup statistics for all member devices.

Examples

Display LB hot backup statistics.

```
<Sysname> display loadbalance hot-backup statistics
Slot 2:
               TryAdd    TryDel    AckDel    AckOK     AckNO     NotSpt
  StiSnd       1         0         0         0         0         0
  StiRcv       0         0         0         0         0         0
  StiSndFail   0         0         0         0         0         0
  StiRcvFail   0         0         0         0         0         0
  MsgSnd       1         0         0         0         0         0
  MsgRcv       0         0         0         0         0         0
  MsgSndFail   0         0         0         0         0         0
  MsgRcvFail   0         0         0         0         0         0
  MAllocFail   0         0         0         0         0         0

  SesBkTotal : 0
  SesBkFail  : 0
  SesResTotal: 0
  SesResFail : 0
  SesUpdate  : 0
```

Table 14 Command output

Field	Description
TryAdd	Message for adding sticky entries.
TryDel	Message for deleting sticky entries.
AckDel	Message for acknowledging the deletion of sticky entries.
AckOK	Message indicating the sticky entries that can be deleted.
AckNO	Message indicating the sticky entries that cannot be deleted.
NotSpt	Message indicating the unsupported sticky entries.
StiSnd	Number of sent sticky entries.
StiRcv	Number of received sticky entries.
StiSndFail	Number of sticky entry sending failures.
StiRcvFail	Number of sticky entry receiving failures.
MsgSnd	Number of sent messages.
MsgRcv	Number of received messages.
MsgSndFail	Number of message sending failures.
MsgRcvFail	Number of message receiving failures.
MAllocFail	Number of memory application failures.
SesBkTotal	Number of session backups.
SesBkFail	Number of session backup failures.
SesResTotal	Number of session restorations.
SesResFail	Number of session restoration failures.
SesUpdate	Number of session updates.

display loadbalance isp

Use **display loadbalance isp** to display ISP information.

Syntax

display loadbalance isp [**ip** *ipv4-address* | **ipv6** *ipv6-address* | **name** *isp-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ip *ipv4-address*: Specifies an IPv4 address. If you do not specify this option, the command displays information about all ISPs.

ipv6 *ipv6-address*: Specifies an IPv6 address. If you do not specify this option, the command displays information about all ISPs.

name *isp-name*: Specifies an ISP by its name, a case-insensitive string of 1 to 63 characters. If you do not specify this option, the command displays information about all ISPs.

Usage guidelines

If you do not specify any parameters, this command displays information about all ISPs.

Examples

Display information about all ISPs.

```
<Sysname> display loadbalance isp
(*) - User-defined object
Last successful auto update time: 04:09:00 UTC Fri 03/16/2012
Last auto update time: 04:09:00 UTC Fri 03/16/2012
Last auto update result: Successful
  ISP update count: 1

LB ISP: isp1
    Whois maintainer object name:
        MAINT-CHINANET
    Description: ISP1
    IPv4 address/Mask length: --
    IPv6 address/Prefix length: --

LB ISP: isp2(*)
    Description:
    IPv4 address/Mask length:
        1.2.3.0/32(*)           1.2.3.4/32              3.3.3.6/32(*)
        192.168.6.131/32(*)     192.168.195.189/32(*)
    IPv6 address/Prefix length:
```

```
        1::2/128
        FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF/128(*)
```

Display information about the ISP corresponding to the IP address 1.2.3.0.

```
<Sysname> display loadbalance isp ip 1.2.3.0
ISP name            Source                  IPv4 address/Mask length
isp2                user-set                1.2.3.0/28
isp2                user-set                1.2.3.0/29
isp2                user-set                1.2.3.0/30
isp2                file-load               1.2.3.0/31
                    auto-update
isp2                user-set                1.2.3.0/32
                    file-load
```

Display information about the ISP corresponding to the IPv6 address 1::1234.

```
<Sysname> display loadbalance isp ipv6 1::1234
ISP name            Source                  IPv6 address/Prefix length
isp2                user-set                1::1234/126
isp2                user-set                1::1234/127
isp2                file-load               1::1234/128
```

Table 15 Command output

Field	Description
(*) - User-defined object	**(*)** indicates that the ISP information is manually configured. If the ISP information is also imported from a file, **(*)** is not displayed.
Last successful auto update time	Time of the most recent successful update.
Last auto update time	Time of the most recent update.
Last auto update result	Result of the most recent auto update: • Successful. • Failed to connect to WHOIS server. • Connection failed. • Failed to query DNS (which means failed to send DNS requests).
ISP update count	Number of ISPs in the most recent update.
LB ISP	ISP name.
Description	Description for the ISP.
Source	Source of the ISP: • **user-set**—Manually configured. • **file-load**—Imported from a file. • **auto-update**—ISP auto update.

display loadbalance limit-policy

Use **display loadbalance limit-policy** to display LB connection limit policy information.

Syntax

display loadbalance limit-policy [**name** *policy-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

policy-name: Specifies an LB connection limit policy by its name, a case-insensitive string of 1 to 63 characters.

Examples

Display information about the LB connection limit policy **lptest**.

```
<Sysname> display loadbalance limit-policy name lptest
Limit-policy: lptest
  Description:
  Limit rule:
limit lptest acl 3000 amount 10 10
```

display loadbalance link

Use **display loadbalance link** to display LB link information or link group member information.

Syntax

display loadbalance link [**brief** | **name** *link-name*]

display loadbalance link link-group *link-group-name* [**name** *link-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

brief: Displays brief information about all LB links. If you do not specify this keyword, the command displays detailed LB link information.

name *link-name*: Displays detailed information about the specified LB link. The *link-name* argument specifies an LB link name, a case-insensitive string of 1 to 63 characters.

link-group *link-group-name*: Displays information about members of a link group. The *link-group-name* argument specifies a link group by its name, a case-insensitive string of 1 to 63 characters.

name *link-name*: Displays information about a link group member. The *link-name* argument specifies a link group member by its name, a case-insensitive string of 1 to 63 characters. If you do not specify this option, the command displays information about all members of a link group.

Usage guidelines

If you do not specify the **brief** keyword or the **name** *link-name* option, the command displays detailed information about all LB links.

Examples

Display brief information about all LB links.

```
<Sysname> display loadbalance link brief
Link         Router IP/Interface    State        VPN instance     Link group
Lk1          192.168.1.1            Busy         vpn1             lg
Lk2          192.168.2.1            Active       vpn1             lg
Lk3          Dialer0                Inactive     vpn1             lg
```

Display detailed information about the LB link **lk**.

```
<Sysname> display loadbalance link name lk
Link: lk
  Description: lk
  State: Busy
  VPN instance: vpn1 (Inherit)
  Inherit VPN: Enabled
  Router IP: 1.2.3.4
  Router IPv6: --
  Link-group: lg
  Weight: 100
  Priority: 4
  Cost: 0
  Slow-shutdown: Disabled
  Connection limit: 0
  Rate limit:
    Connections: 10000
    Bandwidth: 10000 kbps
    Inbound bandwidth: 5000 kbps
    Outbound bandwidth: 5000 kbps
Bandwidth busy:
    Max bandwidth: 10000 kbps
    Max inbound bandwidth: 5000 kbps
    Max outbound bandwidth: 5000 kbps
    Busy rate: 80
    Inbound busy rate: 70
    Outbound busy rate: 60
    Busy recovery rate: 60
    Inbound busy recovery rate: 60
    Outbound busy recovery rate: 60
Probe information:
    Probe success criteria: All
    Probe method                    State
    t4                              Inactive

Link: lk2
  Description: link2
  State: Inactive
```

```
  VPN instance: vpn2 (Config)
  Inherit VPN: Disabled
  IPv4 address state: Active
  IPv6 address state: Inactive
  Router interface: Dialer0
  Link group: lg
  Weight: 150
  Priority: 3
  Cost: 100
  Slow shutdown: Enabled
  Connection limit: 10000
  Rate limit:
    Connections: 10000
    Bandwidth: 10000 kbps
    Inbound bandwidth: 5000 kbps
    Outbound bandwidth: 5000 kbps
  Bandwidth busy:
    Max bandwidth: 10000 kbps
    Max inbound bandwidth: 5000 kbps
    Max outbound bandwidth: 5000 kbps
    Busy rate: 80
    Inbound busy rate: 70
    Outbound busy rate: 60
    Busy recovery rate: 60
    Inbound busy recovery rate: 60
    Outbound busy recovery rate: 60
Probe information:
  Probe success criteria: All
  Probe method                    State
  t4                              Inactive
```

Display information about all members of link group **lg**.

```
<Sysname> display loadbalance link link-group lg
Link group: lg
  Link: lk1
    Description: link 1
    Parent state: Inactive
    State: Inactive
    Weight: 2
    Priority: 2
    Slow shutdown: Disabled
    Connection limit: --
    Connection rate limit: --
    Probe information:
      Probe success criteria: All
      Probe method                      State
      icmp                              Failed

  Link: lk2
```

```
Description: link 2
Parent state: Inactive
State: Inactive
Weight: 100
Priority: 4
Slow shutdown: Disabled
Connection limit: --
Connection rate limit: --
Probe information:
  Probe success criteria: All
  Probe method                        State
  tcp                                 Failed
```

Table 16 Command output

Field	Description
Link	LB link name.
Router IP/Interface	Gateway IP address or outgoing interface of the LB link.
Parent state/State	LB link state/Link group member state: • **Active**—The LB link is available. • **Busy**—The LB link is busy. • **Inactive**—The LB link is unavailable, because the configuration is not complete, the LB link is not referenced, or the virtual server is not enabled. • **Probe-failed**—Health monitoring has failed. • **Ramp**—Ramp-up phase of slow online. • **Shutdown**—The LB link is shut down. • **Standby**—Standby phase of slow online. • **Unknown**—Health monitoring is not configured.
VPN instance	VPN instance of the LB link. • **Config**—Manually configured. • **Inherit**—Inherited.
Link group	Link group to which the LB link belongs.
Description	Description for the LB link.
Inherit VPN	State of VPN instance inheritance: **Enabled** or **Disabled**.
IPv4 address state	IPv4 address state of the LB link: • **Active**—An available IPv4 address is obtained through the outgoing interface of the LB link. • **Inactive**—No available IPv4 address is obtained through the outgoing interface of the LB link. This field is displayed only if an outgoing interface is specified for an LB link.
IPv6 address state	IPv6 address state of the link: • **Active**—An available IPv6 address is obtained through the outgoing interface of the LB link. • **Inactive**—No available IPv6 address is obtained through the outgoing interface of the LB link. This field is displayed only if an outgoing interface is specified for an LB link.
Weight	Weight of the LB link.
Priority	Priority of the LB link.

Field	Description
Cost	Cost for proximity calculation.
Slow shutdown	Slow offline state of the LB link: • Disabled. • Enabled.
Connection limit	Maximum number of connections for the LB link.
Connection rate limit	Maximum number of connections per second for the LB link.
Rate limit	Rate limit of the LB link.
Connections	Maximum number of connections per second for the LB link.
Bandwidth	Maximum bandwidth for the LB link in kbps.
Inbound bandwidth	Maximum inbound bandwidth for the LB link in kbps.
Outbound bandwidth	Maximum outbound bandwidth for the LB link in kbps.
Bandwidth busy	Bandwidth ratio.
Max bandwidth	Maximum expected bandwidth for the LB link in kbps.
Max inbound bandwidth	Maximum inbound expected bandwidth for the LB link in kbps.
Max outbound bandwidth	Maximum outbound expected bandwidth for the LB link in kbps.
Busy rate	Bandwidth ratio for the LB link.
Inbound busy rate	Inbound bandwidth ratio for the LB link.
Outbound busy rate	Outbound bandwidth ratio for the LB link.
Busy recovery rate	Bandwidth recovery ratio for the LB link.
Inbound busy recovery rate	Inbound bandwidth recovery ratio for the LB link.
Outbound busy recovery rate	Outbound bandwidth recovery ratio for the LB link.
Probe information	Detailed health monitoring information for the LB link.
Probe success criteria	Health monitoring success criteria for the LB link: • **All**—Health monitoring succeeds only when all the specified health monitoring methods succeed. • **At least**—Health monitoring succeeds when a specified minimum number of health monitoring methods succeed.
Probe method	Name of the NQA template used by the health monitoring method.
State	State of the health monitoring method: • **Failed**—Health monitoring has failed. • **In progress**—Health monitoring is in progress. • **Invalid**—Health monitoring is unavailable (because the configuration of the NQA template is not complete), or the real server is unavailable. • **Succeeded**—Health monitoring has succeeded.

display loadbalance link out-interface statistics

Use **display loadbalance link out-interface statistics** to display link outbound interface statistics.

Syntax

display loadbalance link out-interface statistics [**name** *link-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

name *link-name*: Specifies a link by its name, a case-insensitive string of 1 to 63 characters. If you do not specify this option, the command displays outbound interface statistics for all links.

Usage guidelines

If the link outbound interface is a logical interface, the rate statistics are calculated based on the interface traffic.

Examples

Display outbound interface statistics for the link **lk1**.

```
<Sysname> display loadbalance link out-interface statistics name lk1
Loadbalance link: lk1
Input rate: 1524 bps
  Output rate: 90 bps
```

Table 17 Command output

Field	Description
Loadbalance link	LB link name.
Input rate	Input rate of the outbound interface in bps.
Output rate	Output rate of the outbound interface in bps.

display loadbalance link statistics

Use **display loadbalance link statistics** to display link statistics or link group member statistics.

Syntax

display loadbalance link statistics [**name** *link-name*] [**slot** *slot-number*]

display loadbalance link statistics link-group *link-group-name* [**name** *link-name*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

name *link-name*: Specifies a link by its name, a case-insensitive string of 1 to 63 characters.

link-group *link-group-name*: Displays statistics for members of a link group. The *link-group-name* argument specifies a link group by its name, a case-insensitive string of 1 to 63 characters.

name *link-name*: Displays statistics for a link group member. The *link-name* argument specifies a link group member by its name, a case-insensitive string of 1 to 63 characters. If you do not specify this option, the command displays statistics for all members of a link group.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays link statistics for all member devices.

Examples

Display statistics for the link **lk1**.

```
<Sysname> display loadbalance link statistics name lk1
Loadbalance link: lk1
  Total connections: 1798
  Active connections: 788
  Max connections: 803
    recorded at 11:02:49 on Tue May 21 2019
  Connections per second: 157
  Max connections per second: 163
    recorded at 11:02:49 on Tue May 21 2019
  Downstream traffic: 333332 bytes
  Upstream traffic: 472054 bytes
  Throughput: 4396 bps
  Inbound throughput: 1214 bps
  Outbound throughput: 3128 bps
  Max throughput: 4564 bps
    recorded at 11:02:49 on Tue May 21 2019
  Max inbound throughput: 1214 bps
    recorded at 11:02:49 on Tue May 21 2019
  Max outbound throughput: 3320 bps
    recorded at 11:02:49 on Tue May 21 2019
  Received packets: 1798
  Sent packets: 0
  Dropped packets: 0
  Packet loss rate: 10
```

Display statistics for all members of link group **lg**.

```
<Sysname> display loadbalance link statistics link-group lg
Loadbalance link group: lg
  Loadbalance link: lk1
    Total connections: 0
```

```
  Active connections: 0
  Max connections: 0
    recorded at 11:02:49 on Tue May 21 2019
  Connections per second: 0
  Max connections per second: 0
    recorded at 11:02:49 on Tue May 21 2019
  Downstream traffic: 0 bytes
  Upstream traffic: 0 bytes
  Throughput: 0 bps
  Inbound throughput: 0 bps
  Outbound throughput: 0 bps
  Max throughput: 0 bps
    recorded at 11:02:49 on Tue May 21 2019
  Max inbound throughput: 0 bps
    recorded at 11:02:49 on Tue May 21 2019
  Max outbound throughput: 0 bps
    recorded at 11:02:49 on Tue May 21 2019
  Received packets: 0
  Sent packets: 0
  Dropped packets: 0

Loadbalance link: lk2
  Total connections: 0
  Active connections: 0
  Max connections: 0
    recorded at 11:02:49 on Tue May 21 2019
  Connections per second: 0
  Max connections per second: 0
    recorded at 11:02:49 on Tue May 21 2019
  Downstream traffic: 0 bytes
  Upstream traffic: 0 bytes
  Throughput: 0 bps
  Inbound throughput: 0 bps
  Outbound throughput: 0 bps
  Max throughput: 0 bps
    recorded at 11:02:49 on Tue May 21 2019
  Max inbound throughput: 0 bps
    recorded at 11:02:49 on Tue May 21 2019
  Max outbound throughput: 0 bps
    recorded at 11:02:49 on Tue May 21 2019
  Received packets: 0
  Sent packets: 0
  Dropped packets: 0
```

Table 18 Command output

Field	Description
Loadbalance link	Link name.
Total connections	Total number of connections.

Field	Description
Active connections	Number of active connections.
Max connections	Maximum number of connections.
Connections per second	Number of connections per second.
Max connections per second	Maximum number of connections per second.
Downstream traffic	Downstream traffic (in bytes) received by the LB device.
Upstream traffic	Upstream traffic (in bytes) sent by the LB device.
Throughput	Total packet throughput in bps.
Inbound throughput	Inbound packet throughput in bps.
Outbound throughput	Outbound packet throughput in bps.
Max throughput	Maximum packet throughput in bps.
Max inbound throughput	Maximum inbound packet throughput in bps.
Max outbound throughput	Maximum outbound packet throughput in bps.
Received packets	Number of received packets.
Sent packets	Number of sent packets.
Dropped packets	Number of dropped packets.
Packet loss rate	Packet loss ratio of the link.

display loadbalance link-group

Use **display loadbalance link-group** to display link group information.

Syntax

display loadbalance link-group [**brief** | **name** *link-group-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

brief: Displays brief information about all link groups. If you do not specify this keyword, the command displays detailed link group information.

name *link-group-name*: Specifies a link group by its name, a case-insensitive string of 1 to 63 characters. If you do not specify this option, the command displays information about all link groups.

Usage guidelines

If you do not specify any parameters, the command displays detailed information about all link groups.

A link is displayed as unavailable if the link group configuration is not complete, the link group is not referenced, or the virtual server is not enabled. This does not mean that the link is not available.

Examples

Display brief information about all link groups.

```
<Sysname> display loadbalance link-group brief
Predictor: RR - Round robin, RD - Random, LC - Least connection,
           BW – Bandwidth, MBW – Max bandwidth,
           IBW – Inbound bandwidth, OBW – Outbound bandwidth,
           MIBW – Max inbound bandwidth, MOBW – Max outbound bandwidth,
           HASH(SIP) - Hash address source IP,
           HASH(DIP) - Hash address destination IP,
           HASH(SIP-PORT) - Hash address source IP-port
NAT/SNAT: Y - Enabled, N - Disabled

Link group       Predictor    NAT   SNAT  Total  Active
lg               RR           Y     N     3      3
```

Display detailed information about all link groups.

```
<Sysname> display loadbalance link-group
Link group: lg1
  Description:
  Predictor: Hash address
  Proximity: Disabled
  NAT: Enabled
  SNAT pool:
  Failed action: Keep
  Active threshold: Enabled
    Lower: 80
    Upper: 90
  Slow-online: Enabled
  Standby time: 5s
  Ramp-up time: 10s
  Selected link: Enabled
    Min link: 100
    Max link: 600
  Probe information:
    Probe success criteria: All
    Probe method:
    aaa
    ddd
  Total link: 1
  Active link: 1
  Link list:
  Name             State         VPN instance    Router IP    Weight    Priority
  Link1            Inactive      vpn1            1.2.3.4      4         100
```

Table 19 Command output

Field	Description
Link group	Link group name.
Description	Description for the link group.
Predictor	Scheduling algorithm of the link group: • **RR**—Weighted round robin algorithm. • **RD**—Random algorithm. • **LC**—Weighted least connection algorithm. • **BW**—Bandwidth algorithm. • **IBW**—Inbound bandwidth algorithm. • **OBW**—Outbound bandwidth algorithm. • **MBW**—Maximum bandwidth algorithm. • **MIBW**—Maximum inbound bandwidth algorithm. • **MOBW**—Maximum outbound bandwidth algorithm. • **HASH(SIP)**—Hash algorithm based on source IP address. • **HASH(DIP)**—Hash algorithm based on destination IP address. • **HASH(SIP-PORT)**—Hash algorithm based on source IP address and port number.
Proximity	Proximity state of the link group: • Disabled. • Enabled.
NAT	NAT state of the link group: • Disabled. • Enabled.
SNAT pool	Name of the SNAT address pool referenced by the link group.
Failed action	Fault processing method of the link group: • **Keep**—Keeps existing connections. • **Reschedule**—Redirects connections. • **Reset**—Terminates existing connections.
Active threshold	State of the criteria to determine that the link group is available: disabled or enabled. If the state is enabled, the following fields are displayed: • **Lower**—Lower percentage value. • **Upper**—Upper percentage value.
Slow-online	State of the slow online feature: disabled or enabled. If the state is enabled, the following fields are displayed: • Standby time. • Ramp-up time.
Selected link	State of link limit to participate in scheduling: disabled or enabled. If the state is enabled, the following fields are displayed: • **Min server**—Minimum number of links that participate in scheduling. • **Max server**—Maximum number of links that participate in scheduling.
Probe success criteria	Health monitoring success criteria for the link group: • **All**—Health monitoring succeeds only when all the specified health monitoring methods succeed. • **At least X**—Health monitoring succeeds when a minimum of *X* health monitoring methods succeed.
Probe method	Name of the NQA template used by the health monitoring method.

Field	Description
Total link	Total number of links.
Active link	Number of active links.
Name	Link name.
State	Link state: • **Active**—The link is available. • **Busy**—The link is busy. When the link is in **Active** or **Ramp** state and enabled with bandwidth statistics collection and link protection, this field displays **Busy** if the maximum expected bandwidth is reached. • **Inactive**—The link is unavailable, because the configuration is not complete, the link is not referenced, or the virtual server is not enabled. • **Probe-failed**—Health monitoring has failed. • **Ramp**—Ramp-up phase of slow online. • **Shutdown**—The link is shut down. • **Standby**—Standby phase of slow online.
VPN instance	VPN instance of the link.
Router IP	IPv4 and IPv6 addresses of the link.
Weight	Weight of the link.
Priority	Priority of the link.

display loadbalance local-dns-server parse-fail-record

Use **display loadbalance local-dns-server parse-fail-record** to display DNS request parse failures.

Syntax

display loadbalance local-dns-server parse-fail-record [**type** { **a** | **aaaa** | **cname** | **mx** | **ns** | **soa** | **srv** | **txt** }] [**domain** *domain-name*] | **ptr** [**ip address** { *ipv4-address* | *ipv6-address* }]] [**vpn-instance** *vpn-instance-name*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

type { **a** | **aaaa** | **cname** | **mx** | **ns** | **ptr** | **soa** | **srv** | **txt** }: Specifies a DNS request type. If you do not specify a DNS request type, this command displays DNS request parse failures for all DNS request types.

domain *domain-name*: Specifies a domain name, a case-insensitive, dot-separated string of 1 to 254 characters for an absolute domain name or 1 to 253 characters for a relative domain name. Each dot-separated label in the domain name can contain a maximum of 63 characters. If you do not specify a domain name, this command displays DNS request parse failures for all domain names.

ip address { *ipv4-address* | *ipv6-address* }: Specifies an IP address used for reverse DNS. If you do not specify this option, the command displays DNS request parse failures for all IP addresses.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays DNS request parse failures for the public network.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays DNS request parse failures for all member devices.

Examples

Display all DNS request parse failures.

```
<Sysname> display loadbalance local-dns-server parse-fail-record
Slot 0:
  ID Time        Type  SIP/Port  DIP/Port   VN instance Domain       Failure cause
--------------------------------------------------------------------------------
---
  1  03 Nov 2016 A     1.2.3.4/1 2.2.2.2/53 vpn1        www.aaa.com  No matched virtual
     19:09:52                                                         server member.
  2  03 Nov 2016 AAAA  1.2.3.4/2 2.2.2.2/53 vpn1       www.lb.com   No matched.
     19:09:43                                                         DNS mapping
  3  03 Nov 2016 MX    1.2.3.5/3 2.2.2.2/53 vpn1        mail.aa.com  No matched record.
     20:09:41
  4  04 Nov 2016 NS    1.2.3.4/4 2.2.2.2/53 vpn1        ns.aaa.com   No matched record.
     11:15:40
  5  05 Nov 2016 CNAME 1.2.3.4/5 2.2.2.2/53 vpn1        www.aaa.com  No matched DNS
     11:16:35                                                         zone.
  6  05 Nov 2016 SOA   1.2.3.4/6 2.2.2.2/53 vpn1        www.aaa.com  No matched DNS
     12:16:25                                                         zone.
  7  05 Dec 2016 PTR   1.2.3.4/7 2.2.2.2/53 vpn1        1.2.3.4      No matched record.
     15:19:16
```

Table 20 Command output

Field	Description
ID	Failure record ID.
Time	Time when the device received a DNS request.
Type	Resource record type: • **A**—IPv4 host address. • **AAAA**—IPv6 host address. • **CNAME**—Canonical name. • **MX**—Mail exchanger. • **NS**—Name server. • **PTR**—Pointer. • **SOA**—Start of authority. • **SRV**—Service. • **TXT**—Text.
SIP/Port	Source IP address and port number of a DNS request.
DIP/Port	Destination IP address and port number of a DNS request.
Failure cause	Failure cause for DNS request parsing:

Field	Description
	• **--**—Parsing succeeded. • No matched DNS listener. • No matched DNS mapping. • No matched virtual server pool. • No matched DNS zone. • Failed to get buffer. • No matched record. • No enough memory resource. • Failed to parse domain. • Failed to find DNS listener by ID. • No scheduling content. • **Scheduling failed**—The scheduling content exists, but scheduling failed. • No matched virtual server member.

display loadbalance policy

Use **display loadbalance policy** to display LB policy information.

Syntax

display loadbalance policy [**name** *policy-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

name *policy-name*: Specifies an LB policy by its name, a case-insensitive string of 1 to 63 characters. If you do not specify this option, the command displays information about all LB policies.

Examples

Display information about all LB policies.

```
<Sysname> display loadbalance policy
LB policy: lbp1
  Description:
  Type: Generic
  Class: lbc1
   Action: lba1
  Default action: lba0

LB policy: lbp2
  Description:
  Type: HTTP
  Default action:
```

```
LB policy: lbp3
  Description:
  Type: Link-generic
  Class: lbc3
  Action: lba3
  Default action: lba3

LB policy: lbp4
  Description:
  Type: DNS
  Class: lbc4
  Action: lba4
  Default action: lba4

LB policy: lbp5
  Description:
  Type: MySQL
  Class: lbc5
  Action: lba5
  Default action: lba5
```

Table 21 Command output

Field	Description
LB policy	LB policy name.
Description	Description for the LB policy.
Type	LB policy type: • DNS. • Generic. • HTTP. • Link-generic. • MySQL. • RADIUS.
Class	LB class for the LB policy.
Action	LB action for the LB class.
Default class action	Default LB action.

display loadbalance probe-template

Use **display loadbalance probe-template** to display LB probe template information.

Syntax

display loadbalance probe-template [**name** *template-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

name *template-name*: Specifies an LB probe template by its name, a case-insensitive string of 1 to 32 characters. If you do not specify this option, the command displays information about all LB probe templates.

Examples

Display information about all LB probe templates.

```
<Sysname> display loadbalance probe-template
Load balancing probe template: rst1
  Description:
  Type: tcp-rst
  Monitoring interval: 20 sec
  RST threshold: 10
  Protection action: auto-shutdown

Load balancing probe template: zero2
  Description:
  Type: tcp-zero-window
  Monitoring interval: 30 sec
  Zero-window threshold: 20
  Protection action: busy
    Probe interval: 30 sec
    Probe times: 3

Load balancing probe template: icmp1
  Description:
  Type: icmp
  Timeout: 3 sec
  Frequency: 300
  Load balancing probe template: http1
  Description:
  Type: http-passive
  Monitoring interval: 1 sec
  Abnormal-url threshold: 10000
  Timeout: 30 sec
  URL list:
    aaa
  Status code list:
    404

Load balancing probe template: test_external
  Description:
  Type: external-monitor
```

```
External script: http.sh
Monitoring interval: 5 sec
Timeout: 6 sec
Argument: 192.168.1.123
Environment variable list:
  Name               Value
  Test3              /opt/lib
  Test4              /usr/bin
```

Table 22 Command output

Field	Description
Load balancing probe template	LB probe template name.
Description	Description for the LB probe template.
Type	LB probe template type: • **external-monitor**—Custom monitoring. • **http-passive**. • **icmp**. • **tcp-rst**. • **tcp-zero-window**.
Monitoring interval	Monitoring time. During the monitoring time, the system counts the number of RST packets or zero-window packets sent by each server farm member in a server farm. This field is displayed only for a custom-monitoring, HTTP passive, TCP-RST, or TCP zero-window LB probe template.
RST threshold	Maximum number of RST packets a real server can send. This field is displayed only for a TCP-RST LB probe template.
Zero-window threshold	Maximum percentage of zero-window packets a real server can send. This field is displayed only for a TCP zero-window LB probe template.
Protection action	Action to take when the RST or zero-window packet threshold is reached: **Auto-shutdown** or **Busy**. This field is displayed only for a TCP-RST or TCP zero-window LB probe template.
Probe interval	Interval to probe the real server in busy state. This field is displayed only for a TCP-RST or TCP zero-window LB probe template.
Probe times	Maximum number of times for probing the real server in busy state. If the number of probe times is reached, the real server is automatically shut down. This field is displayed only for a TCP-RST or TCP zero-window LB probe template.
Timeout	Timeout time for probe responses, HTTP responses, or custom monitoring probe packet responses. This field is displayed only for an ICMP LB probe template, HTTP passive, or custom-monitoring LB probe template.
Frequency	Probe interval for an LB probe template. This field is displayed only for an ICMP LB probe template or HTTP passive LB probe template.
Abnormal-url threshold	Upper limit of URL error times. This field is displayed only for an HTTP passive LB probe template.
URL list	List of URLs to check for an HTTP passive LB probe template This field is displayed only for an HTTP passive LB probe template.

Field	Description
Status code list	List of response status codes to check for an HTTP passive LB probe template This field is displayed only for an HTTP passive LB probe template.
External script	Script file used by a custom-monitoring LB probe template. This field is displayed only for a custom-monitoring LB probe template.
Argument	User-defined information for a custom-monitoring LB probe template. This field is displayed only for a custom-monitoring LB probe template.
Environment variables list	Environment variable list for a custom-monitoring LB probe template. This field is displayed only for a custom-monitoring LB probe template.
Name	Environment variable name. This field is displayed only for a custom-monitoring LB probe template.
Value	Environment variable value. This field is displayed only for a custom-monitoring LB probe template.

Related commands

reset real-server statistics

display loadbalance process-limit

Use **display loadbalance process-limit** to display the maximum number of processes allowed to be started for custom monitoring.

Syntax

display loadbalance process-limit

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display the maximum number processes allowed to be started for custom monitoring.

```
<Sysname> display loadbalance process-limit
Loadbalance process-limit: 200
```

display loadbalance protection-policy

Use **display loadbalance protection-policy** to display the configuration of protection policies.

Syntax

display loadbalance protection-policy [**name** *policy-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

name *policy-name*: Specifies a protection policy by its name, a case-insensitive string of 1 to 63 characters. If you do not specify a protection policy, this command displays the configuration of all protection policies.

Examples

Display the configuration of all protection policies.

```
<Sysname> display loadbalance protection-policy
Policy name: p1
  Description:
  Type: HTTP
  Protection action: verify js
  Rule ID: 3
    URL: /index.php
    Protection period: 2
    Method                    Threshold
    Cookie (Jsessionid)       20
    Source IP                 10
  Rule ID: 5
    URL: /test.php
    Protection period: 20
    Method                    Threshold
    Cookie (A1B2C3D4)         20
```

Table 23 Command output

Field	Description
Protection action	Protection action: • **warning**—Generates a log message. • **drop**—Drops requests. • **verify (insert header)**—Performs cookie verification by inserting an HTTP header. • **verify (js)**—Performs cookie verification by inserting a JS script.
URL	Protected URL.
Method	Threshold type: • **Cookie (xxx)**—Cookie-based threshold (cookie name). • **Source IP**—- Source-IP-based threshold.

display loadbalance proximity

Use **display loadbalance proximity** to display proximity entry information.

Syntax

display loadbalance proximity [**vpn-instance** *vpn-instance-name*] [**ip** [*ipv4-address*] | **ipv6** [*ipv6-address*]] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command displays proximity entry information for the public network.

ip [*ipv4-address*]: Displays IPv4 proximity entry information. If you specify the *ipv4-address* argument, this command displays detailed information about the proximity entry corresponding to the IPv4 address. If you do not specify the *ipv4-address* argument, this command displays brief information about all IPv4 proximity entries.

ipv6 [*ipv6-address*]: Displays IPv6 proximity entry information. If you specify the *ipv6-address* argument, this command displays detailed information about the proximity entry corresponding to the IPv6 address. If you do not specify the *ipv6-address* argument, this command displays brief information about all IPv6 proximity entries.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays proximity information for all member devices.

Usage guidelines

If you do not specify the **vpn-instance**, **ip**, or **ipv6** keyword, this command displays brief information about all IPv4 and IPv6 proximity entries.

Examples

Display brief information about all IPv4 and IPv6 proximity entries for the public network.

```
<Sysname> display loadbalance proximity
(*) – Real server object
Slot :1
  IPv4 address/Mask length       Timeout     Best link  RTT      Dynamic weight
  ------------------------------------------------------------------------------
  1.2.3.0/24                     59          lk1        1        170
  1.2.15.0/24                    58          lk2        2        170
  IPv6 address/Prefix length     Timeout     Best link  RTT      Dynamic weight
  ------------------------------------------------------------------------------
  11:22::/96                     40          lk1        3        200
```

Display detailed information about the proximity entry corresponding to the IP address 1.2.3.1 for the public network.

```
<Sysname> display loadbalance proximity ip 1.2.3.1
```

```
(*) – Real server object
IPv4 address/Mask length: 1.2.3.0/24
Timeout: 40
Link list/RTT:
  lk1/1
  lk2/3
```

Display detailed information about the proximity entry corresponding to the IPv6 address 11:22:: for the VPN instance **vpn1**.

```
<Sysname> display loadbalance proximity vpn-instance vpn1 ipv6 11:22::
(*) – Real server object
IPv6 address/Prefix length: 11:22::/96
Timeout: 34
Link list/RTT:
  lk1/2
  lk2/3
```

Table 24 Command output

Field	Description
Slot	Card for which proximity entry information is displayed.
Timeout	Remaining time of the proximity entries, in seconds.
Link list	Links for the proximity entry. They are listed in descending priority order.
RTT	Network delay for the link in milliseconds.

display loadbalance reverse-zone

Use **display loadbalance reverse-zone** to display DNS reverse zone information.

Syntax

display loadbalance reverse-zone { **ip** [*ipv4-address mask-length*] | **ipv6** [*ipv6-address prefix-length*] }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ip: Displays IPv4 DNS reverse zone information.

ipv4-address mask-length: Specifies an IPv4 address and the mask length. The mask length is in the range of 0 to 32. If you do not specify this argument, the command displays all IPv4 DNS reverse zone information.

ipv6: Displays IPv6 DNS reverse zone information.

ipv6-address prefix-length: Specifies an IPv6 address and the prefix length. The prefix length is in the range of 0 to 128. If you do not specify this argument, the command displays all IPv6 DNS reverse zone information.

Examples

Display all IPv4 DNS reverse zone information.

```
<Sysname> display loadbalance reverse-zone ip
Reverse zone: 10.1.1.0/24
Record list:
Type      TTL      RDATA
PTR       3600     1.1.1.2  a.mail.nsfocus.com.cn
PTR       2700     1.1.1.3  b.mail.nsfocus.com.cn
```

Display all IPv6 DNS reverse zone information.

```
<Sysname> display loadbalance reverse-zone ipv6
Reverse zone: 1::/64
Record list:
Type      TTL     RDATA
PTR       3600    1::1  a.mail.nsfocus.com.cn
PTR       2700    1::2  b.mail.nsfocus.com.cn
```

Table 25 Command output

Field	Description
Reverse zone	IPv4/IPv6 address and mask/prefix length of the DNS reverse zone.
Record list	List of resource records.
Type	Resource record type (only PTR is supported).
TTL	TTL of the resource record, in seconds.
RDATA	Resource data.

display loadbalance snat-global-policy

Use **display loadbalance snat-global-policy** to display SNAT global policy information.

Syntax

display loadbalance snat-global-policy [**name** *policy-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

name *policy-name*: Specifies a SNAT global policy by its name, a case-insensitive string of 1 to 63 characters. If you do not specify this option, the command displays information about all SNAT global policies.

Examples

Display information about all SNAT global policies.

```
<Sysname> display loadbalance snat-global-policy
Policy name: lbsnat1
  Description:
  State: Active
  Priority: 0
  VPN instance:
  Source IP object group: src-obj
  Destination IP object group: dst-obj
  Service object group: proto-obj
  Translation mode: snat-pool sp

Policy name: lbsnat2
  Description:
  State: Inactive(disable)
  Priority: 0
  VPN instance:
  Source IP object group: src-obj
  Destination IP object group:
  Service object group:
  Translation mode: auto-map
```

Table 26 Command output

Field	Description
State	State of the SNAT global policy: • **Active**—The SNAT global policy is enabled and available. • **Inactive**—The SNAT global policy is enabled but unavailable. • **Inactive (disabled)**—The SNAT global policy is disabled and unavailable.

display loadbalance snat-pool

Use **display loadbalance snat-pool** to display SNAT address pool information.

Syntax

display loadbalance snat-pool [**name** *pool-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

name *pool-name*: Specifies a SNAT address pool by its name, a case-insensitive string of 1 to 63 characters. If you do not specify this option, the command displays information about all SNAT address pools.

Examples

Display information about all SNAT address pools.

```
<Sysname> display loadbalance snat-pool
SNAT pool: lbsp1
  Description:
  VPN instance: VPN1
  IPv4 range:
    Start address                   End address
    202.110.10.5                    202.110.10.10
    202.110.20.10                   202.110.20.15
  IPv6 range:
    Start address                   End address
    2002::2                         2002::100
    2002::200                       2002::300
  ARP/ND interfaces:
    GigabitEthernet1/0/1
    GigabitEthernet1/0/3

SNAT pool: lbsp2
  Description:
  VPN instance: VPN1
  IPv4 range:
    Start address                   End address
    203.110.10.10                   203.110.10.15
  IPv6 range:
    Start address                   End address
    2003::2                         2003::100
  ARP/ND interfaces:
    GigabitEthernet1/0/2
```

Table 27 Command output

Field	Description
SNAT pool	SNAT address pool name.
Description	Description for the SNAT address pool.
VPN instance	VPN instance to which the SNAT address pool belongs.
IPv4 range	IPv4 address range.
IPv6 range	IPv6 address range.
ARP/ND interfaces	Interfaces from which gratuitous ARP packets and ND packets are sent out.

display loadbalance virtual-server total-statistics

Use **display loadbalance virtual-server total-statistics** to display cumulative statistics for all virtual servers.

Syntax

display loadbalance virtual-server total-statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays cumulative statistics for all virtual servers on all member devices.

Usage guidelines

This command displays the cumulative connection statistics for all virtual servers. If you execute the **reset virtual-server** command for a virtual server, the statistical values are affected.

Examples

Display cumulative statistics for all virtual servers.

```
<Sysname> display loadbalance virtual-server total-statistics
Slot 1:
  Total connections: 0
  Active connections: 0
  Connections per second: 0

Slot 2:
  Total connections: 0
  Active connections: 0
  Connections per second: 0
```

Table 28 Command output

Field	Description
Total connections	Total number of connections.
Active connections	Number of active connections.
Connections per second	Number of connections per second.

display loadbalance virtual-server-pool

Use **display loadbalance virtual-server-pool** to display virtual server pool information.

Syntax

display loadbalance virtual-server-pool [**brief** | **name** *pool-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

brief: Displays brief information about all virtual server pools.

name *pool-name*: Displays detailed information about the specified virtual server pool.

Usage guidelines

If you do not specify the **brief** keyword or the **name** *pool-name* option, the command displays detailed information about all virtual server pools.

Examples

Display brief information about all virtual server pools.

```
<Sysname> display loadbalance virtual-server-pool brief
Predictor: RR - Round robin, RD - Random, LC - Least connection,
           TOP - Topology, PRO – Proximity
           BW - Bandwidth, MBW - Max bandwidth,
           IBW - Inbound bandwidth, OBW - Outbound bandwidth,
           MIBW - Max inbound bandwidth, MOBW - Max outbound bandwidth,
           HASH(SIP) - Hash address source IP,
           HASH(DIP) - Hash address destination IP,
           HASH(SIP-PORT) - Hash address source IP-port
VSpool           Pre    Alt    Fbk    BWP     Total    Active
vsp              RR     LC            Enabled  0        0
vpp              RR                   Enabled  0        0
vsp1             RD     TOP           Enabled  3        0
```

Display detailed information about the virtual server pool **local-pool**.

```
<Sysname> display loadbalance virtual-server-pool name local-pool
Virtual-server pool: local-pool
  Predictor:
   Preferred RD
   Alternate TOP
   Fallback  --
Bandwidth busy-protection: Disabled
Total virtual servers: 3
Active virtual servers: 0
Virtual server list:
Name      State     Address       Port     Weight  Link
vs1       Active    192.168.1.1   0        150     ct-link1
vs2       Active    192.167.1.1   0        120     ct-link2
```

```
vs3       Active    192.169.1.1   0        80      cnc-link
Virtual IP address list:
Address        State      Weight  Link
10.0.1.1       Active     150     ct-link1
10.1.1.1       Active     120     ct-link2
10.2.1.1       Active     80      cnc-link
Virtual IPv6 address list:
Address        State      Weight  Link
9::5           Active     150     ct-link1
9::6           Active     120     ct-link2
9::7           Active     80      cnc-link
```

Table 29 Command output

Field	Description
Virtual-server pool	Virtual server pool name.
Predictor	Scheduling algorithm of the virtual server pool.
Bandwidth busy-protection	Link protection feature state for the virtual server pool: • Disabled. • Enabled.
Name	Name of the virtual server.
State	Virtual server state: • **Active**—The virtual server is available. • **Busy**—The virtual server is busy. When the virtual server is in **Active** state and enabled with the link protection feature, this field displays **Busy** if the maximum expected bandwidth is reached. • **Inactive**—The virtual server is unavailable, because the configuration is not complete or the associated LB link is unavailable.
Address	IP address of the virtual server or virtual IP address.
Port	Port number of the virtual server.
Weight	Weight of the virtual server or virtual IP address.
Link	LB link used by the virtual server.

display loadbalance zone

Use **display loadbalance zone** to display DNS forward zone information.

Syntax

display loadbalance zone [**name** *domain-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

name *domain-name*: Specifies a domain name. It is a dot-separated, case-insensitive string that can include letters, digits, hyphens (-), underscores (_), and dots (.). The domain name can include a maximum of 253 characters, and each separated string includes no more than 63 characters. If you do not specify a domain name, this command displays DNS forward zone information for all domain names.

Examples

Display all DNS forward zone information.

```
<Sysname> display loadbalance zone
Zone: abc.com
  TTL: 3600s
  SOA:
    Primary name server: ns1.abc.com
    Responsible mail: root.ns1.abc.com
    Serial: 11812
    Retry: 14400s
    Expire: 604800s
    Min TTL: 86400s
  Record list:
    Type    TTL        RDATA
    NS      3600s      ns1.abc.com
    NS      4200s      ns2.abc.com
    NS      4200s      a.abc.com       ns2.abc.com
    MX      3600s      a.mail.abc.com  10
    MX      2700s      b.mail.abc.com  20
    CNAME   5000s      a.test.abc.com  abc1.abc.com
    CNMAE   3600s      b.test.abc.com  abc2.abc.com
    TXT     5000s      v=spf1 include:spf.abcmail.abc.com.cn -all
    SRV     --       _ http._tcp.example.com. www.example.com 5 10 80
```

Table 30 Command output

Field	Description
Zone	Domain name of the DNS forward zone.
TTL	TTL of the resource record in the DNS forward zone, in seconds.
SOA	Start of Authority (SOA) information.
Responsible mail	Email address of the domain administrator.
Serial	Domain serial number.
Retry	Retry interval in seconds.
Expire	Expiration time in seconds.
Min TTL	Minimum TTL in seconds.
Record list	List of resource records.
Type	Resource record type: • **MX**—Mail exchange record. • **CNAME**—Canonical name record. • **NS**—Name server record.

Field	Description
	• **SRV**—Service location record. • **TXT**—Text record.
TTL	TTL of the resource record, in seconds.
RDATA	Resource data.

display parameter-profile

Use **display parameter-profile** to display parameter profile information.

Syntax

display parameter-profile [**name** *parameter-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

name *parameter-name*: Specifies a parameter profile by its name, a case-insensitive string of 1 to 63 characters. If you do not specify this option, the command displays information about all parameter profiles.

Examples

Display information about all parameter profiles.

```
<Sysname> display parameter-profile
Parameter profile: pp1
  Description:
  Type: IP
  IP ToS: 20

Parameter profile: pp2
  Description:
  Type: TCP
  Exceed MSS: Allow
  TCP window size: 65535
  TCP connection idle-timeout: 10
  Time-wait timeout: 5
  Keepalive idle-timeout: 300
  Keepalive retransmission interval: 3
  Keepalive retransmission count: 5
  SYN retransmission-timeout: 5
  Fin-wait1 timeout: 6
  Fin-wait2 timeout: 10
```

```
  Src-addr-option:
    Option number: 29
    Encoding: string
  TCP option insert:
    Option number: 28
    Value: src-ip
    Encoding: string
  TCP option remove:
    Option number: 8
  TCP option remove:
    Option number: 5

Parameter profile: pp3
  Description:
  Type: HTTP
  Rebalance per request: Enabled
  Server connection reuse: Enabled
  Case insensitive: Enabled
  Header modify per request: Enabled
  Content maximum parse length: 8192
  Header maximum parse length: 8192
  Secondary cookie delimiters: !@#$
  Secondary cookie start: ?
  Encrypted cookie name: cookie1
  Header exceed length: Drop

Parameter profile: compress
  Description:
  Type: HTTP compression
  Compression level: 1
  Prefer method: Gzip
  Content length threshold: 1024
  Memory size: 8KB
  Window size: 16KB
  Header Insert: Enabled
  Header Delete: Enabled
  Request version all: Disabled
  Rule 1: Permit url abc

Parameter profile: urlstat
  Description:
  Type: HTTP-statistics
  Node: bank1
    Description:
    rule 1 url url1
    rule 2 url url2
  Node: bank2
    Description:
```

```
    rule 1 url url3
    rule 2 url url4
  Object group name:
    ObjGrp1
    ObjGrp2

Parameter profile: pp4
  Description:
  Type: OneConnect
  Max reuse times: 1000
  Idle time: 10000
  IPv4 source mask length: 24
  IPv6 source prefix length: 120

Parameter profile: pp5
  Description:
  Type: TCP-application
  Match-buffer-time: 5
  Match-buffer-size: 4096
  Match-buffer-end: YY

Parameter profile: pp6
  Description:
  Type: MySQL
  Pool size: 2000
  Server connection reuse: Enabled
  Max reuse times: 1000
  Idle time: 10000 sec
  IPv4 source mask length: 24
  IPv6 source prefix length: 120
```

Table 31 Command output

Field	Description
Parameter profile	Parameter profile name.
Description	Description for the parameter profile.
Type	Parameter profile type: • IP. • HTTP. • HTTP-compression. • HTTP statistics. • MySQL. • OneConnect. • TCP. • TCP-application.
IP ToS	ToS field of the IP packets sent to the server.
Exceed MSS	Action to take on the segments that exceed the MSS in the HTTP requests sent by the client: • **Allow**—Allows the segments to exceed the MSS.

Field	Description
	• **Drop**—Discards the segments that exceed the MSS.
Rebalance per request	Whether or not to enable load balancing for each HTTP request.
Pool size	Size of the MySQL connection pool.
Server connection reuse	Whether or not to reuse the connection between the LB device and the server.
Header modify per request	Whether or not to perform the insert, delete, or modify operation for the header of each HTTP request or response packet.
Case insensitive	Whether or not to enable case sensitivity for matching character strings.
Content maximum parse length	Maximum length of the HTTP entities that can be parsed.
Header maximum parse length	Maximum length of the HTTP headers that can be parsed.
Secondary cookie delimiters	Delimiters that can separate secondary cookies in URLs.
Secondary cookie start	Start delimiter for secondary cookies in URLs.
Encrypted cookie name	Cookie enabled with encryption.
Header exceed length	Action to take on the HTTP requests or responses when their packet headers exceed the maximum length: • **Continue**—Continues to perform load balancing. • **Drop**—Stops performing load balancing, discards the packet, and terminates the connection.
TCP window size	Maximum local window size for TCP connections.
TCP connection idle-timeout	Idle timeout time for TCP connections, in seconds.
Time-wait timeout	TIME_WAIT state timeout time for TCP connections, in seconds.
Keepalive idle-timeout	Idle timeout time for sending TCP keepalive packets.
Keepalive retransmission interval	Retransmission interval for TCP keepalive packets.
Keepalive retransmission count	Retransmission times for TCP keepalive packets.
SYN retransmission-timeout	Retransmission timeout time for TCP SYN packets
Fin-wait1 timeout	FIN-WAIT-1 state timeout time for TCP connections.
Fin-wait2 timeout	FIN-WAIT-2 state timeout time for TCP connections.
Node	Statistics node name and all URL match rules configured for the statistics node.
Object group name	IP address object groups used by the HTTP statistics parameter profile.
Max reuse times	Maximum number of times a TCP connection can be reused.
Idle time	Idle timeout time for TCP connections, in seconds.
IPv4 source mask length	Mask length for connection reuse.
IPv6 source prefix length	Prefix length for connection reuse.

Field	Description
Match-buffer-time	Buffering period for TCP payload matching, in seconds.
Match-buffer-size	Maximum buffering size for TCP payload matching.
Match-buffer-end	Buffering end string for TCP payload matching.
Src-addr-option	TCP option for SNAT address translation.
Option number	TCP option number
Encoding	Encoding mode for the TCP option: • **binary**. • **string**.
TCP option insert	Inserts contents into a TCP option.
Value	Contents to insert into the TCP option
TCP option remove	Removes a TCP option.

display real-server

Use **display real-server** to display real server information or server farm member information.

Syntax

display real-server [**brief** | **name** *real-server-name*]

display real-server server-farm *server-farm-name* [**name** *real-server-name port port-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

brief: Displays brief real server information. If you do not specify this keyword, the command displays detailed real server information.

name *real-server-name*: Displays information about the specified real server. The *real-server-name* argument specifies a real server name, a case-insensitive string of 1 to 63 characters. If you do not specify this option, the command displays information about all real servers.

server-farm *server-farm-name*: Displays information about members of a server farm. The *server-farm-name* argument specifies a server farm by its name, a case-insensitive string of 1 to 63 characters.

name *real-server-name* **port** *port-number*: Displays information about a server farm member. The *real-server-name* argument specifies a server farm member by its name, a case-insensitive string of 1 to 63 characters. The *port-number* argument specifies the port number of the server farm member, in the range of 0 to 65535. If you do not specify this option, the command displays information about all members of a server farm.

Examples

Display brief information about all real servers.

```
<Sysname> display real-server brief
Real server      Address              Port  State     VPN instance     Server farm
rs1              192.168.1.1          0     Active    vpn1             sf
rs2              192.168.1.2          0     Busy                       sf
rs3              192.168.1.3          0     Active                     sf
```

Display detailed information about the real server **rs**.

```
<Sysname> display real-server name rs
Real server: rs
  Description: Real server RS
  State: Active
  VPN instance:
  Inherit VPN: Enable
  IPv4 address: 1.1.1.1
  IPv6 address: 1001::1
  Port: 0 (port number in original packet)
  Server farm: sf
  Weight: 150
  Priority: 3
  Cost: 100
  Slow shutdown: Enabled
  Connection limit: 10000
  Rate limit:
    Connections: 10000
    Bandwidth: 10000 kbps
    Inbound bandwidth: 5000 kbps
    Outbound bandwidth: 5000 kbps
  Bandwidth busy:
    Max bandwidth: 10000 kbps
    Max inbound bandwidth: 5000 kbps
    Max outbound bandwidth: 5000 kbps
    Busy rate: 80
    Inbound busy rate: 70
    Outbound busy rate: 60
    Busy recovery rate: 60
    Inbound busy recovery rate: 60
    Outbound busy recovery rate: 60
  Probe log: Enabled
  Probe information:
    Dynamic weight: 1
    SNMPDCA busy state: Normal
    Probe success criteria: All
    Probe method                   State
    t4                             Succeeded
    External-monitor method        State
    test_external                  Succeeded
    test_external2                 Succeeded
```

Display information about all members of server farm **sf**.

```
<Sysname> display real-server server-farm sf
Server farm: sf
  Real server: rs1
    Description: real server 1
    Parent state: Inactive
    State: Inactive
    Port: 2
    Weight: 2
    Priority: 2
    Slow shutdown: Disabled
    Connection limit: --
    Connection rate limit: --
    Probe log: Enabled
    Probe information:
      Probe success criteria: All
      Probe method                      State
      icmp                              Failed
      External-monitor method         State
      test_external                   Succeeded
      test_external2                  Succeeded

  Real server: rs2
    Description: real server 2
    Parent state: Inactive
    State: Inactive
    Port: 80
    Weight: 100
    Priority: 4
    Slow shutdown: Disabled
    Connection limit: --
    Connection rate limit: --
    Probe log: Enabled
    Probe information:
      Probe success criteria: All
      Probe method                      State
      tcp                               Failed
    Variable information:
      Variable name: variable
      Variable value: 2
```

Table 32 Command output

Field	Description
Real server	Real server name.
Address	IPv4 address of the real server.
Port	Port number of the real server. 0 means the port number in the packet is used.
Parent state/State	Real server state/Server farm member state:

Field	Description
	• **Active**—The real server is available. • **Busy**—The real server is busy. When the real server is in **Active** or **Ramp** state and enabled with bandwidth statistics collection and link protection, this field displays **Busy** if the maximum expected bandwidth is reached. • **Inactive**—The real server is unavailable, because the configuration is not complete, the server is not referenced, or the virtual server is not enabled. • **Probe-failed**—Health monitoring has failed. • **Ramp**—Ramp-up phase of slow online. • **Shutdown**—The real server is shut down. • **Standby**—Standby phase of slow online. • **Unknown**—Health monitoring is not configured. • **Auto shutdown**—The real server is automatically shut down when the RST or zero-window packet threshold is reached or the number of probe times is reached.
VPN instance	VPN instance to which the real server belongs.
Inherit VPN	VPN instance inheritance: **Enabled** or **Disabled**.
Server farm	Server farm of the real server.
Description	Description for the real server.
IPv4 address	IPv4 address of the real server.
IPv6 address	IPv6 address of the real server.
Weight	Weight of the real server.
Priority	Priority of the real server.
Cost	Cost for proximity calculation.
Slow shutdown	Slow offline state of the real server: • Disabled. • Enabled.
Connection limit	Maximum number of connections for the real server.
Connection rate limit	Maximum number of connections per second for the real server.
Rate limit	Rate limit of the real server.
Connections	Maximum number of connections per second for the real server.
Bandwidth	Maximum bandwidth for the real server in kbps.
Inbound bandwidth	Maximum uplink bandwidth for the real server in kbps.
Outbound bandwidth	Maximum downlink bandwidth for the real server in kbps.
Max bandwidth	Maximum expected bandwidth for the real server in kbps.
Max inbound bandwidth	Maximum uplink expected bandwidth for the real server in kbps.
Max outbound bandwidth	Maximum downlink expected bandwidth for the real server in kbps.
Busy rate	Bandwidth ratio for the real server.
Inbound busy rate	Inbound bandwidth ratio for the real server.
Outbound busy rate	Outbound bandwidth ratio for the real server.
Busy recovery rate	Bandwidth recovery ratio for the real server.

Field	Description
Inbound busy recovery rate	Inbound bandwidth recovery ratio for the real server.
Outbound busy recovery rate	Outbound bandwidth recovery ratio for the real server.
Dynamic weight	Dynamic weight calculated by using the dynamic round robin algorithm. This field displays a weight value only if the dynamic round robin algorithm is used. If any other algorithm is used, this field displays two hyphens (**--**).
SNMPDCA busy state	Busy state obtained by using the dynamic round robin algorithm: **Normal** or **Busy**. If the dynamic round robin algorithm is not used, this field displays two hyphens (**--**).
Probe log	Health monitoring logging state of the real server: • Disabled. • Enabled.
Probe success criteria	Health monitoring success criteria for the real server: • **All**—Health monitoring succeeds only when all the specified health monitoring methods succeed. • **At least X**—Health monitoring succeeds when a minimum of *X* health monitoring methods succeed.
Probe method	Name of the NQA template used by the health monitoring method.
State	State of the health monitoring method (custom monitoring or NQA): • **Failed**—Health monitoring has failed. • **In progress**—Health monitoring is in progress. • **Invalid**—Health monitoring is unavailable (because the configuration of the NQA template is not complete), or the real server is unavailable. • **Succeeded**—Health monitoring has succeeded.
External-monitor method	Custom monitoring method.

display real-server statistics

Use **display real-server statistics** to display real server statistics or server farm member statistics.

Syntax

display real-server statistics [**name** *real-server-name*] [**slot** *slot-number*]

display real-server statistics server-farm *server-farm-name* [**name** *real-server-name* **port** *port-number*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

name *real-server-name*: Specifies a real server by its name, a case-insensitive string of 1 to 63 characters. If you do not specify this option, the command displays statistics for all real servers.

server-farm *server-farm-name*: Displays statistics for members of a server farm. The *server-farm-name* argument specifies a server farm by its name, a case-insensitive string of 1 to 63 characters.

name *real-server-name* **port** *port-number*: Displays statistics for a server farm member. The *real-server-name* argument specifies a server farm member by its name, a case-insensitive string of 1 to 63 characters. The *port-number* argument specifies the port number of the server farm member, in the range of 0 to 65535. If you do not specify this option, the command displays statistics for all members of a server farm.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays real server statistics for all member devices.

Examples

Display statistics for the real server **rs**.

```
<Sysname> display real-server statistics name rs
Real server: rs
  Total connections: 1798
  Active connections: 788
  Max connections: 803
    recorded at 11:02:49 on Tue May 21 2019
  Connections per second: 157
  Max connections per second: 163
    recorded at 11:02:49 on Tue May 21 2019
  Server input: 333332 bytes
  Server output: 472054 bytes
  Throughput: 4396 bps
  Inbound throughput: 1214 bps
  Outbound throughput: 3128 bps
  Max throughput: 4564 bps
    recorded at 11:02:49 on Tue May 21 2019
  Max inbound throughput: 1214 bps
    recorded at 11:02:49 on Tue May 21 2019
  Max outbound throughput: 3320 bps
    recorded at 11:02:49 on Tue May 21 2019
  Received packets: 1798
  Sent packets: 0
  Dropped packets: 0
  Received packets per second: 0
  Sent packets per second: 0
  Received requests: 0
  Dropped requests: 0
  Sent responses: 0
  Dropped responses: 0
  Connection failures: 1
  Busy state: Busy
```

Display statistics for all members of server farm **sf**.

```
<Sysname> display real-server statistics server-farm sf
```

```
Server farm: sf
  Real server: rs1
    Total connections: 0
    Active connections: 0
    Max connections: 0
      recorded at 11:02:49 on Tue May 21 2019
    Connections per second: 0
    Max connections per second: 0
      recorded at 11:02:49 on Tue May 21 2019
    Server input: 0 bytes
    Server output: 0 bytes
    Throughput: 0 bps
    Inbound throughput: 0 bps
    Outbound throughput: 0 bps
    Max throughput: 0 bps
      recorded at 11:02:49 on Tue May 21 2019
    Max inbound throughput: 0 bps
      recorded at 11:02:49 on Tue May 21 2019
    Max outbound throughput: 0 bps
      recorded at 11:02:49 on Tue May 21 2019
    Received packets: 0
    Sent packets: 0
    Dropped packets: 0
    Received packets per second: 0
    Sent packets per second: 0
    Received requests: 0
    Dropped requests: 0
    Sent responses: 0
    Dropped responses: 0
    Connection failures: 0
    RST packets: 50
    Max RST packets: 5000
    RST probe protection times: 3
    Max RST probe protection times: 9
    Zero-window packet percentage: 10
    Max zero-window packet percentage: 50
    Zero-window probe protection times: 2
    Max zero-window probe protection times: 8

  Real server: rs2
    Total connections: 0
    Active connections: 0
    Max connections: 0
      recorded at 11:02:49 on Tue May 21 2019
    Connections per second: 0
    Max connections per second: 0
      recorded at 11:02:49 on Tue May 21 2019
    Server input: 0 bytes
```

```
Server output: 0 bytes
Throughput: 0 bps
Inbound throughput: 0 bps
Outbound throughput: 0 bps
Max throughput: 0 bps
  recorded at 11:02:49 on Tue May 21 2019
Max inbound throughput: 0 bps
  recorded at 11:02:49 on Tue May 21 2019
Max outbound throughput: 0 bps
  recorded at 11:02:49 on Tue May 21 2019
Received packets: 0
Sent packets: 0
Dropped packets: 0
Received packets per second: 0
Sent packets per second: 0
Received requests: 0
Dropped requests: 0
Sent responses: 0
Dropped responses: 0
Connection failures: 0
RST packets: 50
Max RST packets: 5000
RST probe protection times: 3
Max RST probe protection times: 9
Zero-window packet percentage: 10
Max zero-window packet percentage: 50
Zero-window probe protection times: 2
Max zero-window probe protection times: 8
Abnormal URL times: 10
Max abnormal URL times: 20
```

Table 33 Command output

Field	Description
Real server	Real server name.
Total connections	Total number of connections.
Active connections	Number of active connections.
Max connections	Maximum number of connections.
Connections per second	Number of connections per second.
Max connections per second	Maximum number of connections per second.
Server input	Traffic (in bytes) received by the server.
Server output	Traffic (in bytes) sent by the server.
Throughput	Total packet throughput in bps.
Inbound throughput	Inbound packet throughput in bps.
Outbound throughput	Outbound packet throughput in bps.
Max throughput	Maximum packet throughput in bps.

Field	Description
Max inbound throughput	Maximum inbound packet throughput in bps.
Max outbound throughput	Maximum outbound packet throughput in bps.
Received packets	Number of received packets.
Sent packets	Number of sent packets.
Dropped packets	Number of dropped packets.
Received requests	Number of received HTTP request packets. This field is displayed only for Layer 7 real servers.
Dropped requests	Number of dropped HTTP request packets. This field is displayed only for Layer 7 real servers.
Sent responses	Number of sent HTTP response packets. This field is displayed only for Layer 7 real servers.
Dropped responses	Number of dropped HTTP response packets. This field is displayed only for Layer 7 real servers.
Connection failures	Number of connection establishment failures.
Busy state	Real server state: • **--**—Unavailable. • **Normal**. • **Busy**.
RST packets	Number of RST packets sent by the real server during the monitoring time.
Max RST packets	Maximum number of RST packets sent by the real server during the monitoring time.
RST probe protection times	Number of probe times for the RST LB probe template.
Max RST probe protection times	Maximum number of probe times for the RST LB probe template.
Zero-window packet percentage	Percentage of zero-window packets sent by the real server during the monitoring time.
Max zero-window packet percentage	Maximum percentage of zero-window packets sent by the real server during the monitoring time.
Zero-window probe protection times	Number of probe times for the zero-window LB probe template.
Max zero-window probe protection times	Maximum number of probe times for the zero-window LB probe template.
Abnormal URL times	Number of URL error times during the current monitoring time during the monitoring time.
Max abnormal URL times	Maximum number of URL error times during the monitoring time.

Related commands

`reset real-server statistics`

display server-farm

Use **`display server-farm`** to display server farm information.

Syntax

display server-farm [**brief** | **name** *server-farm-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

brief: Displays brief server farm information. If you do not specify this keyword, the command displays detailed server farm information.

name *server-farm-name*: Displays information about the specified server farm. The *server-farm-name* argument specifies a server farm name, a case-insensitive string of 1 to 63 characters. If you do not specify this option, the command displays information about all server farms.

Examples

Display brief information about all server farms.

```
<Sysname> display server-farm brief
Predictor: RR - Round robin, RD - Random, LC - Least connection,
           BW – Bandwidth, MBW – Max bandwidth,
           IBW – Inbound bandwidth, OBW – Outbound bandwidth,
           MIBW – Max inbound bandwidth, MOBW – Max outbound bandwidth,
           HASH(SIP) - Hash address source IP,
           HASH(DIP) - Hash address destination IP,
           HASH(SIP-PORT) - Hash address source IP-port
           LT - Least time, DRR - Dynamic round robin
           CARP(SIP) - CARP address source IP
           CARP(DIP) - CARP address destination IP
           CARP(SIP-PORT) - CARP address source IP-port
           CARP(HTTP) - CARP HTTP payload
           HASH(HTTP) - Hash HTTP payload
NAT/SNAT: Y - Enabled, N - Disabled

Server farm       Predictor       NAT  SNAT  Total  Active
sf                RR              Y    N     3      3
```

Display detailed information about all server farms.

```
<Sysname> display server-farm
Server farm: sf1
  Description:
  Predictor: Hash address
  Proximity: Disabled
  NAT: Enabled
  SNAT mode: snat-pool sp
  Failed action: Keep
```

```
Active threshold: Enabled
  Lower: 80
  Upper: 90
Slow-online: Enabled
Standby time: 5s
Ramp-up time: 10s
Selected server: Enabled
  Min server: 100
  Max server: 600
Busy action: Enqueue
  Queue length: 11
  Queue timeout: 12
Probe information:
  Probe success criteria: All
  Probe method:
  aaa
  bbb
  ccc
TCP RST probe template: aaa
TCP zero-window probe template: bbb
HTTP passive probe template: ccc
Auto-shutdown recovery time: 30
Total real server: 1
Active real server: 1
Real server list:
Name      State         VPN instance     Address    Port  Weight Priority  LT-weight
rs1       Inactive                       1.2.3.4    0     4      100       50
rs2       Auto shutdown                  1.2.3.4    0     4      100       50
```

Table 34 Command output

Field	Description
Server farm	Server farm name.
Predictor	Scheduling algorithm of the server farm: • **RR**—Weighted round robin algorithm. • **RD**—Random algorithm. • **LC**—Weighted least connection algorithm. • **BW**—Bandwidth algorithm. • **IBW**—Inbound bandwidth algorithm. • **OBW**—Outbound bandwidth algorithm. • **MBW**—Maximum bandwidth algorithm. • **MIBW**—Maximum inbound bandwidth algorithm. • **MOBW**—Maximum outbound bandwidth algorithm. • **HASH(SIP)**—Hash algorithm based on source IP address. • **HASH(DIP)**—Hash algorithm based on destination IP address. • **HASH(SIP-PORT)**—Hash algorithm based on source IP address and port number. • **LT**—Least time algorithm. • **DRR**—Dynamic round robin algorithm. • **CARP(SIP)**—CARP hash algorithm based on source IP address.

Field	Description
	• **CARP(DIP)**—CARP hash algorithm based on destination IP address. • **CARP(SIP-PORT)**—CARP hash algorithm based on source IP address and port number. • **CARP(HTTP)**—CARP hash algorithm based on HTTP content. • **HASH(HTTP)**—Hash algorithm based on HTTP content.
NAT	NAT state of the server farm: • **N**—Disabled. • **Y**—Enabled.
SNAT	SNAT state of the server farm: • **N**—Disabled. • **Y**—Enabled.
Total	Total number of real servers.
Active	Number of active real servers.
Description	Description for the server farm.
Proximity	Proximity state of the server farm: • Disabled. • Enabled.
NAT	NAT state of the server farm: • **Disabled**—NAT is not configured. • **Enabled**. • **Disabled (no license)**—NAT is disabled because of lack of license.
SNAT mode	SNAT translation mode: • **auto-map**—Automatic mapping mode. • **tcp-option**—TCP option mode. • **snat-pool**—SNAT pool mode, which uses the SNAT address pool (specified by its name) to perform address translation.
Failed action	Fault processing method of the server farm: • **Keep**—Keeps existing connections. • **Reschedule**—Redirects connections. • **Reset**—Terminates existing connections.
Active threshold	State of the criteria to determine that the server farm is available: disabled or enabled. If the state is enabled, the following fields are displayed: • **Lower**—Lower percentage value. • **Upper**—Upper percentage value.
Slow-online	State of the slow online feature: disabled or enabled. If the state is enabled, the following fields are displayed: • Standby time. • Ramp-up time.
Selected server	State of real server limit to participate in scheduling: disabled or enabled. If the state is enabled, the following fields are displayed: • **Min server**—Minimum number of real servers that participate in scheduling. • **Max server**—Maximum number of real servers that participate in scheduling.
Probe success criteria	Health monitoring success criteria for the real server: • **All**—Health monitoring succeeds only when all the specified health monitoring methods succeed. • **At least**—Health monitoring succeeds when a specified minimum number of health monitoring methods succeed.

Field	Description
Busy action	Action to take when the server farm is busy: • **Drop**. • **Enqueue**. • **Force**.
Queue length	This field is displayed only if the busy action is **Enqueue**.
Queue timeout	This field is displayed only if the busy action is **Enqueue**.
Probe method	Name of the NQA template used by the health monitoring method.
Total real server	Total number of real servers.
Active real server	Number of active real servers.
Name	Real server name.
State	Real server state: • **Active**—The real server is available. • **Busy**—The real server is busy. When the real server is in **Active** or **Ramp** state and enabled with bandwidth statistics collection and link protection, this field displays **Busy** if the maximum expected bandwidth is reached. • **Inactive**—The real server is unavailable, because the configuration is not complete, the server is not referenced, or the virtual server is not enabled. • **Probe-failed**—Health monitoring has failed. • **Ramp**—Ramp-up phase of slow online. • **Shutdown**—The real server is shut down. • **Standby**—Standby phase of slow online. • **Unknown**—Health monitoring is not configured. • **Auto shutdown**—The real server is automatically shut down when the RST or zero-window packet threshold is reached or the number of probe times is reached.
Address	IPv4 and IPv6 addresses of the real server.
Port	Port number of the real server.
Weight	Weight of the real server.
Priority	Priority of the real server.
LT-weight	Weight calculated by using the least time algorithm. This field displays a weight value only if the least time algorithm is used. If any other algorithm is used, this field displays two hyphens (**--**).
TCP RST probe template	TCP-RST LB probe template referenced by the server farm. This field is displayed only if a TCP-RST LB probe template is referenced.
TCP zero-window probe template	TCP zero-window LB probe template referenced by the server farm. This field is displayed only if a TCP zero-window LB probe template is referenced.
HTTP passive probe template	HTTP passive LB probe template referenced by the server farm. This field is displayed only if an HTTP passive LB probe template is referenced.
Auto-shutdown recovery time	Automatic recovery time for intelligent monitoring, in minutes.

display sticky dns-proxy

Use **display sticky dns-proxy** to display sticky entry information for transparent DNS proxies.

Syntax

display sticky dns-proxy [**dns-proxy-name** *dns-proxy-name*] [**class** { *class-name* | **default-class** } | **client-addr** { *ipv4-address* | *ipv6-address* } | **dns-server-addr** { *ipv4-address* | *ipv6-address* } | **dns-server-pool** *pool-name* | **dns-server-port** *port-number* | **key** *sticky-key*] * [**brief**] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

dns-proxy *dns-proxy-name*: Specifies a transparent DNS proxy by its name, a case-insensitive string of 1 to 63 characters. If you do not specify this option, the command displays sticky entry information for all transparent DNS proxies.

class { *class-name* | **default-class** }: Specifies an LB class by its name, a case-insensitive string of 1 to 63 characters, or specifies the default LB class.

client-addr { *ipv4-address* | *ipv6-address* }: Specifies a client by its IPv4 or IPv6 address.

dns-server-addr { *ipv4-address* | *ipv6-address* }: Specifies a DNS server by its IPv4 or IPv6 address.

dns-server-pool *pool-name*: Specifies a DNS server pool by its name, a case-insensitive string of 1 to 63 characters.

dns-server-port *port-number*: Specifies a DNS server port number in the range of 0 to 65535.

key *sticky-key*: Specifies a key value, a case-sensitive string of 1 to 36 characters.

brief: Displays brief information about sticky entries. If you do not specify this keyword, the command displays detailed information about sticky entries.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays sticky entry information for all member devices.

Examples

Display detailed sticky entry information for all transparent DNS proxies.

```
<Sysname> display sticky dns-proxy
  DNS proxy name: dsp1
  DNS server pool name: dns-pool
  Class: cl
  Sticky type: Address-port
  Sticky method: Source IP
```

```
  Sticky key: 3.0.0.13
  DNS proxy addr: 33.44.1.1:80
  DNS server addr: 7.0.0.7:80
  Client addr: 3.0.0.1
  Timeout: 100 sec
  Expiration time: 58 sec
```

Display brief sticky entry information for all transparent DNS proxies.

```
<Sysname> display sticky dns-proxy brief
Sticky type      Sticky method   Sticky key        DNS proxy      DNS server addr
Address-port     Src IP          3.0.0.13          dsp1           7.0.0.7:80
Address-port     Src IP          3.0.0.15          dsp2           7.0.0.8:80
```

Table 35 Command output

Field	Description
Sticky group name	Name of the sticky group that generates the sticky entries.
Sticky method	Sticky method corresponding to the sticky entries: • **Src IP**—Source IPv4 address sticky method. • **Src IPv6**—Source IPv6 address sticky method. • **Src IP and port**—Source IPv4 address + source port sticky method. • **Src IPv6 and port**—Source IPv6 address + source port sticky method. • **Dst IP**—Destination IPv4 address sticky method. • **Dst IPv6**—Destination IPv6 address sticky method. • **Dst IP and port**—Destination IPv4 address + destination port sticky method. • **Dst IPv6 and port**—Destination IPv6 address + destination port sticky method. • **Both IP**—Source IPv4 address + destination IPv4 address sticky method. • **Both IPv6**—Source IPv6 address + destination IPv6 address sticky method. • **Both IP and port**—Source IPv4 address + source port + destination IPv4 address + destination port sticky method. • **Both IPv6 and port**—Source IPv6 address + source port + destination IPv6 address + destination port sticky method.
Sticky key	Key value corresponding to the sticky entry.
Timeout	Configured timeout time for sticky entries, in seconds.
Expiration time	Remaining lifetime of the sticky entry, in seconds.

display sticky statistics

Use **display sticky statistics** to display sticky entry statistics

Syntax

display sticky statistics [**dns-proxy** | **virtual-server**] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

dns-proxy: Dispalys sticky entry statistics for transparent DNS proxies.

virtual-server: Displays sticky entry statistics for virtual servers.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays sticky entry statistics for all member devices.

Usage guidelines

If you do not specify the **dns-proxy** or **virtual-server** keyword, this command displays statistics for all sticky entries.

Examples

Display sticky entry statistics for virtual servers.

```
<Sysname> display sticky statistics virtual-server
Virtual server:
Total sticky entries for all sticky types: 27000
  Sticky type     Sticky method     Total sticky entries     Synced sticky entries
  Address-port                      12000                    120
                  Src IP            100                      10
                  Src IPv6          100                      10
                  Dst IP            100                      10
                  Dst IPv6          100                      10
                  Both IP           100                      10
                  Both IPv6         100                      10
                  Src IP port       100                      10
                  Src IPv6 port     100                      10
                  Dst IP port       100                      10
                  Dst IPv6 port     100                      10
                  Both IP port      100                      10
                  Both IPv6 port    100                      10
  HTTP header                       5000                     50
                  HTTP version      100                      10
                  HTTP URL          100                      10
                  HTTP method       100                      10
                  HTTP host         100                      10
                  Header name       100                      10
  HTTP cookie     Cookie get        100                      10
  HTTP content    HTTP content      100                      10
  Payload         Payload           100                      10
  SSL             SSL session       100                      10
  RADIUS          Attribute ID      200                      20
  SIP             SIP Call-ID       100                      10
  HTTP passive    HTTP Passive      100                      10
  UDP passive     Payload Passive   100                      10
  TCP payload     TCP Payload       100                      10
```

Display sticky entry statistics for transparent DNS proxies.

```
<Sysname> display sticky statistics dns-proxy
```

```
DNS proxy:
Total sticky entries for all sticky types: 12000
  Sticky type     Sticky method     Total sticky entries     Synced sticky entries
  Address-port                      12000                    120
                  Src IP            100                      10
                  Src IPv6          100                      10
                  Dst IP            100                      10
                  Dst IPv6          100                      10
                  Both IP           100                      10
                  Both IPv6         100                      10
                  Src IP port       100                      10
                  Src IPv6 port     100                      10
                  Dst IP port       100                      10
                  Dst IPv6 port     100                      10
                  Both IP port      100                      10
                  Both IPv6 port    100                      10
```

Table 36 Command output

Field	Description
Sticky method	Sticky method corresponding to the sticky entries: • **Src IP**—Source IPv4 address sticky method. • **Src IPv6**—Source IPv6 address sticky method. • **Src IP and port**—Source IPv4 address + source port sticky method. • **Src IPv6 and port**—Source IPv6 address + source port sticky method. • **Dst IP**—Destination IPv4 address sticky method. • **Dst IPv6**—Destination IPv6 address sticky method. • **Dst IP and port**—Destination IPv4 address + destination port sticky method. • **Dst IPv6 and port**—Destination IPv6 address + destination port sticky method. • **Both IP**—Source IPv4 address + destination IPv4 address sticky method. • **Both IPv6**—Source IPv6 address + destination IPv6 address sticky method. • **Both IP and port**—Source IPv4 address + source port + destination IPv4 address + destination port sticky method. • **Both IPv6 and port**—Source IPv6 address + source port + destination IPv6 address + destination port sticky method. • **HTTP URL**—HTTP URL based sticky method. • **HTTP header name**—HTTP header name based sticky method. • **HTTP version**—HTTP version based sticky method. • **HTTP host**—HTTP host based sticky method. • **HTTP method**—HTTP Request-Method based sticky method. • **HTTP content**—HTTP entity sticky method. • **Cookie get**—HTTP cookie get sticky method. • **Payload**—HTTP or UDP payload sticky method. • **HTTP passive**—HTTP passive sticky method. • **Payload passive**—UDP payload passive sticky method. • **TCP payload**—TCP payload sticky method. • **RADIUS IP**—Sticky method based on the Framed-IP-Address attribute of RADIUS packets. • **RADIUS ID**—Sticky method based on the specified attribute of RADIUS packets. • **SIP Call-ID**—Sticky method based on the Call-ID header field of SIP packets. • **SSL session ID**—SSL sticky method based on SSL session ID.

Field	Description
Synced sticky entries	Number of sticky entries synchronized from other devices or other cards on the local deivce.

display sticky virtual-server

Use **display sticky virtual-server** to display sticky entry information for virtual servers.

Syntax

display sticky virtual-server [**virtual-server-name** *virtual-server-name*] [[**link** { **ip** *ipv4-address* | **ipv6** *ipv6-address* | **interface** { *interface-type interface-number* | *interface-name* } } | **link-group** *link-group-name*] * | [**real-server-addr** { *ipv4-address* | *ipv6-address* } | **real-server-port** *port-number* | **server-farm** *server-farm-name* | **text** *text*] *] [**class** { *class-name* | **default-class** } | **client-addr** { *ipv4-address* | *ipv6-address* } | **sticky-type** { **address-port** | **http-content** | **http-cookie** | **http-header** | **http-passive** | **payload** | **radius** | **sip** | **ssl** | **tcp-payload** | **udp-passive** } [**key** *sticky-key*]] * [**brief**] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

virtual-server *virtual-server-name*: Specifies a virtual server by its name, a case-insensitive string of 1 to 63 characters. If you do not specify this option, the command displays sticky entry information for all virtual servers.

link { **ip** *ipv4-address* | **ipv6** *ipv6-address* | **interface** { *interface-type interface-number* | *interface-name* } }: Specifies a link by its IPv4 address, IPv6 address, or output interface.

link-group *link-group-name*: Specifies a link group by its name, a case-insensitive string of 1 to 63 characters.

real-server-addr { *ipv4-address* | *ipv6-address* }: Specifies a real server by its IPv4 or IPv6 address.

real-server-port *port-number*: Specifies a real server port number in the range of 0 to 65535.

server-farm *server-farm-name*: Specifies a server farm by its name, a case-insensitive string of 1 to 63 characters.

text *text*: Specifies a text string to match. The string is case sensitive and can contain 1 to 63 characters.

class { *class-name* | **default-class** }: Specifies an LB class by its name, a case-insensitive string of 1 to 63 characters, or specifies the default LB class.

client-addr { *ipv4-address* | *ipv6-address* }: Specifies a client by its IPv4 or IPv6 address.

sticky-type { **address-port** | **http-content** | **http-cookie** | **http-header** | **http-passive** | **payload** | **radius** | **sip** | **ssl** | **tcp-payload** | **udp-passive** }: Specifies a sticky group type.

key *sticky-key*: Specifies a key value, a case-sensitive string of 1 to 36 characters. If you do not specify key value, this command displays sticky entries for all key values.

brief: Displays brief information about sticky entries. If you do not specify this keyword, the command displays detailed information about sticky entries.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays sticky entry information for all member devices.

Examples

Display detailed sticky entry information for all virtual servers.

```
<Sysname> display sticky virtual-server
  Virtual server name: vs
  Server farm name: sf
  Class: cla
  Sticky type: Address-port
  Sticky method: Source IP
  Sticky key: 3.0.0.13
  Virtual server addr: 33.44.1.1:80
  Real server addr: 7.0.0.7:80
  Client addr: 3.0.0.13
  Timeout: 100 sec
  Expiration time: 58 sec

----------------------------------------
  Virtual server name: vs1
  Server farm name: sf_http
  Class: Default Class
  Sticky type: HTTP header
  Sticky method: HTTP header name
  Sticky key: cb3bae31bb1c443fbf3db8889055f2fe
  Text: a1b2c3d4e5
  Virtual server addr: 33.44.1.2:80
  Real server addr: 7.0.0.7:80
  Client addr: 3.0.0.13
  Timeout: 100 sec
  Expiration time: 58 sec

----------------------------------------
  Virtual server name: vs2
  Link group name: lg
  Class: cl2
  Sticky type: Address-port
  Sticky method: Source IP
  Sticky key: 3.0.0.15
  Virtual server addr: 0.0.0.0:0
  link: 20.1.1.1
  Client addr: 3.0.0.15
```

```
  Timeout: 100 sec
  Expiration time: 58 sec
```

Display brief sticky entry information for all virtual servers.

```
<Sysname> display sticky virtual-server brief
Sticky type    Sticky method    Sticky key      Virtual server      Real-server/link
Address-port   Src IP           3.0.0.13        vs                  7.0.0.7:80
Address-port   Src IP           3.0.0.15        vs2                 20.1.1.1
```

Table 37 Command output

Field	Description
Sticky group name	Name of the sticky group that generates the sticky entries.
Sticky method	Sticky method corresponding to the sticky entries: • **Src IP**—Source IPv4 address sticky method. • **Src IPv6**—Source IPv6 address sticky method. • **Src IP and port**—Source IPv4 address + source port sticky method. • **Src IPv6 and port**—Source IPv6 address + source port sticky method. • **Dst IP**—Destination IPv4 address sticky method. • **Dst IPv6**—Destination IPv6 address sticky method. • **Dst IP and port**—Destination IPv4 address + destination port sticky method. • **Dst IPv6 and port**—Destination IPv6 address + destination port sticky method. • **Both IP**—Source IPv4 address + destination IPv4 address sticky method. • **Both IPv6**—Source IPv6 address + destination IPv6 address sticky method. • **Both IP and port**—Source IPv4 address + source port + destination IPv4 address + destination port sticky method. • **Both IPv6 and port**—Source IPv6 address + source port + destination IPv6 address + destination port sticky method. • **HTTP URL**—HTTP URL based sticky method. • **HTTP header name**—HTTP header name based sticky method. • **HTTP version**—HTTP version based sticky method. • **HTTP host**—HTTP host based sticky method. • **HTTP method**—HTTP Request-Method based sticky method. • **HTTP content**—HTTP entity sticky method. • **Cookie get**—HTTP cookie get sticky method. • **Payload**—HTTP or UDP payload sticky method. • **HTTP passive**—HTTP passive sticky method. • **Payload passive**—UDP payload passive sticky method. • **TCP payload**—TCP payload sticky method. • **Framed-IP-Address**—Sticky method based on the Framed-IP-Address attribute of RADIUS packets. • **User-Name**—Sticky method based on the User-Name attribute of RADIUS packets. • **Code=***attribute-code*—Sticky method based on the attribute (specified by *attribute-code*) of RADIUS packets. • **SIP Call-ID**—Sticky method based on the Call-ID header field of SIP packets. • **SSL session ID**—SSL sticky method based on SSL session ID.
Sticky key	Key value corresponding to the sticky entry.
Timeout	Configured timeout time for sticky entries, in seconds. **indefinite** indicates not aging.
Expiration time	Remaining lifetime of the sticky entry, in seconds.

display sticky-group

Use **display sticky-group** to display sticky group information.

Syntax

display sticky-group [**name** *group-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

name *group-name*: Specifies a sticky group by its name, a case-insensitive string of 1 to 63 characters. If you do not specify this option, the command displays information about all sticky groups.

Examples

Display information about all sticky groups.

```
<Sysname> display sticky-group
Sticky group: sg1
  Description:
  Timeout: 60
  Override limit: Disabled
  Stickiness-over-busyness: Enabled
  Matching across services: Enabled
  Matching across virtual servers: Enabled
  Sticky group type: Address-port
    Method: Both IP and port
      Mask: 32

Sticky group: sg2
  Description:
  Timeout: 60
  Override limit: Disabled
  Stickiness-over-busyness: Enabled
  Sticky group type: HTTP header
    Method: HTTP header name
      Name: accept-encoding
      Offset: 4
      Start: gzip
      Length: 10

Sticky group: sg3
  Description:
  Timeout: 60
```

```
  Override limit: Disabled
  Stickiness-over-busyness: Enabled
  Sticky group type: RADIUS
    Method: User-Name

Sticky group: sg4
  Description:
  Timeout: 86400
  Override limit: Disabled
  Stickiness-over-busyness: Disabled
  Sticky group type: HTTP cookie
    Method: HTTP cookie insert
      Name: X-LB
      Domain: test.com
      Path: /test1
      HttpOnly: Enabled
      Secure: Enabled
  Check all packets: Disabled
```

Table 38 Command output

Field	Description
Sticky group	Sticky group name.
Description	Description for the sticky group.
Timeout	Timeout time for sticky entries in seconds. The value **Infinite** indicates that sticky entries never age out.
Override limit	Whether the feature of ignoring the limits for sessions that match sticky entries is enabled: **Enabled** or **Disabled**.
Stickiness-over-busyness	Whether the stickiness-over-busyness feature is enabled: **Enabled** or **Disabled**.
Sticky group type	Sticky group type: • **Address-port**—Address and port. • **HTTP content**—HTTP entity. • **HTTP cookie**. • **HTTP header**. • **HTTP passive**. • **Payload**—HTTP or UDP payload. • **RADIUS**. • **SIP**. • **SSL**. • **UDP passive**. • **TCP payload**.

Table 39 Detailed information for sticky groups

Sticky group type	Field	Description
Address-port	Method	Sticky method: • **Source IP**—Source IPv4 address sticky method. • **Source IPv6**—Source IPv6 address sticky method.

Sticky group type	Field	Description
		• **Source IP and port**—Source IPv4 address + source port sticky method. • **Source IPv6 and port**—Source IPv6 address + source port sticky method. • **Destination IP**—Destination IPv4 address sticky method. • **Destination IPv6**—Destination IPv6 address sticky method. • **Destination IP and port**—Destination IPv4 address + destination port sticky method. • **Destination IPv6 and port**—Destination IPv6 address + destination port sticky method. • **Both IP**—Source IPv4 address + destination IPv4 address sticky method. • **Both IPv6**—Source IPv6 address + destination IPv6 address sticky method. • **Both IP and port**—Source IPv4 address + source port + destination IPv4 address + destination port sticky method. • **Both IPv6 and port**—Source IPv6 address + source port + destination IPv6 address + destination port sticky method.
	Mask	Mask length for the sticky method. This field is displayed only for IPv4 sticky methods.
	Prefix	Prefix length for the sticky method. This field is displayed only for IPv6 sticky methods.
HTTP content	Offset	Offset value of the entity based on the start of the HTTP packet.
	Start	Regular expression that marks the start of the entity.
	End	Regular expression that marks the end of the entity. Either this field or the **Length** field is displayed, but not both of them.
	Length	Length of the entity. Either this field or the **End** field is displayed, but not both of them.
HTTP cookie	Method	Sticky method: • **HTTP cookie insert**—Cookie insert sticky method. • **HTTP cookie rewrite**—Cookie rewrite sticky method. • **HTTP cookie get**—Cookie get sticky method. This field is displayed only for the HTTP cookie sticky method.
	Name	HTTP cookie name. This field is displayed only for the HTTP cookie sticky method.
	Domain	Domain scope of the cookie. This field is displayed only for the HTTP cookie insert sticky method.
	Path	Path scope of the cookie. This field is displayed only for the HTTP cookie insert sticky method.
	Offset	Offset value based on the start of the cookie value. This field is displayed only for the cookie insert sticky method.
	Start	Regular expression that marks the start of the cookie. This field is displayed only for the cookie insert sticky

Sticky group type	Field	Description
		method.
	End	Regular expression that marks the end of the cookie. Either this field or the **Length** field is displayed, but not both of them. This field is displayed only for the cookie insert sticky method.
	Length	Length of the cookie. Either this field or the **End** field is displayed, but not both of them. This field is displayed only for the cookie insert sticky method.
	Cookie secondary name	Name of the secondary cookie to be searched in the URI. This field is displayed only for the cookie insert sticky method.
	HttpOnly	HttpOnly attribute of the cookie. This field is displayed only for the HTTP cookie insert or cookie rewrite sticky method.
	Secure	Secure attribute of the cookie. This field is displayed only for the HTTP cookie insert or cookie rewrite sticky method.
	Check all packets	Whether or not to enable checking for all packets.
HTTP header	Method	Sticky method: • **HTTP host**—HTTP host based sticky method. • **HTTP header name**—HTTP header name based sticky method. • **HTTP method**—HTTP Request-Method based sticky method. • **HTTP URL**—HTTP URL based sticky method. • **HTTP version**—HTTP version based sticky method. This field is displayed only for the HTTP header sticky method.
	Name	HTTP header name. This field is displayed only for the HTTP header name based sticky method.
	Offset	Offset value of the HTTP header based on the start of the HTTP packet. This field is displayed only for the HTTP host or URL based sticky method.
	Start	Regular expression that marks the start of the HTTP header. This field is displayed only for the HTTP host or URL based sticky method.
	End	Regular expression that marks the end of the HTTP header. Either this field or the **Length** field is displayed, but not both of them. This field is displayed only for the HTTP host or URL based sticky method.
	Length	Length of the HTTP header. Either this field or the **End** field is displayed, but not both of them. This field is displayed only for the HTTP host or URL based sticky method.
Payload	Offset	Offset value of the HTTP or UDP payload based on the start of the HTTP packet.
	Start	Regular expression that marks the start of the HTTP or UDP payload.
	End	Regular expression that marks the end of the HTTP or UDP payload. Either this field or the **Length** field is

Sticky group type	Field	Description
		displayed, but not both of them. .
	Length	Length of the HTTP or UDP payload. Either this field or the **End** field is displayed, but not both of them.
RADIUS	Method	Sticky method: • **Framed-IP-Address**—Sticky method based on the Framed-IP-Address attribute of RADIUS packets. • **User-Name**—Sticky method based on the User-Name attribute of RADIUS packets. • **Code=***attribute-code*—Sticky method based on the attribute (specified by *attribute-code*) of RADIUS packets. This field is not displayed if no RADIUS attribute based sticky method is specified.
SIP	Method	Sticky method, which can only be **SIP Call-ID** (SIP sticky method based on the Call-ID header field of SIP packets).
SSL	Method	Sticky method, which can only be **SSL session ID** (SSL sticky method based on SSL session ID). This field is displayed only for the SSL sticky method based on SSL session ID.
HTTP passive	Method	Sticky method: • **HTTP header name**—HTTP header name sticky method. • **HTTP URL**—HTTP URL sticky method. • **HTTP content**—HTTP content sticky method.
	Get	Obtains the specified string in HTTP responses.
	Match	Matches the specified string in HTTP requests.
	Name	HTTP header name. This field is displayed only for the HTTP header name based sticky method.
	Start	Regular expression that marks the start of the HTTP header.
	End	Regular expression that marks the end of the HTTP header. Either this field or the **Length** field is displayed, but not both of them.
	Length	Length of the HTTP header. Either this field or the **End** field is displayed, but not both of them.
UDP passive	Get	Obtains the specified string in UDP responses.
	Match	Matches the specified string in UDP requests.
	Start	Regular expression that marks the start of the UDP payload.
	End	Regular expression that marks the end of the UDP payload. Either this field or the **Length** field is displayed, but not both of them.
	Length	Length of the UDP payload. Either this field or the **End** field is displayed, but not both of them.
TCP payload	Offset	Offset value of the TCP payload based on the start of the TCP packet.
	Start	Regular expression that marks the start of the TCP payload.

Sticky group type	Field	Description
	End	Regular expression that marks the end of the TCP payload. Either this field or the **Length** field is displayed, but not both of them.
	Length	Length of the TCP payload. Either this field or the **End** field is displayed, but not both of them.

display virtual-server

Use **display virtual-server** to display virtual server information.

Syntax

display virtual-server [**brief** | **name** *virtual-server-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

brief: Displays brief virtual server information. If you do not specify this keyword, the command displays detailed virtual server information.

name *virtual-server-name*: Displays information about the specified virtual server. The *virtual-server-name* argument specifies a virtual server name, a case-insensitive string of 1 to 63 characters. If you do not specify this option, the command displays information about all virtual servers.

Examples

Display brief information about all virtual servers.

```
<Sysname> display virtual-server brief
Virtual server   State    Type      VPN instance     Virtual address     Port
vs1              Inactive IP        vpn1             192.168.21.148/32   80
                                                     1111:2222:3333:4444
                                                     :5555:6666:7777:888
                                                     8/128
vs2              Active   HTTP                       61.159.4.100/32     8080
vs3              Active   LINK-IP                    51.139.4.100/32     0
vs4              Active   MySQL                      12.139.5.132/32     3306
```

Display detailed information about all virtual servers.

```
<Sysname> display virtual-server
Virtual server: vs
  Description: Virtual server VS
  Type: HTTP
  State: Active
  VPN instance: vpn1
```

```
Virtual IPv4 address: 1.1.1.1/32
Virtual IPv6 address: 1001::1/128
Port: 0 (any port)
Primary server farm: sf (in use)
Backup server farm: sfb
Primary sticky: sg3
Backup sticky: sg4
LB policy: lbp2
LB limit-policy:
TCP parameter profile (client-side): ptc
TCP parameter profile (server-side): pts
HTTP parameter profile: pp1
HTTP-statistics parameter profile: 1
OneConnect parameter profile: one
DPI application profile: profile1
UDP per-packet: Enabled
Connection limit: 10000
Rate limit:
  Connections: 10000
  Bandwidth: 10000 kbps
  Inbound bandwidth: 5000 kbps
  Outbound bandwidth: 5000 kbps
SSL server policy: ssl-server
SSL server policies with SNI list:
  Name: ssl
    Server name indication: www.aaa.com
  Name: ssl2
    Server name indication: www.bbb.com
SSL client policy: ssl-client
Redirect relocation:
Redirect return-code: 302
VRRP IPv4 Info:
  VRRP IPv4 VRID: 1
  Interface: GigabitEthernet1/0/1
VRRP IPv6 info:
  VRRP IPv6 VRID: 3
  Interface: GigabitEthernet1/0/1
Sticky: test
Sticky synchronization: Disabled
Bandwidth busy protection: Disabled
Interface bandwidth statistics: Disabled
Route advertisement: Enabled
ARP/ND interfaces:
  GigabitEthernet1/0/1
  GigabitEthernet1/0/2
HTTP protection policy: p1
Customlog content: %{is};%{ps}
External-link proxy: Enabled
```

```
  External-link inject URI: proxy
  External-link inject domain suffix: c.com
  External-link SNAT pool: spool1
  External-link domain name whitelist:
    a.com
    b.com

Virtual server: vstcp
  Description: Virtual server VS
  Type: TCP
  State: Active
  VPN instance: vpn1
  Virtual IPv4 address: 1.1.1.1/32
  Virtual IPv6 address: 1001::1/128
  Port: 8080
  Primary server farm: sf (in use)
  Backup server farm: sfb
  Sticky: sg3
  LB policy: lbp2
  LB limit-policy:
  TCP parameter profile (client-side): ptc
  TCP parameter profile (server-side): pts
  TCP-Application parameter profile: ptapp
  DPI application profile: profile1
  Connection limit: 10000
  Rate limit:
    Connections: 10000
    Bandwidth: 10000 kbps
    Inbound bandwidth: 5000 kbps
    Outbound bandwidth: 5000 kbps
  SSL server policy: ssl-server
  SSL server policies with SNI list:
    Name: ssl
      Server name indication: www.aaa.com
    Name: ssl2
      Server name indication: www.bbb.com
  Sticky synchronization: Disabled
  Bandwidth busy protection: Disabled
  Interface bandwidth statistics: Disabled
  Route advertisement: Enabled
  Application-Mode: Enabled
  ARP/ND interfaces:
    GigabitEthernet1/0/1
    GigabitEthernet1/0/2
```

Display detailed information about the virtual server **lk**.

```
<Sysname> display virtual-server name lk
Virtual server: lk
  Description:
```

```
  Type: Link-IP
  State: Active
  VPN instance: vpn1
  Virtual IPv4 address: 1.1.1.1/32
  Virtual IPv6 address: 1001::1/128
  Port: 0
  Primary link group: lg1 (in use)
  Backup link group: lg2
  Sticky: sg3
  LB policy: lbp2
  LB limit-policy:
  Connection limit: 10000
  Rate limit:
    Connections: 10000
    Bandwidth: 10000 kbps
    Inbound bandwidth: 5000 kbps
    Outbound bandwidth: 5000 kbps
  Connection synchronization: Disabled
  Sticky synchronization: Disabled
  Bandwidth busy protection: Disabled
  Interface bandwidth statistics: Disabled
  Route advertisement: Disabled
  ARP/ND interfaces:
    GigabitEthernet1/0/1
```

Display detailed information about the virtual server **vs4**.

```
<Sysname> display virtual-server name vs4
Virtual server: vs4
  Description: Virtual server VS4
  Type: MySQL
  State: Active
  VPN instance: vpn1
  Virtual IPv4 address: 1.1.1.1/32
  Virtual IPv6 address: 1001::1/128
  Port: 3306
  Primary server farm: sf (in use)
  Backup server farm: sfb
  Sticky: sg3
  LB policy: lbp2
  LB limit-policy:
  MySQL parameter profile: my
  Connection limit: 10000
  Rate limit:
    Connections: 10000
    Bandwidth: 10000 kbps
    Inbound bandwidth: 5000 kbps
    Outbound bandwidth: 5000 kbps
  Sticky synchronization: Disabled
  Bandwidth busy protection: Disabled
```

```
Interface bandwidth statistics: Disabled
Route advertisement: Enabled
ARP/ND interfaces:
  GigabitEthernet1/0/1
  GigabitEthernet1/0/2
Version: 5.6
User list:
  Username: wangping
  Username: liqiang
Read server farm: rd
Read sticky group: rsg
Write server farm: wr
Write sticky group: wsg
```

Table 40 Command output

Field	Description
Virtual server	Virtual server name.
State	Virtual server state: • **Active**—The virtual server is available. • **Inactive**—The virtual server is unavailable for any reason other than lack of license and disabled virtual server. • **Inactive (no license)**—The virtual server is unavailable because of lack of license. • **Inactive (disabled)**—The virtual server is unavailable because the virtual server is disabled.
Type	Virtual server type: Fast HTTP, HTTP, IP, MySQL, RADIUS, TCP, UDP, or link-IP.
VPN instance	Name of the VPN instance to which the virtual server belongs.
Virtual address	IPv4 address and mask of the virtual server.
Port	Port number of the virtual server. 0 means any port.
Description	Description of the virtual server.
Virtual IPv4 address	IPv4 address and mask of the virtual server.
Virtual IPv6 address	IPv6 address and prefix of the virtual server.
Primary server farm	Default primary server farm name. **(in use)** indicates the server farm is in use.
Backup server farm	Default backup server farm name. **(in use)** indicates the server farm is in use.
Primary link group	Default primary link group name. **(in use)** indicates the link group is in use.
Backup link group	Default backup link group name. **(in use)** indicates the link group is in use.
Primary sticky	Default primary sticky group name.
Backup sticky	Backup sticky group name. This field is displayed only for HTTP and RADIUS virtual servers.
LB policy	LB policy referenced by the virtual server.
HTTP parameter profile	HTTP parameter profile referenced by the virtual server. This field is displayed only if an HTTP parameter profile is configured.
IP parameter profile	IP parameter profile referenced by the virtual server. This field is displayed only if an IP parameter profile is configured.

Field	Description
TCP parameter profile	TCP parameter profile referenced by the virtual server. This field is displayed only if a TCP parameter profile is configured.
TCP parameter profile (client-side)	Client-side TCP parameter profile referenced by the virtual server. This field is displayed only if a client-side TCP parameter profile is configured.
TCP parameter profile (server-side)	Server-side TCP parameter profile referenced by the virtual server. This field is displayed only if a server-side TCP parameter profile is configured.
OneConnect parameter profile	OneConnect parameter profile referenced by the virtual server. This field is displayed only if a OneConnect parameter profile is configured.
HTTP-statistics parameter profile	HTTP statistics parameter profile referenced by the virtual server. This field is displayed only if an HTTP statistics parameter profile is configured.
TCP-Application parameter profile	TCP-application parameter profile referenced by the virtual server. This field is displayed only if a TCP-application parameter profile is configured.
MySQL parameter profile	MySQL parameter profile referenced by the virtual server. This field is displayed only if a MySQL parameter profile is configured.
DPI application profile	DPI application profile referenced by the virtual server. This field is displayed only if a DPI application profile is configured.
UDP per-packet	State of the per-packet load balancing for UDP traffic: • Disabled. • Enabled. This field is displayed only for UDP virtual servers.
Connection limit	Maximum number of connections of the virtual server.
Rate limit	Rate limit of the virtual server.
Connections	Maximum number of connections per second of the virtual server.
Bandwidth	Maximum bandwidth for the virtual server in kbps.
Inbound bandwidth	Maximum inbound bandwidth for the virtual server in kbps.
Outbound bandwidth	Maximum outbound bandwidth for the virtual server in kbps.
SSL server policy	SSL server policy name. This field is displayed only for HTTP-type virtual servers.
SSL server policies with SNI list	List of SSL server policies with SNIs. This field is displayed only for TCP-type and HTTP-type virtual servers.
Server name indication	Server name indication. This field is displayed only for TCP-type and HTTP-type virtual servers.
SSL client policy	SSL client policy name. This field is displayed only for HTTP-type virtual servers.
Redirect relocation	Redirection URL. This field is displayed only for HTTP-type virtual servers.
Redirect return-code	Status code in the redirection packets. This field is displayed only for HTTP-type virtual servers.
VRRP IPv4 Info	Information about the IPv4 VRRP group bound to the virtual server.
VRRP IPv4 VRID	Virtual router ID of the IPv4 VRRP group bound to the virtual server.
Interface	Interface on which the VRRP group bound to the virtual server is created.
VRRP IPv6 Info	Information about the IPv6 VRRP group bound to the virtual server.
VRRP IPv4 VRID	Virtual router ID of the IPv6 VRRP group bound to the virtual server.
Sticky	Sticky group for the virtual server. This field is displayed only for HTTP-type

Field	Description
	virtual servers.
Connection synchronization	Session extension information synchronization state: **Enabled** or **Disabled**. This field is not displayed for HTTP-type virtual servers.
Sticky synchronization	Sticky entry synchronization state: **Enabled** or **Disabled**.
Bandwidth busy protection	Link protection state: **Enabled** or **Disabled**.
Interface bandwidth statistics	Bandwidth statistics collection by interfaces: Disabled or Enabled.
Route advertisement	IP address advertisement for the virtual server: Disabled or Enabled.
Application-Mode	Layer 7 operating mode for the virtual server: Disabled or Enabled. This field is displayed only for a TCP virtual server.
ARP/ND interfaces	Interfaces from which gratuitous ARP packets and ND packets are sent out.
Version	MySQL database version. This field is displayed only for a MySQL virtual server.
User list	List of users logged in to the MySQL database. This field is displayed only for a MySQL virtual server.
Username	Username used to log in to the MySQL database. This field is displayed only for a MySQL virtual server.
Read server farm	Read server farm referenced by the MySQL virtual server. This field is displayed only for a MySQL virtual server.
Read sticky group	Sticky group associated with the read server farm. This field is displayed only for a MySQL virtual server.
Write server farm	Write server farm referenced by the MySQL virtual server. This field is displayed only for a MySQL virtual server.
Write sticky group	Sticky group associated with the write server farm. This field is displayed only for a MySQL virtual server.
Customlog content	Content output by using the fast log output feature. This field is displayed only for an HTTP virtual server.
HTTP protection policy	HTTP protection policy referenced by the virtual server.
External-link proxy	External link proxy state: **Disabled** or **Enabled**.
External-link inject URI	URI of external link proxy.
External-link inject domain suffix	Domain name suffix of external link proxy.
External-link SNAT pool	SNAT address pool of external link proxy.
External-link domain name whitelist	Whitelist of external link proxy.

display virtual-server statistics

Use **`display virtual-server statistics`** to display virtual server statistics.

Syntax

display virtual-server statistics [**name** *virtual-server-name*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

name *virtual-server-name*: Specifies a virtual server by its name, a case-insensitive string of 1 to 63 characters. If you do not specify this option, the command displays statistics of all virtual servers.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays virtual server statistics for all member devices.

Usage guidelines

The virtual server statistics collection interval is 200 milliseconds and is not configurable.

Examples

Display statistics for the virtual server **vs**.

```
<Sysname> display virtual-server statistics name vs
Virtual server: vs
  Total connections: 979
  Active connections: 618
  Max connections: 661
    recorded at 11:02:49 on Tue May 21 2019
  Connections per second: 146
  Max connections per second: 156
    recorded at 11:02:49 on Tue May 21 2019
  Client input: 333332 bytes
  Client output: 472054 bytes
  Throughput: 4088 bps
  Inbound throughput: 1214 bps
  Outbound throughput: 2874 bps
  Max throughput: 4368 bps
    recorded at 11:02:49 on Tue May 21 2019
  Max inbound throughput: 1214 bps
    recorded at 11:02:49 on Tue May 21 2019
  Max outbound throughput: 3154 bps
    recorded at 11:02:49 on Tue May 21 2019
  Received packets: 979
  Sent packets: 0
  Dropped packets: 0
  Received packets per second: 0
  Sent packets per second: 0
```

```
Received requests: 0
```

Table 41 Command output

Field	Description
Virtual server	Virtual server name.
Total connections	Total number of connections.
Active connections	Number of active connections.
Max connections	Maximum number of connections.
Connections per second	Number of connections per second.
Max connections per second	Maximum number of connections per second.
Client input	Traffic (in bytes) received from the client.
Client output	Traffic (in bytes) sent to the client.
Throughput	Total packet throughput in bps.
Inbound throughput	Inbound packet throughput in bps.
Outbound throughput	Outbound packet throughput in bps.
Max throughput	Maximum packet throughput in bps.
Max throughput	Maximum inbound packet throughput in bps.
Max throughput	Maximum outbound packet throughput in bps.
Received packets	Number of received packets.
Sent packets	Number of packets sent by the virtual server to the client.
Dropped packets	Number of dropped packets.
Received requests	Number of received HTTP request packets. This field is displayed only for HTTP-type virtual servers.
Dropped requests	Number of dropped HTTP request packets. This field is displayed only for HTTP-type virtual servers.
Sent responses	Number of sent HTTP response packets. This field is displayed only for HTTP-type virtual servers.
Dropped responses	Number of dropped HTTP response packets. This field is displayed only for HTTP-type virtual servers.

Related commands

reset virtual-server statistics

dns-server (DNS server pool view)

Use **dns-server** to create a DNS server pool member and enter its view, or enter the view of an existing DNS server pool member.

Use **undo dns-server** to delete a DNS server pool member.

Syntax

dns-server *dns-server-name* **port** *port-number*

undo dns-server *dns-server-name* **port** *port-number*

Default

No DNS server pool members exist.

Views

DNS server pool view

Predefined user roles

network-admin

context-admin

Parameters

dns-server-name: Specifies a DNS server pool member name, a case-insensitive string of 1 to 63 characters.

port-number: Specifies the port number of the DNS server pool member, in the range of 0 to 65535.

Usage guidelines

You can use one of the following methods to add a member to a DNS server pool:

- Use the **dns-server** command in DNS server pool view. NSFOCUS recommends using this method.
- Use the **dns-server-pool** command in DNS server view.

You cannot use both methods to add a member with the same DNS server name and port number to a DNS server pool.

Examples

Add DNS server pool member **ds1** and enter DNS server pool member view.

```
<Sysname> system-view
[Sysname] loadbalance dns-server-pool dsp1
[Sysname-lb-dspool-dsp1] dns-server ds1 port 10
[Sysname-lb-dspool-dsp1-#member#-ds1-port-10]
```

Related commands

dns-server-pool (DNS server view)

dns-server-pool (DNS server view)

Use **dns-server-pool** to specify a DNS server pool for a DNS server.

Use **undo dns-server-pool** to restore the default.

Syntax

dns-server-pool *pool-name*

undo dns-server-pool

Default

A DNS server does not belong to any DNS server pool.

Views

DNS server view

Predefined user roles

network-admin

context-admin

Parameters

pool-name: Specifies a DNS server pool by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

You can specify a DNS server pool that has not been created.

Examples

Specify DNS server pool **dns-pool1** for DNS server **ds1**.

```
<Sysname> system-view
[Sysname] loadbalance dns-server ds1
[Sysname-lb-ds-ds1] dns-server-pool dns-pool1
```

Related commands

display loadbalance dns-server

dns-server-pool (LB action view)

Use **dns-server-pool** to specify a DNS server pool for guiding packet forwarding.

Use **undo dns-server-pool** to restore the default.

Syntax

dns-server-pool *pool-name* [**sticky** *sticky-name*]

undo dns-server-pool

Default

No DNS server pool is specified for guiding packet forwarding.

Views

DNS LB action view

Predefined user roles

network-admin

context-admin

Parameters

pool-name: Specifies a DNS server pool by its name, a case-insensitive string of 1 to 63 characters.

sticky *sticky-name*: Specifies a sticky group by its name, a case-insensitive string of 1 to 63 characters. If you do not specify a sticky group, the DNS server pool does not correspond to any sticky group.

Usage guidelines

This command is mutually exclusive with the **forward all** or **skip current-dns-proxy** command. If you configure one command, the other command (if configured) is automatically cancelled.

Examples

Specify the DNS server pool **dsp** and the sticky group **sg1** for DNS LB action **lba1**.

```
<Sysname> system-view
[Sysname] loadbalance action lba1 type dns
```

```
[Sysname-lba-dns-lba1] dns-server-pool dsp sticky st1
```

Related commands

forward all

domain-name

Use **domain-name** to specify a domain name for a DNS mapping.

Use **undo domain-name** to delete a domain name from a DNS mapping.

Syntax

domain-name *domain-name*

undo domain-name *domain-name*

Default

No domain name is specified for a DNS mapping.

Views

DNS mapping view

Predefined user roles

network-admin

context-admin

Parameters

domain-name: Specifies a domain name, a case-insensitive string of 1 to 253 characters. Each dot-separated label in the domain name can contain a maximum of 63 characters. The domain name can contain letters, digits, hyphens (-), underscores (_), dots (.), and wildcards (asterisks and question marks). Dots cannot be used as the start and end characters.

Usage guidelines

You can specify multiple domain names for a DNS mapping.

When you use wildcards (asterisks and question marks) in a domain name, follow these guidelines:

- An asterisk (*) can substitute a character string.
- A question mark (?) can substitute any single character except for dot (.).

Examples

Specify two domain names for the DNS mapping **dm1**.

```
<Sysname> system-view
[Sysname] loadbalance dns-map dm1
[Sysname-lb-dm-dm1] domain-name www.aaa.domain.com
[Sysname-lb-dm-dm1] domain-name ???.aaa.*.com
```

dpi-app-profile

Use **dpi-app-profile** to specify a DPI application profile for the virtual server.

Use **undo dpi-app-profile** to restore the default.

Syntax

dpi-app-profile *app-profile-name*

undo dpi-app-profile

Default

No DPI application profile is specified for a virtual server.

Views

IP/TCP/UDP/Link IP/HTTP virtual server view

Predefined user roles

network-admin

context-admin

Parameters

app-profile-name: Specifies a DPI application profile by its name, a case-insensitive string of 1 to 63 characters. For more information about DPI application profiles, see DPI engine in *DPI Configuration Guide*.

Usage guidelines

By specifying a DPI application profile, you can apply DPI services to the traffic of a virtual server. For more information about DPI services, see *DPI Configuration Guide*.

Examples

Specify DPI application profile **profile_1** for IP-type virtual server **vs**.

```
<Sysname> system-view
[Sysname] virtual-server vs type ip
[Sysname-vs-ip-vs] dpi-app-profile profile_1
```

Related commands

app-profile (*DPI Command Reference*)

display virtual-server

encrypt-cookie

Use **encrypt-cookie** to encrypt a cookie.

Use **undo encrypt-cookie** to remove the encryption for a cookie.

Syntax

encrypt-cookie name *cookie-name* **key** { **cipher** | **simple** } *string*

undo encrypt-cookie name *cookie-name*

Default

No cookie is encrypted.

Views

HTTP parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

name *cookie-name*: Specifies a cookie by its name, a case-sensitive string of 1 to 63 characters.

key: Specifies a key used to encrypt the cookie.

cipher: Specifies a key in ciphertext form.

simple: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in ciphertext form.

string: Specifies the key. Its plaintext form is a case-sensitive string of 1 to 31 characters. Its ciphertext form is a case-sensitive string of 1 to 73 characters.

Usage guidelines

After you execute this command, the device encrypts the **Set-Cookie** field in HTTP responses to prevent personal information from being revealed. When a client request contains an encrypted cookie, the device decrypts the cookie before sending the request to the server.

Examples

For HTTP parameter profile **p1**, encrypt cookie **cookie1** with encryption key **123456**.

```
<Sysname> system-view
[Sysname] parameter-profile p1 type http
[Sysname-para-http-p1] encrypt-cookie name cookie1 key simple 123456
```

env-variables

Use **env-variables** to configure an environment variable for custom monitoring.

Use **undo env-variables** to delete an environment variable for custom monitoring.

Syntax

env-variables *variable-name* **value** *variable-value*

undo env-variables *variable-name*

Default

No environment variables are configured for custom monitoring.

Views

Custom-monitoring LB probe template view

Predefined user roles

network-admin

context-admin

Parameters

variable-name: Specifies the environment variable name, a case-sensitive string of 1 to 63 characters. The name can contain spaces.

value *variable-value*: Specifies an environment variable value, a case-sensitive string of 1 to 255 characters. The name can contain spaces and cannot contain quotation marks (").

Usage guidelines

You can specify the environment to execute the custom script file by configuring an environment variable.

You can configure a maximum of 16 environment variables.

Examples

In custom-monitoring LB probe template **test_external**, configure an environment variable with name **env** and value **/var/tmp**.

```
<Sysname> system-view
[Sysname] loadbalance probe-template external-monitor test_external
```

```
[Sysname-lbpt-external-monitor-test_external] env-variables env value /var/tmp
```

exceed-mss

Use **exceed-mss** to specify the action to take on the segments that exceed the MSS in the HTTP requests sent by the client.

Use **undo exceed-mss** to restore the default.

Syntax

exceed-mss { **allow** | **drop** }

undo exceed-mss

Default

The device allows the segments to exceed the MSS in the HTTP requests sent by the client.

Views

TCP parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

allow: Allows the segments to exceed the MSS.

drop: Discards the segments that exceed the MSS.

Examples

For the TCP parameter profile **pp3**, specify the **drop** action for the segments that exceed the MSS in the HTTP requests sent by the client.

```
<Sysname> system-view
[Sysname] parameter-profile pp3 type tcp
[Sysname-para-tcp-pp3] exceed-mss drop
```

expire

Use **expire** to set the expiration time for SOA resource records.

Use **undo expire** to restore the default.

Syntax

expire *expire-time*

undo expire

Default

The expiration time is 86400 seconds.

Views

SOA view

Predefined user roles

network-admin

context-admin

Parameters

expire-time: Specifies the expiration time in the range of 500 to 4294967295 seconds.

Usage guidelines

The expiration time for SOA resource records is the amount of time that the secondary DNS server can work after it loses contact with the primary DNS server.

Examples

Set the expiration time for SOA resource records to 7 days for DNS forward zone **abc.com**.

```
<Sysname> system-view
[Sysname] loadbalance zone abc.com
[Sysname-lb-zone-abc.com] soa
[Sysname-lb-zone-abc.com-soa] expire 604800
```

Related commands

display loadbalance zone

external-link inject-domain-suffix

Use **external-link inject-domain-suffix** to configure the domain name suffix for external link proxy.

Use **undo external-link inject-domain-suffix** to delete the domain name suffix for external link proxy.

Syntax

external-link inject-domain-suffix *domain-suffix*

undo external-link inject-domain-suffix

Default

No domain name suffix is configured for external link proxy.

Views

HTTP virtual server view

Predefined user roles

network-admin

context-admin

Parameters

domain-suffix: Specifies the domain name suffix for rewriting domain names of external links. This argument is a case-insensitive, dot-separated string of 1 to 254 characters. Each dot-separated label in the domain name can contain a maximum of 63 characters. The domain name can contain letters, digits, hyphens (-), underscores (_), and dots (.).

Usage guidelines

If DNS packet link selection is performed by inbound link load balancing, make sure the domain name suffixes in DNS mappings are the same as those on the external link proxy.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure the domain name suffix as **b.com** for external link proxy on HTTP virtual server **vs**.

```
<Sysname> system-view
[Sysname] virtual-server vs http
```

```
[Sysname-vs-http-vs] external-link inject-domain-suffix b.com
```

Related commands

display virtual-server

external-link inject-uri

external-link proxy enable

external-link inject-uri

Use **external-link inject-uri** to configure the URI for external link proxy.

Use **undo external-link inject-uri** to delete the URI for external link proxy.

Syntax

external-link inject-uri *string*

undo external-link inject-uri

Default

No URI is configured for external link proxy.

Views

HTTP virtual server view

Predefined user roles

network-admin

context-admin

Parameters

string: Specifies the URI for rewriting domain names of external links. This argument is a case-insensitive string of 1 to 63 characters. The URI can contain letters, digits, hyphens (-), and underscores (_), and cannot contain dots (.).

Usage guidelines

Use this command to rewrite domain names of external links. Upon receiving a response from the IPv6 site server, the LB device rewrites the IPv4 external link in the response by adding the specified parameters to the associated domain name. The parameters include the URI, domain name suffix, and virtual server port number. Suppose the domain name of the original external link is **http://www.aaa.com**, URI is **proxy**, domain name suffix is **bbb.com**, and virtual server port number is **8080**. The external link domain name after rewrite is **http://www.aaa.com.proxy.bbb.com:8080**. Upon receiving a DNS request containing this modified domain name, the LB device performs the following operations:

1. Extracts the original domain name.
2. Requests the associated IPv4 resource on behalf of the IPv6 client.
3. Returns the obtained IPv4 resource to the IPv6 client.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure the URI as **proxy** for external link proxy on HTTP virtual server **vs**.

```
<Sysname> system-view
[Sysname] virtual-server vs http
[Sysname-vs-http-vs] external-link inject-uri proxy
```

Related commands

display virtual-server

external-link inject-domain-suffix

external-link proxy enable

external-link proxy enable (LB action view)

Use **external-link proxy enable** to enable external link proxy.

Use **undo external-link proxy enable** to disable external link proxy.

Syntax

external-link proxy enable

undo external-link proxy enable

Default

External link proxy is disabled.

Views

HTTP LB action view

Predefined user roles

network-admin

context-admin

Usage guidelines

To perform external link proxy for a traffic class instead of all traffic of a virtual server, enable external link proxy in an HTTP LB action. Additionally, configure external link proxy parameters in the view of the virtual server and specify the LB policy for the virtual server.

The external link proxy action does not take effect when any of the following actions is also configured:

- A forwarding LB action (except specifying server farms).
- Specifying a response file used upon load balancing failure.

Examples

Enable external link proxy for HTTP LB action **a1**.

```
<Sysname> system-view
[Sysname] loadbalance action a1 type http
[Sysname-lba-http-a1] external-link proxy enable
```

Related commands

display loabalance action

external-link inject-domain-suffix

external-link inject-uri

external-link proxy enable (virtual sever view)

Use **external-link proxy enable** to enable external link proxy.

Use **undo external-link proxy enable** to disable external link proxy.

Syntax

external-link proxy enable

undo external-link proxy enable

Default

External link proxy is disabled.

Views

HTTP virtual server view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command enables the LB device to operate as a proxy to request IPv4 resources on behalf of IPv6 clients. External link proxy operates as follows:

1. The LB device receives an IPv6 DNS request containing an IPv4 link, and sends the request to the IPv6 site server.
2. Upon receiving a response from the server, the LB device returns a script file with the external link rewritten as configured to the client.
3. The client executes the script file, modifies the external link domain name as instructed, and then sends another DNS request containing the modified domain name.
4. Upon receiving the request, the LB device extracts the original domain name and requests the associated IPv4 resource on behalf of the client.
5. The LB device returns the obtained IPv4 resource to the client.

Examples

Enable external link proxy for HTTP virtual server **vs**.

```
<Sysname> system-view
[Sysname] virtual-server vs http
[Sysname-vs-http-vs] external-link proxy enable
```

Related commands

display virtual-server

external-link snat-pool

Use **external-link snat-pool** to specify the SNAT address pool for external link proxy.

Use **undo external-link snat-pool** to restore the default.

Syntax

external-link snat-pool *pool-name*

undo external-link snat-pool

Default

No SNAT address pool is specified for external link proxy.

Views

HTTP virtual server view

Predefined user roles

network-admin

context-admin

Parameters

pool-name: Specifies a SNAT address pool by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

To request an IPv4 resource as an external link proxy, the LB device will choose an IP address from the specified SNAT pool. The LB device uses this IP address as the client IP address to initiate a request on behalf of the IPv6 client.

If you do not specify a SNAT address pool, the LB device uses the IP address of the output interface to the server as the client IP address.

Examples

Specify the SNAT address pool as **spool1** for external link proxy on HTTP virtual server **vs**.

```
<Sysname> system-view
[Sysname] virtual-server vs http
[Sysname-vs-http-vs] external-link snat-pool spool1
```

Related commands

display virtual-server

loadbalance snat-pool

external-link whitelist domain

Use **external-link whitelist domain** to add a domain name to the whitelist for external link proxy.

Use **undo external-link whitelist domain** to delete a domain name from the whitelist for external link proxy.

Syntax

external-link whitelist domain *domain-name*

undo external-link whitelist domain *domain-name*

Default

No domain names are added to the whitelist for external link proxy.

Views

HTTP virtual server view

Predefined user roles

network-admin

context-admin

Parameters

domain-name: Specifies a domain name, a case-insensitive, dot-separated string of 1 to 254 characters. Each dot-separated label in the domain name can contain a maximum of 63 characters. The domain name can contain letters, digits, hyphens (-), underscores (_), and dots (.).

Usage guidelines

The LB device does not rewrite the external links containing any domain names in the whitelist. You can add specific domain names (for example, those of the IPv6 external links in the IPv6 site) to the whitelist.

Examples

Add domain name **a.com** to the whitelist for external link proxy on HTTP virtual server **vs**.

```
<Sysname> system-view
[Sysname] virtual-server vs http
[Sysname-vs-http-vs] external-link whitelist domain a.com
```

Related commands

display virtual-server

external-script

Use **external-script** to specify a script file used for custom monitoring.

Use **undo external-script** to restore the default.

Syntax

external-script *file-name*

undo external-script

Default

No script file is specified for custom monitoring.

Views

Custom-monitoring LB probe template view

Predefined user roles

network-admin

context-admin

Parameters

file-name: Specifies a script file by its name, a case-insensitive string of 1 to 255 characters.

Usage guidelines

The device detects the state of real severs according to the detection contents in the script file.

Before specifying a script file, upload the file to the device.

The device supports specifying only script files with the **.py** suffix.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

In custom-monitoring LB probe template **test_external**, use script file **test.py** for custom monitoring.

```
<Sysname> system-view
[Sysname] loadbalance probe-template external-monitor test-external
[Sysname-lbpt-external-monitor-test-external] external-script test.py
```

fail-action (link group view)

Use **fail-action** to specify the fault processing method for a link group.

Use **undo fail-action** to restore the default.

Syntax

fail-action { **keep** | **reschedule** | **reset** }

undo fail-action

Default

The fault processing method is to keep existing connections.

Views

Link group view

Predefined user roles

network-admin

context-admin

Parameters

keep: Keeps the connection with the failed link. Keeping or terminating the connection depends on the timeout mechanism of the protocol.

reschedule: Redirects the connection to another available link in the link group.

reset: Terminates the connection with the failed link by sending RST packets (for TCP packets) or ICMP unreachable packets (for other types of packets).

Usage guidelines

The fault processing method applies when the link that processes packets fails.

Examples

Specify the fault processing method for the link group **lg** as **reschedule**.

```
<Sysname> system-view
[Sysname] loadbalance link-group lg
[Sysname-lb-lgroup-lg] fail-action reschedule
```

fail-action (server farm view)

Use **fail-action** to specify the fault processing method for a server farm.

Use **undo fail-action** to restore the default.

Syntax

fail-action { **keep** | **reschedule** | **reset** }

undo fail-action

Default

The fault processing method is to keep existing connections.

Views

Server farm view

Predefined user roles

network-admin

context-admin

Parameters

keep: Keeps the connection with the failed real server. Keeping or terminating the connection depends on the timeout mechanism of the protocol.

reschedule: Redirects the connection to another available real server in the server farm.

reset: Terminates the connection with the failed real server by sending RST packets (for TCP packets) or ICMP unreachable packets (for other types of packets).

Usage guidelines

The fault processing method applies when the real server that processes packets fails.

Examples

Specify the fault processing method for the server farm **sf** as **reschedule**.

```
<Sysname> system-view
[Sysname] server-farm sf
[Sysname-sfarm-sf] fail-action reschedule
```

fallback

Use **fallback** to specify a processing method for DNS mapping search failure.

Use **undo fallback** to restore the default.

Syntax

fallback { **dns-proxy** | **no-response** | **reject** }

undo fallback

Default

A DNS listener sends a DNS reject packet for DNS mapping search failure.

Views

DNS listener view

Predefined user roles

network-admin

context-admin

Parameters

dns-proxy: Responds to DNS requests through a transparent DNS proxy.

no-response: Does not respond to DNS requests.

reject: Sends a DNS reject packet.

Examples

Specify the processing method for DNS mapping search failure as **no-response**.

```
<Sysname> system-view
[Sysname] loadbalance dns-listener ct-listener
[Sysname-lb-dl-ct-listener] fallback no-response
```

fallback-action close

Use **fallback-action close** to configure the method of closing TCP connections upon failure to find a real server.

Use **undo fallback-action** to restore the default.

Syntax

fallback-action close { **fin** | **rst** }

undo fallback-action

Default

Packets are dropped when no real servers are available for the current LB action.

Views

Generic/HTTP LB action view

Predefined user roles

network-admin

context-admin

Parameters

fin: Closes TCP connections by sending FIN packets.

rst: Closes TCP connections by sending RST packets.

Usage guidelines

This command enables the device to close TCP connections matching the LB policy by sending FIN or RST packets if the device fails to find a real server according to the LB action.

Examples

In HTTP LB action **a1**, configure the method of closing TCP connections by sending RST packets.

```
<Sysname> system-view
[Sysname] loadbalance action a1 type http
[Sysname-lba-http-a1] fallback-action close rst
```

fallback-action continue

Use **fallback-action continue** to match the next rule upon failure to find an available server.

Use **undo fallback-action** to restore the default.

Syntax

fallback-action continue

undo fallback-action

Default

Packets are dropped when no servers are available for the current LB action.

Views

LB action view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command enables packets to match the next rule in an LB policy when no servers are available for the current LB action.

This command does not apply to SIP virtual servers.

Examples

Match the next rule upon failure to find a real server for the HTTP LB action **a1**.

```
<Sysname> system-view
[Sysname] loadbalance action a1 type http
[Sysname-lba-http-a1] fallback-action continue
```

Match the next rule upon failure to find a DNS server for the DNS LB action **a2**.

```
<Sysname> system-view
[Sysname] loadbalance action a2 type dns
[Sysname-lba-dns-a2] fallback-action continue
```

fallback-action response raw-file

Use **fallback-action response raw-file** to specify a response file used upon load balancing failure.

Use **undo fallback-action** to restore the default.

Syntax

fallback-action response raw-file *raw-filename*

undo fallback-action

Default

Packets are discarded upon load balancing failure.

Views

HTTP LB action view

Predefined user roles

network-admin

context-admin

Parameters

raw-filename: Specifies a response file by its name, a case-insensitive string of 1 to 255 characters.

Usage guidelines

This command enables the device to respond to client requests when the device fails to find an available real server or fails to find the response file specified in the **response** command. The response file specified in the **fallback-action response raw-file** command must contain a complete HTTP packet and cannot contain only the HTTP content.

The **fallback-action response raw-file** command and the **fallback-action continue** command are mutually exclusive.

Examples

Specify the **301.raw** file as the response file used upon load balancing failure.

```
<Sysname> system-view
```

```
[Sysname] loadbalance action a_http type http
[Sysname-lba-http-a_http] fallback-action response raw-file 301.raw
```

Related commands

display loadbalance action

fallback-action continue

fin-wait1 timeout

Use **fin-wait1 timeout** to set the FIN-WAIT-1 state timeout time for TCP connections.

Use **undo fin-wait1 timeout** to restore the default.

Syntax

fin-wait1 timeout *timeout-value*

undo fin-wait1 timeout

Default

The FIN-WAIT-1 state timeout time is 5 seconds for TCP connections.

Views

TCP parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

timeout-value: Specifies the FIN-WAIT-1 state timeout time in the range of 1 to 65535 seconds.

Examples

Set the FIN-WAIT-1 state timeout time for TCP connections to 10 seconds in the TCP parameter profile **profile**.

```
<Sysname> system-view
[Sysname] parameter-profile profile type tcp
[Sysname-para-tcp-profile] fin-wait1 timeout 10
```

Related commands

display parameter-profile

fin-wait2 timeout

Use **fin-wait2 timeout** to set the FIN-WAIT-2 state timeout time for TCP connections.

Use **undo fin-wait2 timeout** to restore the default.

Syntax

fin-wait1 timeout *timeout-value*

undo fin-wait1 timeout

Default

The FIN-WAIT-2 state timeout time is 5 seconds for TCP connections.

Views

TCP parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

timeout-value: Specifies the FIN-WAIT-2 state timeout time in the range of 1 to 65535 seconds.

Examples

Set the FIN-WAIT-2 state timeout time for TCP connections to 10 seconds in the TCP parameter profile **profile**.

```
<Sysname> system-view
[Sysname] parameter-profile profile type tcp
[Sysname-para-tcp-profile] fin-wait2 timeout 10
```

Related commands

display parameter-profile

forward all

Use **forward all** to configure the packet forwarding mode.

Use **undo forward** to restore the default.

Syntax

forward all

undo forward

Default

The packet forwarding mode is to discard packets.

Views

DNS/Generic/Link-generic LB action view

Predefined user roles

network-admin

context-admin

Usage guidelines

In DNS LB action view, this command is mutually exclusive with the **dns-server-pool** or **skip current-dns-proxy** command. In generic LB action view, the **forward all** and **server-farm** commands are mutually exclusive. In link-generic LB action view, the **forward all** and **link-group** commands are mutually exclusive. If you configure one command, the other command (if configured) is automatically cancelled.

This command does not apply to SIP vertual servers.

Examples

Configure the packet forwarding mode for the generic LB action **lba1**.

```
<Sysname> system-view
[Sysname] loadbalance action lba1 type generic
[Sysname-lba-generic-lba1] forward all
```

Related commands

dns-server-pool

link-group (LB action view)

server-farm (LB action view)

frequency

Use **frequency** to set the probe interval for an LB probe template.

Use **undo frequency** to restore the default.

Syntax

frequency *interval*

undo frequency

Default

The probe interval is 300 seconds.

Views

Load balancing probe template view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies the probe interval in the range of 5 to 604800 seconds.

Usage guidelines

This command specifies the interval for sending probe packets.

Examples

Set the probe interval to 3600 seconds for ICMP probe template **icmptplt**.

```
<Sysname> system-view
[Sysname] loadbalance probe-template icmp icmptplt
[Sysname-lb-pt-icmp-icmptplt] frequency 3600
```

header (HTTP header sticky group view)

Use **header** to configure the HTTP header sticky method.

Use **undo header** to restore the default.

Syntax

header { { { **host** | **name** *header-name* | **url** } [**offset** *offset*] [**start** *start-string*] [**end** *end-string* | **length** *length*] } | **request-method** | **version** }

undo header

Default

No HTTP header sticky methods exist.

Views

HTTP header sticky group view

Predefined user roles

network-admin

context-admin

Parameters

host: Specifies the HTTP host based sticky method.

name *header-name*: Specifies the HTTP header name based sticky method. The *header-name* argument is a case-insensitive string of 1 to 63 characters.

url: Specifies the HTTP URL based sticky method.

offset *offset*: Specifies the offset value of the HTTP header based on the start of the HTTP packet, in the range of 0 to 1000 bytes. The default is 0.

start *start-string*: Specifies the regular expression that marks the start of the HTTP header, a case-sensitive string of 1 to 127 characters starting from the *offset* value. The string cannot contain question marks (?).

end *end-string*: Specifies the regular expression that marks the end of the HTTP header, a case-sensitive string of 1 to 127 characters starting from the *start-string* value. The string cannot contain question marks (?).

length *length*: Specifies the length of the HTTP header, in the range of 0 to 1000 bytes. The default is 0, which indicates all lengths.

request-method: Specifies the HTTP Request-Method based sticky method.

version: Specifies the HTTP version based sticky method.

Usage guidelines

Use this command to obtain the HTTP header information used to generate sticky entries based on the *offset*, *start-string*, *end-string*, and *length* values. The *start-string* and *end-string* values are not included in the sticky entry information.

Examples

Configure the HTTP header sticky method for the HTTP header sticky group **sg4**: Specify the HTTP host based sticky method.

```
<Sysname> system-view
[Sysname] sticky-group sg4 type http-header
[Sysname-sticky-http-header-sg4] header host
```

header (HTTP passive sticky group view)

Use **header** to configure the HTTP header passive sticky method.

Use **undo header** to delete the HTTP header passive sticky method.

Syntax

header { **get** *id* **name** *header-name* | **match** *id* { **name** *header-name* | **url** } } **start** *start-string* { **end** *end-string* | **length** *length* }

undo { **get** | **match** } *id*

Default

No HTTP header passive sticky methods exist.

Views

HTTP passive sticky group view

Predefined user roles

network-admin

context-admin

Parameters

get: Obtains the specified string in the HTTP response header, which is used to generate an HTTP header passive sticky entry.

match: Obtains the specified string in the HTTP request header, which is used to match an HTTP header passive sticky entry.

id: Specifies the string ID in the range of 1 to 4.

name *header-name*: Specifies the HTTP header name based sticky method. The *header-name* argument is a case-insensitive string of 1 to 63 characters.

url: Specifies the HTTP URL based sticky method.

start *start-string*: Specifies the regular expression that marks the start of the HTTP header or URL, a case-sensitive string of 1 to 127 characters. The string cannot contain question marks (?).

end *end-string*: Specifies the regular expression that marks the end of the HTTP header or URL, a case-sensitive string of 1 to 127 characters. The string cannot contain question marks (?).

length *length*: Specifies the length of the HTTP header or URL, in the range of 0 to 1000 bytes. The default is 0, which indicates all lengths.

Usage guidelines

The *start-string* and *end-string* values are not included in the sticky entry information.

Both the **header get** and **header match** commands are required for an HTTP header passive sticky method.

The device obtains the header or URL information of an incoming HTTP request based on the **header match** command and obtains the header information of an incoming HTTP response based on the **header get** command. If the header or URL information of the HTTP request matches the header information of the HTTP response, the device generates a sticky entry based on the header information of the HTTP response. Subsequent HTTP requests that match the sticky entry are forwarded according to the sticky entry.

The following rules apply to use of the **header match** and **header get** commands:

- You can execute a maximum of four **header get** commands and four **header match** commands for one HTTP passive sticky method.
- A number of *n* strings that are obtained based on *n* **header get** commands generates 2^n-1 strings in ascending order of string IDs. If the string obtained based on the **header match** command matches any one of these generated strings, the match is successful.
- A number of *n* strings that are obtained based on *n* **header match** commands combine as one string in ascending order of string IDs.

For example, three **header get** commands are executed with string IDs 1, 2, and 3. The device obtains three strings a, b, and c in the HTTP response header, generates seven strings a, b, c, ab, ac, bc, and abc, and generates seven sticky entries. Then, three **header match** commands are executed with string IDs 2, 3, and 4. The device obtains three strings a, b, and c in the HTTP request header and generates one string abc. If the string matches one of the seven strings, the device generates a sticky entry based on the string abc. Subsequent HTTP requests that match the sticky entry are forwarded according to the sticky entry.

Examples

Configure the HTTP passive sticky method for the HTTP passive sticky group **sg4**: Obtain the string between **callid** and **&** in the URL of the HTTP request. If the string matches the string between **phone-number** and **&** in HTTP response header **x-forward-callid**, the device generates a sticky entry based on the string between **phone-number** and **&**.

```
<Sysname> system-view
[Sysname] sticky-group sg4 type http-passive
[Sysname-sticky-http-passive-sg4] header get 1 name x-forward-callid start phone-number end &
[Sysname-sticky-http-passive-sg4] header match 1 url start callid end &
```

Related commands

content (HTTP passive sticky group view)

display sticky-group

header call-id

Use **header call-id** to configure the SIP call ID sticky method.

Use **undo header call-id** to restore the default.

Syntax

header call-id

undo header call-id

Default

No sticky methods exist.

Views

SIP sticky group view

Predefined user roles

network-admin

context-admin

Usage guidelines

The SIP call ID sticky method allows the device to generate sticky entries based on the Call-ID header field in SIP messages. Packets with the same call ID are assigned to the same real server.

Examples

Configure the SIP call ID sticky method for the SIP sticky group **sg6**.

```
<Sysname> system-view
[Sysname] sticky-group sg6 type sip
[Sysname-sticky-sip-sg6] header call-id
```

header delete

Use **header delete** to delete the HTTP header.

Use **undo header delete** to keep the HTTP header.

Syntax

header delete { **both** | **request** | **response** } **name** *header-name*

undo header delete { **both** | **request** | **response** } **name** *header-name*

Default

The HTTP header is kept.

Views

HTTP LB action view

Predefined user roles

network-admin

context-admin

Parameters

both: Specifies both the HTTP request and response packets.

request: Specifies the HTTP request packets.

response: Specifies the HTTP response packets.

name *header-name*: Specifies the name of the HTTP packet header, including standard and user-defined headers that must match the header in the packet. The *header-name* argument is a case-insensitive string of 1 to 63 characters excluding brackets ({ }, ( ),[ ], < >), at sign (@), comma (,), semicolon (;), colon (:), backslash (\), quotation mark ("), slash (/), question mark (?), equal sign (=), space character (SP), and horizontal tab (HT). The character string also excludes ASCII codes that are less than or equal to 31 and greater than or equal to 127. You can enter a question mark (?) to obtain a list of standard header names. For more information about the header names, see RFC 4229.

Usage guidelines

This command deletes the specified header from HTTP packets.

Examples

Delete the header named **host** from HTTP request packets for the HTTP LB action **lba2**.

```
<Sysname> system-view
[Sysname] loadbalance action lba2 type http
[Sysname-lba-http-lba2] header delete request name host
```

header delete request accept-encoding

Use **header delete request accept-encoding** to delete the Accept-Encoding header from HTTP requests.

Use **undo header delete request accept-encoding** to keep the Accept-Encoding header in HTTP requests.

Syntax

header delete request accept-encoding

undo header delete request accept-encoding

Default

The LB device deletes the Accept-Encoding header from HTTP requests.

Views

HTTP-compression parameter profile view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command enables the LB device to delete the Accept-Encoding header from the HTTP request before sending it to the server. If the response packet sent by the server matches the specified match rule, the LB device compresses the packet before sending it to the requesting client. If the HTTP request sent by the client does not contain the Accept-Encoding header, the LB device does not compress the response packet regardless of whether this command is executed.

By default, the LB device does not modify request packets. If the response packet sent by the server is compressed, the LB device sends the packet to the requesting client without compressing it. If the response packet sent by the server is not compressed and matches the specified match rule, the LB device compresses the packet before sending it to the requesting client.

Examples

Create the HTTP-compression parameter profile **http1**, and delete the Accept-Encoding header from HTTP requests.

```
<Sysname> system-view
[Sysname] parameter-profile http1 type http-compression
[Sysname-para-http-compression-http1] header delete request accept-encoding
```

header exceed-length

Use **header exceed-length** to specify the action to take on the HTTP requests or responses when their packet headers exceed the maximum length.

Use **undo header exceed-length** to restore the default.

Syntax

header exceed-length { **continue** | **drop** }

undo header exceed-length

Default

The system continues to perform load balancing for HTTP requests or responses when their packet headers exceed the maximum length.

Views

HTTP parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

continue: Continues to perform load balancing.

drop: Stops performing load balancing, discards the packet, and terminates the connection.

Usage guidelines

This command is not supported by virtual servers of the fast HTTP type.

When the HTTP packet header length exceeds the processing capability of load balancing, the **drop** method applies.

Examples

For the HTTP parameter profile **pp1**, specify the **drop** action for the HTTP requests or responses with their packet headers exceeding the maximum length.

```
<Sysname> system-view
[Sysname] parameter-profile pp1 type http
[Sysname-para-http-pp1] header exceed-length drop
```

header insert

Use **header insert** to insert the HTTP header.

Use **undo header insert** to remove the configuration.

Syntax

header insert { **both** | **request** | **response** } **name** *header-name* **value** *value* [**encode** { **base64** | **url** }]

undo header insert { **both** | **request** | **response** } **name** *header-name*

Default

The HTTP header is not inserted.

Views

HTTP LB action view

Predefined user roles

network-admin

context-admin

Parameters

both: Specifies both the HTTP request and response packets.

request: Specifies the HTTP request packets.

response: Specifies the HTTP response packets.

name *header-name*: Specifies the name of the HTTP packet header, including standard and user-defined headers. The *header-name* argument is a case-sensitive string of 1 to 63 characters excluding brackets ({ }, ( ),[ ], < >), at sign (@), comma (,), semicolon (;), colon (:), backslash (\), quotation mark ("), slash (/), question mark (?), equal sign (=), space character (SP), and horizontal tab (HT). The character string also excludes ASCII codes that are less than or equal to 31 and greater than or equal to 127. You can enter a question mark (?) to obtain a list of standard header names. For more information about the header names, see RFC 4229.

value *value*: Specifies the header content to be inserted to the HTTP packet, a string of 1 to 255 characters. You can also specify the following replacement strings:

- **%is**—Source IP address in HTTP requests.
- **%ps**—Source port number in HTTP requests.
- **%id**—Destination IP address in HTTP requests.
- **%pd**—Destination port number in HTTP requests.
- **%sps**—Source port number in HTTP responses.
- **%spd**—Destination port number in HTTP responses.
- **%sis**—Source IP address in HTTP responses.
- **%sid**—Destination IP address in HTTP responses.
- **%{x509v}**—Certificate version.
- **%{x509snum}**—Certificate serial number.

- **%{x509sigalgo}**—Certificate signature algorithm.
- **%{x509issuer}**—Certificate issuer.
- **%{x509before}**—Certificate effective time.
- **%{x509after}**—Certificate expiration time.
- **%{x509sub}**—Certificate subject.
- **%{x509spktype}**—Public key type for the certificate subject.
- **%{x509spk}**—Public key for the certificate subject.
- **%{x509spkRSA}**—Length of the RSA public key for the certificate subject (this field is available only for an RSA public key).
- **%{x509hash}**—MD5 hash value of the client certificate.
- **%{dncn}**—Issuee.
- **%{dne}**—Email.
- **%{dno}**—Company/Organization.
- **%{dnou}**—Department.
- **%{dnc}**—Country.
- **%{dns}**—State/Province.
- **%{dnl}**—City.

encode { **base64** | **url** }: Specifies an encoding method for replacement strings. If you do not specify an encoding method, replacement strings are not encoded.

Usage guidelines

This command inserts the specified header to HTTP packets.

URL encoding encodes only special characters in replacement strings, for example, colons in IPv6 addresses. Base64 encoding encodes entire replacement strings.

Examples

Insert the header named **source** with source IP address and source port number as the content to HTTP request packets for the HTTP LB action **lba2**.

```
<Sysname> system-view
[Sysname] loadbalance action lba2 type http
[Sysname-lba-http-lba2] header insert request name source value %is:%ps
```

header insert response vary

Use **header insert response vary** to insert the Vary header into HTTP responses.

Use **undo header insert response vary** to remove the configuration.

Syntax

header insert response vary

undo header insert response vary

Default

The Vary header is inserted into HTTP responses.

Views

HTTP-compression parameter profile view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command inserts the Vary header to HTTP responses and sets the header content to Accept-Encoding before sending them to the client. The command takes effect regardless of whether the response packets contain the Vary header or whether the packets are compressed.

Examples

Create the HTTP-compression parameter profile **http1**, and insert the Vary header into HTTP responses.

```
<Sysname> system-view
[Sysname] parameter-profile http1 type http-compression
[Sysname-para-http-compression-http1] header insert response vary
```

header maxparse-length

Use **header maxparse-length** to set the maximum length of HTTP headers that can be parsed.

Use **undo header maxparse-length** to restore the default.

Syntax

header maxparse-length *length*

undo header maxparse-length

Default

The maximum length of HTTP headers that can be parsed is 4096.

Views

HTTP parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

length: Specifies the maximum length of HTTP headers that can be parsed, in the range of 1 to 65535 bytes.

Usage guidelines

This command is not supported by the virtual servers of the fast HTTP type.

Examples

Set the maximum length of HTTP headers that can be parsed to 8192 for the HTTP parameter profile **pp1**.

```
<Sysname> system-view
[Sysname] parameter-profile pp1 type http
[Sysname-para-http-pp1] header maxparse-length 8192
```

header modify per-request

Use **header modify per-request** to perform the insert, delete, or modify operation for the header of each HTTP request or response packet.

Use **undo header modify per-request** to restore the default.

Syntax

header modify per-request

undo header modify per-request

Default

The insert, delete, or modify operation is performed for the header of the first HTTP request or response packet of a connection.

Views

HTTP parameter profile view

Predefined user roles

network-admin

context-admin

Examples

For the HTTP parameter profile **pp1**, perform the insert, delete, or modify operation for the header of each HTTP request or response packet.

```
<Sysname> system-view
[Sysname] parameter-profile pp1 type http
[Sysname-para-http-pp1] header modify per-request
```

header rewrite

Use **header rewrite** to rewrite the HTTP header.

Use **undo header rewrite** to remove the configuration.

Syntax

header rewrite { **both** | **request** | **response** } **name** *header-name* **value** *value* **replace** *replace* [**encode** { **base64** | **url** }]

undo header rewrite { **both** | **request** | **response** } **name** *header-name*

Default

The HTTP header is not rewritten.

Views

HTTP LB action view

Predefined user roles

network-admin

context-admin

Parameters

both: Specifies both the HTTP request and response packets.

request: Specifies the HTTP request packets.

response: Specifies the HTTP response packets.

name *header-name*: Specifies the name of the HTTP packet header, including standard and user-defined headers that must match the header in the packet. The *header-name* argument is a case-insensitive string of 1 to 63 characters excluding brackets ({ }, ( ),[ ], < >), at sign (@), comma (,), semicolon (;), colon (:), backslash (\), quotation mark ("), slash (/), question mark (?), equal sign (=), space character (SP), and horizontal tab (HT). The character string also excludes ASCII codes that are less than or equal to 31 and greater than or equal to 127. You can enter a question mark (?) to obtain a list of standard header names. For more information about the header names, see RFC 4229.

value *value*: Specifies the HTTP packet header content to be rewritten, a case-sensitive string of 1 to 127 characters. The string cannot contain question marks (?).

replace *replace*: Specifies the content after rewrite, a case-sensitive string of 1 to 127 characters. You can also specify the following replacement strings:

- **%is**—Source IP address in HTTP requests.
- **%ps**—Source port number in HTTP requests.
- **%id**—Destination IP address in HTTP requests.
- **%pd**—Destination port number in HTTP requests.
- **%sps**—Source port number in HTTP responses.
- **%spd**—Destination port number in HTTP responses.
- **%sis**—Source IP address in HTTP responses.
- **%sid**—Destination IP address in HTTP responses.
- %{**x509v**}—Certificate version.
- %{**x509snum**}—Certificate serial number.
- %{**x509sigalgo**}—Certificate signature algorithm.
- %{**x509issuer**}—Certificate issuer.
- %{**x509before**}—Certificate effective time.
- %{**x509after**}—Certificate expiration time.
- %{**x509sub**}—Certificate subject.
- %{**x509spktype**}—Public key type for the certificate subject.
- %{**x509spk**}—Public key for the certificate subject.
- %{**x509spkRSA**}—Length of the RSA public key for the certificate subject (this field is available only for an RSA public key).
- %{**x509hash**}—MD5 hash value of the client certificate.
- %{**dncn**}—Issuee.
- %{**dne**}—Email.
- %{**dno**}—Company/Organization.
- %{**dnou**}—Department.
- %{**dnc**}—Country.
- %{**dns**}—State/Province.
- %{**dnl**}—City.

encode { **base64** | **url** }: Specifies an encoding method for replacement strings. If you do not specify an encoding method, replacement strings are not encoded.

Usage guidelines

This command rewrites the *value* setting of the specified header in HTTP packets to the *replace* setting.

URL encoding encodes only special characters in replacement strings, for example, colons in IPv6 addresses. Base64 encoding encodes entire replacement strings.

Examples

For the HTTP LB action **lba2**, rewrite the content **www.hello.com** of the header named **host** in HTTP request packets to **www.he.com.cn**.

```
<Sysname> system-view
[Sysname] loadbalance action lba2 type http
[Sysname-lba-http-lba2] header rewrite request name host value www\.(he)(llo)\.com
replace www.%1.com.cn encode url
```

header rewrite request url

Use **header rewrite request url** to rewrite the URL in HTTP requests.

Use **undo header rewrite request url** to restore the default.

Syntax

header rewrite request url value *value* **replace** *replace* [**encode** { **base64** | **url** }]

undo header rewrite request url

Default

The URL in HTTP requests is not rewritten.

Views

HTTP LB action view

Predefined user roles

network-admin

context-admin

Parameters

value *value*: Specifies the URL to be rewritten, a case-sensitive string of 1 to 127 characters. The string cannot contain question marks (?).

replace *replace*: Specifies the URL after rewrite, a case-sensitive string of 1 to 127 characters. You can also specify the following replacement strings:

- **%is**—Source IP address in HTTP requests.
- **%ps**—Source port number in HTTP requests.
- **%id**—Destination IP address in HTTP requests.
- **%pd**—Destination port number in HTTP requests.
- **%sps**—Source port number in HTTP responses.
- **%spd**—Destination port number in HTTP responses.
- **%sis**—Source IP address in HTTP responses.
- **%sid**—Destination IP address in HTTP responses.
- **%{x509v}**—Certificate version.

- %{**x509snum**}—Certificate serial number.
- %{**x509sigalgo**}—Certificate signature algorithm.
- %{**x509issuer**}—Certificate issuer.
- %{**x509before**}—Certificate effective time.
- %{**x509after**}—Certificate expiration time.
- %{**x509sub**}—Certificate subject.
- %{**x509spktype**}—Public key type for the certificate subject.
- %{**x509spk**}—Public key for the certificate subject.
- %{**x509spkRSA**}—Length of the RSA public key for the certificate subject (this field is available only for an RSA public key).
- %{**x509hash**}—MD5 hash value of the client certificate.
- %{**dncn**}—Issuee.
- %{**dne**}—Email.
- %{**dno**}—Company/Organization.
- %{**dnou**}—Department.
- %{**dnc**}—Country.
- %{**dns**}—State/Province.
- %{**dnl**}—City.

encode { **base64** | **url** }: Specifies an encoding method for replacement strings. If you do not specify an encoding method, replacement strings are not encoded.

Usage guidelines

This command rewrites the *value* setting in the HTTP request URL to the *replace* setting.

URL encoding encodes only special characters in replacement strings, for example, colons in IPv6 addresses. Base64 encoding encodes entire replacement strings.

Examples

For the HTTP LB action **lba2**, rewrite the URL **www.hello.com** in HTTP requests to **www.he.com.cn**.

```
<Sysname> system-view
[Sysname] loadbalance action lba2 type http
[Sysname-lba-http-lba2] header rewrite request url value www\.(he)(llo)\.com replace
www.%1.com.cn encode url
```

idle-time

Use **idle-time** to set the idle timeout time for TCP connections between the LB device and servers.

Use **undo idle-time** to restore the default.

Syntax

idle-time *idle-time*

undo idle-time

Default

The idle timeout time for TCP connections between the LB device and servers is 86400 seconds.

Views

OneConnect parameter profile view

MySQL parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

idle-time: Specifies the idle timeout time in the range of 1 to 4294967295 seconds.

Usage guidelines

The idle timeout time is the amount of time that a TCP connection can stay idle before it is disconnected. After the TCP connection is disconnected, new connection requests trigger establishment of a new TCP connection.

Examples

In OneConnect parameter profile **ocp**, set the idle timeout time to 10000 seconds for TCP connections between the LB device and servers.

```
<Sysname> system-view
[Sysname] parameter-profile ocp type oneconnect
[Sysname-para-oneconnect-ocp] idle-time 10000
```

inherit vpn-instance disable (link view)

Use **inherit vpn-instance disable** to disable VPN instance inheritance for a link.

Use **undo inherit vpn-instance disable** to enable VPN instance inheritance for a link.

Syntax

inherit vpn-instance disable

undo inherit vpn-instance disable

Default

VPN instance inheritance is enabled for a link.

Views

Link view

Predefined user roles

network-admin

context-admin

Usage guidelines

When VPN instance inheritance is enabled, a link without a VPN instance specified inherits the VPN instance of the virtual server. When VPN instance inheritance is disabled, a link without a VPN instance specified belongs to the public network.

To specify a VPN instance for a link, use the **vpn-instance** *vpn-instance-name* command in link view.

You can display the VPN instance for a link by using the **display loadbalance link** command.

Examples

Disable VPN instance inheritance for link **lk1**.

```
<Sysname> system-view
[Sysname] loadbalance link lk1
[Sysname-lb-link-lk1] inherit vpn-instance disable
```

Related commands

display loadbalance link

vpn-instance (link view)

inherit vpn-instance disable (real server view)

Use **inherit vpn-instance disable** to disable VPN instance inheritance for a real server.

Use **undo inherit vpn-instance disable** to enable VPN instance inheritance for a real server.

Syntax

inherit vpn-instance disable

undo inherit vpn-instance disable

Default

VPN instance inheritance is enabled for a real server.

Views

Real server view

Predefined user roles

network-admin

context-admin

Usage guidelines

When VPN instance inheritance is enabled, a real server without a VPN instance specified inherits the VPN instance of its virtual server. When VPN instance inheritance is disabled, a real server without a VPN instance specified belongs to the public network.

To specify a VPN instance for a real server, use the **vpn-instance** command in real server view.

Examples

Disable VPN instance inheritance for real server **rs**.

```
<Sysname> system-view
[Sysname] real-server rs
[Sysname-rserver-rs] inherit vpn-instance disable
```

Related commands

vpn-instance (real server view)

vpn-instance (virtual server view)

ip

Use **ip** to configure the IPv4 sticky method.

Use **undo ip** to restore the default.

Syntax

ip [**port**] { **both** | **destination** | **source** } [**mask** *mask-length*]

undo ip

Default

No IPv4 sticky method is configured.

Views

Sticky group view

Predefined user roles

network-admin

context-admin

Parameters

port: Specifies the sticky method as IPv4 address + port number. If you do not specify this keyword, the sticky method is IPv4 address.

both: Specifies the sticky method as source IPv4 address + destination IPv4 address (if you do not specify the **port** keyword), or source IPv4 address + source port number + destination IPv4 address + destination port number (if you specify the **port** keyword).

destination: Specifies the sticky method as destination IPv4 address if you do not specify the **port** keyword, or destination IPv4 address + destination port number if you specify the **port** keyword.

source: Specifies the sticky method as source IPv4 address if you do not specify the **port** keyword, or source IPv4 address + source port number if you specify the **port** keyword.

mask *mask-length*: Specifies the mask length for the sticky method.

Examples

Configure the sticky method for the address and port-based sticky group **sg1** as source IPv4 address.

```
<Sysname> system-view
[Sysname] sticky-group sg1 type address-port
[Sysname-sticky-address-port-sg1] ip source
```

Configure the sticky method for the address and port-based sticky group **sg1** as source IPv4 address + source port number.

```
<Sysname> system-view
[Sysname] sticky-group sg1 type address-port
[Sysname-sticky-address-port-sg1] ip port source
```

Related commands

sticky-group

ip address (DNS listener view)

Use **ip address** to specify an IPv4 address and a port number for a DNS listener.

Use **undo ip address** to restore the default.

Syntax

ip address *ipv4-address* [**port** *port-number*]

undo ip address

Default

No IPv4 address or port number is specified for a DNS listener.

Views

DNS listener view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-address: Specifies an IPv4 address, which cannot be a loopback address, multicast address, broadcast address, or an address in the format of 0.X.X.X.

port-number: Specifies a port number in the range of 1 to 65535. The default port number is 53.

Usage guidelines

You can specify only one IPv4 address for a DNS listener. If you execute this command multiple times, the most recent configuration takes effect. A DNS listener without an IPv4 address configured does not process IPv4 DNS requests.

To ensure correct operation of inbound link load balancing when server load balancing is also enabled, do not specify the virtual server's IP address as the DNS listener's IP address.

Examples

Specify the IPv4 address for the DNS listener as **1.2.3.4** and port number as **8080**.

```
<Sysname> system-view
[Sysname] loadbalance dns-listener ct-listener
[Sysname-lb-dl-ct-listener] ip address 1.2.3.4 port 8080
```

Related commands

display loadbalance dns-listener

ip address (DNS server view)

Use **ip address** to specify an IPv4 address for a DNS server.

Use **undo ip address** to restore the default.

Syntax

ip address *ipv4-address*

undo ip address

Default

No IPv4 address is specified for a DNS server.

Views

DNS server view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-address: Specifies an IPv4 address, which cannot be a loopback address, multicast address, broadcast address, or an address in the format of 0.X.X.X.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the IPv4 address for DNS server **ds1** as **1.2.3.4**.

```
<Sysname> system-view
[Sysname] loadbalance dns-server ds1
[Sysname-lb-ds-ds1] ip address 1.2.3.4
```

ip address (ISP view)

Use **ip address** to configure an IPv4 address for an ISP.

Use **undo ip address** to restore the default.

Syntax

ip address *ipv4-address* { *mask-length* | *mask* }

undo ip address *ipv4-address* { *mask-length* | *mask* }

Default

No IPv4 address is configured for an ISP.

Views

ISP view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-address: Specifies an IPv4 address.

mask-length: Specifies the mask length for the IPv4 address, in the range of 0 to 32.

mask: Specifies the mask for the IPv4 address.

Examples

Configure the IPv4 address for the ISP **isp1** as **1.1.1.1**.

```
<Sysname> system-view
[Sysname] loadbalance isp name isp1
[Sysname-lbisp-isp1] ip address 1.1.1.1 24
```

ip address (real server view)

Use **ip address** to configure an IPv4 address for a real server.

Use **undo ip address** to restore the default.

Syntax

ip address *ipv4-address*

undo ip address

Default

No IPv4 address is configured for a real server.

Views

Real server view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-address: Specifies an IPv4 address, which cannot be a loopback address, multicast address, broadcast address, or an address in the format of 0.X.X.X.

Examples

Configure the IPv4 address for the real server **rs** as **1.1.1.1**.

```
<Sysname> system-view
[Sysname] real-server rs
[Sysname-rserver-rs] ip address 1.1.1.1
```

ip address (transparent DNS proxy view)

Use **ip address** to specify an IPv4 address for a transparent DNS proxy.

Use **undo ip address** to restore the default.

Syntax

ip address *ipv4-address* [*mask-length* | *mask*]

undo ip address

Default

No IPv4 address is specified for a transparent DNS proxy.

Views

Transparent DNS proxy view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-address: Specifies an IPv4 address, which cannot be a loopback address, multicast address, broadcast address, or an address in the format of 0.X.X.X.

mask-length: Specifies a mask length in the range of 0 to 32.

mask: Specifies a subnet mask.

Usage guidelines

A transparent DNS proxy processes a DNS request only when the destination IP address and port number of the DNS request match those of the transparent DNS proxy.

If server load balancing is configured, configure different IP addresses and port numbers for the transparent DNS proxy and the virtual server of the UDP type.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the IPv4 address for transparent DNS proxy **dns-proxy1** as 1.2.3.4/24.

```
<Sysname> system-view
[Sysname] loadbalance dns-proxy dns_proxy1
[Sysname-lb-dp-udp-dns-proxy1] ip address 1.2.3.4 24
```

ip mask

Use **ip mask** to set the mask length for IPv4 proximity entries.

Use **undo ip mask** to restore the default.

Syntax

ip mask { *mask-length* | *mask* }

undo ip mask

Default

The mask length for IPv4 proximity entries is 24.

Views

Proximity view

Predefined user roles

network-admin

context-admin

Parameters

mask-length: Specifies the mask length for IPv4 proximity entries, in the range of 0 to 32. A value of 0 indicates the natural mask.

mask: Specifies the mask for IPv4 proximity entries.

Examples

Set the mask length for IPv4 proximity entries to 30.

```
<Sysname> system-view
[Sysname] loadbalance proximity
[Sysname-lb-proximity] ip mask 30
```

ip range

Use **ip range** to add an IPv4 address range to a SNAT address pool.

Use **undo ip range** to remove an IPv4 address range from a SNAT address pool.

Syntax

ip range start *start-ipv4-address* **end** *end-ipv4-address*

undo ip range start *start-ipv4-address* **end** *end-ipv4-address*

Default

An SNAT address pool does not contain IPv4 address ranges.

Views

SNAT address pool view

Predefined user roles

network-admin

context-admin

Parameters

start *start-ipv4-address*: Specifies the start IPv4 address.

end *end-ipv4-address*: Specifies the end IPv4 address, which must be greater than or equal to the start IPv4 address.

Usage guidelines

You can execute this command multiple times to add multiple IPv4 address ranges to a SNAT address pool. Each address range can have a maximum of 256 IPv4 addresses. No overlapping IPv4 addresses are allowed in the same SNAT address pool or different SNAT address pools.

If the SNAT address pool has an IP address on the same network as the IP address of the device interface connected to the server, you must execute the **arp-nd interface** command for the SNAT address pool. In the situation does not exist, you do not need to execute the **arp-nd interface** command.

Examples

Add IPv4 address range 1.1.1.1 to 1.1.1.100 to the SNAT address pool **lbsp**.

```
<Sysname> system-view
[Sysname] loadbalance snat-pool lbsp
[Sysname-lbsnat-pool-lbsp] ip range start 1.1.1.1 end 1.1.1.100
```

Related commands

arp-nd interface (SNAT address pool view)

loadbalance snat-pool

ip source mask

Use **ip source mask** to specify the IPv4 mask for connection reuse.

Use **undo ip source mask** to restore the default.

Syntax

ip source mask { *mask-length* | *mask* }

undo ip source mask

Default

The IPv4 mask for connection reuse is the natural mask.

Views

OneConnect parameter profile view

MySQL parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

mask-length: Specifies the mask length in the range of 0 to 32. A value of 0 indicates the natural mask.

mask: Specifies the subnet mask in dotted decimal notation.

Usage guidelines

This command limits the network segment of clients that can reuse connections between the LB device and servers. If the client that initiates a connection request is in the same network segment as the idle TCP connection, the idle TCP connection is reused. If the client does not match this requirement, a new TCP connection is established.

Examples

In OneConnect parameter profile **ocp**, set the mask length for connection reuse to 24.

```
<Sysname> system-view
[Sysname] parameter-profile ocp type oneconnect
[Sysname-para-oneconnect-ocp] ip source mask 24
```

ipv6

Use **ipv6** to configure the IPv6 sticky method.

Use **undo ipv6** to restore the default.

Syntax

ipv6 [**port**] { **both** | **destination** | **source** } [**prefix** *prefix-length*]

undo ipv6

Default

No IPv6 sticky method is configured.

Views

Sticky group view

Predefined user roles

network-admin

context-admin

Parameters

port: Specifies the sticky method as IPv6 address + port number. If you do not specify this keyword, the sticky method is IPv6 address.

both: Specifies the sticky method as source IPv6 address + destination IPv6 address if you do not specify the **port** keyword, or source IPv6 address + source port number + destination IPv6 address + destination port number if you specify the **port** keyword.

destination: Specifies the sticky method as destination IPv6 address if you do not specify the **port** keyword, or destination IPv6 address + destination port number if you specify the **port** keyword.

source: Specifies the sticky method as source IPv6 address if you do not specify the **port** keyword, or source IPv6 address + source port number if you specify the **port** keyword.

prefix *prefix-length*: Specifies the prefix length for the sticky method.

Examples

Configure the sticky method for the address- and port-based sticky group **sg1** as source IPv6 address.

```
<Sysname> system-view
[Sysname] sticky-group sg1 type address-port
[Sysname-sticky-address-port-sg1] ipv6 source
```

Configure the sticky method for the address- and port-based sticky group **sg1** as source IPv6 address + source port number.

```
<Sysname> system-view
[Sysname] sticky-group sg1 type address-port
[Sysname-sticky-address-port-sg1] ipv6 port source
```

Related commands

sticky-group

ipv6 address (DNS listener view)

Use **ipv6 address** to configure an IPv6 address and a port number for a DNS listener.

Use **undo ipv6 address** to restore the default.

Syntax

ipv6 address *ipv6-address* [**port** *port-number*]

undo ipv6 address

Default

No IPv6 address or port number is configured for a DNS listener.

Views

DNS listener view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address: Specifies an IPv6 address, which cannot be a loopback address, IPv6 multicast address, link-local address, or all-zero address.

port *port-number*: Specifies a port number in the range of 1 to 65535. The default is 53.

Usage guidelines

A DNS listener can be configured with only one IPv6 address. A DNS listener without an IPv6 address configured does not process IPv6 DNS requests.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure the IPv6 address and port number for DNS listener **ct-listener** as 1001::1 and 64.

```
<Sysname> system-view
[Sysname] loadbalance dns-listener ct-listener
[Sysname-lb-dl-ct-listener] ipv6 address 1001::1 port 64
```

Related commands

display loadbalance dns-listener

ipv6 address (DNS server view)

Use **ipv6 address** to configure an IPv6 address for a DNS server.

Use **undo ipv6 address** to restore the default.

Syntax

ipv6 address *ipv6-address*

undo ipv6 address

Default

No IPv6 address is configured for a DNS server.

Views

DNS server view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address: Specifies an IPv6 address, which cannot be a loopback address, IPv6 multicast address, link-local address, or all-zero address.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure the IPv6 address for DNS server **ds1** as 1001::1.

```
<Sysname> system-view
[Sysname] loadbalance dns-server ds1
[Sysname-lb-ds-ds1] ipv6 address 1001::1
```

ipv6 address (ISP view)

Use **ipv6 address** to configure an IPv6 address for an ISP.

Use **undo ipv6 address** to restore the default.

Syntax

ipv6 address *ipv6-address prefix-length*

undo ipv6 address *ipv6-address prefix-length*

Default

No IPv6 address is configured for an ISP.

Views

ISP view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address: Specifies an IPv6 address.

prefix-length: Specifies the prefix length for the IPv6 address, in the range of 1 to 128.

Examples

Configure the IPv6 address for the ISP **isp1** as 200::1.

```
<Sysname> system-view
[Sysname] loadbalance isp name isp1
[Sysname-lbisp-isp1] ipv6 address 200::1 100
```

ipv6 address (real server view)

Use **ipv6 address** to configure an IPv6 address for a real server.

Use **undo ipv6 address** to restore the default.

Syntax

ipv6 address *ipv6-address*

undo ipv6 address

Default

No IPv6 address is configured for a real server.

Views

Real server view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address: Specifies an IPv6 address, which cannot be a loopback address, IPv6 multicast address, link-local address, or all-zero address.

Examples

Configure the IPv6 address for the real server **rs** as 1001::1.

```
<Sysname> system-view
[Sysname] real-server rs
[Sysname-rserver-rs] ipv6 address 1001::1
```

ipv6 address (transparent DNS proxy view)

Use **ipv6 address** to configure an IPv6 address for a transparent DNS proxy.

Use **undo ipv6 address** to restore the default.

Syntax

ipv6 address *ipv6-address* [*prefix-length*]

undo ipv6 address

Default

No IPv6 address is configured for a transparent DNS proxy.

Views

Transparent DNS proxy view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address: Specifies an IPv6 address, which cannot be a loopback address, IPv6 multicast address, link-local address, or all-zero address (If the prefix length is 0, you can specify the all-zero address.).

prefix-length: Specifies a prefix length for the IPv6 address, in the range of 0 to 128.

Usage guidelines

A transparent DNS proxy processes a DNS request only when the destination IP address and port number of the DNS request match those of the transparent DNS proxy.

If server load balancing is configured, configure different IP addresses and port numbers for the transparent DNS proxy and the virtual server of the UDP type.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure the IPv6 address for transparent DNS proxy **dns-proxy1** as 1::2:3/112.

```
<Sysname> system-view
[Sysname] loadbalance dns-proxy dns-proxy1
[Sysname-lb-dp-udp-dns-proxy1] ipv6 address 1::2:3 112
```

ipv6 prefix

Use **ipv6 prefix** to configure the prefix length for IPv6 proximity entries.

Use **undo ipv6 prefix** to restore the default.

Syntax

ipv6 prefix *prefix-length*

undo ipv6 prefix

Default

The prefix length for IPv6 proximity entries is 96.

Views

Proximity view

Predefined user roles

network-admin

context-admin

Parameters

prefix-length: Specifies the prefix length for IPv6 proximity entries, in the range of 1 to 128.

Examples

Specify the prefix length for IPv6 proximity entries as 64.

```
<Sysname> system-view
[Sysname] loadbalance proximity
[Sysname-lb-proximity] ipv6 prefix 64
```

ipv6 range

Use **ipv6 range** to add an IPv6 address range to a SNAT address pool.

Use **undo ipv6 range** to remove an IPv6 address range from a SNAT address pool.

Syntax

Default

An SNAT address pool does not contain IPv6 address ranges.

Views

SNAT address pool view

Predefined user roles

network-admin

context-admin

Parameters

start *start-ipv6-address*: Specifies the start IPv6 address.

end *end-ipv6-address*: Specifies the end IPv6 address, which must be greater than or equal to the start IPv6 address.

Usage guidelines

You can execute this command multiple times to add multiple IPv6 address ranges to a SNAT address pool. Each address range can have a maximum of 10000 IPv6 addresses. No overlapping IPv6 addresses are allowed in the same SNAT address pool or different SNAT address pools.

If the SNAT address pool has an IP address on the same network as the IP address of the device interface connected to the server, you must execute the **arp-nd interface** command for the SNAT address pool. In the situation does not exist, you do not need to execute the **arp-nd interface** command.

Examples

Add IPv6 address range 1001::1 to 1001::100 to the SNAT address pool **lbsp**.

```
<Sysname> system-view
[Sysname] loadbalance snat-pool lbsp
[Sysname-lbsnat-pool-lbsp] ipv6 range start 1001::1 end 1001::100
```

Related commands

arp-nd interface (SNAT address pool view)

loadbalance snat-pool

ipv6 source prefix

Use **ipv6 source prefix** to specify the IPv6 prefix length for connection reuse.

Use **undo ipv6 source prefix** to restore the default.

Syntax

ipv6 source prefix *prefix-length*

undo ipv6 source prefix

Default

Client IPv6 addresses with a prefix length of 0 can reuse connections.

Views

OneConnect parameter profile view

MySQL parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

prefix-length: Specifies the prefix length in the range of 0 to 128.

Usage guidelines

This command limits the network segment of clients that can reuse connections between the LB device and servers. If the client that initiates a connection request is in the same network segment as the idle TCP connection, the idle TCP connection is reused. If the client does not match this requirement, a new TCP connection is established.

Examples

In OneConnect parameter profile **ocp**, set the prefix length for connection reuse to 24.

```
<Sysname> system-view
[Sysname] parameter-profile ocp type oneconnect
[Sysname-para-oneconnect-ocp] ipv6 source prefix 24
```

isp

Use **isp** to add an ISP to a region.

Use **undo isp** to delete an ISP from a region.

Syntax

isp *isp-name*

undo isp *isp-name*

Default

A region does not contain any ISPs.

Views

Region view

Predefined user roles

network-admin

context-admin

Parameters

isp-name: Specifies an ISP by its name, a case-insensitive string of 1 to 63 characters.

Examples

Add the ISP **isp-ct** to the region **region-ct**.

```
<Sysname> system-view
[Sysname] loadbalance region region-ct
[Sysname-lb-region-region-ct] isp isp-ct
```

Related commands

loadbalance region

keepalive idle-timeout

Use **keepalive idle-timeout** to set the idle timeout time for sending keepalive packets.

Use **undo keepalive idle-timeout** to restore the default.

Syntax

keepalive idle-timeout *timeout-value*

undo keepalive idle-timeout

Default

The idle timeout time for sending keepalive packets is 1800 seconds.

Views

TCP parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

timeout-value: Specifies the idle timeout time for sending keepalive packets, in the range of 1 to 65535 seconds.

Examples

Set the timeout time for sending keepalive packets to 5 seconds in the TCP parameter profile **profile**.

```
<Sysname> system-view
[Sysname] parameter-profile profile type tcp
[Sysname-para-tcp-profile] keepalive idle-timeout 5
```

Related commands

display parameter-profile

keepalive retransmission interval

Use **keepalive retransmission interval** to set the retransmission interval and retransmission times for keepalive packets.

Use **undo keepalive retransmission interval** to restore the default.

Syntax

keepalive retransmission interval *interval* **count** *count*

undo keepalive retransmission

Default

The retransmission interval is 10 seconds, and the retransmission times is 3.

Views

TCP parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies the retransmission interval for keepalive packets, in the range of 1 to 65535 seconds.

count: Specifies the retransmission times for keepalive packets, in the range of 1 to 65535.

Examples

Set the retransmission interval and retransmission times for keepalive packets to 5 seconds and 10, respectively, in the TCP parameter profile **profile**.

```
<Sysname> system-view
[Sysname] parameter-profile profile type tcp
[Sysname-para-tcp-profile] keepalive retransmission interval 5 count 10
```

Related commands

display parameter-profile

lb-limit-policy

Use **lb-limit-policy** to apply an LB connection limit policy to a virtual server.

Use **undo lb-limit-policy** to restore the default.

Syntax

lb-limit-policy *policy-name*

undo lb-limit-policy

Default

No LB connection limit policies are applied to a virtual server.

Views

Virtual server view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies an LB connection limit policy by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

Use this command to implement rate limit for user traffic.

This command takes effect only on new sessions and does not take effect on existing sessions.

Examples

Apply the LB connection limit policy **llp** to the HTTP-type virtual server **vs**.

```
<Sysname> system-view
[Sysname] virtual-server vs type http
[Sysname-vs-http-vs]lb-limit-policy llp
```

Related commands

loadbalance limit-policy

lb-policy (transparent DNS proxy view)

Use **lb-policy** to specify an LB policy to be referenced by a transparent DNS proxy.

Use **undo lb-policy** to restore the default.

Syntax

lb-policy *policy-name*

undo lb-policy

Default

No LB policy is referenced by a transparent DNS proxy.

Views

Transparent DNS proxy view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies an LB policy by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

By referencing an LB policy, a transparent DNS proxy implements load balancing for matching packets based on the packet contents.

A transparent DNS proxy can reference only a DNS policy template.

Examples

Specify the LB policy **dns-policy1** to be referenced by transparent DNS proxy **dns-proxy1**.

```
<Sysname> system-view
[Sysname] loadbalance dns-proxy dns-proxy1
[Sysname-lb-dp-udp-dns-proxy1] lb-policy dns-policy1
```

lb-policy (virtual server view)

Use **lb-policy** to specify an LB policy to be referenced by the specified virtual server.

Use **undo lb-policy** to restore the default.

Syntax

lb-policy *policy-name*

undo lb-policy

Default

No LB policy is referenced by a virtual server.

Views

Virtual server view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies an LB policy by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

By referencing an LB policy, the virtual server implements load balancing for matching packets based on the packet contents.

A virtual server can reference the policy template of the specified type. For example, a virtual server of the fast HTTP or HTTP type can reference a policy template of the generic type or HTTP type. A virtual server of the IP, SIP, TCP, or UDP type can reference a policy template of the generic type only.

Examples

Specify the LB policy **lbp1** to be referenced by the IP-type virtual server **vs3**.

```
<Sysname> system-view
[Sysname] virtual-server vs3 type ip
[Sysname-vs-ip-vs3] lb-policy lbp1
```

limit

Use **limit** to configure an LB connection limit rule.

Use **undo limit** to delete an LB connection limit rule.

Syntax

limit *limit-id* **acl** [**ipv6**] { *acl-number* | **name** *acl-name* } [**per-destination** | **per-service** | **per-source**] * **amount** *max-amount min-amount*

undo limit *limit-id*

Default

No rules are configured for an LB connection limit policy.

Views

LB connection limit policy view

Predefined user roles

network-admin

context-admin

Parameters

limit-id: Specifies an LB connection limit rule ID. The value range for this argument is 1 to 65535.

acl: Specifies an ACL to limit user connections of a specified user range.

ipv6: Specifies an IPv6 ACL. If you do not specify this keyword, the command uses an IPv4 ACL.

acl-number: Specifies the ACL number in the range of 2000 to 3999.

name *acl-name*: Specifies an ACL by its name.

per-destination: Limits user connections by destination IP address.

per-service: Limits user connections by service. Services are classified by transport layer protocol and service port number.

per-source: Limits user connections by source IP address.

max-amount: Specifies the upper limit of connections, in the range of 1 to 4294967295. When the number of connections in a specified range or for a certain type reaches the upper limit, the device does not accept new connection requests.

min-amount: Specifies the lower limit of connections, in the range of 1 to 4294967295. The *min-amount* must be equal to or smaller than the *max-amount*. The device accepts new connection requests only when the number of connections drops below the lower limit.

Usage guidelines

An LB connection limit policy can have multiple rules. You can specify an ACL, a type, and the upper and lower limits for each rule. You can specify one or more of the **per-destination**, **per-service**, and **per-source** keywords for the command. For example, you can specify both the **per-destination** and **per-source** keywords to limit user connections by destination address and source address of packets.

You must specify a different ACL for each rule in an LB connection limit policy.

If the **per-destination**, **per-service**, and **per-source** keywords are not specified, the command limits all user connections matching the specified ACL.

The rules in an LB connection limit policy are matched in ascending order of the rule IDs until a match is found.

When the specified ACL changes, the device uses a new LB connection limit policy to process existing connections again.

Examples

Configure rule **1** for the LB connection limit policy **1**. Use ACL 3000 to permit user connections sourced from the network 192.168.0.0/24, and set the upper and lower limits to 2000 and 1800 for the user connections by source and destination addresses.

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule permit ip source 192.168.0.0 0.0.0.255
[Sysname-acl-ipv4-adv-3000] quit
[Sysname] loadbalance limit-policy 1
[Sysname-lb-limit-policy-1] limit 1 acl 3000 per-destination per-source amount 2000 1800
```

link (DNS server view)

Use **link** to associate a link with a DNS server.

Use **undo link** to restore the default.

Syntax

link *link-name*

undo link

Default

No link is associated with a DNS server.

Views

DNS server view

Predefined user roles

network-admin

context-admin

Parameters

link-name: Specifies a link by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

A DNS server can be associated with only one link. A link can be associated with multiple DNS servers.

Examples

Associate link **link1** with DNS server **ds1**.

```
<Sysname> system-view
[Sysname] loadbalance dns-server ds1
[Sysname-lb-ds-ds1] link link1
```

link (link group view)

Use **link** to create a link group member and enter its view, or enter the view of an existing link group member.

Use **undo link** to delete a link group member.

Syntax

link *link-name*

undo link *link-name*

Default

No link group members exist.

Views

Link group view

Predefined user roles

network-admin

context-admin

Parameters

link-name: Specifies a link group member name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

You can use one of the following methods to add a member to a link group:

- Use the **link** command in link group view. NSFOCUS recommends using this method.
- Use the **link-group** command in link view.

You cannot use both methods to add a member with the same link name to a link group.

Examples

Add link group member **lk1** and enter link group member view.

```
<Sysname> system-view
[Sysname] loadbalance link-group lg
[Sysname-lb-lgroup-lg] link lk1
[Sysname-lb-lgroup-lg-#member#-lk1]
```

Related commands

link-group (link view)

link-group (LB action view)

Use **link-group** to specify the primary link group.

Use **undo link-group** to restore the default.

Syntax

link-group *link-group-name* [**backup** *backup-link-group-name*] [**sticky** *sticky-name*]

undo link-group

Default

No primary link group is specified.

Views

LB action view

Predefined user roles

network-admin

context-admin

Parameters

link-group-name: Specifies a primary link group name, a case-insensitive string of 1 to 63 characters.

backup *backup-link-group-name*: Specifies a backup link group name, a case-insensitive string of 1 to 63 characters.

sticky *sticky-name*: Specifies the name of the sticky group corresponding to the link group. It is a case-insensitive string of 1 to 63 characters.

Usage guidelines

The **link-group** and **forward all** commands are mutually exclusive. If you configure one command, the other command (if configured) is automatically cancelled.

When the primary link group is available (contains links), packets are forwarded through the primary link group. When the primary link group is not available, packets are forwarded through the backup link group.

Examples

Specify the primary link group **lg**, the backup link group **lgb**, and the sticky group **sg1** for the link-generic LB action **lba1**.

```
<Sysname> system-view
[Sysname] loadbalance action lba1 type link-generic
[Sysname-lba-link-generic-lba1] server-farm sf backup sfb sticky sg1
```

Related commands

forward all

link-group (link view)

Use **link-group** to specify a link group for a link.

Use **undo link-group** to restore the default.

Syntax

link-group *link-group-name*

undo link-group

Default

A link does not belong to any link group.

Views

Link view

Predefined user roles

network-admin

context-admin

Parameters

link-group-name: Specifies a link group name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

The device selects the best link from the matching link group to perform link load balancing.

Examples

Specify the link group **lkg1** for the link **lk1**.

```
<Sysname> system-view
[Sysname] loadbalance link lk1
[Sysname-lb-link-lk1] link-group lkg1
```

loadbalance action

Use **loadbalance action** to create an LB action and enter its view, or enter the view of an existing LB action.

Use **undo loadbalance action** to delete the specified LB action.

Syntax

loadbalance action *action-name* [**type** { **dns** | **generic** | **http** | **link-generic** | **radius** }]

undo loadbalance action *action-name*

Default

No LB actions exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

action-name: Specifies the LB action name, a case-insensitive string of 1 to 63 characters.

type { **dns** | **generic** | **http** | **link-generic** | **radius** }: Specifies an LB action type.

- **dns**: DNS load balancing action.

- **generic**: Generic server load balancing action.
- **http**: HTTP load balancing action.
- **link-generic**: Link load balancing action.
- **radius**: RADIUS load balancing action.

Usage guidelines

When you create an LB action, you must specify the LB action type. You can enter an existing LB action view without entering the type of the LB action.

You can create generic, HTTP, and RADIUS LB actions only if the device has licenses installed. For information about licensing, see license management in *Fundamentals Configuration Guide*.

Examples

Create the LB action **lba1** with the **generic** type, and enter LB action view.

```
<Sysname> system-view
[Sysname] loadbalance action lba1 type generic
[Sysname-lba-generic-lba1]
```

loadbalance alg

Use **loadbalance alg** to enable ALG for the specified protocols.

Use **undo loadbalance alg** to disable ALG for the specified protocols.

Syntax

loadbalance alg { **dns** | **ftp** | **h323** | **icmp-error** | **ils** | **mgcp** | **nbt** | **pptp** | **rsh** | **rtsp** | **sccp** | **sip** | **sqlnet** | **tftp** | **xdmcp** }

undo loadbalance alg { **dns** | **ftp** | **h323** | **icmp-error** | **ils** | **mgcp** | **nbt** | **pptp** | **rsh** | **rtsp** | **sccp** | **sip** | **sqlnet** | **tftp** | **xdmcp** }

Default

ALG is enabled for the DNS, FTP, PPTP, and RTSP protocols and ICMP error packets.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

dns: Specifies the DNS protocol.

ftp: Specifies the FTP protocol.

h323: Specifies the H.323 protocol.

icmp-error: Specifies the ICMP error packets.

ils: Specifies the Internet Locator Service (ILS) protocol.

mgcp: Specifies the Media Gateway Control Protocol (MGCP).

nbt: Specifies the NetBIOS over TCP/IP (NBT) protocol.

pptp: Specifies the Point-to-Point Tunneling Protocol (PPTP).

rsh: Specifies the Remote Shell (RSH) protocol.

rtsp: Specifies the Real Time Streaming Protocol (RTSP).

sccp: Specifies the Skinny Client Control Protocol (SCCP).

sip: Specifies the Session Initiation Protocol (SIP).

sqlnet: Specifies the SQLNET protocol.

tftp: Specifies the TFTP protocol.

xdmcp: Specifies the X Display Manager Control Protocol (XDMCP).

Usage guidelines

The ALG feature distributes parent and child sessions to the same link.

SIP fragmentation packets do not suppport ALG.

Examples

Enable ALG for TFTP.

```
<Sysname> system-view
[Sysname] loadbalance alg tftp
```

loadbalance alg all-enable

Use **loadbalance alg all-enable** to enable ALG for all protocols.

Use **loadbalance alg all-disable** to disable ALG for all protocols.

Syntax

loadbalance alg all-enable

loadbalance alg all-disable

Default

ALG is enabled for the DNS, FTP, PPTP, and RTSP protocols and ICMP error packets.

Views

System view

Predefined user roles

network-admin

context-admin

Examples

Enable ALG for all protocols.

```
<Sysname> system-view
[Sysname] loadbalance alg all-enable
```

loadbalance class

Use **loadbalance class** to create an LB class and enter its view, or enter the view of an existing LB class.

Use **undo loadbalance class** to delete the specified LB class.

Syntax

loadbalance class *class-name* [**type** { **dns** | **generic** | **http** | **link-generic** | **mysql** | **radius** } [**match-all** | **match-any**]]

undo loadbalance class *class-name*

Default

No LB classes exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

class-name: Specifies the LB class name, a case-insensitive string of 1 to 63 characters.

type { **dns** | **generic** | **http** | **link-generic** | **mysql** | **radius** }: Specifies an LB class type.

- **dns**: DNS load balancing class.
- **generic**: Generic server load balancing class.
- **http**: HTTP load balancing class.
- **link-generic**: Link load balancing class.
- **mysql**: MySQL load balancing class.
- **radius**: RADIUS load balancing class.

[**match-all** | **match-any**]: Requires matching all rules or any rule of the LB class. **match-all** is the default match mode.

Usage guidelines

When you create an LB class, you must specify an LB class type. You can enter an existing LB class view without entering the type of the LB class.

You can create generic, HTTP, MySQL, and RADIUS LB classes only if the device has licenses installed. For information about licensing, see license management in *Fundamentals Configuration Guide*.

Examples

Create the LB class **lbc1** with the generic type, and enter LB class view.

```
<Sysname> system-view
[Sysname] loadbalance class lbc1 type generic
[Sysname-lbc-generic-lbc1]
```

loadbalance dns-cache aging-time

Use **loadbalance dns-cache aging-time** to set the aging time for DNS cache entries.

Use **undo loadbalance dns-cache aging-time** to restore the default.

Syntax

loadbalance dns-cache aging-time *aging-time*

undo loadbalance dns-cache aging-time

Default

The aging time for DNS cache entries is 60 minutes.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

aging-time: Specifies the aging time for DNS cache entries, in the range of 1 to 1440 minutes.

Examples

Set the aging time for DNS cache entries to 100 minutes.

```
<Sysname> system-view
[Sysname] loadbalance dns-cache aging-time 100
```

loadbalance dns-listener

Use **loadbalance dns-listener** to create a DNS listener and enter its view, or enter the view of an existing DNS listener.

Use **undo loadbalance dns-listener** to delete a DNS listener.

Syntax

loadbalance dns-listener *dns-listener-name*

undo loadbalance dns-listener *dns-listener-name*

Default

No DNS listeners exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

dns-listener-name: Specifies the DNS listener name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

A DNS listener listens for DNS requests on the LB device.

Examples

Create the DNS listener **ct-listener**, and enter DNS listener view.

```
<Sysname> system-view
[Sysname] loadbalance dns-listener ct-listener
[Sysname-lb-dl-ct-listener]
```

loadbalance dns-map

Use **loadbalance dns-map** to create a DNS mapping and enter its view, or enter the view of an existing DNS mapping.

Use **undo loadbalance dns-map** to delete a DNS mapping.

Syntax

loadbalance dns-map *dns-map-name*

undo loadbalance dns-map *dns-map-name*

Default

No DNS mappings exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

dns-map-name: Specifies the DNS mapping name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

A DNS mapping maps a domain name to the IP address of a virtual server pool. A domain name can be mapped to only one virtual server pool.

Examples

Create the DNS mapping **dm1**, and enter DNS mapping view.

```
<Sysname> system-view
[Sysname] loadbalance dns-map dm1
[Sysname-lb-dm-dm1]
```

loadbalance dns-proxy

Use **loadbalance dns-proxy** to create a transparent DNS proxy and enter its view, or enter the view of an existing transparent DNS proxy.

Use **undo loadbalance dns-proxy** to delete a transparent DNS proxy.

Syntax

loadbalance dns-proxy *dns-proxy-name* **type udp**

undo loadbalance dns-proxy *dns-proxy-name*

Default

No transparent DNS proxies exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

dns-proxy-name: Specifies the transparent DNS proxy name, a case-insensitive string of 1 to 63 characters.

type udp: Specifies the transparent DNS proxy type as UDP.

Examples

Create the UDP transparent DNS proxy **dns-proxy1**, and enter UDP transparent DNS proxy view.

```
<Sysname> system-view
[Sysname] loadbalance dns-proxy dns-proxy1 type udp
[Sysname-lb-dp-udp-dns-proxy1]
```

Related commands

display loadbalance dns-proxy

loadbalance dns-server

Use **loadbalance dns-server** to create a DNS server and enter its view, or enter the view of an existing DNS server.

Use **undo loadbalance dns-server** to delete a DNS server.

Syntax

loadbalance dns-server *dns-server-name*

undo loadbalance dns-server *dns-server-name*

Default

No DNS servers exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

dns-server-name: Specifies the DNS server name, a case-insensitive string of 1 to 63 characters.

Examples

Create the DNS server **ds1**, and enter DNS server view.

```
<Sysname> system-view
[Sysname] loadbalance dns-server ds1
[Sysname-lb-ds-ds1]
```

loadbalance dns-server-pool

Use **loadbalance dns-server-pool** to create a DNS server pool and enter its view, or enter the view of an existing DNS server pool.

Use **undo loadbalance dns-server-pool** to delete a DNS server pool.

Syntax

loadbalance dns-server-pool *pool-name*

undo loadbalance dns-server-pool *pool-name*

Default

No DNS server pools exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

pool-name: Specifies the DNS server pool name, a case-insensitive string of 1 to 63 characters.

Examples

Create the DNS server pool **dns-pool1**, and enter DNS server pool view.

```
<Sysname> system-view
[Sysname] loadbalance dns-server-pool dns-pool1
[Sysname-lb-dspool-dns-pool1]
```

loadbalance isp auto-update enable

Use **loadbalance isp auto-update enable** to enable ISP auto update.

Use **undo loadbalance isp auto-update enable** to disable ISP auto update.

Syntax

loadbalance isp auto-update enable

undo loadbalance isp auto-update enable

Default

ISP auto update is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

With ISP auto update enabled, the device regularly queries IP address information from the whois server according to the whois maintainer object of the ISP.

Examples

Enable ISP auto update.

```
<Sysname> system-view
[Sysname] loadbalance isp auto-update enable
```

Related commands

loadbalance isp auto-update frequency
loadbalance isp auto-update whois-server

loadbalance isp auto-update frequency

Use **loadbalance isp auto-update frequency** to configure the ISP auto update frequency.

Use **undo loadbalance isp auto-update frequency** to restore the default.

Syntax

loadbalance isp auto-update frequency { **per-day** | **per-week** | **per-month** }

undo loadbalance isp auto-update frequency

Default

The ISP auto update is performed once per week.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

per-day: Updates ISP address information once per day.

per-week: Updates ISP address information once per week.

per-month: Updates ISP address information once per month.

Usage guidelines

The specific update time is about 04:00:00 a.m. For the first auto update, the specific update time is 04:00:00 a.m on the next day.

Examples

Configure the ISP auto update frequency as per day.

```
<Sysname> system-view
[Sysname] loadbalance isp auto-update frequency per-day
```

Related commands

loadbalance isp auto-update enable

loadbalance isp auto-update whois-server

Use **loadbalance isp auto-update whois-server** to specify the whois server to be queried for ISP auto update.

Use **undo loadbalance isp auto-update whois-server** to restore the default.

Syntax

loadbalance isp auto-update whois-server { **domain** *domain-name* | **ip** *ip-address* }

undo loadbalance isp auto-update whois-server

Default

No whois server is specified for ISP auto update.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

domain *domain-name*: Specify a whois server by its domain name, a case-insensitive, dot-separated string of 1 to 253 characters (for example, example.com). Each dot-separated part in the domain name can contain a maximum of 63 characters. The domain name can contain letters, digits, hyphens (-), underscores (_), and periods (.).

ip *ip-address*: Specify a whois server by its IPv4 address.

Examples

Specify the whois server with IP address 20.1.1.1 for ISP auto update.

```
<Sysname> system-view
[Sysname] loadbalance isp auto-update whois-server ip 20.1.1.1
```

loadbalance isp file

Use **loadbalance isp file** to import an ISP file.

Use **undo loadbalance isp file** to delete an ISP file.

Syntax

loadbalance isp file *isp-file-name*

undo loadbalance isp file

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

isp-file-name: Specifies the ISP file name, a case-insensitive string of 1 to 255 characters.

Usage guidelines

The system keeps the imported information intact when detecting the following problems:

- The file does not exist.
- The file name is invalid.
- File decryption occurs.

If the system quits the import operation because of IP address parsing failure, the system performs the following operations:

- Clears the most recently imported information.
- Saves the information imported this time.

You cannot delete the imported ISP and its IPv4 or IPv6 address. If the manually configured and imported ISP information overlaps, you can delete the manually configured ISP information.

To perform an active/standby MPU switchover, make sure the standby MPU has the same ISP file as the active MPU.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Import the ISP file **isp2**.

```
<Sysname> system-view
[Sysname] loadbalance isp file isp2
```

loadbalance isp name

Use **loadbalance isp name** to create an ISP and enter its view, or enter the view of an existing ISP.

Use **undo loadbalance isp name** to delete the specified ISP.

Syntax

loadbalance isp name *isp-name*

undo loadbalance isp name *isp-name*

Default

No ISPs exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

isp-name: Specifies the ISP name, a case-insensitive string of 1 to 63 characters.

Examples

Create ISP **isp1**, and enter ISP view.

```
<Sysname> system-view
[Sysname] loadbalance isp name isp1
[Sysname-lbisp-isp1]
```

loadbalance limit-policy

Use **loadbalance limit-policy** to create an LB connection limit policy and enter its view, or enter the view of an existing LB connection limit policy.

Use **undo loadbalance limit-policy** to delete an LB connection limit policy.

Syntax

loadbalance limit-policy *policy-name*

undo loadbalance limit-policy *policy-name*

Default

No LB connection limit policies exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies the LB connection limit policy name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

Using an LB connection limit policy can limit the number of connections on the device. It helps prevent a large number of connections from consuming too many device system resources and server resources. In this way, internal network resources (hosts or servers) are protected, and device system resources can be used more appropriately.

Examples

Create the LB connection limit policy **llp**, and enter LB connection limit policy view.

```
<Sysname> system-view
[Sysname] loadbalance limit-policy llp
[Sysname-lb-limit-policy-llp]
```

loadbalance link

Use **loadbalance link** to create an LB link and enter its view, or enter the view of an existing LB link.

Use **undo loadbalance link** to delete an LB link.

Syntax

loadbalance link *link-name*

undo loadbalance link *link-name*

Default

No LB links exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

link-name: Specifies the LB link name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

Each physical link connected to the external network corresponds to an LB link.

Examples

Create the LB link **lk1**, and enter LB link view.

```
<Sysname> system-view
[Sysname] loadbalance link lk1
[Sysname-lb-link-lk1]
```

loadbalance link-group

Use **loadbalance link-group** to create a link group and enter its view, or enter the view of an existing link group.

Use **undo loadbalance link-group** to delete a link group.

Syntax

loadbalance link-group *link-group-name*

undo loadbalance link-group *link-group-name*

Default

No link groups exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

link-group-name: Specifies the link group name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

You can add links that contain similar functions to a link group to facilitate management.

Examples

Create the link group **lg**, and enter link group view.

```
<Sysname> system-view
[Sysname] loadbalance link-group lg
[Sysname-lb-lgroup-lg]
```

loadbalance local-dns-server parse-fail-record type

Use **loadbalance local-dns-server parse-fail-record type** to configure the types of DNS request parse failures to be recorded.

Use **undo loadbalance local-dns-server parse-fail-record type** to remove the configuration.

Syntax

loadbalance local-dns-server parse-fail-record type { **a** | **aaaa** | **all-disable** | **all-enable** | **cname** | **mx** | **ns** | **ptr** | **soa** | **srv** | **txt** }

undo loadbalance local-dns-server parse-fail-record type { **a** | **aaaa** | **cname** | **mx** | **ns** | **ptr** | **soa** | **srv** | **txt** }

Default

All types of DNS request parse failures are recorded.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

a: Specifies the A (host address) type.

aaaa: Specifies the AAAA type.

all-disable: Specifies no type.

all-enable: Specifies all types.

cname: Specifies the canonical name type.

mx: Specifies the mail exchanger type.

ns: Specifies the name server type.

ptr: Specifies the pointer type.

soa: Specifies the start of authority type.

srv: Specifies the service type.

txt: Specifies the text type.

Examples

Configure the A-type DNS request parse failures to be recorded.

```
<Sysname> system-view
[Sysname] loadbalance local-dns-server parse-fail-record type a
```

loadbalance local-dns-server parse-fail-record max-number

Use **loadbalance local-dns-server parse-fail-record max-number** to set the maximum number of DNS request parse failures to be recorded.

Use **undo loadbalance local-dns-server parse-fail-record max-number** to restore the default.

Syntax

loadbalance local-dns-server parse-fail-record max-number *max-number*

undo loadbalance local-dns-server parse-fail-record max-number

Default

The maximum number of DNS request parse failures to be recorded is 10000.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

max-number: Specifies the maximum number of DNS request parse failures to be recorded, in the range of 0 to 4294967295.

Examples

Set the maximum number of DNS request parse failures to be recorded to 600.

```
<Sysname> system-view
[Sysname] loadbalance local-dns-server parse-fail-record max-number 600
```

loadbalance local-dns-server schedule-test ip

Use **loadbalance local-dns-server schedule-test ip** to perform an IPv4 inbound link load balancing test for DNS resolution.

Syntax

loadbalance local-dns-server schedule-test ip [**vpn-instance** *vpn-instance-name*] **destination** *destination-address* [**destination-port** *destination-port*] **source** *source-address* **source-port** *source-port* **type** { { **a** | **aaaa** | **cname** | **mx** | **ns** | **soa** | **srv** | **txt** } **domain** *domain-name* | **ptr ip address** { *ipv4-address* | *ipv6-address* } } [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command is executed for the public network.

destination *destination-address*: Specifies the destination IPv4 address, the IPv4 address of the DNS listener.

destination-port *destination-port*: Specifies the destination port number in the range of 0 to 65535. The default is 53.

source *source-address*: Specifies the source IPv4 address.

source-port *source-port*: Specifies the source port number in the range of 0 to 65535.

type: Specifies a DNS request type.

a: Specifies the A (host address) type.

aaaa: Specifies the AAAA type.

cname: Specifies the canonical name type.

mx: Specifies the mail exchanger type.

ns: Specifies the name server type.

soa: Specifies the start of authority type.

srv: Specifies the service type.

txt: Specifies the text type.

domain *domain-name*: Specifies the domain name to be resolved, a case-insensitive, dot-separated string of 1 to 254 characters for an absolute domain name or 1 to 253 characters for a relative domain name. Each dot-separated label in the domain name can contain a maximum of 63 characters.

ptr: Specifies the pointer type, which is used to resolve an IP address into a domain name.

ip address { *ipv4-address* | *ipv6-address* }: Specifies the IP address to be resolved into a domain name.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command tests all member devices.

Examples

Perform an IPv4 inbound link load balancing test on A-type DNS requests.

```
<Sysname> loadbalance local-dns-server schedule-test ip destination 7.7.7.7
destination-port 53 source 2.2.2.2 source-port 5 type a domain www.aaa.com
Slot 0:
    Matched DNS listener: dl2
    Matched zone: --
    Matched DNS mapping: dm2
    Matched virtual server pool: vsp2
    Preferred scheduling algorithm: Round robin
    Alternative scheduling algorithm: --
    Fallback scheduling algorithm: --
    Preferred algorithm failure cause: --
    Alternative algorithm failure cause: --
    Fallback algorithm failure cause: --
    Selected virtual server: vs2
    Response type: Send response
    Failure cause: --
```

Perform an IPv4 inbound link load balancing test on MX-type DNS requests.

```
<Sysname> loadbalance local-dns-server schedule-test ip destination 7.7.7.7
destination-port 53 source 2.2.2.2 source-port 5 type mx domain www.aaa.com
Slot 0:
    Matched DNS listener: dl2
    Matched zone: nsfocus.com.cn
    Response type: Send response
    Failure cause: --
```

Perform an IPv4 inbound link load balancing test on PTR-type DNS requests.

```
<Sysname> loadbalance local-dns-server schedule-test ip destination 7.7.7.7
destination-port 53 source 2.2.2.2 source-port 5 type ptr ip address 1.2.3.4
Slot 0:
    Matched DNS listener: dl2
    Matched zone: 1.2.3.0/24
    Response type: Send response
    Failure cause: --
```

Table 42 Command output

Field	Description
Matched zone	Matched DNS zone. • For a PTR-type DNS request, this field displays the IP address of the DNS reverse zone. • For a DNS request other than the PTR type, this field displays the domain name of the DNS forward zone.
Preferred scheduling algorithm	Preferred scheduling algorithm: • Round robin. • Random. • Least connection.

Field	Description
	• Topology. • Proximity. • Bandwidth. • Inbound bandwidth. • Outbound bandwidth. • Max bandwidth. • Max inbound bandwidth. • Max outbound bandwidth. • Hash address source IP. • Hash address destination IP. • Hash address source IP-port.
Alternative scheduling algorithm	Alternative scheduling algorithm: • Round robin. • Random. • Least connection. • Topology. • Proximity. • Bandwidth. • Inbound bandwidth. • Outbound bandwidth. • Max bandwidth. • Max inbound bandwidth. • Max outbound bandwidth. • Hash address source IP. • Hash address destination IP. • Hash address source IP-port.
Fallback scheduling algorithm	Backup scheduling algorithm: • Round robin. • Random. • Least connection. • Topology. • Proximity. • Bandwidth. • Inbound bandwidth. • Outbound bandwidth. • Max bandwidth. • Max inbound bandwidth. • Max outbound bandwidth. • Hash address source IP. • Hash address destination IP. • Hash address source IP-port.
Preferred algorithm failure cause	Preferred algorithm failure cause: • **--**—Scheduling succeeded. • No scheduling content. • **Scheduling failed**—The scheduling content exists, but scheduling failed. • No matched virtual server member.
Alternative algorithm failure cause	Alternative algorithm failure cause: • **--**—Scheduling succeeded.

Field	Description
	• No scheduling content. • **Scheduling failed**—The scheduling content exists, but scheduling failed. • No matched virtual server member.
Fallback algorithm failure cause	Backup algorithm failure cause: • **--**—Scheduling succeeded. • No scheduling content. • **Scheduling failed**—The scheduling content exists, but scheduling failed. • No matched virtual server member.
Response type	Response type for a DNS request: • **Send response**—Replies with a DNS response. • **Send reject**—Replies with a DNS reject. • **No response**—Does not respond to the DNS request.
Failure cause	Failure cause for DNS request parsing: • **--**—Parsing succeeded. • No matched DNS listener. • No matched DNS mapping. • No matched virtual server pool. • No matched DNS zone. • Failed to get buffer. • No matched record. • No enough memory resource. • Failed to parse domain. • Failed to find DNS listener by ID. • No scheduling content. • **Scheduling failed**—The scheduling content exists, but scheduling failed. • No matched virtual server member.

loadbalance local-dns-server schedule-test ipv6

Use **loadbalance local-dns-server schedule-test ipv6** to perform an IPv6 inbound link load balancing test for DNS resolution.

Syntax

loadbalance local-dns-server schedule-test ipv6 [**vpn-instance** *vpn-instance-name*] **destination** *destination-address* [**destination-port** *destination-port*] **source** *source-address* **source-port** *source-port* **type** { { **a** | **aaaa** | **cname** | **mx** | **ns** | **soa** | **srv** | **txt** } **domain** *domain-name* | **ptr ip address** *ipv4-address* } [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command is executed for the public network.

destination *destination-address*: Specifies the destination IPv6 address, the IPv6 address of the DNS listener.

destination-port *destination-port*: Specifies the destination port number in the range of 0 to 65535. The default is 53.

source *source-address*: Specifies the source IPv6 address.

source-port *source-port*: Specifies the source port number in the range of 0 to 65535.

type: Specifies a DNS request type.

a: Specifies the IPv4 host address type.

aaaa: Specifies the IPv6 host address type.

cname: Specifies the canonical name type.

mx: Specifies the mail exchanger type.

ns: Specifies the name server type.

soa: Specifies the start of authority type.

srv: Specifies the service type.

txt: Specifies the text type.

domain *domain-name*: Specifies the domain name to be resolved, a case-insensitive, dot-separated string of 1 to 254 characters for an absolute domain name or 1 to 253 characters for a relative domain name. Each dot-separated label in the domain name can contain a maximum of 63 characters.

ptr: Specifies the pointer type, which is used to resolve an IP address to a domain name.

ip address { *ipv4-address* | *ipv6-address* }: Specifies the IP address to be resolved to a domain name.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command tests all member devices.

Examples

Perform an IPv6 inbound link load balancing test on A-type DNS requests.

```
<Sysname> loadbalance local-dns-server schedule-test ipv6 destination 1::51 source 1::5
source-port 5 type a domain www.aaa.com
Slot 0:
    Matched DNS listener: dl2
    Matched zone: --
    Matched DNS mapping: dm2
    Matched virtual server pool: vsp2
    Preferred scheduling algorithm: Round robin
    Alternative scheduling algorithm: --
    Fallback scheduling algorithm: --
    Preferred algorithm failed cause: --
    Alternative algorithm failed cause: --
    Fallback algorithm failed cause: --
    Selected virtual server: vsa1
```

```
    Response type: Send response
    Failure cause: --
```

Perform an IPv6 inbound link load balancing test on MX-type DNS requests.

```
<Sysname> loadbalance local-dns-server schedule-test ipv6 destination 1::51
destination-port 953 source 1::5 source-port 5 type mx domain www.aaa.com
Slot 0:
    Matched DNS listener: dl2
    Matched zone: nsfocus.com.cn
    Response type: Send response
    Failure cause: --
```

Perform an IPv6 inbound link load balancing test on PTR-type DNS requests.

```
<Sysname> loadbalance local-dns-server schedule-test ipv6 destination 1::51 source 1::5
source-port 5 type ptr ip address 1.2.3.4
Slot 0:
    Matched DNS listener: dl2
    Matched zone: 1.2.3.0/24
    Response type: Send response
    Failure cause: --
```

Table 43 Command output

Field	Description
Matched zone	Matched DNS zone. • For a PTR-type DNS request, this field displays the IPv6 address of the DNS reverse zone. • For a DNS request other than the PTR type, this field displays the domain name of the DNS forward zone.
Preferred scheduling algorithm	Preferred scheduling algorithm: • Round robin. • Random. • Least connection. • Topology. • Proximity. • Bandwidth. • Inbound bandwidth. • Outbound bandwidth. • Max bandwidth. • Max inbound bandwidth. • Max outbound bandwidth. • Hash address source IP. • Hash address destination IP. • Hash address source IP-port.
Alternative scheduling algorithm	Alternative scheduling algorithm: • Round robin. • Random. • Least connection. • Topology. • Proximity. • Bandwidth. • Inbound bandwidth.

Field	Description
	• Outbound bandwidth. • Max bandwidth. • Max inbound bandwidth. • Max outbound bandwidth. • Hash address source IP. • Hash address destination IP. • Hash address source IP-port. • **--**—No alternative scheduling algorithm is configured.
Fallback scheduling algorithm	Backup scheduling algorithm: • Round robin. • Random. • Least connection. • Topology. • Proximity. • Bandwidth. • Inbound bandwidth. • Outbound bandwidth. • Max bandwidth. • Max inbound bandwidth. • Max outbound bandwidth. • Hash address source IP. • Hash address destination IP. • Hash address source IP-port. • **--**—No alternative scheduling algorithm is configured.
Preferred algorithm failure cause	Preferred algorithm failure cause: • **--**—Scheduling succeeded. • No scheduling content. • **Scheduling failed**—The scheduling content exists, but scheduling failed. • No matched virtual server member.
Alternative algorithm failure cause	Alternative algorithm failure cause: • **--**—Scheduling succeeded. • No scheduling content. • **Scheduling failed**—The scheduling content exists, but scheduling failed. • No matched virtual server member.
Fallback algorithm failure cause	Backup algorithm failure cause: • **--**—Scheduling succeeded. • No scheduling content. • **Scheduling failed**—The scheduling content exists, but scheduling failed. • No matched virtual server member.
Response type	Response type for a DNS request: • **Send response**—Replies with a DNS response. • **Send reject**—Replies with a DNS reject. • **No response**—Does not respond to the DNS request.
Failure cause	Failure cause for DNS request parsing: • **--**—Parsing succeeded. • No matched DNS listener.

Field	Description
	• No matched DNS mapping. • No matched virtual server pool. • No matched DNS zone. • Failed to get buffer. • Failed to get CONTEXT. • No matched record. • No enough memory resource. • Failed to parse domain. • Failed to find DNS listener by ID. • No scheduling content. • **Scheduling failed**—The scheduling content exists, but scheduling failed. • No matched virtual server member.

loadbalance log enable bandwidth-busy

Use **loadbalance log enable bandwidth-busy** to enable load balancing link busy state logging.

Use **undo loadbalance log enable bandwidth-busy** to disable load balancing link busy state logging.

Syntax

loadbalance log enable bandwidth-busy

undo loadbalance log enable bandwidth-busy

Default

Load balancing link busy state logging is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

Load balancing link busy state logging records busy states for all links.

Examples

Enable load balancing link busy state logging.

```
<Sysname> system-view
[Sysname] loadbalance log enable bandwidth-busy
```

loadbalance log enable base

Use **loadbalance log enable base** to enable load balancing basic logging.

Use **undo loadbalance log enable base** to disable load balancing basic logging.

Syntax

loadbalance log enable base

undo loadbalance log enable base

Default

Load balancing basic logging is enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

Load balancing basic logging generates logs for the following events:

- The state of a real server, real server group, link, or link group changes.
- The health monitoring result of a real server or link changes.
- The number of connections on a real server, virtual server, or link reaches or drops below the upper limit.
- The connection establishment rate on a real server, virtual server, or link reaches or drops below the upper limit.
- A primary/backup server farm switchover occurs between server farms specified for a virtual server.
- A primary/backup link group switchover occurs between link groups specified for a virtual server.
- A primary/backup server farm switchover occurs between server farms specified for an LB action.
- A primary/backup link group switchover occurs between link groups specified for an LB action.

Examples

Enable load balancing basic logging.

```
<Sysname> system-view
[Sysname] loadbalance log enable base
```

loadbalance log enable link-flow

Use **loadbalance log enable link-flow** to enable load balancing link flow logging.

Use **undo loadbalance log enable link-flow** to disable load balancing link flow logging.

Syntax

loadbalance log enable link-flow

undo loadbalance log enable link-flow

Default

Load balancing link flow logging is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

Use this command to enable logging for flows forwarded through all links.

Examples

Enable load balancing link flow logging.

```
<Sysname> system-view
[Sysname] loadbalance log enable link-flow
```

loadbalance log enable nat

Use **loadbalance log enable nat** to enable load balancing NAT logging.

Use **undo loadbalance log enable nat** to disable load balancing NAT logging.

Syntax

loadbalance log enable nat

undo loadbalance log enable nat

Default

Load balancing NAT logging is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

Load balancing NAT logging records NAT session information, including IP address and port translation information and access information.

Load balancing NAT logs are exported as flow logs. To export load balancing NAT logs, you must also configure flow log settings.

For more information about flow logs, see *Network Management and Monitoring Configuration Guide*.

Examples

Enable load balancing NAT logging.

```
<Sysname> system-view
[Sysname] loadbalance log enable nat
```

loadbalance policy

Use **loadbalance policy** to create an LB policy and enter its view, or enter the view of an existing LB policy.

Use **undo loadbalance policy** to delete the specified LB policy.

Syntax

loadbalance policy *policy-name* [**type** { **dns** | **generic** | **http** | **link-generic** | **mysql** | **radius** }]

undo loadbalance policy *policy-name*

Default

No LB policies exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies the LB policy name, a case-insensitive string of 1 to 63 characters.

type { **dns** | **generic** | **http** | **link-generic** | **mysql** | **radius** }: Specifies an LB policy type.

- **dns**: DNS load balancing policy.
- **generic**: Generic server load balancing policy.
- **http**: HTTP load balancing policy.
- **link-generic**: Link load balancing policy.
- **mysql**: MySQL load balancing policy.
- **radius**: RADIUS load balancing policy.

Usage guidelines

When you create an LB policy, you must specify the LB policy type. You can enter existing LB policy view without entering the type of the LB policy.

You can create generic, HTTP, MySQL, and RADIUS LB policies only if the device has licenses installed. For information about licensing, see license management in *Fundamentals Configuration Guide*.

Examples

Create the LB policy **lbp1** with the generic type, and enter LB policy view.

```
<Sysname> system-view
[Sysname] loadbalance policy lbp1 type generic
[Sysname-lbp-generic-lbp1]
```

loadbalance probe-template

Use **loadbalance probe-template** to create an LB probe template and enter its view, or enter the view of an existing LB probe template.

Use **undo loadbalance probe-template** to delete an LB probe template.

Syntax

loadbalance probe-template { **external-monitor** | **http-passive** | **icmp** | **tcp-rst** | **tcp-zero-window** } *template-name*

undo loadbalance probe-template { **external-monitor** | **http-passive** | **icmp** | **tcp-rst** | **tcp-zero-window** } *template-name*

Default

No LB probe templates exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

external-monitor: Specifies the custom-monitoring-type template.

http-passive: Specifies the HTTP-passive-type template.

icmp: Specifies the ICMP-type template.

tcp-rst: Specifies the TCP-RST template.

tcp-zero-window: Specifies the TCP zero-window template.

template-name: Specifies a template name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

A server farm, a server farm member, or a real server can use a custom-monitoring LB probe template to detect the health state of each real server.

A server farm can use an HTTP passive LB probe template to count the number of URL error times by monitoring the responses of HTTP requests to each real server.

The proximity feature can use an ICMP LB probe template to start ICMP tests and identify the reachability of hosts according to received ICMP responses.

A server farm can use a TCP-RST or TCP zero-window LB probe template to count the number of RST packets or zero-window packets sent by each server farm member.

Examples

Create an LB probe template named **icmptplt**, and enter LB probe template view.

```
<Sysname> system-view
[Sysname] loadbalance probe-template icmp icmptplt
[Sysname-lbpt-icmp-icmptplt]
```

loadbalance process-limit

Use **loadbalance process-limit** to set the maximum number of processes allowed to be started for custom monitoring.

Use **undo loadbalance process-limit** to restore the default.

Syntax

loadbalance process-limit *number*

undo loadbalance process-limit

Default

Only one process can be started for custom monitoring.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

number: Specifies the maximum number of processes, in the range of 1 to 16.

Examples

Set the maximum number of processes allowed to be started for custom monitoring to 200.

```
<Sysname> system-view
[Sysname] loadbalance process-limit 200
```

Related commands

display loadbalance process-limit

loadbalance protection-policy

Use **loadbalance protection-policy** to create a protection policy and enter its view, or enter the view of an existing protection policy.

Use **undo loadbalance protection-policy** to delete a protection policy.

Syntax

loadbalance protection-policy *policy-name* [**type http**]

undo loadbalance protection-policy *policy-name*

Default

No protection policies exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies a protection policy name, a case-insensitive string of 1 to 63 characters.

type http: Specifies the HTTP-type protection policy. When you create a protection policy, you must specify the policy type. You can enter the view of an existing protection policy without specifying the policy type.

Examples

Create an HTTP protection policy named **p1** and enter its view.

```
<Sysname> system-view
[Sysname] loadbalance protection-policy p1 type http
[Sysname-lbpp-http-p1]
```

loadbalance proximity

Use **loadbalance proximity** to create proximity and enter its view, or enter the view of the existing proximity.

Use **undo loadbalance proximity** to delete proximity view and clear all configuration in proximity view.

Syntax

loadbalance proximity [**vpn-instance** *vpn-instance-name*]

undo loadbalance proximity [**vpn-instance** *vpn-instance-name*]

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command is executed for the public network.

Examples

Create and enter proximity view for the VPN instance **vpn1**.

```
<Sysname> system-view
[Sysname] loadbalance proximity vpn vpn1
[Sysname-lb-proximity-vpn1]
```

loadbalance region

Use **loadbalance region** to create a region and enter its view, or enter the view of an existing region.

Use **undo loadbalance region** to delete a region.

Syntax

loadbalance region *region-name*

undo loadbalance region *region-name*

Default

No regions exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

region-name: Specifies the region name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

A region contains network segments corresponding to different ISPs.

Examples

Create the region **isp-ct**, and enter region view.

```
<Sysname> system-view
[Sysname] loadbalance region isp-ct
[Sysname-lb-region-isp-ct]
```

loadbalance reload external-link file

Use **loadbalance reload external-link file** to load an external link rewrite file.

Use **undo loadbalance reload external-link file** to remove the configuration.

Syntax

loadbalance reload external-link file *filename*

undo loadbalance reload external-link file

Default

No external link rewrite file is used.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

filename: Specifies a file by its complete name, a case-insensitive string of 1 to 256 characters.

Usage guidelines

If the file content has changed, you must reload the external link rewrite file to ensure it is effective.

Make sure the file format is supported by the client browser. As a best practice, use the JS script file.

Make sure the name of the external link rewrite file is different from the response file for HTTP requests.

Examples

Load external link rewrite file **/sub_lb_sw.js**.

```
<Sysname> system-view
[Sysname] loadbalance reload external-link file /sub_lb_sw.js
```

Related commands

external-link inject-domain-suffix

external-link inject-uri

external-link proxy enable

external-link whitelist domain

loadbalance reverse-zone

Use **loadbalance reverse-zone** to create a DNS reverse zone and enter its view, or enter the view of an existing DNS reverse zone.

Use **undo loadbalance reverse-zone** to delete a DNS reverse zone.

Syntax

loadbalance reverse-zone { **ip** *ipv4-address mask-length* | **ipv6** *ipv6-address prefix-length* }

undo loadbalance reverse-zone { **ip** *ipv4-address mask-length* | **ipv6** *ipv6-address prefix-length* }

Default

No DNS reverse zones exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ip *ipv4-address mask-length*: Specifies an IPv4 address and mask length for the DNS reverse zone. The value range for the *mask-length* argument is 0 to 32.

ipv6 *ipv6-address prefix-length*: Specifies an IPv6 address and prefix length for the DNS reverse zone. The value range for the *prefix-length* argument is 0 to 128.

Examples

Create a DNS reverse zone with IPv4 address 10.11.2.0/24, and enter DNS reverse zone view.

```
<Sysname> system-view
[Sysname] loadbalance reverse-zone ip 10.11.2.0 24
[Sysname-lb-rzone-10.11.2.0/24]
```

Create a DNS reverse zone with IPv6 address 1001::0/64, and enter DNS reverse zone view.

```
<Sysname> system-view
[Sysname] loadbalance reverse-zone ipv6 1001::0 64
[Sysname-lb-rzone-1001::/64]
```

Related commands

display loadbalance reverse-zone

loadbalance schedule-test ip

Use **loadbalance schedule-test ip** to perform an IPv4 load balancing test.

Syntax

loadbalance schedule-test ip [**vpn-instance** *vpn-instance-name*] { **application http** { **message-file** *file-name* | **method** { **get** | **post** } **url** *url* [**header** *header*]&<1-10> [**content** *content-value*] } | **protocol** { *protocol-number* | **icmp** | **tcp** | **udp** } } **destination** *destination-address* **destination-port** *destination-port* **source** *source-address* **source-port** *source-port* [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command is executed for the public network.

application: Specifies an application to be tested.

http: Specifies the HTTP application.

message-file *file-name*: Specifies the file that contains HTTP packet contents. The file name is a case-insensitive string of 1 to 255 characters. The file size cannot exceed 5000 bytes.

method: Specifies an HTTP request method.

get: Specifies the GET method.

post: Specifies the POST method.

url *url*: Specifies a URL for the HTTP packet, a case-insensitive string of 1 to 255 characters. A URL can contain letters, digits, hyphens (-), underscores (_), and periods (.). The URL cannot contain consecutive periods.

[**header** *header*]&<1-10>: Specifies a space-separated list of up to 10 HTTP packet headers. A header is a case-sensitive string of 1 to 127 characters excluding question marks (?).

content *content-value*: Specifies the content of the HTTP packet body, a case-sensitive string of 1 to 255 characters excluding question marks (?).

protocol { *protocol-number* | **icmp** | **tcp** | **udp** }: Specifies a protocol by its number in the range of 0 to 255 or by its name. For ICMP (1), TCP (6), and UDP (17), you can enter the protocol number or protocol name.

destination *destination-address*: Specifies the destination IPv4 address.

destination-port *destination-port*: Specifies the destination port number in the range of 0 to 65535. This option is not supported by some protocols.

source *source-address*: Specifies the source IPv4 address.

source-port *source-port*: Specifies the source port number in the range of 0 to 65535. This option is not supported by some protocols.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command tests all member devices.

Examples

Perform an IPv4 load balancing test for the TCP protocol.

```
<Sysname> loadbalance schedule-test ip protocol tcp destination 7.7.7.7 destination-port
4 source 2.2.2.2 source-port 5
    Matched virtual server: vs2
    Matched default server farm: sf
    Forward type: Forwarding to real server
    Selected real server: rs2
        Scheduling algorithm: Predictor
```

Perform an IPv4 load balancing test for the TCP protocol.

```
<Sysname> loadbalance schedule-test ip protocol tcp destination 7.7.7.7 destination-port
4 source 2.2.2.2 source-port 5
    Matched virtual server: vs2
    Matched default link group: lg
    Forward type: Forwarding to link
    Selected link: link2
        Scheduling algorithm: Predictor
```

Table 44 Command output

Field	Description
Forward type	Forwarding mode: • **The destination address is not supported. Load balancing is not performed**. • **Matching HTTP virtual server is not supported**—An HTTP virtual server is matched. Load balancing is not supported. • **Forward all**—Forwards packets. • **Forwarding to real server**—Forwards packets to the real server. • **Forwarding to link**—Forwards packets to the link. • **Drop**—Drops packets. • **Redirect**—Redirects packets. • **Waiting**—Enqueues packets.
Drop reason	Packet drop reason: • Number of connections or bandwidth for the virtual server exceeded the limit. • No class matched and no valid default server farm/link group configured. • No valid real server/link in the server farm/link group. • Action is drop. • A sticky entry was matched but the number of connections or bandwidth for the real server/link exceeded the limit. • A class was matched but no valid server farm/link group exists in the action of the class. • The HTTP message is not valid. • The HTTP request line is not valid. • The HTTP header is not valid. • The chunk HTTP content is not valid. • The server farm is busy. • **Queue overflow** (which means the wait queue is full).
Scheduling algorithm	Scheduling algorithm used to select the real server or link: • **Predictor**—The real server or link is selected by using the scheduling algorithm. • **Sticky method**—The real server or link is selected by using the sticky method. • **Proximity**—The link is selected by using the proximity feature.

loadbalance schedule-test ipv6

Use **`loadbalance schedule-test ipv6`** to perform an IPv6 load balancing test.

Syntax

loadbalance schedule-test ipv6 [**vpn-instance** *vpn-instance-name*] { **application http** { **message-file** *file-name* | **method** { **get** | **post** } **url** *url* [**header** *header*]&<1-10> [**content** *content-value*] } | **protocol** { *protocol-number* | **icmpv6** | **tcp** | **udp** } } **destination** *destination-address* **destination-port** *destination-port* **source** *source-address* **source-port** *source-port* [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command is executed for the public network.

application: Specifies an application to be tested.

http: Specifies the HTTP application.

message-file *file-name*: Specifies the file that contains HTTP packet contents. The file name is a case-insensitive string of 1 to 255 characters. The file size cannot exceed 5000 bytes.

method: Specifies an HTTP request method.

get: Specifies the GET method.

post: Specifies the POST method.

url *url*: Specifies a URL for the HTTP packet, a case-insensitive string of 1 to 255 characters. A URL can contain letters, digits, hyphens (-), underscores (_), and periods (.). The URL cannot contain consecutive periods.

[**header** *header*]&<1-10>: Specifies a space-separated list of up to 10 HTTP packet headers. A header is a case-sensitive string of 1 to 127 characters excluding question marks (?).

content *content-value*: Specifies the content of the HTTP packet body, a case-sensitive string of 1 to 255 characters excluding question marks (?).

protocol { *protocol-number* | **icmpv6** | **tcp** | **udp** }: Specifies a protocol by its number in the range of 0 to 255 or by its name. For ICMPv6 (58), TCP (6), and UDP (17), you can enter the protocol number or protocol name.

destination *destination-address*: Specifies the destination IPv6 address.

destination-port *destination-port*: Specifies the destination port number in the range of 0 to 65535. This option is not supported by some protocols.

source *source-address*: Specifies the source IPv6 address.

source-port *source-port*: Specifies the source port number in the range of 0 to 65535. This option is not supported by some protocols.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command tests all member devices.

Examples

Schedule an IPv6 load balancing test for the ICMPv6 protocol.

```
<Sysname> loadbalance schedule-test ipv6 protocol icmpv6 destination 10::1 source 12::2
```

```
    Matched virtual server: vs2
    Matched default server farm: sf
    Forward type: Forwarding to real server
    Selected real server: rs2
        Scheduling algorithm: Predictor
```

Schedule an IPv6 load balancing test for the ICMPv6 protocol.

```
<Sysname> loadbalance schedule-test ipv6 protocol icmpv6 destination 10::1 source 12::2
    Matched virtual server: vs2
    Matched default link group: lg
    Forward type: Forwarding to link
    Selected link: link2
        Scheduling algorithm: Predictor
```

Table 45 Command output

Field	Description
Forward type	Forwarding mode: • **The destination address is not supported. Load balancing is not performed**. • **Matching HTTP virtual server is not supported**—An HTTP virtual server is matched. Load balancing is not supported. • **Forward all**—Forwards packets. • **Forwarding to real server/link**—Forwards packets to the real server or link. • **Drop**—Drops packets. • **Redirect**—Redirects packets. • **Waiting**—Enqueues packets.
Drop reason	Packet drop reason: • Number of connections or bandwidth for the virtual server exceeded the limit. • No class matched and no valid default server farm/link group configured. • No valid real server/link in the server farm/link group. • Action is drop. • A sticky entry was matched but the number of connections or bandwidth for the real server/link exceeded the limit. • A class was matched but no valid server farm/link group exists in the action of the class. • The HTTP message is not valid. • The HTTP request line is not valid. • The HTTP header is not valid. • The chunk HTTP content is not valid. • The server farm is busy. • **Queue overflow** (which means the wait queue is full).
Scheduling algorithm	Scheduling algorithm used to select the real server or link: • **Predictor**—The real server or link is selected by using the scheduling algorithm. • **Sticky method**—The real server or link is selected by using the sticky method. • **Proximity**—The link is selected by using the proximity feature.

loadbalance snat-global-policy

Use **loadbalance snat-global-policy** to create a SNAT global policy and enter its view, or enter the view of an existing SNAT global policy.

Use **undo loadbalance snat-global-policy** to delete the specified SNAT global policy.

Syntax

loadbalance snat-global-policy *policy-name*

undo loadbalance snat-global-policy *policy-name*

Default

No SNAT global policies exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies the SNAT global policy name, a case-insensitive string of 1 to 63 characters.

Examples

Create the SNAT global policy **sn1**, and enter SNAT global policy view.

```
<Sysname> system-view
[Sysname] loadbalance snat-global-policy sn1
[Sysname-lb-snat-gp-sn1]
```

Related commands

snat-mode

snat-pool (server farm view)

loadbalance snat-pool

Use **loadbalance snat-pool** to create a SNAT address pool and enter its view, or enter the view of an existing SNAT address pool.

Use **undo loadbalance snat-pool** to delete the specified SNAT address pool.

Syntax

loadbalance snat-pool *pool-name*

undo loadbalance snat-pool *pool-name*

Default

No SNAT address pools exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

pool-name: Specifies the SNAT address pool name, a case-insensitive string of 1 to 63 characters.

Examples

Create the SNAT address pool **lbsp**, and enter SNAT address pool view.

```
<Sysname> system-view
[Sysname] loadbalance snat-pool lbsp
[Sysname-lbsnat-pool-lbsp]
```

loadbalance test pcre

Use **loadbalance test pcre** to perform a PCRE regular expression match test and display the match result.

Syntax

loadbalance test pcre value *value* { **string** *string* | **file** *file-name* } [**offset** *offset*] [**case-insensitive**]

Views

Any view

Predefined user roles

network-admin

context-admin

Parameters

value *value*: Specifies a PCRE regular expression, a case-sensitive string of 1 to 255 characters excluding question marks (?).

string *string*: Specifies the string to be tested, a case-sensitive string of 1 to 255 characters.

file *file-name*: Specifies the file to be tested by its name, a case-insensitive string of 1 to 255 characters. The file size cannot exceed 5000 bytes.

offset *offset*: Specifies the offset from the content to be tested, in the range of 0 to 255 bytes. The default is 0.

case-insensitive: Enables case-insensitivity matching. If you do not specify this keyword, case-sensitivity matching applies.

Usage guidelines

If the specified string or file matches the PCRE regular expression multiple times, the device displays only the result of the first match.

For a string test, the device displays the match result in text strings. For a file test, the device displays the match result in both hexadecimal characters and text strings. Characters that cannot be displayed are represented as periods (.).

Examples

Perform a PCRE regular expression match test for string **ABCDAAaefg**.

```
<Sysname> loadbalance test pcre value aaa string ABCDAAaefg case-insensitive
Matched string content: AAa
```

Perform a PCRE regular expression match test for file **123.txt**.

```
<Sysname> loadbalance test pcre value dzckgjlfdsfdsfsdnfsdkjgnf file 123.txt
```

```
Matched file content:
64 7a 63 6b 67 6a 6c 66 64  73 66 64 73 66 73 64   dzckgjlf dsfdsfsd
6e 66 73 64 6b 6a 67 6e 66  64                     nfsdkjgn f
```

loadbalance test rewrite

Use **loadbalance test rewrite** to perform a regular-expression-based rewrite test and display the rewrite result.

Syntax

loadbalance test rewrite value *value* **replace** *replace-string* { **string** *string* | **file** *file-name* } [**offset** *offset*] [**case-insensitive**]

Views

Any view

Predefined user roles

network-admin

context-admin

Parameters

value *value*: Specifies a regular expression to match the content to be rewritten, a case-sensitive string of 1 to 255 characters excluding question marks (?). You can also specify the following character strings:

- **%is**—Source IP address.
- **%ps**—Source port number.
- **%id**—Destination IP address.
- **%pd**—Destination port number.

replace *replace-string*: Specifies the content after rewrite, a case-sensitive string of 1 to 255 characters.

string *string*: Specifies the string to be tested, a case-sensitive string of 1 to 255 characters.

file *file-name*: Specifies the file to be tested by its name, a case-insensitive string of 1 to 255 characters. The file size cannot exceed 5000 bytes.

offset *offset*: Specifies the offset from the content to be tested, in the range of 0 to 255 bytes. The default is 0.

case-insensitive: Enables case-insensitivity matching. If you do not specify this keyword, case-sensitivity matching applies.

Usage guidelines

If the string or file to be tested matches the regular expression, the device replaces the matching content with the content after rewrite.

If the string or file matches the regular expression multiple times, the device displays only the rewrite result of the first match.

For a string test, the device displays the rewrite result in text strings. For a file test, the device displays the rewrite result in both hexadecimal characters and text strings. Characters that cannot be displayed are represented as periods (.).

Examples

Perform a rewrite test for string **ABCDAAaefg**.

```
<Sysname> loadbalance test rewrite value %id replace ip:%id,port:%pd string ABCDAAaefg
case-insensitive
Rewritten string content: ABCD172.0.0.1fg
```

Perform a rewrite test for file **123.txt**.

```
<Sysname> loadbalance test rewrite value dzckgjlfdsfdsfsdnfsdkjgnf replace
ip:%id,port:%pd file 123.txt
Rewritten file content:
66 67 73 2d 61 47 76 61 73  64 64 73 61 67 76 62   fgs-aGva sddsagvb
64 6a 63 78 6b 6c 63 78 76  0d 0a 0d 0a 0d 0a 0d   djcxklcx v.......
0a 69 70 3a 31 37 32 2e 30  2e 30 2e 31 2c 70 6f   .ip:172. 0.0.1,po
72 74 3a 38 30 09 6a 6b 64  67 6e 66 64 6a 6b 67   rt:80.jk dgnfdjkg
6e 66 64 6b 6a 67 6e 66 64  6b 6e 67 76 73 64 66   nfdkjgnf dkngvsdf
6c 0d 0a 0d 0a 0d 0a 0d 0a  66 67 73 2b 61 67 76   l....... .fgs+agv
61 73 64 64 73 61 67 76 62  64 6a 63 78 6b 6c 63   asddsagv bdjcxklc
78 76 0d 0a 66 67 73 64 61  67 76 61 73 64 64 73   xv..fgsd agvasdds
61 67 76 62 64 6a 63 78 6b  6c 63 78 76            agvbdjcx klcxv
```

loadbalance virtual-server-pool

Use **loadbalance virtual-server-pool** to create a virtual server pool and enter its view, or enter the view of an existing virtual server pool.

Use **undo loadbalance virtual-server-pool** to delete a virtual server pool.

Syntax

loadbalance virtual-server-pool *pool-name*

undo loadbalance virtual-server-pool *pool-name*

Default

No virtual server pools exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

pool-name: Specifies the virtual server pool name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

You can add virtual servers with similar functions to a virtual server pool to facilitate management.

Examples

Create the virtual server pool **local-pool**, and enter virtual server pool view.

```
<Sysname> system-view
[Sysname] loadbalance virtual-server-pool local-pool
[Sysname-lb-vspool-local-pool]
```

loadbalance zone

Use **loadbalance zone** to create a DNS forward zone and enter its view, or enter the view of an existing DNS forward zone.

Use **undo loadbalance zone** to delete a DNS forward zone.

Syntax

loadbalance zone *domain-name*

undo loadbalance zone *domain-name*

Default

No DNS forward zones exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

domain-name: Specifies a domain name for the DNS forward zone, a case-insensitive string of 1 to 253 characters. Each dot-separated part in the domain name can contain a maximum of 63 characters. The domain name can contain letters, digits, hyphens (-), underscores (_), and dots (.).

Examples

Create a DNS forward zone with domain name **abc.com**, and enter DNS forward zone view.

```
<Sysname> system-view
[Sysname] loadbalance zone abc.com
[Sysname-lb-zone-abc.com]
```

Related commands

display loadbalance zone

match

Use **match** to specify the proximity probe method for packets.

Use **undo match** to restore the default.

Syntax

match [*match-id*] **tcp** { **lb-probe** *lb-template* | **probe** *nqa-template* }

undo match *match-id*

Default

No proximity probe method is specified.

Views

Proximity view

Predefined user roles

network-admin

context-admin

Parameters

match-id: Specifies a proximity probe method by its ID in the range of 1 to 65535. If the rule does not exist, the command creates the proximity probe method. If the rule already exists, the command modifies the proximity probe method. If you do not specify this argument, the system automatically assigns an available rule ID with the smallest available ID.

tcp: Specifies TCP packets.

lb-probe *lb-template*: Specifies an LB probe template by its name, a case-insensitive string of 1 to 32 characters.

probe *nqa-template*: Specifies an NQA template by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

If the **match** command is configured, the specified proximity probe method applies. If no packets match the type in the **match** command or the **match** command is not configured, the default proximity probe method specified by using the **match default** command applies.

You can specify only one proximity probe method for each type of packets.

If both the **match** command and the **match default** command are configured, specify the same template type in the two commands as a best practice for both templates to take effect. If you specify different template types, the NQA template does not take effect.

Examples

Create the ICMP-type NQA template **t4**, and specify the NQA template as the proximity probe method for TCP packets.

```
<Sysname> system-view
[Sysname] nqa template icmp t4
[Sysname-nqatplt-icmp-t4] quit
[Sysname] loadbalance proximity
[Sysname-lb-proximity] match tcp probe t4
```

Related commands

match default

match acl

Use **match class** to create an ACL match rule or modify an existing ACL match rule.

Use **undo match** to delete a match rule.

Syntax

match [*match-id*] **acl** [**ipv6**] { *acl-number* | **name** *acl-name* }

undo match *match-id*

Default

No match rules exist.

Views

LB class view

Predefined user roles

network-admin

context-admin

Parameters

match-id: Specifies a match rule by its ID in the range of 1 to 65535. If you do not specify this argument, the system automatically assigns an available rule ID with the smallest number.

ipv6: Specifies an IPv6 ACL. If you do not specify this keyword, the command creates an IPv4 ACL.

acl-number: Specifies the ACL number in the range of 2000 to 3999.

name *acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters starting with a letter.

Usage guidelines

If the specified ACL does not exist, this rule is not matched.

You can create a maximum of 65535 match rules for an LB class.

Examples

Create an ACL match rule for the generic LB class **lbc1**.

```
<Sysname> system-view
[Sysname] loadbalance class lbc1 type generic
[Sysname-lbc-generic-lbc1] match acl 2000
```

match app-group

Use **match app-group** to create an application group match rule or modify an existing application group match rule.

Use **undo match app-group** to delete a match rule.

Syntax

match [*match-id*] **app-group** *group-name*

undo match *match-id*

Default

No match rules exist.

Views

Link-generic LB class view

Predefined user roles

network-admin

context-admin

Parameters

match-id: Specifies a match rule ID in the range of 1 to 65535. If you do not specify this argument, the system automatically assigns an available rule ID with the smallest number.

app-group *group-name*: Specifies an application group by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

If the specified application group does not exist, the rule does not take effect.

Examples

Create an application group match rule for the link-generic LB class **lbc1**.

```
<Sysname> system-view
[Sysname] loadbalance class lbc1 type link-generic
```

```
[Sysname-lbc-link-generic-lbc1] match app-group http
```

Related commands

app-group (*Security Command Reference*)

match class

Use **match class** to create a match rule that references an LB class or modify an existing match rule that references an LB class.

Use **undo match** to delete a match rule.

Syntax

match [*match-id*] **class** *class-name*

undo match *match-id*

Default

An LB class does not have a match rule.

Views

LB class view

Predefined user roles

network-admin

context-admin

Parameters

match-id: Specifies a match rule by its ID in the range of 1 to 65535. If you do not specify this argument, the system automatically assigns an available rule ID with the smallest number.

class-name: Specifies an LB class by its name, a case-insensitive string of 1 to 63 characters, to be referenced by the match rule. The current LB class cannot be referenced.

Usage guidelines

A match rule cannot reference an LB class that has already been referenced.

You can create a maximum of 65535 match rules for an LB class.

Examples

Create a match rule that references the LB class **lbc2** for the generic LB class **lbc1**.

```
<Sysname> system-view
[Sysname] loadbalance class lbc1 type generic
[Sysname-lbc-generic-lbc1] match class lbc2
```

match content

Use **match content** to create an HTTP entity match rule or modify an existing HTTP entity match rule.

Use **undo match** to delete a match rule.

Syntax

match [*match-id*] **content** *content* [**offset** *offset*]

undo match *match-id*

Default

An LB class does not have a match rule.

Views

HTTP LB class view

Predefined user roles

network-admin

context-admin

Parameters

match-id: Specifies a match rule by its ID in the range of 1 to 65535. If you do not specify this argument, the system automatically assigns an available rule ID with the smallest number.

content *content*: Specifies the HTTP entity regular expression, a case-sensitive string of 1 to 255 characters. The string cannot contain question marks (?).

offset *offset*: Specifies the offset value of the HTTP entity based on the start of the HTTP packet, in the range of 0 to 1000 bytes. The default is 0.

Usage guidelines

If the entity of an HTTP packet after the offset value matches the specified regular expression, the packet matches the rule.

You can create a maximum of 65535 match rules for an LB class.

Examples

Create an HTTP entity match rule for the HTTP LB class **lbc2**: Specify the offset value as 10 and regular expression as **abc**.

```
<Sysname> system-view
[Sysname] loadbalance class lbc2 type http
[Sysname-lbc-http-lbc2] match content abc.* offset 10
```

match cookie

Use **match cookie** to create an HTTP cookie match rule or modify an existing HTTP cookie match rule.

Use **undo match** to delete a match rule.

Syntax

match [*match-id*] **cookie** *cookie-name* **value** *value*

undo match *match-id*

Default

An LB class does not have a match rule.

Views

HTTP LB class view

Predefined user roles

network-admin

context-admin

Parameters

match-id: Specifies a match rule by its ID in the range of 1 to 65535. If you do not specify this argument, the system automatically assigns an available rule ID with the smallest number.

cookie *cookie-name*: Specifies the name of the HTTP cookie, a case-sensitive string of 1 to 63 characters excluding brackets ({ }, ( ),[ ], < >), at sign (@), comma (,), semicolon (;), colon (:), backslash (\), quotation mark ("), slash (/), question mark (?), equal sign (=), space character (SP), and horizontal tab (HT). The character string also excludes ASCII codes that are less than or equal to 31 and greater than or equal to 127.

value *value*: Specifies the cookie value regular expression, a case-sensitive string of 1 to 255 characters. The string cannot contain question marks (?).

Usage guidelines

If an HTTP packet contains the specified cookie with the value matching the specified regular expression, the packet matches the rule.

You can create a maximum of 65535 match rules for an LB class.

Examples

Create an HTTP cookie match rule for the HTTP LB class **lbc2**: Specify the cookie name as **JSession-id** and cookie value regular expression as **abc**.

```
<Sysname> system-view
[Sysname] loadbalance class lbc2 type http
[Sysname-lbc-http-lbc2] match cookie JSession-id value abc.*
```

match default

Use **match default** to specify the default proximity probe method.

Use **undo match default** to restore the default.

Syntax

match default { **lb-probe** *lb-template* | **probe** *nqa-template* }

undo match default

Default

The default proximity probe method is not specified.

Views

Proximity view

Predefined user roles

network-admin

context-admin

Parameters

lb-probe *lb-template*: Specifies an LB probe template by its name, a case-insensitive string of 1 to 32 characters.

probe *nqa-template*: Specifies an NQA template by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

If the **match** command is configured, the specified proximity probe method applies. If no packets match the type in the **match** command or the **match** command is not configured, the default proximity probe method applies.

If both the **match** command and the **match default** command are configured, you must specify the same template type (load balancing or NQA) in the two commands as a best practice for both templates to take effect. If you specify different template types, the NQA template does not take effect.

Examples

Create the ICMP-type NQA template **t4**, and specify the NQA template as the default proximity probe method.

```
<Sysname> system-view
[Sysname] nqa template icmp t4
[Sysname-nqatplt-icmp-t4] quit
[Sysname] loadbalance proximity
[Sysname-lb-proximity] match default probe t4
```

Related commands

loadbalance probe-template

match

nqa template (*Network Management and Monitoring Command Reference*)

match destination

Use **match destination** to create a destination IP address match rule or modify an existing destination IP address match rule.

Use **undo match** to delete a match rule.

Syntax

match [*match-id*] **destination** { **ip address** *ipv4-address* [*mask-length* | *mask*] | **ipv6 address** *ipv6-address* [*prefix-length*] }

undo match *match-id*

Default

An LB class does not have a match rule.

Views

DNS/Link-generic LB class view

Predefined user roles

network-admin

context-admin

Parameters

match-id: Specifies a match rule by its ID in the range of 1 to 65535. If you do not specify this argument, the system automatically assigns an available rule ID with the smallest number.

ip address *ipv4-address*: Specifies an IPv4 address.

mask-length: Specifies a mask length in the range of 0 to 32. The default is 32.

mask: Specifies a subnet mask. The default is 255.255.255.255.

ipv6 address *ipv6-address*: Specifies an IPv6 address.

prefix-length: Specifies a prefix length in the range of 0 to 128. The default is 128.

Usage guidelines

You can create a maximum of 65535 match rules for an LB class.

Examples

Create a match rule to match destination IPv4 address 1.1.1.1/32 for the DNS LB class **lbc1**.

```
<Sysname> system-view
[Sysname] loadbalance class lbc1 type dns
[Sysname-lbc-dns-lbc1] match destination ip address 1.1.1.1
```

Create a match rule to match destination IPv4 address 1.1.1.1/32 for the link-generic LB class **lbc2**.

```
<Sysname> system-view
[Sysname] loadbalance class lbc2 type link-generic
[Sysname-lbc-link-generic-lbc2] match destination ip address 1.1.1.1
```

match destination domain-name

Use **match destination domain-name** to create a domain name match rule or modify an existing domain name match rule.

Use **undo match** to delete a match rule.

Syntax

match [*match-id*] **destination domain-name** *domain-name*

undo match *match-id*

Default

An LB class does not have a match rule.

Views

Link-generic LB class view

Predefined user roles

network-admin

context-admin

Parameters

match-id: Specifies a match rule by its ID in the range of 1 to 65535. If you do not specify this argument, the system automatically assigns an available rule ID with the smallest number.

domain-name: Specifies a domain name, a case-insensitive string of 1 to 253 characters. Each dot-separated part in the domain name can contain a maximum of 63 characters. The domain name can contain letters, digits, hyphens (-), underscores (_), dots (.), and wildcards (asterisks and question marks).

Usage guidelines

When you use wildcards (asterisks and question marks) in a domain name, follow these guidelines:

- The wildcards can substitute any characters except for dots (.).
- An asterisk (*) can substitute a character string.
- A question mark (?) can substitute a single character.

You can create a maximum of 65535 match rules for an LB class.

Examples

Create a domain name match rule for the link-generic LB class **lbc1** to match domain name **www.abc.com**.

```
<Sysname> system-view
[Sysname] loadbalance class lbc1 type link-generic
[Sysname-lbc-link-generic-lbc1] match destination domain-name www.aaa.com
```

match domain-name

Use **match domain-name** to create a domain name match rule or modify an existing domain name match rule.

Use **undo match** to delete a match rule.

Syntax

match [*match-id*] **domain-name** *domain-name*

undo match *match-id*

Default

An LB class does not have a match rule.

Views

DNS LB class view

Predefined user roles

network-admin

context-admin

Parameters

match-id: Specifies a match rule by its ID in the range of 1 to 65535. If you do not specify this argument, the system automatically assigns an available rule ID with the smallest number.

domain-name: Specifies a domain name, a case-insensitive string of 1 to 253 characters. Each dot-separated part in the domain name can contain a maximum of 63 characters. The domain name can contain letters, digits, hyphens (-), underscores (_), dots (.), and wildcards (asterisks and question marks).

Usage guidelines

When you use wildcards (asterisks and question marks) in a domain name, follow these guidelines:

- The wildcards can substitute any characters except for dots (.).
- An asterisk (*) can substitute a character string.
- A question mark (?) can substitute a single character.

You can create a maximum of 65535 match rules for an LB class.

Examples

Create a domain name match rule for DNS LB class **lbc1** to match domain name **www.abc.com**.

```
<Sysname> system-view
[Sysname] loadbalance class lbc1 type dns
[Sysname-lbc-dns-lbc1] match domain-name www.abc.com
```

match header

Use **match header** to create an HTTP header match rule or modify an existing HTTP header match rule.

Use **undo match** to delete a match rule.

Syntax

match [*match-id*] **header** *header-name* **value** *value*

undo match *match-id*

Default

An LB class does not have a match rule.

Views

HTTP LB class view

Predefined user roles

network-admin

context-admin

Parameters

match-id: Specifies a match rule by its ID in the range of 1 to 65535. If you do not specify this argument, the system automatically assigns an available rule ID with the smallest number.

header *header-name*: Specifies the name of the HTTP packet header, a case-insensitive string of 1 to 63 characters excluding brackets ({ }, ( ), [ ], < >), at sign (@), comma (,), semicolon (;), colon (:), backslash (\), quotation mark ("), slash (/), question mark (?), equal sign (=), space character (SP), and horizontal tab (HT). The character string also excludes ASCII codes that are less than or equal to 31 and greater than or equal to 127.

value *value*: Specifies the header value regular expression, a case-sensitive string of 1 to 255 characters. The string cannot contain question marks (?).

Usage guidelines

If an HTTP packet contains the specified header with the value matching the specified regular expression, the packet matches the rule.

You can create a maximum of 65535 match rules for an LB class.

Examples

Create an HTTP header match rule for the HTTP LB class **lbc2**: Specify the HTTP packet header name as **user-agent** and header value regular expression as **abcd**.

```
<Sysname> system-view
[Sysname] loadbalance class lbc2 type http
[Sysname-lbc-http-lbc2] match header user-agent value abcd
```

match interface

Use **match interface** to create an interface match rule or modify an existing interface match rule.

Use **undo match** to delete a match rule.

Syntax

match [*match-id*] **interface** *interface-type interface-number*

undo match *match-id*

Default

An LB class does not have a match rule.

Views

Generic/HTTP/Link-generic LB class view

Predefined user roles

network-admin

context-admin

Parameters

match-id: Specifies a match rule by its ID in the range of 1 to 65535. If you do not specify this argument, the system automatically assigns an available rule ID with the smallest number.

interface *interface-type interface-number*: Specifies an interface by its type and number. The interface type can be Layer 3 Ethernet interface and Layer 3 aggregate interface.

Usage guidelines

If the specified interface does not exist, the rule does not take effect.

Examples

Create an interface match rule for the link-generic LB class **lbc1** to match interface GigabitEthernet 1/0/0.

```
<Sysname> system-view
[Sysname] loadbalance class lbc1 type link-generic
[Sysname-lbc-link-generic-lbc1] match interface gigabitethernet 1/0/1
```

match isp

Use **match isp** to create an ISP match rule or modify an existing ISP match rule.

Use **undo match** to delete a match rule.

Syntax

match [*match-id*] **isp** *isp-name*

undo match *match-id*

Default

An LB class does not have a match rule.

Views

LB class view

Predefined user roles

network-admin

context-admin

Parameters

match-id: Specifies a match rule by its ID in the range of 1 to 65535. If you do not specify this argument, the system automatically assigns an available rule ID with the smallest number.

isp-name: Specifies an ISP name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

If the specified ISP does not exist or is not configured with an IP network segment, this rule is not matched.

You can create a maximum of 65535 match rules for an LB class.

Examples

Create an ISP match rule for the generic LB class **lbc1**. Specify the ISP name as **isp1**.

```
<Sysname> system-view
[Sysname] loadbalance class lbc1 type generic
[Sysname-lbc-generic-lbc1] match isp isp1
```

match method

Use **match method** to create an HTTP method match rule or modify an existing HTTP method match rule.

Use **undo match** to delete a match rule.

Syntax

match [*match-id*] **method** { **ext** *ext-type* | **rfc** *rfc-type* }

undo match *match-id*

Default

An LB class does not have a match rule.

Views

HTTP LB class view

Predefined user roles

network-admin

context-admin

Parameters

match-id: Specifies a match rule by its ID in the range of 1 to 65535. If you do not specify this argument, the system automatically assigns an available rule ID with the smallest number.

ext *ext-type*: Specifies the extended type, a case-sensitive string of 1 to 63 characters excluding brackets ({ }, ( ),[ ], < >), at sign (@), comma (,), semicolon (;), colon (:), backslash (\), quotation mark ("), slash (/), question mark (?), equal sign (=), space character (SP), and horizontal tab (HT). The character string also excludes ASCII codes that are less than or equal to 31 and greater than or equal to 127.

rfc *rfc-type*: Specifies the RFC type to process the resources identified by the URI in HTTP request packets:

- **CONNECT**—Maintain the resources.
- **DELETE**—Delete the resources.
- **GET**—Request for the resources.
- **HEAD**—Request for the header of the response message of the resources.
- **OPTIONS**—Request to query the resources-related options and requirements supported by the server.
- **POST**—Add new data to the resources.
- **PUT**—Request the server to store the resource identified by the URI.

- **TRACE**—Request the server to return the request message it receives for test or diagnosis.

Usage guidelines

You can create a maximum of 65535 match rules for an LB class.

Examples

Create a packet matching method match rule with extended type **user** for the HTTP LB class **lbc2**.

```
<Sysname> system-view
[Sysname] loadbalance class lbc2 type http
[Sysname-lbc-http-lbc2] match method ext user
```

Create a packet matching method match rule with RFC type **CONNECT** for the HTTP LB class **lbc2**.

```
<Sysname> system-view
[Sysname] loadbalance class lbc2 type http
[Sysname-lbc-http-lbc2] match method rfc CONNECT
```

match payload

Use **match payload** to create a TCP payload match rule or modify an existing TCP payload match rule.

Use **undo match** to delete a match rule.

Syntax

match [*match-id*] **payload** *payload* [**case-insensitive**] [**not**]

undo match *match-id*

Default

An LB class does not have a match rule.

Views

Generic LB class view

Predefined user roles

network-admin

context-admin

Parameters

match-id: Specifies a match rule by its ID in the range of 1 to 65535. If you do not specify this argument, the system automatically assigns an available rule ID with the smallest number.

payload: Specifies the TCP payload regular expression, a case-sensitive string of 1 to 255 characters.

case-insensitive: Disables case sensitivity for matching character strings. If you do not specify this keyword, case sensitivity is enabled.

not: Negates the match rule. If you do not specify this keyword, the LB action is taken when the TCP payload regular expression is matched.

Usage guidelines

The device takes the corresponding LB action on TCP packets matching a TCP payload match rule. If you specify the **not** keyword for a TCP payload match rule, the device takes the corresponding LB action on TCP packets not matching the TCP payload match rule.

You can create a maximum of 65535 match rules for an LB class.

Examples

Create a match rule to match the payload **hello** for generic LB class **c1**.

```
<Sysname> system-view
[Sysname] loadbalance class c1 type generic
[Sysname-lbc-generic-c1] match payload hello
```

match radius-attribute

Use **match radius-attribute** to create a RADIUS attribute match rule or modify an existing RADIUS attribute match rule.

Use **undo match** to delete a match rule.

Syntax

match [*match-id*] **radius-attribute** { **code** *attribute-code* | **user-name** } **value** *attribute-value*

undo match *match-id*

Default

An LB class does not have a match rule.

Views

RADIUS LB class view

Predefined user roles

network-admin

context-admin

Parameters

match-id: Specifies a match rule by its ID in the range of 1 to 65535. If you do not specify this argument, the system automatically assigns an available rule ID with the smallest number.

code *attribute-code*: Specifies the code of the RADIUS attribute type, in the range of 1 to 255.

user-name: Specifies the RADIUS attribute type as **user-name** (code 1).

value *attribute-value*: Specifies the RADIUS attribute regular expression, a case-sensitive string of 1 to 255 characters.

Usage guidelines

You can create a maximum of 65535 match rules for an LB class.

Examples

Create a match rule to match usernames that contain **aaa** for RADIUS LB class **lbc1**.

```
<Sysname> system-view
[Sysname] loadbalance class lbc1 type radius
[Sysname-lbc-radius-lbc1] match radius-attribute user-name value aaa*
```

match source

Use **match source** to create a source IP address match rule or modify an existing source IP address match rule.

Use **undo match** to delete a match rule.

Syntax

match [*match-id*] **source** { **ip address** *ipv4-address* [*mask-length* | *mask*] | **ipv6 address** *ipv6-address* [*prefix-length*] }

undo match *match-id*

Default

An LB class does not have a match rule.

Views

LB class view

Predefined user roles

network-admin

context-admin

Parameters

match-id: Specifies a match rule by its ID in the range of 1 to 65535. If you do not specify this argument, the system automatically assigns an available rule ID with the smallest number.

source: Specifies the match rule type as source IP address.

ip address *ipv4-address*: Specifies an IPv4 address.

mask-length: Specifies a mask length in the range of 0 to 32. The default is 32.

mask: Specifies a subnet mask. The default is 255.255.255.255.

ipv6 address *ipv6-address*: Specifies an IPv6 address.

prefix-length: Specifies a prefix length in the range of 0 to 128. The default is 128.

Usage guidelines

You can create a maximum of 65535 match rules for an LB class.

Examples

Create a match rule that matches source IP address 1.1.1.1/32 for the generic LB class **lbc1**.

```
<Sysname> system-view
[Sysname] loadbalance class lbc1 type generic
[Sysname-lbc-generic-lbc1] match source ip address 1.1.1.1
```

match sql

Use **match sql** to create a MySQL statement match rule or modify an existing MySQL statement match rule.

Use **undo match** to delete a match rule.

Syntax

match [*match-id*] **sql** *sql* [**case-insensitive**] [**not**]

undo match *match-id*

Default

An LB class does not have a match rule.

Views

MySQL LB class view

Predefined user roles

network-admin

context-admin

Parameters

match-id: Specifies a match rule by its ID in the range of 1 to 65535. If you do not specify this argument, the system automatically assigns an available rule ID with the smallest number.

sql: Specifies a regular expression used to match MySQL statements, a case-sensitive string of 1 to 255 characters.

case-insensitive: Disables case sensitivity for matching character strings. If you do not specify this keyword, case sensitivity is enabled.

not: Specifies that the LB action is taken when the MySQL statement regular expression is not matched. If you do not specify this keyword, the LB action is taken when the MySQL statement regular expression is matched.

Usage guidelines

You can create a maximum of 65535 match rules for an LB class.

Examples

Create a match rule that matches MySQL statement **select** for the MySQL LB class **c1**.

```
<Sysname> system-view
[Sysname] loadbalance class c1 type mysql
[Sysname-lbc-mysql-lbc1] match sql select
```

match url

Use **match url** to create an HTTP URL match rule or modify an existing HTTP URL match rule.

Use **undo match** to delete a match rule.

Syntax

match [*match-id*] **url** *url*

undo match *match-id*

Default

An LB class does not have a match rule.

Views

HTTP LB class view

Predefined user roles

network-admin

context-admin

Parameters

match-id: Specifies a match rule by its ID in the range of 1 to 65535. If you do not specify this argument, the system automatically assigns an available rule ID with the smallest number.

url *url*: Specifies a URL regular expression, a case-sensitive string of 1 to 255 characters. The string cannot contain question marks (?).

Usage guidelines

You can create a maximum of 65535 match rules for an LB class.

Examples

Create an HTTP URL match rule with regular expression **.*.html** for the HTTP LB class **lbc2**.

```
<Sysname> system-view
[Sysname] loadbalance class lbc2 type http
[Sysname-lbc-http-lbc2] match url .*.html
```

match user

Use **match user** to create a user match rule or modify an existing user match rule.

Use **undo match** to delete a match rule.

Syntax

match [*match-id*] [**identity-domain** *domain-name*] **user** *user-name*

undo match *match-id*

Default

An LB class does not have a match rule.

Views

Generic/HTTP/Link-generic LB class view

Predefined user roles

network-admin

context-admin

Parameters

match-id: Specifies a match rule by its ID in the range of 1 to 65535. If you do not specify this argument, the system automatically assigns an available rule ID with the smallest number.

identity-domain *domain-name*: Matches the user in an identity domain. The *domain-name* argument represents the identity domain name, a case-insensitive string of 1 to 255 characters excluding question marks (?). If you do not specify this option, the system matches the user among users that do not belong to any identity domain.

user-name: Specifies a username, a case-sensitive string of 1 to 55 characters.

Usage guidelines

If the specified user does not exist, the rule does not take effect.

Examples

Create a user match rule for the link-generic LB class **lbc1** to match user **u1** in identity domain **domain1**.

```
<Sysname> system-view
[Sysname] loadbalance class lbc1 type link-generic
[Sysname-lbc-link-generic-lbc1] match identity-domain domain1 user u1
```

Related commands

display loadbalance class

match user-group

Use **match user-group** to create a user group match rule or modify an existing user group match rule.

Use **undo match** to delete a match rule.

Syntax

match [*match-id*] [**identity-domain** *domain-name*] **user-group** *user-group-name*

undo match *match-id*

Default

An LB class does not have a match rule.

Views

Generic/HTTP/Link-generic LB class view

Predefined user roles

network-admin

context-admin

Parameters

match-id: Specifies a match rule by its ID in the range of 1 to 65535. If you do not specify this argument, the system automatically assigns an available rule ID with the smallest number.

identity-domain *domain-name*: Matches the user group in an identity domain. The *domain-name* argument represents the identity domain name, a case-insensitive string of 1 to 255 characters excluding question marks (?). If you do not specify this option, the system matches the user group among user groups that do not belong to any identity domain.

user-group-name: Specifies a user group by its name, a case-insensitive string of 1 to 200 characters.

Usage guidelines

If the specified user group does not exist, the rule does not take effect.

Examples

Create a user group match rule for the link-generic LB class **lbc1** to match user group **lb-group** in identity domain **domain1**.

```
<Sysname> system-view
[Sysname] loadbalance class lbc1 type link-generic
[Sysname-lbc-link-generic-lbc1] match identity-domain domain1 user-group lb-group
```

Related commands

display loadbalance class

match version

Use **match version** to create an HTTP version match rule or modify an existing HTTP version match rule.

Use **undo match** to delete a match rule.

Syntax

match [*match-id*] **version** { **1.0** | **1.1** }

undo match *match-id*

Default

An LB class does not have a match rule.

Views

HTTP LB class view

Predefined user roles

network-admin

context-admin

Parameters

match-id: Specifies a match rule by its ID in the range of 1 to 65535. If you do not specify this argument, the system automatically assigns an available rule ID with the smallest number.

1.0: Specifies HTTP 1.0.

1.1: Specifies HTTP 1.1.

Usage guidelines

You can create a maximum of 65535 match rules for an LB class.

Examples

Create an HTTP version match rule with HTTP 1.0 for the HTTP LB class **lbc1**.

```
<Sysname> system-view
[Sysname] loadbalance class lbc1 type http
[Sysname-lbc-dns-lbc1] match version 1.0
```

match-across-service enable

Use **match-across-service enable** to enable sticky entry matching across services.

Use **undo match-across-service enable** to disable sticky entry matching across services.

Syntax

match-across-service enable

undo match-across-service enable

Default

Sticky entry matching across services is disabled.

Views

Address-port sticky group view

RADIUS sticky group view

Predefined user roles

network-admin

context-admin

Usage guidelines

When the device fails to find matching a stikcy entry for traffic of a virtual server, this feature allows the device to match the sticky entries of other virtual servers with the same IP address as the current virtual server.

With this feature enabled, the device can distribute requests from the same client to different services of the same virtual server to the same server farm member.

Examples

In address-port sticky group **sg1**, enable sticky entry matching across services.

```
<Sysname> system-view
[Sysname] sticky-group sg1 type address-port
[Sysname-sticky-address-port-sg1] match-across-service enable
```

match-across-virtual-server enable

Use **match-across-virtual-server enable** to enable sticky entry matching across virtual servers.

Use **undo match-across-virtual-server enable** to disable sticky entry matching across virtual servers.

Syntax

match-across-virtual-server enable

undo match-across-virtual-server enable

Default

Sticky entry matching across virtual servers is disabled.

Views

Address-port sticky group view

RADIUS sticky group view

Predefined user roles

network-admin

context-admin

Usage guidelines

When the device fails to find matching a stikcy entry for traffic of a virtual server, this feature allows the device to match the sticky entries of other virtual servers.

With this feature enabled, the device can distribute requests from the same client to different virtual servers to the same server farm member.

Examples

In address-port sticky group **sg1**, enable sticky entry matching across virtual servers.

```
<Sysname> system-view
[Sysname] sticky-group sg1 type address-port
[Sysname-sticky-address-port-sg1] match-across-virtual-server enable
```

match-buffer-end

Use **match-buffer-end** to configure the buffering end string for TCP payload matching.

Use **undo match-buffer-end** to restore the default.

Syntax

match-buffer-end *string*

undo match-buffer-end

Default

No buffering end string is configured.

Views

TCP-application parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

string: Specifies a string that indicates the end of buffering, a case-insensitive string of 1 to 31 characters.

Usage guidelines

For the TCP payload match rule, the device buffers traffic from clients for TCP payload matching during the buffering period. The device stops buffering traffic when any of the following events occurs:

- The device receives the buffering end string from clients.
- The size of buffered data exceeds the specified buffering size.
- The buffered data matches the TCP payload match rule.

This command specifies the string that indicates the end of buffering for traffic received from clients.

Examples

In TCP-application parameter profile **p1**, configure the buffering end string as **over**.

```
<Sysname> system-view
[Sysname] parameter-profile p1 type tcp-application
[Sysname-para-tcp-application-p1] match-buffer-end over
```

Related commands

match-buffer-size

match-buffer-time

match payload

match-buffer-size

Use **match-buffer-size** to set the maximum buffering size for TCP payload matching.

Use **undo match-buffer-size** to restore the default.

Syntax

match-buffer-size *size*

undo match-buffer-size

Default

The maximum buffering size is 4096 bytes.

Views

TCP-application parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

size: Specifies the maximum buffering size in the range of 1 to 4096 bytes.

Usage guidelines

For the TCP payload match rule, the device buffers traffic from clients for TCP payload matching during the buffering period. The device stops buffering traffic when any of the following events occurs:

- The device receives the buffering end string from clients.
- The size of buffered data exceeds the specified buffering size.
- The buffered data matches the TCP payload match rule.

This command specifies the maximum size of TCP data from clients that the device can buffer.

Examples

In TCP-application parameter profile **p1**, set the maximum buffering size to 2048 bytes for TCP payload matching.

```
<Sysname> system-view
[Sysname] parameter-profile p1 type tcp-application
[Sysname-para-tcp-application-p1] match-buffer-size 2048
```

Related commands

match-buffer-end

match-buffer-time

match payload

match-buffer-time

Use **match-buffer-time** to set the buffering period for TCP payload matching.

Use **undo match-buffer-time** to restore the default.

Syntax

match-buffer-time *time*

undo match-buffer-time

Default

The buffering period for TCP payload matching is 3 seconds.

Views

TCP-application parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

time: Specifies the buffering period in the range of 1 to 5 seconds.

Usage guidelines

For the TCP payload match rule, the device buffers traffic from clients for TCP payload matching during the buffering period. The device stops buffering traffic when any of the following events occurs:

- The device receives the buffering end string from clients.

- The size of buffered data exceeds the specified buffering size.
- The buffered data matches the TCP payload match rule.

This command specifies the amount of time for the device to buffer TCP data sent by clients.

Examples

In TCP-application parameter profile **p1**, set the buffering period for TCP payload matching to 3 seconds.

```
<Sysname> system-view
[Sysname] parameter-profile p1 type tcp-application
[Sysname-para-tcp-application-p1] match-buffer-time 3
```

Related commands

match-buffer-end

match-buffer-size

match payload

max-bandwidth

Use **max-bandwidth** to set the maximum expected bandwidth of an LB link.

Use **undo max-bandwidth** to restore the default.

Syntax

max-bandwidth [**inbound** | **outbound**] *bandwidth-value* **kbps**

undo max-bandwidth [**inbound** | **outbound**]

Default

The maximum expected bandwidth of an LB link is not limited.

Views

Link view

Predefined user roles

network-admin

context-admin

Parameters

inbound: Specifies the maximum inbound expected bandwidth.

outbound: Specifies the maximum outbound expected bandwidth.

bandwidth-value: Specifies the maximum expected bandwidth in the range of 0 to 4294967295. The value 0 means the bandwidth is not limited.

kbps: Specifies the bandwidth unit as kbps.

Usage guidelines

If you do not specify the **inbound** or **outbound** keyword, the maximum expected bandwidth equals the inbound expected bandwidth plus the outbound expected bandwidth.

This command takes effect only on new sessions and does not take effect on existing sessions.

In addition to being used for link protection, the maximum expected bandwidth is used for remaining bandwidth calculation in the bandwidth algorithm, maximum bandwidth algorithm, and dynamic proximity algorithm.

Examples

Set the maximum expected bandwidth of the LB link **lk1** to 1 kbps.

```
<Sysname> system-view
[Sysname] loadbalance link lk1
[Sysname-lb-link-lk1] max-bandwidth 1 kbps
```

Set the maximum inbound expected bandwidth of the LB link **lk1** to 1 kbps.

```
<Sysname> system-view
[Sysname] loadbalance link lk1
[Sysname-lb-link-lk1] max-bandwidth inbound 1 kbps
```

Set the maximum outbound expected bandwidth of the LB link **lk1** to 1 kbps.

```
<Sysname> system-view
[Sysname] loadbalance link lk1
[Sysname-lb-link-lk1] max-bandwidth outbound 1 kbps
```

max-number

Use **max-number** to set the maximum number of proximity entries.

Use **undo max-number** to restore the default.

Syntax

max-number *number*

undo max-number

Default

The maximum number of proximity entries is 65535.

Views

Proximity view

Predefined user roles

network-admin

context-admin

Parameters

number: Specifies the maximum number of proximity entries, in the range of 0 to 10000000. The value 0 indicates that the maximum number of proximity entries is not limited.

Examples

Set the maximum number of proximity entries to 100.

```
<Sysname> system-view
[Sysname] loadbalance proximity
[Sysname-lb-proximity] max-number 100
```

max-reuse

Use **max-reuse** to set the maximum number of times that a TCP connection can be reused.

Use **undo max-reuse** to restore the default.

Syntax

max-reuse *reuse-number*

undo max-reuse

Default

A TCP connection can be reused for a maximum of 1000 times.

Views

OneConnect parameter profile view

MySQL parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

reuse-number: Specifies the maximum number of reuse times, in the range of 1 to 4294967295.

Usage guidelines

After connection reuse is enabled, a TCP connection is not disconnected until the maximum number of reuse times is reached. After the TCP connection is disconnected, new connection requests trigger establishment of a new TCP connection.

Examples

In OneConnect parameter profile **ocp**, set the maximum number of reuse times to 10000.

```
<Sysname> system-view
[Sysname] parameter-profile ocp type oneconnect
[Sysname-para-oneconnect-ocp] max-reuse 10000
```

memory-size

Use **memory-size** to set the memory size used for compression.

Use **undo memory-size** to restore the default.

Syntax

memory-size *size*

undo memory-size

Default

The memory size used for compression is 8 KB.

Views

HTTP-compression parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

size: Specifies the memory size in KB used for compression. The value can only be 1, 2, 4, 8, 16, 32, or 64.

Examples

Create the HTTP-compression parameter profile **pa1**, and set the memory size used for compression to 32 KB.

```
<Sysname> system-view
[Sysname] parameter-profile pa1 type http-compress
[Sysname-para-http-compress-pa1] memory-size 32
```

min-ttl

Use **min-ttl** to set the minimum TTL.

Use **undo min-ttl** to restore the default.

Syntax

min-ttl *ttl-value*

undo min-ttl

Default

The minimum TTL is 3600 seconds.

Views

SOA view

Predefined user roles

network-admin

context-admin

Parameters

ttl-value: Specifies the minimum TTL in the range of 0 to 4294967295 seconds.

Usage guidelines

The minimum TTL is the amount of time that resource records on the primary DNS server are cached on the secondary DNS server.

Examples

Set the minimum TTL to 1 day for DNS forward zone **abc.com**.

```
<Sysname> system-view
[Sysname] loadbalance zone abc.com
[Sysname-lb-zone-abc.com] soa
[Sysname-lb-zone-abc.com-soa] min-ttl 86400
```

Related commands

display loadbalance zone

monitor-interval

Use **monitor-interval** to set the monitoring time for an LB probe template.

Use **undo monitor-interval** to restore the default.

Syntax

monitor-interval *interval-time*

undo monitor-interval

Default

The monitoring time is 10 seconds for a TCP-RST or TCP zero-window LB probe template, 1 second for an HTTP passive LB probe template, and 5 seconds for a custom-monitoring LB probe template.

Views

HTTP passive LB probe template view

TCP-RST LB probe template view

TCP zero-window LB probe template view

Custom-monitoring LB probe template view

Predefined user roles

network-admin

context-admin

Parameters

interval-time: Specifies the monitoring time in the range of 5 to 255 seconds for a TCP-RST or TCP zero-window LB probe template, in the range of 1 to 5 seconds for an HTTP passive LB probe template, and in the range of 1 to 86400 seconds for a custom-monitoring LB probe template.

Usage guidelines

During the monitoring time, the system counts the number of RST packets or zero-window packets sent by each server farm member in a server farm.

During the monitoring time, the system monitors the responses of matching HTTP requests and counts the number of URL error times.

After a custom-monitoring LB probe template is specified, the system executes the custom script file during the monitoring time to detect the state of real servers.

Examples

In TCP RST LB probe template **rsttplt**, set the monitoring time to 60 seconds.

```
<Sysname> system-view
[Sysname] loadbalance probe-template tcp-rst rsttplt
[Sysname-lbpt-tcp-rst-rsttplt] monitor-interval 60
```

Related commands

external-script

node

Use **node** to create a statistics node and enter its view, or enter the view of an existing statistics node.

Use **undo node** to delete the specified statistics node.

Syntax

node *node-name*

undo node *node-name*

Default

No statistics nodes exist.

Views

HTTP statistics parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

node-name: Specifies the statistics node name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

You can configure a maximum of 256 statistics nodes in one HTTP statistics parameter profile.

Examples

In HTTP statistics parameter profile **http1**, create statistics node **node1** and enter statistics node view.

```
<Sysname> system-view
[Sysname] parameter-profile http1 type http-statistics
[Sysname-para-http-statistics-http1] node node1
[Sysname-para-http-statistics-http1-node-node1]
```

override-limit enable

Use **override-limit enable** to ignore the limits for sessions that match sticky entries.

Use **undo override-limit enable** to remove the configuration.

Syntax

override-limit enable

undo override-limit enable

Default

The session limits apply to sessions that match sticky entries.

Views

Sticky group view

Predefined user roles

network-admin

context-admin

Usage guidelines

Use this command to ignore the following limits for sessions that match sticky entries:

- Bandwidth and connection parameters on real servers or links.
- Bandwidth ratios and maximum expected bandwidths for real servers or links.
- LB connection limit policies on virtual servers.

This command takes effect only on new sessions and does not take effect on existing sessions.

Examples

Ignore the limits for sessions that match sticky entries generated in the sticky group **st**.

```
<Sysname> system-view
[Sysname] sticky-group st type http-cookie
[Sysname-sticky-http-cookie-st] override-limit enable
```

packet-loss-rate weight

Use **packet-loss-rate weight** to set the packet loss ratio weight for proximity calculation.

Use **undo packet-loss-rate weight** to restore the default.

Syntax

packet-loss-rate weight *packet-loss-rate-weight*

undo packet-loss-rate weight

Default

The packet loss ratio weight for proximity calculation is 0.

Views

Proximity view

Predefined user roles

network-admin

context-admin

Parameters

packet-loss-rate-weight: Specifies the packet loss ratio weight in the range of 0 to 255. The greater the weight value, the higher the weight.

Usage guidelines

This command sets the weight of the packet loss ratio in calculating the link quality. The packet loss ratio is used to calculate the link quality only if the proximity feature is enabled or the link quality algorithm is configured. The proximity feature and the link quality algorithm are mutually exclusive.

Examples

Set the packet loss ratio weight for proximity calculation to 200.

```
<Sysname> system-view
[Sysname] loadbalance proximity
[Sysname-lb-proximity] packet-loss-rate weight 200
```

Related commands

predictor (link group view)

proximity enable (link group view)

parameter

Use **parameter** to specify a parameter profile to be referenced by a virtual server.

Use **undo parameter** to restore the default.

Syntax

parameter { **http** | **http-compression** | **http-statistics** | **ip** | **mysql** | **oneconnect** | **tcp** | **tcp-application** } *profile-name* [**client-side** | **server-side**]

undo parameter { **http** | **http-compression** | **http-statistics** | **ip** | **mysql** | **oneconnect** | **tcp** | **tcp-application** } [**client-side** | **server-side**]

Default

No parameter profile is referenced by a virtual server.

Views

Virtual server view

Predefined user roles

network-admin

context-admin

Parameters

{ **http** | **http-compression** | **http-statistics** | **ip** | **mysql** | **oneconnect** | **tcp** | **tcp-application** }: Specifies a parameter profile type, HTTP, HTTP-compression, HTTP statistics, IP, OneConnect, TCP, or TCP-application. The **http** and **tcp** keywords are supported by the virtual servers of the fast HTTP or HTTP type. The **http-compression**, **http-statistics**, and **oneconnect** keywords are supported only by the virtual servers of the HTTP type. The **mysql** keyword is supported only by MySQL virtual servers. The **tcp-application** keyword is supported only by TCP virtual servers operating at Layer 7.

profile-name: Specifies a parameter profile by its name, a case-insensitive string of 1 to 63 characters.

client-side: Specifies a client-side parameter profile.

server-side: Specifies a server-side parameter profile.

Usage guidelines

The virtual server references the parameter profile to implement analysis, processing, and optimization for service traffic.

The virtual servers of the RADIUS type can only reference the IP parameter profile.

A client-side parameter profile optimizes and processes TCP connections between the client and the device. A server-side parameter profile optimizes and processes TCP connections between the device and the server. Only TCP parameter profiles support the **client-side** and **server-side** keywords.

Examples

Specify the IP parameter profile **pp2** to be referenced by the IP-type virtual server **vs3**.

```
<Sysname> system-view
[Sysname] virtual-server vs3 type ip
[Sysname-vs-ip-vs3] parameter ip pp2
```

parameter-profile

Use **parameter-profile** to create a parameter profile and enter its view, or enter the view of an existing parameter profile.

Use **undo parameter-profile** to delete the specified parameter profile.

Syntax

parameter-profile *profile-name* [**type** { **http** | **http-compression** | **http-statistics** | **ip** | **mysql** | **oneconnect** | **tcp** | **tcp-application** }]

undo parameter-profile *profile-name*

Default

No parameter profiles exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

profile-name: Specifies a parameter profile name, a case-insensitive string of 1 to 63 characters.

type { **http** | **http-compression** | **http-statistics** | **ip** | **mysql** | **oneconnect** | **tcp** | **tcp-application** }: Specifies a parameter profile type, HTTP, HTTP-compression, HTTP statistics, IP, MySQL, OneConnect, TCP, or TCP-application. When you create a parameter profile, you must specify the parameter profile type. You can enter an existing parameter profile view without entering the parameter profile type.

Usage guidelines

You can configure advanced parameters through the parameter profile. The virtual server references the parameter profile to implement analysis, processing, and optimization for service traffic.

You can create HTTP, HTTP-compression, MySQL, HTTP statistics, OneConnect, or TCP-application parameter profiles only if the device has licenses installed. For information about licensing, see license management in *Fundamentals Configuration Guide*.

Examples

Create the IP parameter profile **pp2**, and enter parameter profile view.

```
<Sysname> system-view
[Sysname] parameter-profile pp2 type ip
[Sysname-para-ip-pp2]
```

payload (HTTP/UDP payload sticky group view)

Use **payload** to configure the HTTP or UDP payload sticky method.

Use **undo payload** to delete the HTTP or UDP payload sticky method.

Syntax

payload [**offset** *offset*] [**start** *start-string*] [**end** *end-string* | **length** *length*]

undo payload

Default

No sticky methods exist.

Views

HTTP/UDP payload sticky group view

Predefined user roles

network-admin

context-admin

Parameters

offset *offset*: Specifies the offset value of the HTTP or UDP payload based on the start of the HTTP or UDP packet, in the range of 0 to 1000 bytes. The default is 0.

start *start-string*: Specifies the regular expression that marks the start of the HTTP or UDP payload, a case-sensitive string of 1 to 127 characters starting from the *offset* value. The string cannot contain question marks (?).

end *end-string*: Specifies the regular expression that marks the end of the HTTP or UDP payload, a case-sensitive string of 1 to 127 characters starting from the *start-string* value. The string cannot contain question marks (?).

length *length*: Specifies the length of the HTTP or UDP payload, in the range of 0 to 1000 bytes. The default is 0, which indicates all lengths.

Usage guidelines

Use this command to obtain the HTTP or UDP payload information used to generate sticky entries based on the *offset*, *start-string*, *end-string*, and *length* values. The *start-string* and *end-string* values are not included in the sticky entry information.

This command is not supported by the virtual servers of the fast HTTP type.

Examples

Configure the HTTP payload sticky method for the HTTP payload sticky group **sg5**: Starting from the 10th byte of start of the HTTP packet, use the 20-byte HTTP payload to generate sticky entries.

```
<Sysname> system-view
[Sysname] sticky-group sg5 type payload
[Sysname-sticky-payload-sg5] payload offset 10 length 20
```

Configure the UDP payload sticky method for the UDP payload sticky group **sg6**: Starting from the 28th byte of start of the UDP packet, use the 6-byte UDP payload to generate sticky entries.

```
<Sysname> system-view
[Sysname] sticky-group sg6 type payload
[Sysname-sticky-payload-sg6] payload offset 28 length 6
```

payload (UDP passive sticky group view)

Use **payload** to configure the UDP payload passive sticky method.

Use **undo payload** to delete the UDP payload passive sticky method.

Syntax

payload { **get** | **match** } [**offset** *offset*] [**start** *start-string*] [**end** *end-string* | **length** *length*]

undo payload { **get** | **match** }

Default

No UDP payload passive sticky methods exist.

Views

UDP passive sticky group view

Predefined user roles

network-admin

context-admin

Parameters

get: Obtains the specified string in the UDP response payload, which is used to generate a UDP payload passive sticky entry.

match: Obtains the specified string in the UDP request payload, which is used to match a UDP payload passive sticky entry.

offset *offset*: Specifies the offset value of the UDP payload based on the start of the UDP packet, in the range of 0 to 1000 bytes. The default is 0.

start *start-string*: Specifies the regular expression that marks the start of the UDP payload, a case-sensitive string of 1 to 127 characters starting from the *offset* value. The string cannot contain question marks (?).

end *end-string*: Specifies the regular expression that marks the end of the UDP payload, a case-sensitive string of 1 to 127 characters starting from the *start-string* value. The string cannot contain question marks (?).

length *length*: Specifies the length of the UDP payload, in the range of 0 to 1000 bytes. The default is 0, which indicates all lengths.

Usage guidelines

Use the **payload get** command to obtain the UDP response payload information based on the *offset*, *start-string*, *end-string*, and *length* values. Use the **payload match** command to obtain the UDP request payload information based on those values.

The *start-string* and *end-string* values are not included in the sticky entry information.

Both the **payload get** and **payload match** commands are required for a UDP payload passive sticky method.

The device obtains the payload information of an incoming UDP request based on the **payload match** command and obtains the payload information of an incoming UDP response based on the **payload get** command. If the payload information of the UDP request matches the payload information of the UDP response, the device generates a sticky entry based on the payload information of the UDP response. Subsequent UDP requests that match the sticky entry are forwarded according to the sticky entry.

Examples

Configure the UDP payload passive sticky method for the UDP passive sticky group **sg5**: Obtain the 20-byte UDP payload string starting with **id** in the UDP response. If the obtained string matches the 20-byte UDP payload string starting with **id** in the UDP request, the device generates a sticky entry based on the string obtained from the UDP response.

```
<Sysname> system-view
[Sysname] sticky-group sg5 type udp-passive
[Sysname-sticky-udp-passive-sg5] payload get start id length 20
[Sysname-sticky-udp-passive-sg5] payload match start id length 20
```

payload rewrite

Use **payload rewrite** to rewrite the TCP payload.

Use **undo payload rewrite** to remove the configuration.

Syntax

payload rewrite { **both** | **request** | **response** } **value** *value* **replace** *replace-string*

undo payload rewrite { **both** | **request** | **response** } **value** *value*

Default

The TCP payload is not rewritten.

Views

Generic LB action view

Predefined user roles

network-admin

context-admin

Parameters

both: Specifies both the TCP request and response packets.

request: Specifies the TCP request packets.

response: Specifies the TCP response packets.

value *value*: Specifies the TCP packet header content to be rewritten, a case-sensitive string of 1 to 127 characters.

replace *replace-string*: Specifies the content after rewrite, a case-sensitive string of 1 to 127 characters. You can also specify the following replacement strings:

- **%[***variable***]**—Replaces the specified value with the variable associated with the server farm member. The *variable* is the variable name.
- **%[1-9]**—Replaces the specified value with the content in the corresponding parentheses of the specified value. For example, executing the **payload rewrite value** (Wel)(co)(me) **replace** %2 command will replace the string **Welcome** with **co** in the second pair of parentheses.

Usage guidelines

You can replace the specified value with the variable associated with the server farm member by specifying the replacement string **%[***variable***]**. For example, you can replace the string QMGR.S01 in the payload with QMGR.S0_1 by executing the following commands:

- **variable** var1 **value** _1 (in server farm member view).
- **payload rewrite request value** "QMGR.S01" **replace** QMGR.S01%[var1] (in generic LB action view).

For TCP virtual servers operating at Layer 7 (with the **application-mode enable** command configured), make sure the packet length before and after TCP payload rewrite is not greater than 2048 bytes. If this condition is not met, TCP payload rewrite might fail.

Examples

In generic LB action **lba1**, replace **QMGR.S01** in the payload of TCP requests with **QMGR.S01%[var1]**. **var1** is the name of the variable associated with the server farm member.

```
<Sysname> system-view
[Sysname] loadbalance action lba1 type generic
[Sysname-lba-generic-lba1] payload rewrite request value QMGR.S01 replace QMGR.S01%[var1]
```

Related commands

variable

pool-size

Use **pool-size** to set the maximum number of connections allowed in the MySQL connection pool.

Use **undo pool-size** to restore the default.

Syntax

pool-size *pool-size*

undo pool-size

Default

The maximum number of connections allowed in the MySQL connection pool is 1024.

Views

MySQL parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

pool-size: Specifies the maximum number of connections allowed in the MySQL connection pool, in the range of 1 to 64000.

Usage guidelines

After MySQL data transfer is completed, the TCP connection is stored in a connection pool instead of being closed. For a new connection request, the device selects an available connection from the connection pool before attempting to open a new connection.

Examples

Set the maximum number of connections allowed in the MySQL connection pool to 2000 for the MySQL parameter profile **p1**.

```
<Sysname> system-view
[Sysname] parameter-profile p1 type mysql
[Sysname-para-mysql-p1] pool-size 2000
```

port (DNS server view)

Use **port** to configure the port number of a DNS server.

Use **undo port** to restore the default.

Syntax

port *port-number*

undo port

Default

The port number of a DNS server is 0.

Views

DNS server view

Predefined user roles

network-admin

context-admin

Parameters

port-number: Specifies a port number in the range of 0 to 65535. The value 0 means that the original port number is used.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the port number of DNS server **ds1** as **5353**.

```
<Sysname> system-view
[Sysname] loadbalance dns-server ds1
[Sysname-lb-ds-ds1] port 5353
```

port (real server view)

Use **port** to configure the port number of a real server.

Use **undo port** to restore the default.

Syntax

port *port-number*

undo port

Default

The port number of a real server is 0. (The original port number is used.)

Views

Real server view

Predefined user roles

network-admin

context-admin

Parameters

port-number: Specifies a port number in the range of 0 to 65535. 0 means the original port number is used.

Usage guidelines

This configuration takes effect only when you enable the NAT feature for the server farm.

Examples

Specify the port number of the real server **rs** as **8080**.

```
<Sysname> system-view
[Sysname] real-server rs
[Sysname-rserver-rs] port 8080
```

Related commands

transparent enable (server farm view)

port (transparent DNS proxy view)

Use **port** to configure the port number of a transparent DNS proxy.

Use **undo port** to restore the default.

Syntax

port *port-number*

undo port

Default

The port number of a transparent DNS proxy is 53.

Views

Transparent DNS proxy view

Predefined user roles

network-admin

context-admin

Parameters

port-number: Specifies a port number in the range of 1 to 65535.

Usage guidelines

A transparent DNS proxy processes a DNS request only when the destination IP address and port number of the DNS request matches those of the transparent DNS proxy.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the port number of transparent DNS proxy **dns-proxy1** as **5353**.

```
<Sysname> system-view
[Sysname] loadbalance dns-proxy dns-proxy1
[Sysname-lb-dp-dns-proxy1] port 5353
```

Related commands

display loadbalance dns-proxy

port (virtual server view)

Use **port** to configure the port number of a virtual server.

Use **undo port** to restore the default.

Syntax

port { *port-number* [**to** *port-number*] } &<1-n>

undo port

Default

The port number is 0 (indicates any port) for the virtual server of the IP, RADIUS, TCP, or UDP type. The port number is 80 for the virtual server of the fast HTTP or HTTP type. The port number is 5060 for the virtual server of the SIP type.

Views

Virtual server view

Predefined user roles

network-admin

context-admin

Parameters

port-number [**to** *port-number*] &<1-n>: Specifies a space-separated list of up to *n* port number items. Each port number item specifies a port number or a range of port numbers in the form of *start-port-number* **to** *end-port-number*. For IP, RADIUS, TCP, and UDP virtual servers, the value range for the *port-number* argument is 0 to 65535 (0 means any port) and the value range for *n* is 1 to 32. For HTTP, fast HTTP, and SIP virtual servers, the value range for the *port-number* argument is 1 to 65535 and the value of *n* can only be 1.

Usage guidelines

If the virtual server has referenced an SSL policy, you must configure a non-default port number (typically 443) for the virtual server.

For a TCP virtual server operating at Layer 7 (with the **application-mode enable** command configured), you can configure a maximum of 200 port numbers through the **port** command.

Examples

Specify the port number of the IP-type virtual server **vs3** as **8080**.

```
<Sysname> system-view
[Sysname] virtual-server vs3 type ip
[Sysname-vs-ip-vs3] port 8080
```

Related commands

ssl-server-policy

predictor (DNS server pool view)

Use **predictor** to specify a scheduling algorithm for a DNS server pool.

Use **undo predictor** to restore the default.

Syntax

predictor hash address { **destination** | **source** | **source-ip-port** } [**mask** *mask-length*] [**prefix** *prefix-length*]

predictor { **random** | **round-robin** | { **bandwidth** | **max-bandwidth** } [**inbound** | **outbound**] }

undo predictor

Default

The scheduling algorithm for a DNS server pool is weighted round robin.

Views

DNS server pool view

Predefined user roles

network-admin

context-admin

Parameters

hash address: Specifies the hash algorithm based on the IP address.

destination: Specifies the hash algorithm based on the destination IP address.

source: Specifies the hash algorithm based on the source IP address.

source-ip-port: Specifies the hash algorithm based on the source IP address and port number.

mask *mask-length*: Specifies the mask length of the IPv4 address used in the hash algorithm. The value range for the *mask-length* argument is 0 to 32. The default is 32.

prefix *prefix-length*: Specifies the prefix length of the IPv6 address used in the hash algorithm. The value range for the *prefix-length* argument is 0 to 128. The default is 128.

random: Specifies the random algorithm, which randomly assigns DNS requests to DNS servers.

round-robin: Specifies the weighted round robin algorithm, which assigns DNS requests to DNS servers based on the weights of the DNS servers. A higher weight indicates more DNS requests will be assigned. The weight value used in this algorithm is configured in DNS server pool member view.

bandwidth: Specifies the bandwidth algorithm, which assigns DNS requests to DNS servers based on the weight and remaining bandwidth of the DNS servers. The weight value used in this algorithm is configured in DNS server view.

max-bandwidth: Specifies the maximum bandwidth algorithm, which always assigns DNS requests to the DNS server corresponding to the idle link with the largest remaining bandwidth.

inbound: Selects a DNS server based on the inbound bandwidth.

outbound: Selects a DNS server based on the outbound bandwidth.

Usage guidelines

If you do not specify the **inbound** or **outbound** keyword, the total bandwidth is used to select a DNS server.

In the bandwidth algorithm and maximum bandwidth algorithm, the remaining bandwidth is the maximum expected bandwidth minus the current bandwidth. If the maximum expected bandwidth is not configured, the remaining bandwidth is the maximum bandwidth of the link minus the current bandwidth.

Examples

Specify the scheduling algorithm as **random** for DNS server pool **dns-pool**.

```
<Sysname> system-view
[Sysname] loadbalance dns-server-pool dns-pool
[Sysname-lb-dspool-dns-pool] predictor random
```

Related commands

max-bandwidth (link view)

rate-limit bandwidth (link view)

predictor (link group view)

Use **predictor** to specify a scheduling algorithm for a link group.

Use **undo predictor** to restore the default.

Syntax

Link-based:

predictor { **least-connection** | { **bandwidth** | **max-bandwidth** } [**inbound** | **outbound**] }

undo predictor

Link group member-based:

predictor hash address { **destination** | **source** | **source-ip-port** } [**mask** *mask-length*] [**prefix** *prefix-length*]

predictor { **least-connection member** | **random** | **round-robin** }

undo predictor

Default

The scheduling algorithm for a link group is weighted round robin.

Views

Link group view

Predefined user roles

network-admin

context-admin

Parameters

hash address: Performs the hash algorithm based on IP address.

destination: Performs the hash algorithm based on destination IP address.

source: Performs the hash algorithm based on source IP address.

source-ip-port: Performs the hash algorithm based on source IP address and port number.

mask *mask-length*: Specifies the IPv4 address mask length, in the range of 0 to 32. The default is 32.

prefix *prefix-length*: Specifies the IPv6 address prefix length, in the range of 0 to 128. The default is 128.

least-connection: Specifies the link-based weighted least connection algorithm. This algorithm always assigns new connections to the link with the fewest number of weighted active connections (the total number of active connections in all link groups divided by weight). The weight value used in this algorithm is configured in link view.

least-connection member: Specifies the link group member-based weighted least connection algorithm. This algorithm always assigns new connections to the link with the fewest number of weighted active connections (the number of active connections in the specified link group divided by weight). The weight value used in this algorithm is configured in link group member view.

random: Specifies the random algorithm, which randomly assigns new connections to links.

round-robin: Specifies the weighted round robin algorithm, which assigns new connections to links based on the weights of links. A higher weight indicates more new connections will be assigned. The weight value used in this algorithm is configured in link group member view.

bandwidth: Specifies the bandwidth algorithm, which assigns packets to links based on the weight multiplied by the remaining bandwidth of the links. The weight value used in this algorithm is configured in link view.

max-bandwidth: Specifies the maximum bandwidth algorithm, which always assigns packets to the idle link with the largest remaining bandwidth.

inbound: Selects a link based on the inbound bandwidth.

outbound: Selects a link based on the outbound bandwidth.

Usage guidelines

If you do not specify the **inbound** or **outbound** keyword, the total bandwidth is used to select a link.

In the bandwidth algorithm and maximum bandwidth algorithm, the remaining bandwidth is the maximum expected bandwidth minus the current bandwidth. If the maximum expected bandwidth is not configured, the remaining bandwidth is the maximum bandwidth of the link minus the current bandwidth.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the scheduling algorithm **random** for the link group **lg**.

```
<Sysname> system-view
[Sysname] loadbalance link-group lg
[Sysname-lb-lgroup-lg] predictor random
```

Related commands

max-bandwidth (link view)

proximity enable (link group view)

rate-limit bandwidth (link view)

predictor (server farm view)

Use **predictor** to specify a scheduling algorithm for a server farm.

Use **undo predictor** to restore the default.

Syntax

Real server-based:

predictor { **dync-round-robin** | **least-connection** | **least-time** | { **bandwidth** | **max-bandwidth** } [**inbound** | **outbound**] }

undo predictor

Server farm member-based:

predictor hash [**carp**] **address** { **destination** | **source** | **source-ip-port** } [**mask** *mask-length*] [**prefix** *prefix-length*]

predictor hash [**carp**] **http** [**offset** *offset*] [**start** *start-string*] [[**end** *end-string*] | [**length** l*ength*]]

predictor { **least-connection member** | **least-time member** | **random** | **round-robin** | }

undo predictor

Default

The scheduling algorithm for a server farm is weighted round robin.

Views

Server farm view

Predefined user roles

network-admin

context-admin

Parameters

hash address: Performs the hash algorithm based on IP address.

carp: Specifies the Cache Array Routing Protocol (CARP) hash algorithm. When the number of available real servers changes, this protocol makes all available real servers have the smallest load changes.

destination: Performs the hash algorithm based on destination IP address.

source: Performs the hash algorithm based on source IP address.

source-ip-port: Performs the hash algorithm based on source IP address and port number.

mask *mask-length*: Specifies the IPv4 address mask length, in the range of 0 to 32. The default is 32.

prefix *prefix-length*: Specifies the IPv6 address prefix length, in the range of 0 to 128. The default is 128.

http: Performs the hash algorithm based on the HTTP content.

offset *offset*: Specifies the offset value based on the start of the HTTP content, in the range of 0 to 1000 bytes. The default is 0.

start *start-string*: Specifies the regular expression that marks the start of the HTTP content, a case-sensitive string of 1 to 127 characters starting from the *offset* value. The string cannot contain question marks (?).

end *end-string*: Specifies the regular expression that marks the end of the HTTP content, a case-sensitive string of 1 to 127 characters starting from the *start-string* value. The string cannot contain question marks (?).

length *length*: Specifies the length of the HTTP content, in the range of 0 to 1000 bytes. The default is 0, which indicates all lengths.

dync-round-robin: Specifies the dynamic round robin algorithm, which assigns new connections to real servers based on load weight values calculated by using the memory usage, CPU usage, and disk usage of the real servers. The smaller the load, the greater the weight value. A real server with a greater weight value is assigned more connections.

least-connection: Specifies the real server-based weighted least connection algorithm, which always assigns new connections to the real server with the fewest number of weighted active connections (the total number of active connections in all server farms divided by weight). The weight value used in this algorithm is configured in real server view.

least-connection member: Specifies the server farm member-based weighted least connection algorithm, which always assigns new connections to the server farm member with the fewest number of weighted active connections (the number of active connections in the specified server farm divided by weight). The weight value used in this algorithm is configured in server farm member view.

least-time: Specifies the least time algorithm, which assigns new connections to real servers based on load weight values calculated by using the response time of the real servers. The shorter the response time, the greater the weight value. A real server with a greater weight value is assigned more connections.

least-time member: Specifies the server farm member-based least time algorithm, which assigns new connections to server farm members based on load weight values calculated by using the response time of the server farm members. The shorter the response time, the greater the weight value. A server farm member with a greater weight value is assigned more connections.

random: Specifies the random algorithm, which randomly assigns new connections to real servers.

round-robin: Specifies the weighted round robin algorithm, which assigns new connections to real servers based on the weights of real servers. A higher weight indicates more new connections will be assigned. The weight value used in this algorithm is configured in server farm member view.

bandwidth: Specifies the bandwidth algorithm, which assigns packets to real servers based on the weight of the real servers and the bandwidth ratio. The weight value used in this algorithm is configured in real server view.

max-bandwidth: Specifies the maximum bandwidth algorithm, which always assigns packets to the idle real server with the largest remaining bandwidth.

inbound: Selects a real server based on the inbound bandwidth.

outbound: Selects a real server based on the outbound bandwidth.

Usage guidelines

The dynamic round robin algorithm can take effect only if you specify an SNMP-DCA NQA template. If no SNMP-DCA NQA template is specified, the non-weighted round robin algorithm is used. For more information about NQA templates, see NQA configuration in *Network Management and Monitoring Configuration Guide*.

If you do not specify the **inbound** or **outbound** keyword, the total bandwidth is used to select a real server.

In the bandwidth algorithm and maximum bandwidth algorithm, the remaining bandwidth is the maximum expected bandwidth minus the current bandwidth. If the maximum expected bandwidth is not configured, the remaining bandwidth is the maximum bandwidth of the real server minus the current bandwidth.

Examples

Specify the scheduling algorithm for the server farm **sf** as **random**.

```
<Sysname> system-view
[Sysname] server-farm sf
[Sysname-sfarm-sf] predictor random
```

Related commands

max-bandwidth (real server view)

rate-limit bandwidth (real server view)

predictor (virtual server pool view)

Use **predictor** to specify a scheduling algorithm for a virtual server pool.

Use **undo predictor** to restore the default.

Syntax

predictor { **alternate** | **fallback** | **preferred** } { **least-connection** | **proximity** | **random** | **round-robin** | **topology** | { **bandwidth** | **max-bandwidth** } [**inbound** | **outbound**] | **hash address** { **source** | **source-ip-port** | **destination** } [**mask** *mask-length* | **prefix** *prefix-length*] }

undo predictor { **alternate** | **fallback** }

Default

The scheduling algorithm for a virtual server pool is weighted round robin. No alternative or backup scheduling algorithm is specified.

Views

Virtual server pool view

Predefined user roles

network-admin

context-admin

Parameters

alternate: Specifies the alternative scheduling algorithm.

fallback: Specifies the backup scheduling algorithm.

preferred: Specifies the preferred scheduling algorithm.

least-connection: Specifies the weighted least connection algorithm. This algorithm always assigns DNS requests to the virtual server with the fewest number of weighted active connections (the number of active connections divided by weight).

proximity: Specifies the dynamic proximity algorithm, which assigns DNS requests to virtual servers based on dynamic proximity entries.

random: Specifies the random algorithm, which randomly assigns DNS requests to virtual servers.

round-robin: Specifies the weighted round robin algorithm, which assigns DNS requests to virtual servers based on the weights of the virtual servers. A higher weight indicates more DNS requests will be assigned.

topology: Specifies the static proximity algorithm, which assigns DNS requests to virtual servers based on static proximity entries.

bandwidth: Specifies the bandwidth algorithm, which assigns DNS requests to virtual servers based on the weight of the virtual servers and the remaining bandwidth.

max-bandwidth: Specifies the maximum bandwidth algorithm, which always assigns DNS requests to the virtual server corresponding to the idle link with the largest remaining bandwidth.

inbound: Selects a virtual server based on the inbound bandwidth.

outbound: Selects a virtual server based on the outbound bandwidth.

hash address: Specifies the hash algorithm based on the IP address.

source: Specifies the hash algorithm based on the source IP address.

source-ip-port: Specifies the hash algorithm based on the source IP address and port number.

destination: Specifies the hash algorithm based on the destination IP address.

mask *mask-length*: Specifies the mask length of the IPv4 address used in the hash algorithm. The value range for the *mask-length* argument is 0 to 32. The default is 32.

prefix *prefix-length*: Specifies the prefix length of the IPv6 address used in the hash algorithm. The value range for the *prefix-length* argument is 0 to 128. The default is 128.

Usage guidelines

If you do not specify the **inbound** or **outbound** keyword, the total bandwidth is used to select a virtual server.

In the bandwidth algorithm and maximum bandwidth algorithm, the remaining bandwidth is the maximum expected bandwidth minus the current bandwidth. If the maximum expected bandwidth is not configured, the remaining bandwidth is the maximum bandwidth of the link minus the current bandwidth.

Examples

Specify the preferred scheduling algorithm for the virtual server pool **local-pool** as **random**, and alternative scheduling algorithm as **least-connection**.

```
<Sysname> system-view
[Sysname] loadbalance virtual-server-pool local-pool
[Sysname-lb-vspool-local-pool] predictor preferred random
[Sysname-lb-vspool-local-pool] predictor alternate least-connection
```

Related commands

max-bandwidth (link view)

rate-limit bandwidth (link view)

prefer-method

Use **prefer-method** to specify the preferred compression algorithm.

Use **undo prefer-method** to restore the default.

Syntax

prefer-method { **deflate** | **gzip** }

undo prefer-method

Default

The preferred compression algorithm is **gzip**.

Views

HTTP-compression parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

deflate: Specifies the Deflate compression algorithm.

gzip: Specifies the default GNU zip compression algorithm.

Usage guidelines

If the client request supports the configured compression algorithm, the configured compression algorithm applies. If the client request does not support the configured compression algorithm, the compression algorithm contained in the request applies.

Examples

Create the HTTP-compression parameter profile **http1**, and specify the preferred compression algorithm as **deflate**.

```
<Sysname> system-view
[Sysname] parameter-profile http1 type http-compression
[Sysname-para-http-compression-http1] prefer-method deflate
```

primary-nameserver

Use **primary-nameserver** to configure the host name for the primary DNS server.

Use **undo primary-nameserver** to restore the default.

Syntax

primary-nameserver *host-name*

undo primary-nameserver

Default

No host name is configured for the primary DNS server.

Views

SOA view

Predefined user roles

network-admin

context-admin

Parameters

host-name: Specifies the host name for the primary DNS server, a case-insensitive and dot-separated string of up to 254 characters. The string can contain letters, digits, hyphens (-), underscores (_), and dots (.). Each dot-separated part can have a maximum of 63 characters.

Usage guidelines

The host name of the primary DNS server can be a relative domain name (does not end with a dot) or an absolute domain name (ends with a dot). For an absolute domain name, the host name is not automatically expanded and cannot exceed 254 characters. For a relative domain name, the current domain name is automatically appended to the host name. The host name plus the appended domain name cannot exceed 254 characters.

Examples

Configure the host name for the primary DNS server as **ns1.abc.com** for DNS forward zone **abc.com**.

```
<Sysname> system-view
[Sysname] loadbalance zone abc.com
[Sysname-lb-zone-abc.com] soa
[Sysname-lb-zone-abc.com-soa] primary-nameserver ns1.abc.com
```

Related commands

display loadbalance zone

priority (DNS server pool member view)

Use **priority** to set the priority of a DNS server pool member.

Use **undo priority** to restore the default.

Syntax

priority *priority*

undo priority

Default

The priority of a DNS server pool member is 4.

Views

DNS server pool member view

Predefined user roles

network-admin

context-admin

Parameters

priority: Specifies the priority value in the range of 1 to 8. A greater value means a higher priority.

Usage guidelines

Typically, only the members with the highest priority in a DNS server pool participate in scheduling. If the number of such members is smaller than the required minimum number, more members are selected by priority in descending order. If the allowed maximum number is exceeded after members with a certain priority are added, only some of the members with that priority are added.

Use this command together with the **selected-server** command in DNS server pool view.

Examples

Set the priority of DNS server pool member **ds1** to **3**.

```
<Sysname> system-view
[Sysname] loadbalance dns-server-pool dsp1
[Sysname-lb-dspool-dsp1] dns-server ds1 port 10
```

```
[Sysname-dspool-dsp1-#member#-ds1-port-10] priority 3
```

Related commands

selected-server (DNS server pool view)

priority (DNS server view)

Use **priority** to set the priority of a DNS server.

Use **undo priority** to restore the default.

Syntax

priority *priority*

undo priority

Default

The priority of a DNS server is 4.

Views

DNS server view

Predefined user roles

network-admin

context-admin

Parameters

priority: Specifies the priority value in the range of 1 to 8. A greater value means a higher priority.

Usage guidelines

Typically, only the DNS servers with the highest priority participate in scheduling. If the number of such DNS servers is smaller than the required minimum number, more DNS servers are selected by priority in descending order. If the allowed maximum number is exceeded after DNS servers with a certain priority are added, only some of the DNS servers with that priority are added.

Use this command together with the **selected-server** command in DNS server pool view.

Examples

Set the priority of DNS server **ds1** to **3**.

```
<Sysname> system-view
[Sysname] loadbalance dns-server ds1
[Sysname-lb-ds-ds1] priority 3
```

Related commands

selected-server (DNS server pool view)

priority (link group member view)

Use **priority** to set the priority of a link group member.

Use **undo priority** to restore the default.

Syntax

priority *priority*

undo priority

Default

The priority of a link group member is 4.

Views

Link group member view

Predefined user roles

network-admin

context-admin

Parameters

priority: Specifies the priority value in the range of 1 to 8. A greater value means a higher priority.

Usage guidelines

Typically, only the members with the highest priority in a link group participate in scheduling. If the number of such members is smaller than the required minimum number, more members are selected by priority in descending order. If the allowed maximum number is exceeded after members with a certain priority are added, only some of the members with that priority are added.

Use this command together with the **selected-server** command.

Examples

Set the priority of link group member **lk1** to **3**.

```
<Sysname> system-view
[Sysname] loadbalance link-group lg
[Sysname-lb-lgroup-lg] link lk1
[Sysname-lb-lgroup-lg-#member#-lk1] priority 3
```

Related commands

selected- link

priority (link view)

Use **priority** to set the priority of a link.

Use **undo priority** to restore the default.

Syntax

priority *priority*

undo priority

Default

The priority of a link is 4.

Views

Link view

Predefined user roles

network-admin

context-admin

Parameters

priority: Specifies the priority value in the range of 1 to 8. A greater value means a higher priority.

Usage guidelines

Typically only the links with the highest priority participate in scheduling. If the number of such links is smaller than the required minimum number, more links are selected by priority in descending order.

Examples

Set the priority of the link **lk1** to **3**.

```
<Sysname> system-view
[Sysname] loadbalance link lk1
[Sysname-lb-link-lk1] priority 3
```

Related commands

selected-link

priority (real server view)

Use **priority** to set the priority of a real server.

Use **undo priority** to restore the default.

Syntax

priority *priority*

undo priority

Default

The priority of a real server is 4.

Views

Real server view

Predefined user roles

network-admin

context-admin

Parameters

priority: Specifies the priority value of the real server, in the range of 1 to 8. A greater value means a higher priority to be referenced.

Usage guidelines

Typically only the real servers with the highest priority participate in scheduling. If the number of such real servers is smaller than the required minimum number, more real servers are selected by priority in descending order.

Examples

Set the priority of the real server **rs** to **3**.

```
<Sysname> system-view
[Sysname] real-server rs
[Sysname-rserver-rs] priority 3
```

Related commands

selected-server

priority (server farm member view)

Use **priority** to set the priority of a server farm member.

Use **undo priority** to restore the default.

Syntax

priority *priority*

undo priority

Default

The priority of a server farm member is 4.

Views

Server farm member view

Predefined user roles

network-admin

context-admin

Parameters

priority: Specifies the priority value in the range of 1 to 8. A greater value means a higher priority.

Usage guidelines

Typically, only the members with the highest priority in a server farm participate in scheduling. If the number of such members is smaller than the required minimum number, more members are selected by priority in descending order. If the allowed maximum number is exceeded after members with a certain priority are added, only some of the members with that priority are added.

Use this command together with the **selected-server** command in server farm view.

Examples

Set the priority of server farm member **rs1** to **3**.

```
<Sysname> system-view
[Sysname] server-farm sf
[Sysname-sfarm-sf] real-server rs1 port 80
[Sysname-sfarm-sf-#member#-rs1-port-80] priority 3
```

Related commands

selected-server (server farm view)

priority (SNAT global policy view)

Use **priority** to set the priority of a SNAT global policy.

Use **undo priority** to restore the default.

Syntax

priority *priority*

undo priority

Default

The priority of a SNAT global policy is 0.

Views

SNAT global policy view

Predefined user roles

network-admin

context-admin

Parameters

priority: Specifies the priority value in the range of 0 to 65535. A greater value means a higher priority.

Usage guidelines

You can configure multiple SNAT global policies with different priorities. They are matched in descending order of priority values.

Examples

Set the priority of SNAT global policy **sn1** to **100**.

```
<Sysname> system-view
[Sysname] loadbalance snat-global-policy sn1
[Sysname-lb-snat-gp-sn1] priority 100
```

probe (DNS server pool member view)

Use **probe** to specify a health monitoring method for a DNS server pool member.

Use **undo probe** to restore the default.

Syntax

probe *template-name*

undo probe *template-name*

Default

No health monitoring method is specified for a DNS server pool member.

Views

DNS server pool member view

Predefined user roles

network-admin

context-admin

Parameters

template-name: Specifies an NQA template by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

Use the **nqa template** command to create an NQA template to be referenced by the health monitoring method. The DNS server pool uses the parameters defined in the NQA template to detect the availability of the pool members.

The health monitoring method configuration in DNS server pool member view takes precedence over the configuration in DNS server pool view.

The health monitoring result for a DNS server affects the availability of a DNS server pool member. The health monitoring result for a DNS server pool member does not affect the availability of a DNS server.

Examples

Create the ICMP-type NQA template **t4**, and specify the health monitoring method for the DNS server pool member **ds1** as **t4**.

```
<Sysname> system-view
[Sysname] nqa template icmp t4
[Sysname-nqatplt-icmp-t4] quit
[Sysname] loadbalance dns-server-pool dsp1
[Sysname-lb-dspool-dsp1] dns-server ds1 port 10
[Sysname-lb-dspool-dsp1-#member#-ds1-port-10] probe t4
```

Related commands

nqa template (*Network Management and Monitoring Command Reference*)

success-criteria (DNS server pool member view)

probe (DNS server pool view)

Use **probe** to specify a health monitoring method for a DNS server pool.

Use **undo probe** to restore the default.

Syntax

probe *template-name*

undo probe *template-name*

Default

No health monitoring method is specified for a DNS server pool.

Views

DNS server pool view

Predefined user roles

network-admin

context-admin

Parameters

template-name: Specifies an NQA template by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

Use the **nqa template** command to create an NQA template to be referenced by the health monitoring method. The DNS server pool uses the parameters defined in the NQA template to detect the availability of DNS servers.

The health monitoring method configuration in DNS server view takes precedence over the configuration in DNS server pool view.

Examples

Create the ICMP-type NQA template **t4**, and specify the health monitoring method for the DNS server pool **dns-pool** as **t4**.

```
<Sysname> system-view
```

```
[Sysname] nqa template icmp t4
[Sysname-nqatplt-icmp-t4] quit
[Sysname] loadbalance dns-server-pool dns-pool
[Sysname-lb-dspool-dns-pool] probe t4
```

Related commands

nqa template (*Network Management and Monitoring Command Reference*)

success-criteria (DNS server pool view)

probe (DNS server view)

Use **probe** to specify a health monitoring method for a DNS server.

Use **undo probe** to restore the default.

Syntax

probe *template-name*

undo probe *template-name*

Default

No health monitoring method is specified for a DNS server.

Views

DNS server view

Predefined user roles

network-admin

context-admin

Parameters

template-name: Specifies an NQA template by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

Use the **nqa template** command to create an NQA template to be referenced by the health monitoring method.

The health monitoring method configuration in DNS server view takes precedence over the configuration in DNS server pool view.

Examples

Create the ICMP-type NQA template **t4**, and specify the health monitoring method for DNS server **ds1** as **t4**.

```
<Sysname> system-view
[Sysname] nqa template icmp t4
[Sysname-nqatplt-icmp-t4] quit
[Sysname] loadbalance dns-server ds1
[Sysname-lb-ds-ds1] probe t4
```

Related commands

nqa template (*Network Management and Monitoring Command Reference*)

success-criteria (DNS server view)

probe (link group member view)

Use **probe** to specify a health monitoring method for a link group member.

Use **undo probe** to restore the default.

Syntax

probe *template-name*

undo probe *template-name*

Default

No health monitoring method is specified for a link group member.

Views

Link group member view

Predefined user roles

network-admin

context-admin

Parameters

template-name: Specifies an NQA template by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

Use the **nqa template** command to create an NQA template to be referenced by the health monitoring method. The link group uses the parameters defined in the NQA template to detect the availability of the link group members.

The health monitoring method configuration in link group member view takes precedence over the configuration in link group view.

The health monitoring result for a link affects the availability of a link group member. The health monitoring result for a link group member does not affect the availability of a link.

Examples

Create the ICMP-type NQA template **t4**, and specify the health monitoring method for the link group member **lk1** as **t4**.

```
<Sysname> system-view
[Sysname] nqa template icmp t4
[Sysname-nqatplt-icmp-t4] quit
[Sysname] loadbalance link-group lg
[Sysname-lb-lgroup-lg] link lk1
[Sysname-lb-lgroup-lg-#member#-lk1] probe t4
```

Related commands

nqa template (*Network Management and Monitoring Command Reference*)

success-criteria (link group member view)

probe (link group view)

Use **probe** to specify a health monitoring method for a link group.

Use **undo probe** to restore the default.

Syntax

probe *template-name*

undo probe *template-name*

Default

No health monitoring method is specified for a link group.

Views

Link group view

Predefined user roles

network-admin

context-admin

Parameters

template-name: Specifies an NQA template by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

The link group uses the parameters defined in the NQA template to detect the availability of links.

The health monitoring method configuration in link view takes precedence over the configuration in link group view.

Examples

Create the ICMP-type NQA template **t4**, and specify the health monitoring method for the link group **lg** as **t4**.

```
<Sysname> system-view
[Sysname] nqa template icmp t4
[Sysname-nqatplt-icmp-t4] quit
[Sysname] loadbalance link-group lg
[Sysname-lb-lgroup-lg] probe t4
```

Related commands

nqa template (*Network Management and Monitoring Command Reference*)

success-criteria (link group view)

probe (link view)

Use **probe** to specify a health monitoring method for an LB link.

Use **undo probe** to restore the default.

Syntax

probe *template-name*

undo probe *template-name*

Default

No health monitoring method is specified for an LB link.

Views

Link view

Predefined user roles

network-admin

context-admin

Parameters

template-name: Specifies an NQA template by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

Use the **nqa template** command to create an NQA template to be referenced by the health monitoring method.

You can configure multiple health monitoring methods for an LB link. By default, health monitoring succeeds only when all the specified health monitoring methods succeed. You can use the **success-criteria** command to specify the health monitoring success criteria for the LB link.

Examples

Create the ICMP-type NQA template **t4**, and specify the health monitoring method for the LB link **lk1** as **t4**.

```
<Sysname> system-view
[Sysname] nqa template icmp t4
[Sysname-nqatplt-icmp-t4] quit
[Sysname] loadbalance link lk1
[Sysname-lb-link-lk1] probe t4
```

Related commands

nqa template (*Network Management and Monitoring Command Reference*)

success-criteria (link view)

probe (real server view)

Use **probe** to specify a health monitoring method for a real server.

Use **undo probe** to restore the default.

Syntax

probe *template-name* [**nqa-template-port**]

undo probe *template-name*

Default

No health monitoring method is specified for a real server.

Views

Real server view

Predefined user roles

network-admin

context-admin

Parameters

template-name: Specifies an NQA template by its name, a case-insensitive string of 1 to 32 characters.

nqa-template-port: Uses the destination port number specified in the NQA template for detection. If you do not specify this keyword, the real server's port number is used for detection.

Usage guidelines

Use the **nqa template** command to create an NQA template to be referenced by the health monitoring method.

The health monitoring method configuration in real server view takes precedence over the configuration in server farm view.

Examples

Create the ICMP-type NQA template **t4**, and specify the health monitoring method for the real server **rs** as **t4**.

```
<Sysname> system-view
[Sysname] nqa template icmp t4
[Sysname-nqatplt-icmp-t4] quit
[Sysname] real-server rs
[Sysname-rserver-rs] probe t4
```

Related commands

nqa template (*Network Management and Monitoring Command Reference*)

success-criteria (real server view)

probe (server farm member view)

Use **probe** to specify a health monitoring method for a server farm member.

Use **undo probe** to restore the default.

Syntax

probe *template-name* [**nqa-template-port**]

undo probe *template-name*

Default

No health monitoring method is specified for a server farm member.

Views

Server farm member view

Predefined user roles

network-admin

context-admin

Parameters

template-name: Specifies an NQA template by its name, a case-insensitive string of 1 to 32 characters.

nqa-template-port: Uses the destination port number specified in the NQA template for detection. If you do not specify this keyword, the server farm member's port number is used for detection.

Usage guidelines

Use the **nqa template** command to create an NQA template to be referenced by the health monitoring method. The server farm uses the parameters defined in the NQA template to detect the availability of the server farm members.

The health monitoring method configuration in server farm member view takes precedence over the configuration in server farm view.

The health monitoring result for a real server affects the availability of a server farm member. The health monitoring result for a server farm member does not affect the availability of a real server.

Examples

Create the ICMP-type NQA template **t4**, and specify the health monitoring method for the server farm member **rs1** as **t4**.

```
<Sysname> system-view
[Sysname] nqa template icmp t4
[Sysname-nqatplt-icmp-t4] quit
[Sysname] server-farm sf
[Sysname-sfarm-sf] real-server rs1 port 80
[Sysname-sfarm-sf-#member#-rs1-port-80] probe t4
```

Related commands

nqa template (*Network Management and Monitoring Command Reference*)

success-criteria (server farm member view)

probe (server farm view)

Use **probe** to specify a health monitoring method for a server farm.

Use **undo probe** to delete a health monitoring method from a server farm.

Syntax

probe *template-name* [**nqa-template-port**]

undo probe *template-name*

Default

No health monitoring method is specified for a server farm.

Views

Server farm view

Predefined user roles

network-admin

context-admin

Parameters

template-name: Specifies an NQA template by its name, a case-insensitive string of 1 to 32 characters.

nqa-template-port: Uses the destination port number specified in the NQA template for detection. If you do not specify this keyword, the real server's port number is used for detection.

Usage guidelines

Use the **nqa template** command to create an NQA template to be referenced by the health monitoring method.

The health monitoring method configuration in real server view takes precedence over the configuration in server farm view.

Examples

Create the ICMP-type NQA template **t4**, and specify the health monitoring method for the server farm **sf** as **t4**.

```
<Sysname>system-view
[Sysname] nqa template icmp t4
[Sysname-nqatplt-icmp-t4] quit
[Sysname] server-farm sf
[Sysname-sfarm-sf] probe t4
```

Related commands

nqa template (*Network Management and Monitoring Command Reference*)

success-criteria (server farm view)

probe-template (real server view)

Use **probe-template** to specify a custom-monitoring LB probe template for a real server.

Use **undo probe-template** to remove a custom-monitoring LB probe template from a real server.

Syntax

probe-template external-monitor *template-name*

undo probe-template external-monitor *template-name*

Default

No custom-monitoring LB probe template is specified for a real server.

Views

Real server view

Predefined user roles

network-admin

context-admin

Parameters

template-name: Specifies a custom-monitoring template by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

This command can monitor a real sever by referencing a custom-monitoring LB probe template.

The monitoring result of a real server affects the availability of a server farm member, but the monitoring result of a server farm member does not affect the availability of a real server.

Examples

Specify custom-monitoring LB probe template **test_external** for real server **rs**.

```
<Sysname>system-view
[Sysname] real-server rs
[Sysname-rserver-rs] probe-template external-monitor test_external
```

Related commands

loadbalance probe-template

probe-template (server farm member view)

Use **probe-template** to specify a custom-monitoring probe template for a server farm member.

Use **undo probe-template** to remove a custom-monitoring LB probe template from a server farm member.

Syntax

probe-template external-monitor *template-name*

undo probe-template external-monitor *template-name*

Default

No custom-monitoring probe template is specified for a server farm member.

Views

Server farm member view

Predefined user roles

network-admin

context-admin

Parameters

template-name: Specifies a custom-monitoring template by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

This command can monitor a sever farm member by referencing a custom-monitoring LB probe template.

You can configure this command for all server farm members in server farm view or for a single server farm member in server farm member view. If you configure this command in both server farm view and server farm member view, the configuration in server farm member view takes effect.

The monitoring result of a real server affects the availability of a server farm member, but the monitoring result of a server farm member does not affect the availability of a real server.

Examples

Specify custom-monitoring LB probe template **test_external** for server farm member **rs1**.

```
<Sysname> system-view
[Sysname] server-farm sf
[Sysname-sfarm-sf] real-server rs1 port 80
[Sysname-sfarm-sf-#member#-rs1-port-80] probe-template external-monitor test_external
```

Related commands

loadbalance probe-template

probe-template (server farm view)

Use **probe-template** to specify an LB probe template for a server farm.

Use **undo probe-template** to remove an LB probe template for a server farm.

Syntax

probe-template { **external-monitor** | **http-passive** | **tcp-rst** | **tcp-zero-window** } *template-name*

undo probe-template { **external-monitor** | **http-passive** | **tcp-rst** | **tcp-zero-window** }

Default

No LB probe template is specified for a server farm.

Views

Server farm view

Predefined user roles

network-admin

context-admin

Parameters

external-monitor: Specifies a custom-monitoring LB probe template.

http-passive: Specifies an HTTP passive LB probe template.

tcp-rst: Specifies a TCP-RST LB probe template.

tcp-zero-window: Specifies a TCP zero-window LB probe template.

template-name: Specifies the template name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

This command can monitor all real severs in a server farm.

A server farm can reference only one HTTP passive LB probe template, one TCP-RST LB probe template, and one TCP zero-window LB probe template at the same time.

You can specify multiple custom-monitoring LB probe templates for a server farm.

Examples

Specify TCP-RST LB probe template **r1** for server farm **sf**.

```
<Sysname>system-view
[Sysname] server-farm sf
[Sysname-sfarm-sf] probe-template tcp-rst r1
```

Related commands

loadbalance probe-template

probe log enable (real server view)

Use **probe log enable** to enable health monitoring logging for a real server.

Use **undo probe log enable** to disable health monitoring logging for a real server.

Syntax

probe log enable

undo probe log enable

Default

Health monitoring logging is enabled for a real server.

Views

Real server view

Predefined user roles

network-admin

context-admin

Usage guidelines

This feature generates logs when the health of a real server changes.

Examples

Enable health monitoring logging for real server **rs**.

```
<Sysname>system-view
[Sysname] real-server rs
[Sysname-rserver-rs] probe log enable
```

probe log enable (server farm member view)

Use **probe log enable** to enable health monitoring logging for a server farm member.

Use **undo probe log enable** to disable health monitoring logging for a server farm member.

Syntax

probe log enable

undo probe log enable

Default

Health monitoring logging is enabled for a server farm member.

Views

Server farm member view

Predefined user roles

network-admin

context-admin

Usage guidelines

This feature generates logs when the health of a server farm member changes.

Examples

Enable health monitoring logging for server farm member **rs1**.

```
<Sysname> system-view
[Sysname] server-farm sf
[Sysname-sfarm-sf] real-server rs1 port 80
[Sysname-sfarm-sf-#member#-rs1-port-80] probe log enable
```

protect-action

Use **protect-action** to configure the protection action for an LB probe template.

Use **undo protect-action** to restore the default.

Syntax

protect-action { **auto-shutdown** | **busy** [**probe-interval** *interval*] [**probe-times** *times*] }

undo protect-action

Default

The protection action is to place a real server in busy state.

Views

TCP-RST LB probe template view

TCP zero-window LB probe template view

Predefined user roles

network-admin

context-admin

context-admin

Parameters

auto-shutdown: Automatically shuts down a real server.

busy: Places a real server in busy state.

probe-interval *interval*: Specifies the interval for probing the real server in busy state, in the range of 5 to 3600 seconds. The default is 30 seconds.

probe-times *times*: Specifies the maximum number of times for probing the real server in busy state, in the range of 0 to 255. The default is 0, which means that the number of probe times is not limited.

Usage guidelines

For the **busy** action, after placing a real server in busy state, the device starts probing the real server at the specified probe intervals. If the number of RST or zero-window packets sent does not reach the threshold in a probe interval, the real server is placed back in normal state. If threshold violation persists when the maximum probe times is reached, the system automatically shuts down the real server.

A real server that is shut down due to packet threshold violation or exceeded probe times will be restored to normal state immediately when the specified LB probe template is deleted.

If a real server is shut down due to packet threshold violation or exceeded probe times, you can restore the normal state of the real server as follows:

- Execute the **auto-shutdown recovery-time** command. The real server will be restored to normal state when the automatic recovery timer expires.
- Execute the **recover-from-auto-shutdown** command in real server view to restore the real server to normal state immediately.

Examples

In TCP-RST LB probe template **rsttplt**, configure the protection action as **busy**, set the probe interval to 30 seconds, and set the probe times to 3.

```
<Sysname>system-view
[Sysname] loadbalance probe-template tcp-rst rsttplt
[Sysname-lbpt-tcp-rst-rsttplt] protect-action busy probe-interval 30 probe-times 3
```

Related commands

auto-shutdown recovery-time

recover-from-auto-shutdown (real server view)

protected-url

Use **protected-url** to configure the URLs to be protected.

Use **undo protected-url** to remove all protected URLs.

Syntax

protected-url *url*

undo protected-url

Default

No URLs are protected.

Views

Protection rule view

Predefined user roles

network-admin

context-admin

Parameters

url: Specifies a regular expression to match URLs, a case-sensitive string of 1 to 255 characters. The regular expression cannot contain question marks (?).

Usage guidelines

If the number of times that a user accesses a protected URL exceeds the request threshold during the protection period, the protection action is taken.

The device does not match the parameters in a URL and matches only the portion before the question mark (?).

If you execute this command multiple times, the most recent configuration takes effect.

Examples

In protection rule 5, configure www.aaa.com/index.html as a protected URL.

```
<Sysname>system-view
[Sysname] loadbalance protection-policy p1
[Sysname-lbpp-http-p1] rule 5
[Sysname-lbpp-http-p1-rule-5] protected-url www.aaa.com/index.html
```

Related commands

cookie (protection policy view)

protection-action

protection-period

source-ip

protection-action

Use **protection-action** to configure a protection action.

Use **undo protection-action** to restore the default.

Syntax

protection-action { **warning** | { **drop** | **verify** { **insert-header** | **js** } } } *

undo protection-action

Default

No protection action is configured.

Views

HTTP protection policy view

Predefined user roles

network-admin

context-admin

Parameters

warning: Generates a log message.

drop: Drops requests.

verify: Performs cookie verification on subsequent requests.

insert-header: Performs cookie verification by inserting an HTTP header.

js: Performs cookie verification by inserting a JS script.

Usage guidelines

The protection action is taken when protection rules in a protection policy are matched. The device supports the following protection actions:

- **Warning**—Generates a log message and sends it to the information center.
- **Drop**—Drops requests.
- **Verify cookie**—Returns a response carrying a cookie value to the client. If a subsequent request carries the returned cookie value, it passes the verification. If a subsequent request does not carry a cookie value or carries a different cookie value, it fails to pass the verification and is dropped. This protection action is useful in scenarios where attackers cannot insert cookie values into attack packets. The device supports returning a cookie value by inserting an HTTP header or a JS script.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

In HTTP protection policy **p1**, configure generating log messages and performing cookie verification by inserting an HTTP header as the protection actions.

```
<Sysname> system-view
[Sysname] loadbalance protection-policy p1 type http
[Sysname-lbpp-http-p1] protection-action warning verify insert-header
```

protection-period

Use **protection-period** to set the protection period.

Use **undo protection-period** to restore the default.

Syntax

protection-period *period*

undo protection-period

Default

The protection period is 120 seconds.

Views

Protection rule view

Predefined user roles

network-admin

context-admin

Parameters

period: Specifies a protection period in the range of 1 to 900 seconds.

Usage guidelines

If the number of times that a user accesses a protected URL exceeds the request threshold during the protection period, the protection action is taken.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

In protection rule 5, set the protection period to 5 seconds.

```
<Sysname> system-view
[Sysname] loadbalance protection-policy p1
[Sysname-lbpp-http-p1] rule 5
[Sysname-lbpp-http-p1-rule-5] protection-period 5
```

Related commands

protected-url

protection-action

protection-policy

Use **protection-policy** to specify a protection policy for a virtual server.

Use **undo protection-policy** to restore the default.

Syntax

protection-policy http *policy-name*

undo protection-policy http

Default

No protection policy is specified for a virtual server.

Views

HTTP virtual server view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies a protection policy by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

The protection policy specified for a virtual server protects the traffic matching the virtual server.

Examples

Specify protection policy **p1** for HTTP virtual server **vs**.

```
<Sysname> system-view
```

```
[Sysname] virtual-server vs type http
[Sysname-vs-http-vs]protection-policy http p1
```

Related commands

loadbalance protection-policy

proximity enable (link group view)

Use **proximity enable** to enable the proximity feature for a link group.

Use **undo proximity enable** to disable the proximity feature for a link group.

Syntax

proximity enable

undo proximity enable

Default

The proximity feature is disabled for a link group.

Views

Link group view

Predefined user roles

network-admin

context-admin

Usage guidelines

The proximity feature takes precedence over the scheduling algorithm in selecting a link. If no link is selected according to the proximity feature, the scheduling algorithm is used.

Examples

Enable the proximity feature for the link group **lg**.

```
<Sysname> system-view
[Sysname] loadbalance link-group lg
[Sysname-lb-lgroup-lg] proximity enable
```

Related commands

predictor (link group view)

proximity enable (server farm view)

Use **proximity enable** to enable the proximity feature for a server farm.

Use **undo proximity enable** to disable the proximity feature for a server farm.

Syntax

proximity enable

undo proximity enable

Default

The proximity feature is disabled for a server farm.

Views

Server farm view

Predefined user roles

network-admin

context-admin

Usage guidelines

The proximity feature takes precedence over the scheduling algorithm in selecting a real server. If no real server is selected according to the proximity feature, the scheduling algorithm is used.

Examples

Enable the proximity feature for the server farm **sf**.

```
<Sysname> system-view
[Sysname] server-farm sf
[Sysname-sfarm-sf] proximity enable
```

radius-attribute

Use **radius-attribute** to configure the RADIUS attribute sticky method.

Use **undo radius-attribute** to delete the RADIUS attribute sticky method.

Syntax

radius-attribute { **code** *attribute-code* | **framed-ip-address** | **user-name** }

undo radius-attribute

Default

No RADIUS sticky methods exist.

Views

RADIUS sticky group view

Predefined user roles

network-admin

context-admin

Parameters

code *attribute-code*: Specifies the code of the RADIUS attribute type, in the range of 1 to 255.

framed-ip-address: Specifies the RADIUS attribute type as **framed-ip-address** (code 8).

user-name: Specifies the RADIUS attribute type as **user-name** (code 1).

Usage guidelines

The RADIUS attribute sticky method takes effect only on RADIUS packets.

Examples

Configure the RADIUS attribute sticky method for sticky group **s1** by specifying the RADIUS attribute type as **user-name**.

```
<Sysname> system-view
[Sysname] sticky-group s1 type radius
[Sysname-sticky-radius-s1] radius-attribute user-name
```

rate-limit bandwidth (link view)

Use **rate-limit bandwidth** to set the maximum bandwidth of a link.

Use **undo rate-limit bandwidth** to restore the default.

Syntax

rate-limit bandwidth [**inbound** | **outbound**] *bandwidth-value* **kbps**

undo rate-limit bandwidth [**inbound** | **outbound**]

Default

The maximum bandwidth of a link is not limited.

Views

Link view

Predefined user roles

network-admin

context-admin

Parameters

inbound: Specifies the maximum inbound bandwidth.

outbound: Specifies the maximum outbound bandwidth.

bandwidth-value: Specifies the maximum bandwidth in the range of 0 to 4294967295. The value 0 means the bandwidth is not limited.

kbps: Specifies the bandwidth unit as kbps.

Usage guidelines

If you do not specify the **inbound** or **outbound** keyword, the maximum bandwidth equals the inbound bandwidth plus the outbound bandwidth.

This command takes effect only on new sessions and does not take effect on existing sessions.

Examples

Set the maximum bandwidth of the link **lk1** to 1 kbps.

```
<Sysname> system-view
[Sysname] loadbalance link lk1
[Sysname-lb-link-lk1] rate-limit bandwidth 1 kbps
```

Set the maximum inbound bandwidth of the link **lk1** to 1 kbps.

```
<Sysname> system-view
[Sysname] loadbalance link lk1
[Sysname-lb-link-lk1] rate-limit bandwidth inbound 1 kbps
```

Set the maximum outbound bandwidth of the link **lk1** to 1 kbps.

```
<Sysname> system-view
[Sysname] loadbalance link lk1
[Sysname-lb-link-lk1] rate-limit bandwidth outbound 1 kbps
```

rate-limit bandwidth (real server view)

Use **rate-limit bandwidth** to set the maximum bandwidth of a real server.

Use **undo rate-limit bandwidth** to restore the default.

Syntax

rate-limit bandwidth [**inbound** | **outbound**] *bandwidth-value* **kbps**

undo rate-limit bandwidth [**inbound** | **outbound**]

Default

The maximum bandwidth of a real server is not limited.

Views

Real server view

Predefined user roles

network-admin

context-admin

Parameters

inbound: Specifies the maximum inbound bandwidth.

outbound: Specifies the maximum outbound bandwidth.

bandwidth-value: Specifies the maximum bandwidth in the range of 0 to 4294967295. The value 0 means the bandwidth is not limited.

kbps: Specifies the bandwidth unit as kbps.

Usage guidelines

If you do not specify the **inbound** or **outbound** keyword, the maximum bandwidth equals the inbound bandwidth plus the outbound bandwidth.

This command takes effect only on new sessions and does not take effect on existing sessions.

Examples

Set the maximum bandwidth of the real server **rs** to 1 kbps.

```
<Sysname> system-view
[Sysname] real-server rs
[Sysname-rserver-rs] rate-limit bandwidth 1 kbps
```

Set the maximum inbound bandwidth of the real server **rs** to 1 kbps.

```
<Sysname> system-view
[Sysname] real-server rs
[Sysname-rserver-rs] rate-limit bandwidth inbound 1 kbps
```

Set the maximum outbound bandwidth of the real server **rs** to 1 kbps.

```
<Sysname> system-view
[Sysname] real-server rs
[Sysname-rserver-rs] rate-limit bandwidth outbound 1 kbps
```

rate-limit bandwidth (virtual server view)

Use **rate-limit bandwidth** to set the maximum bandwidth of a virtual server.

Use **undo rate-limit bandwidth** to restore the default.

Syntax

rate-limit bandwidth [**inbound** | **outbound**] *bandwidth-value* **kbps**

undo rate-limit bandwidth [**inbound** | **outbound**]

Default

The maximum bandwidth of a virtual server is not limited.

Views

Virtual server view

Predefined user roles

network-admin

context-admin

Parameters

inbound: Specifies the maximum inbound bandwidth.

outbound: Specifies the maximum outbound bandwidth.

bandwidth-value: Specifies the maximum bandwidth in the range of 0 to 4294967295. The value 0 means the bandwidth is not limited.

kbps: Specifies the bandwidth unit as kbps.

Usage guidelines

If you do not specify the **inbound** or **outbound** keyword, the maximum bandwidth equals the inbound bandwidth plus the outbound bandwidth.

Examples

Set the maximum bandwidth of the IP-type virtual server **vs3** to 1 kbps.

```
<Sysname> system-view
[Sysname] virtual-server vs3 type ip
[Sysname-vs-ip-vs3] rate-limit bandwidth 1 kbps
```

Set the maximum inbound bandwidth of the IP-type virtual server **vs3** to 1 kbps.

```
<Sysname> system-view
[Sysname] virtual-server vs3 type ip
[Sysname-vs-ip-vs3] rate-limit bandwidth inbound 1 kbps
```

Set the maximum outbound bandwidth of the IP-type virtual server **vs3** to 1 kbps.

```
<Sysname> system-view
[Sysname] virtual-server vs3 type ip
[Sysname-vs-ip-vs3] rate-limit bandwidth outbound 1 kbps
```

rate-limit connection (link group member view)

Use **rate-limit connection** to set the maximum number of connections per second of a link group member.

Use **undo rate-limit connection** to restore the default.

Syntax

rate-limit connection *connection-number*

undo rate-limit connection

Default

The maximum number of connections per second of a link group member is 0.

Views

Link group member view

Predefined user roles

network-admin

context-admin

Parameters

connection-number: Specifies the maximum number of connections per second in the range of 0 to 4294967295. 0 means the number is not limited.

Examples

Set the maximum number of connections per second of the link group member **lk1** to 1000.

```
<Sysname> system-view
[Sysname] loadbalance link-group lg
[Sysname-lb-lgroup-lg] link lk1
[Sysname-lb-lgroup-lg-#member#-lk1] rate-limit connection 1000
```

rate-limit connection (link view)

Use **rate-limit connection** to set the maximum number of connections per second of a link.

Use **undo rate-limit connection** to restore the default.

Syntax

rate-limit connection *connection-number*

undo rate-limit connection

Default

The maximum number of connections per second of a link is 0.

Views

Link view

Predefined user roles

network-admin

context-admin

Parameters

connection-number: Specifies the maximum number of connections per second in the range of 0 to 4294967295. 0 means the number is not limited.

Usage guidelines

This command takes effect only on new sessions and does not take effect on existing sessions.

Examples

Set the maximum number of connections per second of the link **lk1** to 10000.

```
<Sysname> system-view
[Sysname] loadbalance link lk1
[Sysname-lb-link-lk1] rate-limit connection 10000
```

rate-limit connection (real server view)

Use **rate-limit connection** to set the maximum number of connections per second of a real server.

Use **undo rate-limit connection** to restore the default.

Syntax

rate-limit connection *connection-number*

undo rate-limit connection

Default

The maximum number of connections per second of a real server is 0.

Views

Real server view

Predefined user roles

network-admin

context-admin

Parameters

connection-number: Specifies the maximum number of connections per second in the range of 0 to 4294967295. 0 means the number is not limited.

Usage guidelines

This command takes effect only on new sessions and does not take effect on existing sessions.

Examples

Set the maximum number of connections per second of the real server **rs** to 10000.

```
<Sysname> system-view
[Sysname] real-server rs
[Sysname-rserver-rs] rate-limit connection 10000
```

rate-limit connection (server farm member view)

Use **rate-limit connection** to set the maximum number of connections per second of a server farm member.

Use **undo rate-limit connection** to restore the default.

Syntax

rate-limit connection *connection-number*

undo rate-limit connection

Default

The maximum number of connections per second of a server farm member is 0.

Views

Server farm member view

Predefined user roles

network-admin

context-admin

Parameters

connection-number: Specifies the maximum number of connections per second in the range of 0 to 4294967295. 0 means the number is not limited.

Examples

Set the maximum number of connections per second of the server farm member **rs1** to 1000.

```
<Sysname> system-view
[Sysname] server-farm sf
[Sysname-sfarm-sf] real-server rs1 port 80
[Sysname-sfarm-sf-#member#-rs1-port-80] rate-limit connection 1000
```

rate-limit connection (virtual server view)

Use **rate-limit connection** to set the maximum number of connections per second of a virtual server.

Use **undo rate-limit connection** to restore the default.

Syntax

rate-limit connection *connection-number*

undo rate-limit connection

Default

The maximum number of connections per second of a virtual server is 0.

Views

Virtual server view

Predefined user roles

network-admin

context-admin

Parameters

connection-number: Specifies the maximum number of connections per second in the range of 0 to 4294967295. 0 means the number is not limited.

Examples

Set the maximum number of connections per second of the IP-type virtual server **vs3** to 10000.

```
<Sysname> system-view
[Sysname] virtual-server vs3 type ip
[Sysname-vs-ip-vs3] rate-limit connection 10000
```

rate-limit http-request (real server view)

Use **rate-limit http-request** to set the maximum number of HTTP requests per second for a real server.

Use **undo rate-limit http-request** to restore the default.

Syntax

rate-limit http-request *request-number*

undo rate-limit http-request

Default

The maximum number of HTTP requests per second is 0 for a real server.

Views

Real server view

Predefined user roles

network-admin

context-admin

Parameters

request-number: Specifies the maximum number of HTTP requests per second, in the range of 0 to 4294967295. 0 means the number is not limited.

Examples

Set the maximum number of HTTP requests per second to 10000 for real server **rs**.

```
<Sysname> system-view
[Sysname] real-server rs
[Sysname-rserver-rs] rate-limit http-request 10000
```

rate-limit http-request (server farm member view)

Use **rate-limit http-request** to set the maximum number of HTTP requests per second for a server farm member.

Use **undo rate-limit http-request** to restore the default.

Syntax

rate-limit http-request *request-number*

undo rate-limit http-request

Default

The maximum number of HTTP requests per second is 0 for a server farm member.

Views

Server farm member view

Predefined user roles

network-admin

context-admin

Parameters

request-number: Specifies the maximum number of HTTP requests per second, in the range of 0 to 4294967295. 0 means the number is not limited.

Examples

Set the maximum number of HTTP requests per second to 10000 for server farm member **rs**.

```
<Sysname> system-view
[Sysname] server-farm sf
[Sysname-sfarm-sf] real-server rs1 port 80
[Sysname-sfarm-sf-#member#-rs1-port-80] rate-limit http-request 10000
```

readwrite-separation

Use **readwrite-separation** to enable read/write separation for the MySQL database.

Use **undo readwrite-separation** to disable read/write separation for the MySQL database.

Syntax

readwirte-separation read-server-farm *read-server-farm-name* [**read-sticky-group** *read-sticky-group-name*] **write-server-farm** *write-sever-farm-name* [**write-sticky-group** *write-sticky-group-name*]

undo readwrite-separation

Default

Read/write separation is disabled for the MySQL database.

Views

MySQL virtual server view

Predefined user roles

network-admin

context-admin

Parameters

read-server-farm *read-server-farm-name*: Specifies a read server farm by its name, a case-insensitive string of 1 to 63 characters.

read-sticky *read-sticky-group-name*: Specifies a sticky group for the read server farm by its name, a case-insensitive string of 1 to 63 characters.

write-server-farm *write-server-farm-name*: Specifies a write server farm by its name, a case-insensitive string of 1 to 63 characters.

write-sticky *write-sticky-group-name*: Specifies a sticky group for the write server farm by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

Read/write separation allows read commands and write commands to be executed by the read server farm and write server farm, respectively, which helps reduce the impact of concurrent read/write requests on database performance.

Examples

Enable read/write separation for the MySQL database of MySQL virtual server **vs1**.

```
<Sysname> system-view
[Sysname] virtual-server vs1 type mysql
[Sysname-vs-mysql-vs1] readwrite-separation read-server-farm rd write-server-farm wr
```

real-server (server farm view)

Use **real-server** to create a server farm member and enter its view, or enter the view of an existing server farm member.

Use **undo real-server** to delete a server farm member.

Syntax

real-server *real-server-name* **port** *port-number*

undo real-server *real-server-name* **port** *port-number*

Default

No server farm members exist.

Views

Server farm view

Predefined user roles

network-admin

context-admin

Parameters

real-server-name: Specifies a server farm member by its name, a case-insensitive string of 1 to 63 characters.

port-number: Specifies the port number of the server farm member, in the range of 0 to 65535.

Usage guidelines

You can use one of the following methods to add a member to a server farm:

- Use the **real-server** command in server farm view. NSFOCUS recommends using this method.
- Use the **server-farm** command in real server view.

You cannot use both methods to add a member with the same real server name and port number to a server farm.

Examples

Add server farm member **rs1** and enter server farm member view.

```
<Sysname> system-view
[Sysname] server-farm sf
[Sysname-sfarm-sf] real-server rs1 port 80
[Sysname-sfarm-sf-#member#-rs1-port-80]
```

Related commands

server-farm (real server view)

real-server (system view)

Use **real-server** to create a real server and enter its view, or enter the view of an existing real server.

Use **undo real-server** to delete the specified real server.

Syntax

real-server *real-server-name*

undo real-server *real-server-name*

Default

No real servers exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

real-server-name: Specifies the real server name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

You can configure this command only if the device has licenses installed. For information about licensing, see license management in *Fundamentals Configuration Guide*.

Examples

Create real server **rs** and enter real server view.

```
<Sysname> system-view
[Sysname] real-server rs
[Sysname-rserver-rs]
```

rebalance per-request

Use **rebalance per-request** to enable load balancing for each HTTP request.

Use **undo rebalance per-request** to restore the default.

Syntax

rebalance per-request

undo rebalance per-request

Default

Load balancing applies to the first HTTP request of a connection. Other HTTP requests are processed in the same way.

Views

HTTP parameter profile view

Predefined user roles

network-admin

context-admin

Examples

Enable load balancing for each HTTP request in the HTTP parameter profile **pp1**.

```
<Sysname> system-view
[Sysname] parameter-profile pp1 type http
[Sysname-para-http-pp1] rebalance per-request
```

record

Use **record** to configure a resource record of the specified type.

Use **undo record** to delete a resource record of the specified type.

Syntax

record { **cname alias** *alias-name* **canonical** *canonical-name* | **mx** [**host** *hostname*] **exchanger** *exchanger-name* **preference** *preference* | **ns** [**sub** *subname*] **authority** *ns-name* | **srv** [**service** *service-name*] **host-offering-service** *hostname* **priority** *priority* **weight** *weight* **port** *port-number* | **txt** [**sub** *subname*] **describe-txt** *description* } [**ttl** *ttl-value*]

undo record { **cname alias** *alias-name* **canonical** *canonical-name* | **mx** [**host** *hostname*] **exchanger** *exchanger-name* | **ns** [**sub** *subname*] **authority** *ns-name* }

| **srv** [**service** *hostname*] **host-offering-service** *hostname* **port** *port-number*
| **txt** [**sub** *subname*] **describe-txt** *description*

Default

No resource records exist.

Views

DNS forward zone view

Predefined user roles

network-admin

context-admin

Parameters

cname: Configures a canonical name (CNAME) resource record.

alias *alias-name*: Specifies an alias for a host name, a case-insensitive, dot-separated string that contains a maximum of 254 characters. The string can contain letters, digits, hyphens (-), underscores (_), and dots (.). Each dot-separated part can have a maximum of 63 characters.

canonical *canonical-name*: Specifies the host name, a case-insensitive, dot-separated string that contains a maximum 254 characters. The string can contain letters, digits, hyphens (-), underscores (_), and dots (.). Each dot-separated part can have a maximum of 63 characters.

mx: Configures a mail exchanger (MX) resource record.

host *hostname*: Specifies the host name for the MX resource record, a case-insensitive, dot-separated string that contains a maximum 254 characters. The string can contain letters, digits, hyphens (-), underscores (_), and dots (.). Each dot-separated part can have a maximum of 63 characters.

exchanger *exchanger-name*: Specifies the host name of the mail server, a case-insensitive, dot-separated string that contains a maximum 254 characters. The string can contain letters, digits, hyphens (-), underscores (_), and dots (.). Each dot-separated part can have a maximum of 63 characters.

preference *preference*: Specifies the preference for the MX resource record, in the range of 0 to 65535. The smaller the value, the higher the priority.

ns: Configure a name server (NS) resource record.

sub *subname*: Specifies a subname for the DNS forward zone, a case-insensitive, dot-separated string of 1 to 254 characters for an absolute domain name or 1 to 253 characters for a relative domain name. The string can contain letters, digits, hyphens (-), underscores (_), and dots (.). Each dot-separated part can have a maximum of 63 characters.

authority *ns-name*: Specifies the host name of the authoritative DNS server, a case-insensitive, dot-separated string that contains a maximum of 254 characters. The string can contain letters, digits, hyphens (-), underscores (_), and dots (.). Each dot-separated part can have a maximum of 63 characters.

srv: Configures a service resource record.

service *service-name*: Specifies a service by its name, a case-insensitive, dot-separated string of 1 to 254 characters for an absolute domain name or 1 to 253 characters for a relative domain name. The string can contain letters, digits, hyphens (-), underscores (_), and dots (.). Each dot-separated part can have a maximum of 63 characters. In a service name (for example, **_ftp._tcp.movie.edu**), add an underscore before the application name and the protocol name to distinguish them from host domain names. If you do not specify a service name, the domain name of the DNS forward zone applies.

host-offering-service *host-name*: Specifies the name of the host that provides the service, a case-insensitive, dot-separated string of 1 to 254 characters for an absolute domain name or 1 to 253 characters for a relative domain name. The string can contain letters, digits, hyphens (-), underscores (_), and dots (.). Each dot-separated part can have a maximum of 63 characters.

priority *priority*: Specifies a priority value for the resource record in the range of 0 to 100. The smaller the priority value, the higher the priority.

weight *weight-value*: Specifies a weight value for the resource record in the range of 0 to 100.

port *port-number*: Specifies a port number in the range of 0 to 65535.

txt: Configures a text resource record.

describe-txt *description*: Specifies the description for the TXT resource record, a case-insensitive string of 1 to 255 characters.

ttl *ttl-value*: Specifies the TTL for resource records, in the range of 0 to 4294967295 seconds. The default is 3600.

Usage guidelines

The host name specified in a resource record can be a relative domain name (does not end with a dot) or an absolute domain name (ends with a dot). For an absolute domain name, the host name is not automatically expanded and cannot exceed 254 characters. For a relative domain name, the current domain name is automatically appended to the host name. The relative domain name plus the appended domain name cannot exceed 254 characters.

If a service has multiple resource records, the device first attempts to connect to the record with the lowest priority. If multiple resource records have the same priority, the device first attempts to connect to the record with the highest weight.

The TTL setting in this command takes precedence over the TTL setting in DNS forward zone view.

You can configure multiple resource records for a DNS forward zone.

Examples

Configure an MX resource record for DNS forward zone **abc.com**: Specify the host name of the mail server as **mail.abc.com** and the preference for the resource record as 10.

```
<Sysname> system-view
[Sysname] loadbalance zone abc.com
[Sysname-lb-zone-abc.com] record mx exchanger mail.abc.com preference 10
```

Configure a CNAME resource record for DNS forward zone **abc.com**: Specify alias **test.abc.com** for host name **aaa.abc.com**.

```
<Sysname> system-view
[Sysname] loadbalance zone abc.com
[Sysname-lb-zone-abc.com] record cname alias test.abc.com canonical aaa.abc.com
```

Configure an NS resource record for DNS forward zone **abc.com**: Specify the host name of the authoritative DNS server as **ns1.abc.com**.

```
<Sysname> system-view
[Sysname] loadbalance zone abc.com
[Sysname-lb-zone-abc.com] record ns authority ns1.abc.com
```

Configure a TXT resource record for DNS forward zone **abc.com**.

```
<Sysname> system-view
[Sysname] loadbalance zone abc.com
[Sysname-lb-zone-abc.com] record txt sub hotline describe-txt v=spf1
include:spf.abcmail.abc.com.cn -all
```

Configure an SRV resource record for DNS forward zone **abc.com**.

```
<Sysname> system-view
[Sysname] loadbalance zone abc.com
[Sysname-lb-zone-abc.com] record srv service _http._tcp.example.com.
host-offering-service www.example.com priority 5 weight 10 port 80
```

Related commands

display loadbalance zone

record ptr

Use **record ptr** to configure a pointer record (PTR) resource record.

Use **undo record ptr** to delete a PTR resource record.

Syntax

record ptr { **ip** i*pv4-address* | **ipv6** *ipv6-address* } *domain-name* [**ttl** *ttl-value*]

undo record ptr { **ip** i*pv4-address* | **ipv6** *ipv6-address* } *domain-name*

Default

No PTR resource records exist.

Views

DNS reverse zone view

Predefined user roles

network-admin

context-admin

Parameters

ip i*pv4-address*: Specifies an IPv4 address.

ipv6 *ipv6-address*: Specifies an IPv6 address.

domain-name: Specifies a domain name, a case-insensitive, dot-separated string that contains a maximum of 253 characters. The string can contain letters, digits, hyphens (-), underscores (_), and dots (.). Each dot-separated part can have a maximum of 63 characters.

ttl *ttl-value*: Specifies the TTL for resource records, in the range of 0 to 4294967295 seconds. The default is 3600.

Usage guidelines

You can configure PTR resource records for IP addresses that require reverse DNS resolution.

The IP address specified in a PTR resource record must be within the IP address range of the DNS reverse zone.

You can configure multiple PTR resource records for a DNS reverse zone.

Examples

Configure a PTR resource record for the DNS reverse zone with IPv4 address 10.1.1.0/24.

```
<Sysname> system-view
[Sysname] loadbalance reverse-zone ip 10.1.1.0 24
[Sysname-lb-rzone-10.1.1.0/24] record ptr ip 10.1.1.1 mail.nsfocus.com.cn
```

Related commands

display loadbalance reverse-zone

recover-from-auto-shutdown (real server view)

Use **recover-from-auto-shutdown** to manually recover a real server in Auto shutdown state.

Syntax

recover-from-auto-shutdown

Views

Real server view

Predefined user roles

network-admin

context-admin

Usage guidelines

Use this command to manually recover a real server shut down by intelligent monitoring.

If health monitoring is not configured, a recovered real server is set to Unknown state.

If health monitoring is configured and succeeds, a recovered real server is set to Active state. If health monitoring fails, a recovered real server is set to Probe-failed state.

Examples

Manually recover a real server in Auto shutdown state.

```
<Sysname>system-view
[Sysname] real-server rs
[Sysname-rserver-rs] recover-from-auto-shutdown
```

recover-from-auto-shutdown (server farm member view)

Use **recover-from-auto-shutdown** to manually recover a server farm member in Auto shutdown state.

Syntax

recover-from-auto-shutdown

Views

Server farm member view

Predefined user roles

network-admin

context-admin

Usage guidelines

Use this command to manually recover a server farm member shut down by intelligent monitoring.

If health monitoring is not configured, a recovered server farm member is set to Unknown state.

If health monitoring is configured and succeeds, a recovered server farm member is set to Active state. If health monitoring fails, a recovered server farm member is set to Probe-failed state.

Examples

Manually recover a server farm member in Auto shutdown state.

```
<Sysname> system-view
[Sysname] server-farm sf
[Sysname-sfarm-sf] real-server rs1 port 80
```

```
[Sysname-sfarm-sf-#member#-rs1-port-80] recover-from-auto-shutdown
```

redirect relocation (LB action view)

Use **redirect relocation** to enable the redirection feature and specify a redirection URL for an LB action.

Use **undo redirect relocation** to disable the redirection feature for an LB action.

Syntax

redirect relocation *relocation*

undo redirect relocation

Default

The redirection feature is disabled for an LB action.

Views

HTTP LB action view

Predefined user roles

network-admin

context-admin

Parameters

relocation: Specifies a redirection URL, a case-sensitive string of 1 to 255 characters. You can also specify the question mark (?) or the following character strings as the redirection URL (each character string can be used only once):

- **%h**: Specifies the host name and port number in the client request packet.
- **%{host}**: Specifies the IP address in the client request packet.
- **%{port}**: Specifies the port number in the client request packet.
- **%p**: Specifies the URL in the client request packet.

Usage guidelines

This command and the **server-farm** command are mutually exclusive. If you configure one command, the other command (if configured) is automatically cancelled.

This command redirects all HTTP request packets matching an LB action to the specified URL.

Examples

Enable the redirection feature for the HTTP LB action **lba1**, and specify the redirection URL as **https://%h%p**.

```
<Sysname> system-view
[Sysname] loadbalance action lba1 type http
[Sysname-lba-http-lba1] redirect relocation https://%h%p
```

redirect relocation (virtual server view)

Use **redirect relocation** to enable the redirection feature and specify a redirection URL for a virtual server.

Use **undo redirect relocation** to disable the redirection feature for a virtual server.

Syntax

redirect relocation *relocation*

undo redirect relocation

Default

The redirection feature is disabled for a virtual server.

Views

HTTP virtual server view

Predefined user roles

network-admin

context-admin

Parameters

relocation: Specifies a redirection URL, a case-sensitive string of 1 to 255 characters. The redirection feature redirects all request packets matching the virtual server to the URL. You can also specify the question mark (?) or the following character strings as the redirection URL (each character string can be used only once):

- **%h**: Specifies the host name and port number in the client request packet.
- **%{host}**: Specifies the IP address in the client request packet.
- **%{port}**: Specifies the port number in the client request packet.
- **%p**: Specifies the URL in the client request packet.

Examples

Enable the redirection feature for the HTTP-type virtual server **vs2**, and specify the redirection URL as **https://%h%p**.

```
<Sysname> system-view
[Sysname] virtual-server vs2 type http
[Sysname-vs-http-vs2] redirect relocation https://%h%p
```

redirect return-code (LB action view)

Use **redirect return-code** to specify the status code in the redirection packets that the LB device returns to clients.

Use **undo redirect return-code** to restore the default.

Syntax

redirect return-code { **301** | **302** | **307** }

undo redirect return-code

Default

The status code in the redirection packets that the LB device returns to clients is 302.

Views

HTTP LB action view

Predefined user roles

network-admin

context-admin

Parameters

301: Deletes request resources permanently.

302: Deletes request resources temporarily.

307: Temporarily redirects requests to the URL in the Location header.

Usage guidelines

This configuration takes effect only when the redirection feature is enabled for the HTTP LB action.

Examples

Specify the status code in the redirection packets that the LB device returns to clients as **301** for the HTTP LB action **lba1**.

```
<Sysname> system-view
[Sysname] loadbalance action lba1 type http
[Sysname-lba-http-lba1] redirect return-code 301
```

Related commands

redirect relocation

redirect return-code (virtual server view)

Use **redirect return-code** to specify the status code in the redirection packets that the LB device returns to clients.

Use **undo redirect return-code** to restore the default.

Syntax

redirect return-code { **301** | **302** | **307** }

undo redirect return-code

Default

The status code in the redirection packets that the LB device returns to clients is 302.

Views

HTTP virtual server view

Predefined user roles

network-admin

context-admin

Parameters

301: Deletes request resources permanently.

302: Deletes request resources temporarily.

307: Temporarily redirects requests to the URL in the Location header.

Usage guidelines

This configuration takes effect only when the redirection feature is enabled for the virtual server.

Examples

Specify the status code in the redirection packets that the LB device returns to clients as **301** for the HTTP-type virtual server **vs2**.

```
<Sysname> system-view
[Sysname] virtual-server vs2 type http
[Sysname-vs-http-vs2] redirect return-code 301
```

Related commands

redirect relocation

refresh

Use **refresh** to set the refresh interval.

Use **undo refresh** to restore the default.

Syntax

refresh *refresh-interval*

undo refresh

Default

The refresh interval is 3600 seconds.

Views

SOA view

Predefined user roles

network-admin

context-admin

Parameters

refresh-interval: Specifies the refresh interval in the range of 300 to 2419200 seconds.

Usage guidelines

The secondary DNS server obtains SOA resource records from the primary DNS server at the refresh interval. After obtaining SOA resource records, the secondary DNS server compares them with the local SOA resource records.

Examples

Set the refresh interval to 4 hours for DNS forward zone **abc.com**.

```
<Sysname> system-view
[Sysname] loadbalance zone abc.com
[Sysname-lb-zone-abc.com] soa
[Sysname-lb-zone-abc.com-soa] refresh 14400
```

Related commands

display loadbalance zone

reload http-response

Use **reload http-response** to reload a response file.

Syntax

reload http-response { **file** *filename* }

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

file *filename*: Specifies a file by its name, a case-insensitive string of 1 to 255 characters.

Usage guidelines

If a response file changes, you must reload the file to make it take effect.

Examples

Reload response file **subsys_intf.js**.

```
<Sysname> system-view
[Sysname] reload http-response /index/subsys_intf.js
```

Related commands

fallback-action response raw-file

response

request-version all

Use **request-version all** to enable compression for responses to HTTP 1.0 requests.

Use **undo request-version all** to restore the default.

Syntax

request-version all

undo request-version all

Default

Compression is disabled for responses to HTTP 1.0 requests.

Views

HTTP-compression parameter profile view

Predefined user roles

network-admin

context-admin

Examples

Create the HTTP-compression parameter profile **http1**, and enable compression for responses to HTTP 1.0 requests.

```
<Sysname> system-view
[Sysname] parameter-profile http1 type http-compression
[Sysname-para-http-compression-http1] request-version all
```

reset loadbalance connections

Use **reset loadbalance connections** to clear application layer connections.

Syntax

reset loadbalance connections

Views

User view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command clears all application layer connections, including reused idle connections.

Examples

Clear application layer connections.

```
<Sysname> reset loadbalance connection
```

reset loadbalance dns-cache

Use **reset loadbalance dns-cache** to clear DNS cache information.

Syntax

reset loadbalance dns-cache [**vpn-instance** *vpn-instance-name*] [**domain-name** *domain-name*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears DNS cache information for the public network.

domain-name *domain-name*: Specifies a domain name, a case-insensitive string of 1 to 253 characters. If you do not specify this option, the command clears DNS cache information for all domain names.

Examples

Clear DNS cache information for all domain names.

```
<Sysname> reset loadbalance dns-cache
```

reset loadbalance dns-listener statistics

Use **reset loadbalance dns-listener statistics** to clear DNS listener statistics.

Syntax

reset loadbalance dns-listener statistics [*dns-listener-name*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

dns-listener-name: Specifies a DNS listener by its name, a case-insensitive string of 1 to 63 characters. If you do not specify this argument, the command clears statistics for all DNS listeners.

Examples

Clear statistics for the DNS listener **dl2**.

```
<Sysname> reset loadbalance dns-listener statistics dl2
```

Clear statistics for all DNS listeners.

```
<Sysname> reset loadbalance dns-listener statistics
```

Related commands

display loadbalance dns-listener statistics

reset loadbalance dns-map statistics

Use **reset loadbalance dns-map statistics** to clear DNS mapping statistics.

Syntax

reset loadbalance dns-map statistics [*dns-map-name*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

dns-map-name: Specifies a DNS mapping by its name, a case-insensitive string of 1 to 63 characters. If you do not specify this argument, the command clears statistics for all DNS mappings.

Examples

Clear statistics for the DNS mapping **dm2**.

```
<Sysname> reset loadbalance dns-map statistics dm2
```

Clear statistics for all DNS mappings.

```
<Sysname> reset loadbalance dns-map statistics
```

Related commands

display loadbalance dns-map statistics

reset loadbalance dns-proxy statistics

Use **reset loadbalance dns-proxy statistics** to clear transparent DNS proxy statistics.

Syntax

reset loadbalance dns-proxy statistics [*dns-proxy-name*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

dns-proxy-name: Specifies a transparent DNS proxy by its name, a case-insensitive string of 1 to 63 characters. If you do not specify this argument, the command clears statistics for all DNS transparent proxies.

Examples

Clear statistics for transparent DNS proxy **dns-proxy1**.

```
<Sysname> reset loadbalance dns-proxy statistics dns-proxy1
```

Related commands

display loadbalance dns-proxy statistics

reset loadbalance dns-server statistics

Use **reset loadbalance dns-server statistics** to clear DNS server statistics or DNS server pool member statistics.

Syntax

reset loadbalance dns-server statistics [*dns-server-name*]

reset loadbalance dns-server statistics dns-server-pool *dns-server-pool-name* [**name** *dns-server-name* **port** *port-number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

dns-server-name: Specifies a DNS server by its name, a case-insensitive string of 1 to 63 characters. If you do not specify this argument, the command clears statistics for all DNS servers.

dns-server-pool *dns-server-pool-name*: Clears statistics for members of a DNS server pool. The *dns-server-pool-name* argument specifies a DNS server pool by its name, a case-insensitive string of 1 to 63 characters.

dns-server *dns-server-name* **port** *port-number*: Clears statistics for a DNS server pool member. The *dns-server-name* argument specifies a DNS server pool member by its name, a case-insensitive string of 1 to 63 characters. The *port-number* argument specifies the port number of the DNS server pool member, in the range of 0 to 65535. If you do not specify this option, the command clears statistics for all members of a DNS server pool.

Examples

Clear statistics for DNS server **ds1**.

```
<Sysname> reset loadbalance dns-server statistics ds1
```

Clear statistics for all members in DNS server pool **dsp**.

```
<Sysname> reset loadbalance dns-server statistics dns-server-pool dsp
```

Related commands

display loadbalance dns-server statistics

reset loadbalance hot-backup statistics

Use **reset loadbalance hot-backup statistics** to clear LB hot backup statistics.

Syntax

reset loadbalance hot-backup statistics

Views

User view

Predefined user roles

network-admin

context-admin

Examples

Clear LB hot backup statistics.

```
<Sysname> reset loadbalance hot-backup statistics
```

reset loadbalance link statistics

Use **reset loadbalance link statistics** to clear link statistics or link group member statistics.

Syntax

reset loadbalance link statistics [*link-name*]

reset loadbalance link statistics link-group *link-group-name* [**name** *link-name*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

link-name: Specifies a link by its name, a case-insensitive string of 1 to 63 characters. If you do not specify this argument, the command clears statistics about all links.

link-group *link-group-name*: Clears statistics for members of a link group. The *link-group-name* argument specifies a link group by its name, a case-insensitive string of 1 to 63 characters.

name *link-name*: Clears statistics for of a link group member. The *link-name* argument specifies a link group member by its name, a case-insensitive string of 1 to 63 characters. If you do not specify this option, the command clears statistics for all members of a link group.

Examples

Clear statistics about all links.

```
<Sysname> reset loadbalance link statistics
```

Clear statistics about all members in link group **lg**.

```
<Sysname> reset loadbalance link statistics link-group lg
```

reset loadbalance local-dns-server parse-fail-record

Use **reset loadbalance local-dns-server parse-fail-record** to clear DNS request parse failures.

Syntax

reset loadbalance local-dns-server parse-fail-record

Views

User view

Predefined user roles

network-admin

context-admin

Examples

Clear DNS request parse failures.

```
<Sysname> reset loadbalance local-dns-server parse-fail-record
```

reset loadbalance proximity

Use **reset loadbalance proximity** to clear proximity entry information.

Syntax

reset loadbalance proximity [**vpn-instance** *vpn-instance-name*] [**ip** [*ipv4-address*] | **ipv6** [*ipv6-address*]]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command clears proximity entry information for the public network.

ip [*ipv4-address*]: Clears IPv4 proximity entry information. If you specify the *ipv4-address* argument, this command clears information about the proximity entry corresponding to the IPv4 address. If you do not specify the *ipv4-address* argument, this command clears information about all IPv4 proximity entries.

ipv6 [*ipv6-address*]: Clears IPv6 proximity entry information. If you specify the *ipv6-address* argument, this command clears information about the proximity entry corresponding to the IPv6 address. If you do not specify the *ipv6-address* argument, this command clears information about all IPv6 proximity entries.

Usage guidelines

If you do not specify the **vpn-instance**, **ip**, or **ipv6** keyword, this command clears information about all IPv4 and IPv6 proximity entries for the public network.

Examples

Clear information about the proximity entry corresponding to the IPv4 address 1.1.1.1 for the VPN instance **vrf1**.

```
<Sysname> reset loadbalance proximity vpn vrf1 ip 1.1.1.1
```

Clear information about all IPv6 proximity entries for the public network.

```
<Sysname> reset loadbalance proximity ipv6
```

reset real-server statistics

Use **reset real-server statistics** to clear real server statistics or server farm member statistics.

Syntax

reset real-server statistics [*real-server-name*]

reset real-server statistics server-farm *server-farm-name* [**name** *real-server-name* **port** *port-number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

real-server-name: Clears statistics of the specified real server. The *real-server-name* argument specifies a real server name, a case-insensitive string of 1 to 63 characters. If you do not specify this argument, the command clears statistics of all real servers.

server-farm *server-farm-name*: Clears statistics for members of a server farm. The *server-farm-name* argument specifies a server farm by its name, a case-insensitive string of 1 to 63 characters.

name *real-server-name* **port** *port-number*: Clears statistics for a server farm member. The *real-server-name* argument specifies a server farm member by its name, a case-insensitive string of 1 to 63 characters. The *port-number* argument specifies the port number of the server farm member, in the range of 0 to 65535. If you do not specify this option, the command clears statistics for all members of a server farm.

Examples

Clear statistics of all real servers.

```
<Sysname> reset real-server statistics
```

Clear statistics of all members in server farm **sf**.

```
<Sysname> reset real-server statistics server-farm sf
```

Related commands

display real-server statistics

reset sticky dns-proxy

Use **reset sticky dns-proxy** to clear sticky entry information for transparent DNS proxies.

Syntax

reset sticky dns-proxy [**dns-proxy-name** *dns-proxy-name*] [**class** { *class-name* | **default-class** } | **client-addr** { *ipv4-address* | *ipv6-address* } | **dns-server-addr** { *ipv4-address* | *ipv6-address* } | **dns-server-pool** *pool-name* | **dns-server-port** *port-number* | **key** *sticky-key*] * [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

dns-proxy-name *dns-proxy-name*: Specifies a transparent DNS proxy by its name, a case-insensitive string of 1 to 63 characters. If you do not specify this option, the command clears sticky entry information for all transparent DNS proxies.

class { *class-name* | **default-class** }: Specifies an LB class by its name, a case-insensitive string of 1 to 63 characters, or specifies the default LB class.

client-addr { *ipv4-address* | *ipv6-address* }: Specifies a client by its IPv4 or IPv6 address.

dns-server-addr { *ipv4-address* | *ipv6-address* }: Specifies a DNS server by its IPv4 or IPv6 address.

dns-server-pool *pool-name*: Specifies a DNS server pool by its name, a case-insensitive string of 1 to 63 characters.

dns-server-port *port-number*: Specifies a DNS server port number in the range of 0 to 65535.

key *sticky-key*: Specifies a key value, a case-sensitive string of 1 to 36 characters.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears sticky entry information for all member devices.

Examples

Clear sticky entry information for client address 3.0.0.1 of transparent DNS proxy **dp**.

```
<Sysname> reset sticky dns-proxy dns-proxy-name dp client-addr 3.0.0.1
```

reset sticky virtual-server

Use **reset sticky virtual-server** to clear sticky entry information for virtual servers.

Syntax

reset sticky virtual-server [**virtual-server-name** *virtual-server-name*] [[**link** { **ip** *ipv4-address* | **ipv6** *ipv6-address* | **interface** { *interface-type interface-number* | *interface-name* } } | **link-group** *link-group-name*] * | [**real-server-addr** { *ipv4-address* | *ipv6-address* } | **real-server-port** *port-number* | **server-farm** *server-farm-name* | **text** *text*] *] [**class** { *class-name* | **default-class** } | **client-addr** { *ipv4-address* | *ipv6-address* } | **sticky-type** { **address-port** | **http-content** | **http-cookie** | **http-header** | **http-passive** | **payload** | **radius** | **sip** | **ssl** | **tcp-payload** | **udp-passive** } [**key** *sticky-key*]] * [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

virtual-server-name *virtual-server-name*: Specifies a virtual server by its name, a case-insensitive string of 1 to 63 characters. If you do not specify this option, the command clears sticky entry information for all virtual servers.

link { **ip** *ipv4-address* | **ipv6** *ipv6-address* | **interface** { *interface-type interface-number* | *interface-name* } }: Specifies a link by its IPv4 address, IPv6 address, or output interface.

link-group *link-group-name*: Specifies a link group by its name, a case-insensitive string of 1 to 63 characters.

real-server-addr { *ipv4-address* | *ipv6-address* }: Specifies a real server by its IPv4 or IPv6 address.

real-server-port *port-number*: Specifies a real server port number in the range of 0 to 65535.

server-farm *server-farm-name*: Specifies a server farm by its name, a case-insensitive string of 1 to 63 characters.

text *text*: Specifies a text string to match.

class { *class-name* | **default-class** }: Specifies an LB class by its name, a case-insensitive string of 1 to 63 characters, or specifies the default LB class.

client-addr { *ipv4-address* | *ipv6-address* }: Specifies a client by its IPv4 or IPv6 address.

sticky-type { **address-port** | **http-content** | **http-cookie** | **http-header** | **http-passive** | **payload** | **radius** | **sip** | **ssl** | **tcp-payload** | **udp-passive** }: Specifies a sticky group type.

key *sticky-key*: Specifies a key value, a case-sensitive string of 1 to 36 characters. If you do not specify key value, this command clears sticky entries for all key values.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears sticky entry information for all member devices.

Examples

Clear sticky entry information for client address 3.0.0.1 of virtual server **vs**.

```
<Sysname> reset sticky virtual-server virtual-server-name vs client-addr 3.0.0.1
```

reset virtual-server statistics

Use **reset virtual-server statistics** to clear virtual server statistics.

Syntax

reset virtual-server statistics [*virtual-server-name*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

virtual-server-name: Clears statistics of the specified virtual server. The *virtual-server-name* argument specifies a virtual server name, a case-insensitive string of 1 to 63 characters. If you do not specify this argument, the command clears statistics of all virtual servers.

Examples

Clear statistics of all virtual servers.

```
<Sysname> reset virtual-server statistics
```

Related commands

display virtual-server statistics

response

Use **response** to specify a response file for matching HTTP requests.

Use **undo response** to restore the default.

Syntax

response { **url** *url* **file** *filename* | **workpath** *workpath* **zip-file** *zip-filename* }

undo response { **url** *url* | **workpath** *workpath* }

Default

No response file is specified for HTTP requests.

Views

HTTP LB action view

Predefined user roles

network-admin

context-admin

Parameters

url *url*: Specifies the URL path used to match HTTP requests, a case-sensitive string of 1 to 255 characters. The specified URL path must start with a forward slash (/).

file *filename*: Specifies an uncompressed file by its name, a case-insensitive string of 1 to 255 characters.

workpath *workpath*: Specifies a working path to match the URL in HTTP requests, a case-sensitive string of 1 to 255 characters. The working path can be a single forward slash (/), or a string that starts with a forward slash and does not end with a forward slash.

zip-file *zip-filename*: Specifies a zip file by its name, a case-insensitive string of 1 to 255 characters. The relative path in the zip file is used to match the URL in HTTP requests.

Usage guidelines

If the URL path in a client request matches the specified URL path, the device responds to the request by using an uncompressed file.

If the URL path in a client request matches the specified working path plus a relative path in the zip file, the device responds to the request by using the file in the zip file. For example, if you configure the **response workpath** */index* **zip-file** *flash:/za/zb/test.zip* command and a relative path **/css/col.css** exists in **test.zip**, the matching URL is **/index/css/col.css** and the response file is **col.css**.

URL-encoded URLs cannot be matched.

If you configure both an uncompressed file and a compressed file for the same URL path, the uncompressed file is used to respond to matching HTTP requests.

The path specified in the command must exist on the device.

For the same HTTP LB action, only one uncompressed file can be used for a URL, and one uncompressed file can be used for multiple URLs.

If you specify multiple compressed files for one or more URL paths in the same HTTP LB action, the most recent configuration takes effect.

If you specify multiple uncompressed files for one URL path in the same HTTP LB action, the most recent configuration takes effect. One uncompressed file can be used for different URL paths.

Any two of the following commands are mutually exclusive:

- **response**
- **server-farm** (LB action view)
- **redirect relocation** (LB action view)

Examples

Specify response file **subsys.js** for the HTTP requests with URL path **/index/subsys/subsys_intf.js**.

```
<Sysname> system-view
[Sysname] loadbalance action a_http type http
[Sysname-lba-http-a_http] response url /index/subsys/subsys_intf.js file subsys.js
```

Related commands

display loadbalance action

redirect relocation (LB action view)

server-farm (LB action view)

responsible-mail

Use **responsible-mail** to specify the email address of the administrator.

Use **undo responsible-mail** to restore the default.

Syntax

responsible-mail *mail-address*

undo responsible-mail

Default

No administrator's email address is specified.

Views

SOA view

Predefined user roles

network-admin

context-admin

Parameters

mail-address: Specifies the administrator's email address, a case-insensitive, dot-separated string that contains a maximum of 254 characters. The string can contain letters, digits, hyphens (-), underscores (_), and dots (.). Each dot-separated part can have a maximum of 63 characters.

Usage guidelines

The email address of the administrator can be a relative domain name (does not end with a dot) or an absolute domain name (ends with a dot). For an absolute domain name, the email address is not automatically expanded and cannot exceed 254 characters. For a relative domain name, the current domain name is automatically appended to the email address. The email address plus the appended domain name cannot exceed 254 characters.

Examples

Specify the administrator's email address **root.ns1.abc.com** for DNS forward zone **abc.com**.

```
<Sysname> system-view
[Sysname] loadbalance zone abc.com
[Sysname-lb-zone-abc.com] soa
[Sysname-lb-zone-abc.com-soa] responsible-mail root.ns1.abc.com
```

Related commands

display loadbalance zone

retry

Use **retry** to set the retry interval.

Use **undo retry** to restore the default.

Syntax

retry *retry-interval*

undo retry

Default

The retry interval is 600 seconds.

Views

SOA view

Predefined user roles

network-admin

context-admin

Parameters

retry-interval: Specifies the retry interval in the range of 500 to 1209600 seconds.

Usage guidelines

The retry interval is the amount of time that the secondary DNS server waits after it fails to copy a DNS forward zone.

Examples

Set the retry interval to 30 minutes for DNS forward zone **abc.com**.

```
<Sysname> system-view
[Sysname] loadbalance zone abc.com
```

```
[Sysname-lb-zone-abc.com] soa
[Sysname-lb-zone-abc.com-soa] retry 1800
```

Related commands

display loadbalance zone

route-advertisement enable

Use **route-advertisement enable** to enable IP address advertisement for a virtual server.

Use **undo route-advertisement enable** to disable IP address advertisement for a virtual server.

Syntax

route-advertisement enable

undo route-advertisement enable

Default

IP address advertisement is disabled for a virtual server.

Views

Virtual server view

Predefined user roles

network-admin

context-admin

Usage guidelines

After this feature is configured, the device advertises the IP address of the virtual server to OSPF for route calculation. When the service of a data center switches to another data center, the traffic to the virtual server can also be switched to that data center. For information about OSPF, see *Layer 3—IP Routing Configuration Guide*.

Examples

Enable IP address advertisement for the virtual server **vs**.

```
<Sysname> system-view
[Sysname] virtual-server vs type ip
[Sysname-vs-ip-vs] route-advertisement enable
```

router interface

Use **router interface** to specify an outgoing interface for an LB link.

Use **undo router interface** to delete the outgoing interface for an LB link.

Syntax

router interface *interface-type interface-number*

undo router interface

Default

No outgoing interface is specified for an LB link.

Views

LB link view

Predefined user roles

network-admin

context-admin

Parameters

*interface-type interface-numbe*r: Specifies an outgoing interface.

Usage guidelines

In scenarios where IP addresses are obtained through PPPoE, use this command to dynamically obtain the outbound next hop IP address through the specified outgoing interface.

The specified outgoing interface must be an interface that can dynamically obtain IP addresses.

You can configure both this command and the **router ip** or **router ipv6** command. The command configured later overwrites the command configured first.

If you configure this command after configuring the **vpn-instance** (link view) command, this command overwrites the **vpn-instance** (link view) command. After you configure this command, you cannot configure the **vpn-instance** (link view) command.

Examples

Specify **Dialer0** as the outgoing interface for the LB link **cnc**.

```
<Sysname> system-view
[Sysname] loadbalance link cnc
[Sysname-lb-link-cnc] router interface Dialer0
```

router ip

Use **router ip** to specify the outbound next hop for an LB link.

Use **undo router ip** to restore the default.

Syntax

router ip *ipv4-address*

undo router ip

Default

The outbound next hop is not specified for an LB link.

Views

LB link view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-address: Specifies an IPv4 address, which cannot be a loopback address, multicast address, broadcast address, or an address in the format of 0.X.X.X.

Usage guidelines

You can specify only one outbound next hop for an LB link.

Examples

Specify the outbound next hop as 1.2.3.4 for the LB link **lk1**.

```
<Sysname> system-view
[Sysname] loadbalance link lk1
[Sysname-lb-link-lk1] router ip 1.2.3.4
```

router ipv6

Use **router ipv6** to specify the outbound next hop for an LB link.

Use **undo router ipv6** to restore the default.

Syntax

router ipv6 *ipv6-address*

undo router ipv6

Default

The outbound next hop is not specified for an LB link.

Views

LB link view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address: Specifies an IPv6 address, which cannot be an all-zero address, a multicast address, a loopback address, or a link-local address.

Usage guidelines

You can specify only one outbound next hop for an LB link.

Examples

Specify the outbound next hop as 8008::8 for the LB link **lk1**.

```
<Sysname> system-view
[Sysname] loadbalance link lk1
[Sysname-lb-link-lk1] router ipv6 8008::8
```

rst threshold

Use **rst threshold** to set the RST packet count threshold for a TCP-RST LB probe template.

Use **undo rst threshold** to restore the default.

Syntax

rst threshold *number*

undo rst threshold

Default

The RST packet count threshold is 1000000.

Views

TCP-RST LB probe template view

Predefined user roles

network-admin

context-admin

Parameters

number: Specifies the RST packet count threshold value, in the range of 1 to 4294967295.

Usage guidelines

When the number of RST packets sent by a real server reaches the threshold, the protection action specified in the **protect-action** command is taken.

Examples

In TCP-RST LB probe template **rsttplt**, set the RST packet count threshold to 20.

```
<Sysname>system-view
[Sysname] loadbalance probe-template tcp-rst rsttplt
[Sysname-lbpt-tcp-rst-rsttplt] rst threshold 20
```

Related commands

protect-action

rtt weight

Use **rtt weight** to set the network delay weight for proximity calculation.

Use **undo rtt weight** to restore the default.

Syntax

rtt weight *rtt-weight*

undo rtt weight

Default

The network delay weight for proximity calculation is 100.

Views

Proximity view

Predefined user roles

network-admin

context-admin

Parameters

rtt-weight: Specifies the network delay weight for proximity calculation, in the range of 0 to 255. A larger value indicates a higher weight.

Examples

Set the network delay weight for proximity calculation to 200.

```
<Sysname> system-view
[Sysname] loadbalance proximity
[Sysname-lb-proximity] rtt weight 200
```

rule (parameter profile view)

Use **rule** to configure a filtering rule for compression.

Use **undo rule** to restore the default.

Syntax

rule [*rule-id*] { **deny** | **permit** } { **content-type** | **url** } *expression*

undo rule *rule-id*

Default

No filtering rules are configured.

Views

HTTP-compression parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

rule-id: Specifies a rule by its ID in the range of 1 to 65535. If the rule does not exist, the command creates the rule. If the rule already exists, the command modifies the rule. If you do not specify this argument, the system automatically assigns an available rule ID with the smallest number.

deny: Does not compress matching packets.

permit: Compresses matching packets.

content-type: Matches content types in the content-type header of packets.

url: Matches URLs in packets.

expression: Specifies a regular expression, a case-sensitive string of 1 to 255 characters. The string cannot contain question marks (?).

Examples

Create the HTTP-compression parameter profile **http1**, and configure the device to not compress the response packets containing the string **image** in URLs.

```
<Sysname> system-view
[Sysname] parameter-profile http1 type http-compression
[Sysname-para-http-compression-http1] rule deny url image
```

rule (protection policy view)

Use **rule** to create a protection rule and enter its view, or enter the view of an existing protection rule.

Use **undo rule** to delete a protection rule.

Syntax

rule *rule-id*

undo rule *rule-id*

Default

No protection rules exist.

Views

HTTP protection policy view

Predefined user roles

network-admin

context-admin

Parameters

rule-id: Specifies a rule ID in the range of 1 to 65535.

Usage guidelines

You can configure multiple protection rules in an HTTP protection policy. The device compares the URL in a packet with the URLs configured in the protection rules according to the order of the rule IDs. If a match is found and the configured protection threshold is exceeded, the device performs the associated protection action. If the URL in the packet does not match the URL configured in a specific protection rule, the device compares the URL with the next protection rule.

Examples

In HTTP protection policy **p1**, create protection rule 5 and enter its view.

```
<Sysname> system-view
[Sysname] loadbalance protection-policy p1
[Sysname-lbpp-http-p1] rule 5
[Sysname-lbpp-http-p1-rule-5]
```

secondary-cookie delimiters

Use **secondary-cookie delimiters** to configure the delimiter that separates secondary cookies in URLs.

Use **undo secondary-cookie delimiters** to restore the default.

Syntax

secondary-cookie delimiters *text*

undo secondary-cookie delimiters

Default

The delimiter that separates secondary cookies in URLs can be slash (/), ampersand (&), number sign (#), or plus (+).

Views

HTTP parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

text: Specifies the delimiter, a string of 1 to 4 characters including exclamation mark (!), quotation mark (',"), number sign (#), semicolon (;), brackets (( ),[ ], < >), question mark (?), backslash (\), caret (^), grave accent (`), vertical bar (|), colon (:), at sign (@), ampersand (&), dollar sign ($), plus (+), asterisk (*), comma (,), and slash (/). Each character in the string is considered as a delimiter.

Examples

For the HTTP parameter profile **pp1**, configure the delimiter that separates secondary cookies in URLs as slash (/), at sign (@), number sign (#), or dollar sign ($).

```
<Sysname> system-view
[Sysname] parameter-profile pp1 type http
```

```
[Sysname-para-http-pp1] secondary-cookie delimiters !@#$
```

secondary-cookie start

Use **secondary-cookie start** to configure the start delimiter for secondary cookies in URLs.

Use **undo secondary-cookie start** to restore the default.

Syntax

secondary-cookie start *text*

undo secondary-cookie start

Default

The start delimiter for secondary cookies in URLs is question mark (?).

Views

HTTP parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

text: Specifies the delimiter, a string of 1 to 2 characters including exclamation mark (!), quotation mark ("), number sign (#), semicolon (;), brackets ([ ], < >), question mark (?), backslash (\), caret (^), grave accent (`), and vertical bar (|).

Examples

For the HTTP parameter profile **pp1**, configure the start delimiter for secondary cookies in URLs as question mark (?) or exclamation mark (!).

```
<Sysname> system-view
[Sysname] parameter-profile pp1 type http
[Sysname-para-http-pp1] secondary-cookie start ?!
```

selected-link

Use **selected-link** to specify the number of links to participate in scheduling.

Use **undo selected-link** to restore the default.

Syntax

selected-link min *min-number* **max** *max-number*

undo selected-link

Default

The links with the highest priority participate in scheduling.

Views

Link group view

Predefined user roles

network-admin

context-admin

Parameters

min *min-number*: Specifies the minimum number of links to participate in scheduling, in the range of 1 to 1000.

max *max-number*: Specifies the maximum number of links to participate in scheduling, in the range of 1 to 1000. The value of the *max-number* argument must be greater than or equal to the value of the *min-number* argument.

Usage guidelines

If the number of links available to participate in scheduling exceeds the *max-number* setting, the *max-number* setting applies.

If the number of links available to participate in scheduling is smaller than the *min-number* setting, more links are selected by priority in descending order.

Examples

Configure the minimum number and maximum number of links in the link group **lg** to participate in scheduling as 20 and 30, respectively.

```
<Sysname> system-view
[Sysname] loadbalance link-group lg
[Sysname-lb-lgroup-lg] selected-link min 20 max 30
```

Related commands

predictor (link group view)

priority (link view)

selected-server (DNS server pool view)

Use **selected-server** to specify the number of DNS servers to participate in scheduling.

Use **undo selected-server** to restore the default.

Syntax

selected-server min *min-number* **max** *max-number*

undo selected-server

Default

The DNS servers with the highest priority participate in scheduling.

Views

DNS server pool view

Predefined user roles

network-admin

context-admin

Parameters

min *min-number*: Specifies the minimum number of DNS servers to participate in scheduling, in the range of 1 to 1000.

max *max-number*: Specifies the maximum number of DNS servers to participate in scheduling, in the range of 1 to 1000. The value of the *max-number* argument must be greater than or equal to the value of the *min-number* argument.

Usage guidelines

If the number of DNS servers available to participate in scheduling exceeds the *max-number* setting, the *max-number* setting applies.

If the number of DNS servers available to participate in scheduling is less than the *min-number* setting, more DNS servers are selected by priority in descending order.

Examples

Configure the minimum number and maximum number of DNS servers in DNS server pool **dns-pool** to participate in scheduling as 20 and 30, respectively.

```
<Sysname> system-view
[Sysname] loadbalance dns-server-pool dns-pool
[Sysname-lb-dspool-dns-pool] selected-server min 20 max 30
```

selected-server (server farm view)

Use **selected-server** to specify the number of real servers to participate in scheduling.

Use **undo selected-server** to restore the default.

Syntax

selected-server min *min-number* **max** *max-number*

undo selected-server

Default

The real servers with the highest priority participate in scheduling.

Views

Server farm view

Predefined user roles

network-admin

context-admin

Parameters

min *min-number*: Specifies the minimum number of real servers to participate in scheduling, in the range of 1 to 1000.

max *max-number*: Specifies the maximum number of real servers to participate in scheduling, in the range of 1 to 1000. The value of the *max-number* argument must be greater than or equal to the value of the *min-number* argument.

Usage guidelines

If the number of real servers available to participate in scheduling exceeds the *max-number* setting, the *max-number* setting applies.

If the number of real servers available to participate in scheduling is less than the *min-number* setting, more real servers are selected by priority in descending order.

Examples

Configure the minimum number and maximum number of real servers in the server farm **sf** to participate in scheduling as 20 and 30, respectively.

```
<Sysname> system-view
[Sysname] server-farm sf
[Sysname-sfarm-sf] selected-server min 20 max 30
```

Related commands

predictor (server farm view)

priority (real server view)

serial

Use **serial** to configure the serial number for a DNS forward zone.

Use **undo serial** to restore the default.

Syntax

serial *number*

undo serial

Default

The serial number for a DNS forward zone is 1.

Views

SOA view

Predefined user roles

network-admin

context-admin

Parameters

number: Specifies the serial number in the range of 1 to 4294967295.

Usage guidelines

The serial number indicates the configuration order of a DNS forward zone. A newly configured DNS forward zone has a greater serial number than an old DNS forward zone.

The secondary DNS server periodically queries the serial numbers of DNS forward zones on the primary DNS server and compares them with local serial numbers.

Examples

Configure the serial number as 123 for DNS forward zone **abc.com**.

```
<Sysname> system-view
[Sysname] loadbalance zone abc.com
[Sysname-lb-zone-abc.com] soa
[Sysname-lb-zone-abc.com-soa] serial 123
```

Related commands

display loadbalance zone

server-connection reuse

Use **server-connection reuse** to enable connection reuse between the LB device and the server.

Use **undo server-connection reuse** to disable connection reuse between the LB device and the server.

Syntax

server-connection reuse

undo server-connection reuse

Default

Connection reuse between the LB device and the server is disabled.

Views

HTTP parameter profile view

MySQL parameter profile view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command allows the LB device to establish connections to the server that can be reused by clients. Because multiple clients can use the same connection, the number of connections between the clients and the server is reduced.

This command is not supported by the virtual servers of the fast HTTP type.

Examples

Enable connection reuse between the LB device and the server for the HTTP parameter profile **pp1**.

```
<Sysname> system-view
[Sysname] parameter-profile pp1 type http
[Sysname-para-http-pp1] server-connection reuse
```

server-farm (LB action view)

Use **server-farm** to specify the primary server farm.

Use **undo server-farm** to restore the default.

Syntax

server-farm *server-farm-name* [**backup** *backup-server-farm-name*] [**sticky** *sticky-name* [**backup** *backup-sticky-name*]]

undo server-farm

Default

No primary server farm is specified.

Views

LB action view

Predefined user roles

network-admin

context-admin

Parameters

server-farm-name: Specifies a primary server farm name, a case-insensitive string of 1 to 63 characters.

backup *backup-server-farm-name*: Specifies a backup server farm name, a case-insensitive string of 1 to 63 characters.

sticky *sticky-name*: Specifies a primary sticky group by its name, a case-insensitive string of 1 to 63 characters.

backup *backup-sticky-name*: Specifies a backup sticky group by its name, a case-insensitive string of 1 to 63 characters. This option is supported only by HTTP virtual servers and RADIUS virtual servers.

Usage guidelines

This command is mutually exclusive with the **forward all** or **redirect relocation** command. If you configure one command, the other command (if configured) is automatically cancelled.

When the primary server farm is available (contains real servers), packets are forwarded through the primary server farm. When the primary server farm is not available, packets are forwarded through the backup server farm.

If you specify both a primary sticky group and a backup sticky group, the device generates both primary sticky entries and backup sticky entries. If packets do not match primary sticky entries, backup sticky entries will apply.

The device generates backup sticky entries for only the following sticky group combinations:

- RADIUS-type primary sticky group and port-address-type backup sticky group.
- HTTP cookie-type primary sticky group and port-address-type backup sticky group.
- HTTP cookie-type primary sticky group and HTTP passive-type backup sticky group.

Examples

Specify the primary server farm **sf**, the backup server farm **sfb**, and the sticky group **sg1** for the generic LB action **lba1**.

```
<Sysname> system-view
[Sysname] loadbalance action lba1 type generic
[Sysname-lba-generic-lba1] server-farm sf backup sfb sticky sg1
```

Related commands

forward all

server-farm (real server view)

Use **server-farm** to specify the server farm for a real server.

Use **undo server-farm** to restore the default.

Syntax

server-farm *server-farm-name*

undo server-farm [*server-farm-name*]

Default

A real server does not belong to any server farm.

Views

Real server view

Predefined user roles

network-admin

context-admin

Parameters

server-farm-name: Specifies a server farm name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

You can specify a server farm that has not been created.

Examples

Specify the server farm **sf** for the real server **rs**.

```
<Sysname> system-view
[Sysname] real-server rs
[Sysname-rserver-rs] server-farm sf
```

server-farm (system view)

Use **server-farm** to create a server farm and enter its view, or enter the view of an existing server farm.

Use **undo server-farm** to delete the specified server farm.

Syntax

server-farm *server-farm-name*

undo server-farm *server-farm-name*

Default

No server farms exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

server-farm-name: Specifies a server farm name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

You can add servers with common attributes to a server farm to facilitate management.

You can configure this command only if the device has licenses installed. For information about licensing, see license management in *Fundamentals Configuration Guide*.

Examples

Create the server farm **sf** and enter server farm view.

```
<Sysname> system-view
[Sysname] server-farm sf
[Sysname-sfarm-sf]
```

service enable (DNS listener view)

Use **service enable** to enable the DNS listener feature.

Use **undo service enable** to disable the DNS listener feature.

Syntax

service enable

undo service enable

Default

The DNS listener feature is disabled.

Views

DNS listener view

Predefined user roles

network-admin

context-admin

Examples

Enable the DNS listener feature for the DNS listener **ct-listener**.

```
<Sysname> system-view
[Sysname] loadbalance dns-listener ct-listener
[Sysname-lb-dl-ct-listener] service enable
```

service enable (DNS mapping view)

Use **service enable** to enable the DNS mapping feature.

Use **undo service enable** to disable the DNS mapping feature.

Syntax

service enable

undo service enable

Default

The DNS mapping feature is disabled.

Views

DNS mapping view

Predefined user roles

network-admin

context-admin

Examples

Enable the DNS mapping feature for the DNS mapping **dm1**.

```
<Sysname> system-view
[Sysname] loadbalance dns-map dm1
[Sysname-lb-dm-dm1] service enable
```

service enable (transparent DNS proxy view)

Use **service enable** to enable the transparent DNS proxy feature.

Use **undo service enable** to disable the transparent DNS proxy feature.

Syntax

service enable

undo service enable

Default

The transparent DNS proxy feature is disabled.

Views

Transparent DNS proxy view

Predefined user roles

network-admin

context-admin

Examples

Enable the transparent DNS proxy feature for transparent DNS proxy **dns-proxy1**.

```
<Sysname> system-view
[Sysname] loadbalance dns-proxy dns-proxy1
[Sysname-lb-dp-udp-dns-proxy1] service enable
```

service enable (virtual server view)

Use **service enable** to enable a virtual server.

Use **undo service enable** to disable a virtual server.

Syntax

service enable

undo service enable

Default

A virtual server is disabled.

Views

Virtual server view

Predefined user roles

network-admin

context-admin

Examples

Enable the IP-type virtual server **vs3**.

```
<Sysname> system-view
[Sysname] virtual-server vs3 type ip
[Sysname-vs-ip-vs3] service enable
```

service object-group

Use **service object-group** to specify a service object group for address translation.

Use **undo service object-group** to restore the default.

Syntax

service object-group *object-group-name*

undo service object-group

Default

All packets matching a virtual server are translated.

Views

SNAT global policy view

Predefined user roles

network-admin

context-admin

Parameters

object-group-name: Specifies a service object group by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

If you specify a service object group, the device performs SNAT on only packets with a matching service. For information about configuring a service object group, see object group configuration in *Security Configuration Guide*.

Examples

Specify a service object group **obj1** for SNAT global policy **sn1**.

```
<Sysname> system-view
[Sysname] loadbalance snat-global-policy sn1
[Sysname-lb-snat-gp-sn1] service object-group obj1
```

Related commands

object-group (*Security Command Reference*)

set ip tos (LB action view)

Use **set ip tos** to set the ToS field value of IP packets sent to the server.

Use **undo set ip tos** to restore the default.

Syntax

set ip tos *tos-number*

undo set ip tos

Default

The ToS field of IP packets sent to the server is not changed.

Views

LB action view

Predefined user roles

network-admin

context-admin

Parameters

tos-number: Specifies the ToS field value in the range of 0 to 255.

Examples

Set the ToS field value to 20 for IP packets sent to the server for the generic LB action **lba1**.

```
<Sysname> system-view
[Sysname] loadbalance action lba1 type generic
[Sysname-lba-generic-lba1] set ip tos 20
```

set ip tos (parameter profile view)

Use **set ip tos** to set the ToS field value of IP packets sent to the client.

Use **undo set ip tos** to restore the default.

Syntax

set ip tos *tos-number*

undo set ip tos

Default

The ToS field of IP packets sent to the client is not changed.

Views

Parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

tos-number: Specifies the ToS field value in the range of 0 to 255.

Usage guidelines

This command is available in IP parameter profile view only.

Examples

Set the ToS field value to 20 for IP packets sent to the client for the IP parameter profile **pp2**.

```
<Sysname> system-view
[Sysname] parameter-profile pp2 type ip
[Sysname-para-ip-pp2] set ip tos 20
```

shutdown (link group member view)

Use **shutdown** to shut down a link group member.

Use **undo shutdown** to activate a link group member.

Syntax

shutdown

undo shutdown

Default

A link group member is activated.

Views

Link group member view

Predefined user roles

network-admin

context-admin

Examples

Shut down the link group member **lk1**.

```
<Sysname> system-view
[Sysname] loadbalance link-group lg
[Sysname-lb-lgroup-lg] link lk1
[Sysname-lb-lgroup-lg-#member#-lk1] shutdown
```

shutdown (link view)

Use **shutdown** to shut down a link.

Use **undo shutdown** to activate a link.

Syntax

shutdown

undo shutdown

Default

A link is activated.

Views

Link view

Predefined user roles

network-admin

context-admin

Examples

Shut down the link **lk1**.

```
<Sysname> system-view
[Sysname] loadbalance link lk1
[Sysname-lb-link-lk1] shutdown
```

shutdown (real server view)

Use **shutdown** to shut down a real server.

Use **undo shutdown** to activate a real server.

Syntax

shutdown

undo shutdown

Default

A real server is activated.

Views

Real server view

Predefined user roles

network-admin

context-admin

Examples

Shut down the real server **rs**.

```
<Sysname> system-view
[Sysname] real-server rs
[Sysname-rserver-rs] shutdown
```

shutdown (server farm member view)

Use **shutdown** to shut down a server farm member.

Use **undo shutdown** to activate a server farm member.

Syntax

shutdown

undo shutdown

Default

A server farm member is activated.

Views

Server farm member view

Predefined user roles

network-admin

context-admin

Examples

Shut down the server farm member **rs1**.

```
<Sysname> system-view
[Sysname] server-farm sf
[Sysname-sfarm-sf] real-server rs1 port 80
[Sysname-sfarm-sf-#member#-rs1-port-80] shutdown
```

skip current-dns-proxy

Use **skip current-dns-proxy** to skip the current transparent DNS proxy.

Use **undo skip current-dns-proxy** to restore the default.

Syntax

skip current-dns-proxy

undo skip current-dns-proxy

Default

The forwarding mode is to discard packets.

Views

DNS LB action view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command enables DNS requests to skip the current transparent DNS proxy and match the next transparent DNS proxy or virtual server.

A DNS request can skip a maximum of five transparent DNS proxies and virtual servers.

This command is mutually exclusive with the **dns-server-pool** or **forward all** command. If you configure one command, the other command (if configured) is automatically cancelled.

Examples

Skip the current transparent DNS proxy in DNS LB action **lba1**.

```
<Sysname> system-view
[Sysname] loadbalance action lba1 type dns
[Sysname-lba-dns-lba1] skip current-dns-proxy
```

slow-online (link group view)

Use **slow-online** to enable the slow online feature for a link group.

Use **undo slow-online** to disable the slow online feature for a link group.

Syntax

slow-online [**standby-time** *standby-time* **ramp-up-time** *ramp-up-time*]

undo slow-online

Default

The slow online feature is disabled for a link group.

Views

Link group view

Predefined user roles

network-admin

context-admin

Parameters

standby-time *standby-time*: Specifies the standby timer in the range of 0 to 600 seconds. The default is 5 seconds.

ramp-up-time *ramp-up-time*: Specifies the ramp-up timer in the range of 3 to 600 seconds. The default is 5 seconds.

Usage guidelines

The links newly added to a link group might be unable to immediately process large numbers of services assigned by the LB device. To resolve this issue, enable the slow online feature for the link group. The feature uses the standby timer and ramp-up timer. When a link is added, the LB device does not assign any service to the link until the standby timer expires.

When the standby timer expires, the ramp-up timer starts. During the ramp-up time, the LB device increases the service amount according to the processing capability of the link, until the ramp-up timer expires.

Examples

Enable the slow online feature for the link group **lg**.

```
<Sysname> system-view
[Sysname] loadbalance link-group lg
[Sysname-lb-lgroup-lg] slow-online
```

slow-online (server farm view)

Use **slow-online** to enable the slow online feature for a server farm.

Use **undo slow-online** to disable the slow online feature for a server farm.

Syntax

slow-online [**standby-time** *standby-time* **ramp-up-time** *ramp-up-time*]

undo slow-online

Default

The slow online feature is disabled for a server farm.

Views

Server farm view

Predefined user roles

network-admin

context-admin

Parameters

standby-time *standby-time*: Specifies the standby timer in the range of 0 to 600 seconds. The default is 5 seconds.

ramp-up-time *ramp-up-time*: Specifies the ramp-up timer in the range of 3 to 600 seconds. The default is 5 seconds.

Usage guidelines

The real servers newly added to a server farm might not be able to immediately process large numbers of services assigned by the LB device. To resolve this issue, enable the slow online feature for the server farm. The feature uses the standby timer and ramp-up timer. When a real server is added, the LB device does not assign any service to the real server until the standby timer expires.

When the standby timer expires, the ramp-up timer starts. During the ramp-up time, the LB device increases the service amount according to the processing capability of the real server, until the ramp-up timer expires.

Examples

Enable the slow online feature for the server farm **sf**.

```
<Sysname> system-view
[Sysname] server-farm sf
[Sysname-sfarm-sf] slow-online
```

slow-shutdown enable (link group member view)

Use **slow-shutdown enable** to enable the slow offline feature for a link group member.

Use **undo slow-shutdown enable** to disable the slow offline feature for a link group member.

Syntax

slow-shutdown enable

undo slow-shutdown enable

Default

The slow offline feature is disabled for a link group member.

Views

Link group member view

Predefined user roles

network-admin

context-admin

Usage guidelines

The **shutdown** command immediately terminates existing connections of a link group member. The slow offline feature ages out the connections, and does not establish new connections.

To enable the slow offline feature for a link group member, you must execute the **slow-shutdown enable** command and then the **shutdown** command. If you execute the **shutdown** command and then the **slow-shutdown enable** command, the slow offline feature does not take effect and the link group member is shut down.

Examples

Enable the slow offline feature for the link group member **lk1**.

```
<Sysname> system-view
[Sysname] loadbalance link-group lg
[Sysname-lb-lgroup-lg] link lk1
[Sysname-lb-lgroup-lg-link-lk1] slow-shutdown enable
```

Related commands

shutdown (link group member view)

slow-shutdown enable (link view)

Use **slow-shutdown enable** to enable the slow offline feature for a link.

Use **undo slow-shutdown enable** to disable the slow offline feature for a link.

Syntax

slow-shutdown enable

undo slow-shutdown enable

Default

The slow offline feature is disabled for a link.

Views

Link view

Predefined user roles

network-admin

context-admin

Usage guidelines

The **shutdown** command immediately terminates existing connections of a link. The slow offline feature ages out the connections, and does not establish new connections.

To enable the slow offline feature for a link, you must execute the **slow-shutdown enable** command and then the **shutdown** command. If you execute the **shutdown** command and then the **slow-shutdown enable** command, the slow offline feature does not take effect and the link is shut down.

Examples

Enable the slow offline feature for the link **lk1**.

```
<Sysname> system-view
[Sysname] loadbalance link lk1
[Sysname-lb-link-lk1] slow-shutdown enable
```

Related commands

shutdown (link view)

slow-shutdown enable (real server view)

Use **slow-shutdown enable** to enable the slow offline feature for a real server.

Use **undo slow-shutdown enable** to disable the slow offline feature for a real server.

Syntax

slow-shutdown enable

undo slow-shutdown enable

Default

The slow offline feature is disabled for a real server.

Views

Real server view

Predefined user roles

network-admin

context-admin

Usage guidelines

The **shutdown** command immediately terminates existing connections of a real server. The slow offline feature ages out the connections, and does not establish new connections.

To enable the slow offline feature for a real server, you must execute the **slow-shutdown enable** command and then the **shutdown** command. If you execute the **shutdown** command and then the **slow-shutdown enable** command, the slow offline feature does not take effect and the real server is shut down.

Examples

Enable the slow offline feature for the real server **rs**.

```
<Sysname> system-view
[Sysname] real-server rs
[Sysname-rserver-rs] slow-shutdown enable
```

Related commands

shutdown (real server view)

slow-shutdown enable (server farm member view)

Use **slow-shutdown enable** to enable the slow offline feature for a server farm member.

Use **undo slow-shutdown enable** to disable the slow offline feature for a server farm member.

Syntax

slow-shutdown enable

undo slow-shutdown enable

Default

The slow offline feature is disabled for a server farm member.

Views

Server farm member view

Predefined user roles

network-admin

context-admin

Usage guidelines

The **shutdown** command immediately terminates existing connections of a server farm member. The slow offline feature ages out the connections, and does not establish new connections.

To enable the slow offline feature for a server farm member, you must execute the **slow-shutdown enable** command and then the **shutdown** command. If you execute the **shutdown** command and then the **slow-shutdown enable** command, the slow offline feature does not take effect and the server farm member is shut down.

Examples

Enable the slow offline feature for the server farm member **rs1**.

```
<Sysname> system-view
[Sysname] server-farm sf
[Sysname-sfarm-sf] real-server rs1 port 80
[Sysname-sfarm-sf-#member#-rs1-port-80] slow-shutdown enable
```

Related commands

shutdown (server farm member view)

snat enable

Use **snat enable** to enable a SNAT global policy.

Use **undo snat enable** to disable a SNAT global policy.

Syntax

snat enable

undo snat enable

Default

A SNAT global policy is disabled.

Views

SNAT global policy view

Predefined user roles

network-admin

context-admin

Examples

Enable SNAT global policy **sn1**.

```
<Sysname> system-view
[Sysname] loadbalance snat-global-policy sn1
[Sysname-lb-snat-gp-sn1] snat enable
```

snat-mode

Use **snat-mode** to specify a translation mode for a server farm.

Use **undo snat-mode** to restore the default.

Syntax

snat-mode { **auto-map** | **tcp-option** }

undo snat-mode

Default

No translation mode is specified for a server farm.

Views

Server farm view

Predefined user roles

network-admin

context-admin

Parameters

auto-map: Specifies the automatic mapping mode.

tcp-option: Specifies the TCP option mode.

Usage guidelines

The device supports the following translation modes for a server farm:

- **Automatic mapping**—Translates the source IP address into the IP address of the interface connecting to the real servers.
- **TCP option**—Translates the source IP address into the IP address carried in the TCP option field of packets.
- **SNAT address pool**—Translates the source IP address into an IP address in the SNAT address pool specified by using the **snat-pool** (server farm view) command.

You can configured only one translation mode for a server farm. This command and the **snat-pool** (server farm view) command are mutually exclusive.

If SNAT global policies are configured and SNAT is not configured for a server farm, the server farm uses SNAT global policies for address translation.

SNAT in TCP option mode does not support translating an IPv4 address into an IPv6 address or translating an IPv6 address into an IPv4 address.

Examples

Specify the automatic mapping translation mode for server farm **sf**.

```
<Sysname> system-view
[Sysname] server-farm sf
[Sysname-sfarm-sf] snat-mode auto-map
```

Related commands

loadbalance snat-global-policy

snat-pool (server farm view)

snat-pool (link group view)

Use **snat-pool** to specify the SNAT address pool to be referenced by a link group.

Use **undo snat-pool** to restore the default.

Syntax

snat-pool *pool-name*

undo snat-pool

Default

No SNAT address pool is referenced by a link group.

Views

Link group view

Predefined user roles

network-admin

context-admin

Parameters

pool-name: Specifies the SNAT address pool name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

After a link group references a SNAT address pool, the LB device replaces the source address of packets it receives with an SNAT address before forwarding the packets.

Examples

Specify the SNAT address pool **lbsp** to be referenced by the link group **lg**.

```
<Sysname> system-view
[Sysname] loadbalance link-group lg
[Sysname-lb-lgroup-lg] snat-pool lbsp
```

snat-pool (server farm view)

Use **snat-pool** to specify the SNAT address pool to be referenced by a server farm.

Use **undo snat-pool** to restore the default.

Syntax

snat-pool *pool-name*

undo snat-pool

Default

No SNAT address pool is referenced by a server farm.

Views

Server farm view

Predefined user roles

network-admin

context-admin

Parameters

pool-name: Specifies the SNAT address pool name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

After a server farm references a SNAT address pool, the LB device replaces the source address of packets it receives with an SNAT address before forwarding the packets.

Examples

Specify the SNAT address pool **lbsp** to be referenced by the server farm **sf**.

```
<Sysname> system-view
[Sysname] server-farm sf
[Sysname-sfarm-sf] snat-pool lbsp
```

snmp-agent trap enable loadbalance

Use **snmp-agent trap enable loadbalance** to enable SNMP notifications for load balancing.

Use **undo snmp-agent trap enable loadbalance** to disable SNMP notifications for load balancing.

Syntax

snmp-agent trap enable loadbalance

undo snmp-agent trap enable loadbalance

Default

All SNMP notifications are enabled for load balancing.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

To report critical load balancing events to an NMS, enable SNMP notifications for load balancing. For load balancing event notifications to be sent correctly, you must also configure SNMP as described in the network management and monitoring configuration guide for the device.

Examples

Disable SNMP notifications for load balancing.

```
<Sysname> system-view
[Sysname] undo snmp-agent trap enable loadbalance
```

soa

Use **soa** to create an SOA resource record and enter SOA view, or enter the view of an existing SOA resource record.

Use **undo soa** to delete the SOA resource record and all its setting.

Syntax

soa

undo soa

Default

No SOA resource record exists.

Views

DNS forward zone view

Predefined user roles

network-admin

context-admin

Examples

Create an SOA resource record for DNS forward zone **abc.com** and enter SOA view.

```
<Sysname> system-view
[Sysname] loadbalance zone abc.com
[Sysname-lb-zone-abc.com] soa
[Sysname-lb-zone-abc.com-soa]
```

Related commands

display loadbalance zone

source-ip

Use **source-ip** to configure a source-IP-based request threshold.

Use **undo source-ip** to restore the default.

Syntax

source-ip request-threshold *threshold*

undo source-ip

Default

The source-IP-based request threshold is not configured.

Views

Protection rule view

Predefined user roles

network-admin

context-admin

Parameters

request-threshold *threshold*: Specifies a request threshold in the range of 1 to 4294967295.

Usage guidelines

If the number of times that a user accesses a protected URL exceeds the request threshold during the protection period, the protection action is taken. The device determines whether requests belong to the same user based on the following elements:

- **Cookie**—Requests with the same cookie value for a cookie (specified in the **cookie** command in protection rule view) belong to the same user.
- **Source IP address**—Requests with the same source IP address belong to the same user.

If you configure both a cookie-based request threshold and a source-IP-based request threshold, the protection action is taken when either threshold is exceeded.

Examples

In protection rule 5, configure a source-IP-based request threshold of 2.

```
<Sysname> system-view
[Sysname] loadbalance protection-policy p1
[Sysname-lbpp-http-p1] rule 5
[Sysname-lbpp-http-p1-rule-5] source-ip request-threshold 2
```

Related commands

cookie (protection policy view)

protected-url

protection-action

protection-period

source-ip object-group (parameter profile view)

Use **source-ip object-group** to enable collection of HTTP traffic statistics by source IP address object group.

Use **undo source-ip object-group** to remove a source IP address object group for HTTP traffic statistics collection.

Syntax

source-ip object-group *object-group-name*

undo source-ip object-group *object-group-name*

Default

HTTP traffic statistics are collected on a per-IP address basis.

Views

HTTP statistics parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

object-group-name: Specifies a source IP address object group by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

If HTTP packets match the specified URL and source IP address object group, they are counted based on the source IP address object group. If HTTP packets match the specified URL but do not

match the specified source IP address object group, they are counted based on the source IP address.

You can specify a maximum of 1024 source IP address object groups in one HTTP statistics parameter profile.

This command takes effect only on IP address objects configured by using the **host**, **subnet**, and **range** keywords in the **network** command. For information about configuring IP address objects, see object group configuration in *Security Configuration Guide*.

Examples

In HTTP statistics parameter profile **http1**, enable collection of HTTP traffic statistics by source IP address object group **cnc**.

```
<Sysname> system-view
[Sysname] parameter-profile http1 type http-statistics
[Sysname-para-http-statistics-http1] source-ip object-group cnc
```

Related commands

network (*Security Command Reference*)

object-group (*Security Command Reference*)

source-ip object-group (SNAT global policy view)

Use **source-ip object-group** to specify a source IP address object group for address translation.

Use **undo source-ip object-group** to restore the default.

Syntax

source-ip object-group *object-group-name*

undo source-ip object-group

Default

All packets are translated.

Views

SNAT global policy view

Predefined user roles

network-admin

context-admin

Parameters

object-group-name: Specifies a source IP address object group by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

If you specify a source IP address object group, the device performs SNAT on only packets with a matching source IP address. For information about configuring an IP address object group, see object group configuration in *Security Configuration Guide*.

Examples

Specify source IP address object group **obj1** for SNAT global policy **sn1**.

```
<Sysname> system-view
[Sysname] loadbalance snat-global-policy sn1
```

```
[Sysname-lb-snat-gp-sn1] source-ip object-group obj1
```

Related commands

object-group (*Security Command Reference*)

src-addr-option

Use **src-addr-option** to configure the TCP option for SNAT.

Use **undo src-addr-option** to restore the default.

Syntax

src-addr-option *option-number* [**encode** { **binary** | **string** }]

undo src-addr-option

Default

No TCP option is configured for SNAT.

Views

TCP parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

option-number: Specifies a TCP option by its number. Valid numbers are 6, 7, 9 to 18, and 22 to 254.

encode { **binary** | **string** }: Specifies the bindary or string encoding mode. The default is the binary mode.

Usage guidelines

This command enables the device to parse the IP address in the TCP option by using the specified encoding mode. Then, the device translates the source IP address according to the configured translation mode.

This command takes effect only in a TCP parameter profile that is referenced as a client-side parameter profile by a virtual server.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

In TCP parameter profile **pp3**, specify TCP option 28 with binary encoding mode for SNAT.

```
<Sysname> system-view
[Sysname] parameter-profile pp3 type tcp
[Sysname-para-tcp-pp3] src-addr-option 28 encode binary
```

ssl session-id

Use **ssl session-id** to configure an SSL sticky method based on SSL session ID.

Use **undo ssl session-id** to restore the default.

Syntax

ssl session-id

undo ssl session-id

Default

No sticky methods exist.

Views

SSL sticky group view

Predefined user roles

network-admin

context-admin

Usage guidelines

The SSL sticky method based on SSL session ID applies only to HTTPS request packets. This sticky method requires specifying an SSL server policy for the virtual server.

Examples

Configure the SSL sticky method based on SSL session ID for the SSL sticky group **sg6**.

```
<Sysname> system-view
[Sysname] sticky-group sg6 type ssl
[Sysname-sticky-ssl-sg6] ssl session-id
```

ssl url rewrite

Use **ssl url rewrite** to rewrite the URL in the Location header of HTTP response packets sent by the server.

Use **undo ssl url rewrite** to remove the configuration.

Syntax

ssl url rewrite location *location* [**clearport** *clear-port*] [**sslport** *ssl-port*]

undo ssl url rewrite location *location* [**clearport** *clear-port*]

Default

The URL in the Location header of HTTP response packets sent by the server is not rewritten.

Views

HTTP LB action view

Predefined user roles

network-admin

context-admin

Parameters

location *location*: Specifies the Location header URL regular expression, a case-sensitive string of 1 to 255 characters.

clearport *clear-port*: Specifies the HTTP port number to be rewritten, in the range of 1 to 65535. The default is 80.

sslport *ssl-port*: Specifies the SSL port number after rewrite, in the range of 1 to 65535. The default is 443.

Usage guidelines

If the Location header of an HTTP response packet contains the *location* and *clear-port* values, the system rewrites HTTP in the URL to HTTPS and rewrites the *clear-port* value to the *ssl-port* value.

Examples

For the HTTP LB action **lba2**, rewrite the URL **http://www.ss.com:8080** in the Location header of HTTP response packets sent by the server to **https://www.ss.com:443**.

```
<Sysname> system-view
[Sysname] loadbalance action lba2 type http
[Sysname-lba-http-lba2] ssl url rewrite location www.ss.com clearport 8080 sslport 443
```

ssl-client-policy (LB action view)

Use **ssl-client-policy** to specify an SSL client policy to encrypt traffic between the LB device (SSL client) and the SSL server.

Use **undo ssl-client-policy** to restore the default.

Syntax

ssl-client-policy *policy-name*

undo ssl-client-policy *policy-name*

Default

No SSL client policy is referenced.

Views

HTTP LB action view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies an SSL policy by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

The virtual servers of the fast HTTP type do not support this command.

You must disable and then enable a virtual server for a modified SSL policy to take effect.

The device does not support specifying an SSL client policy that uses the following cipher suites:

- **exp_rsa_des_cbc_sha**.
- **exp_rsa_rc2_md5**.
- **exp_rsa_rc4_md5**.
- **rsa_des_cbc_sha**.

Examples

Specify the SSL client policy **scp** for the HTTP LB action **lba2**.

```
<Sysname> system-view
[Sysname] loadbalance action lba2 type http
[Sysname-lba-http-lba2] ssl-client-policy scp
```

ssl-client-policy (virtual server view)

Use **ssl-client-policy** to specify an SSL client policy for a virtual server to encrypt traffic between the LB device (SSL client) and the SSL server.

Use **undo ssl-client-policy** to restore the default.

Syntax

ssl-client-policy *policy-name*

undo ssl-client-policy *policy-name*

Default

A virtual server does not reference any SSL client policy.

Views

HTTP virtual server view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies an SSL policy by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

The virtual servers of the fast HTTP type do not support this command.

You must disable and then enable a virtual server for a modified SSL policy to take effect.

The device does not support specifying an SSL client policy that uses the following cipher suites:

- **exp_rsa_des_cbc_sha**.
- **exp_rsa_rc2_md5**.
- **exp_rsa_rc4_md5**.
- **rsa_des_cbc_sha**.

Examples

Specify the SSL client policy **scp** for the HTTP virtual server **vs2**.

```
<Sysname> system-view
[Sysname] virtual-server vs2 type http
[Sysname-vs-http-vs2] ssl-client-policy scp
```

ssl-server-policy

Use **ssl-server-policy** to specify an SSL server policy for a virtual server to encrypt traffic between the LB device (SSL server) and the SSL client.

Use **undo ssl-server-policy** to remove an SSL server policy from a virtual server.

Syntax

ssl-server-policy *policy-name* [**sni** *server-name*]

undo ssl-server-policy *policy-name* [*policy-name* **sni**]

Default

A virtual server does not reference any SSL server policy.

Views

HTTP/TCP virtual server view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies an SSL policy by its name, a case-insensitive string of 1 to 31 characters.

sni *server-name*: Specifies an SSL server indication, a case-insensitive string of 1 to 253 characters.

Usage guidelines

The virtual servers of the fast HTTP type do not support this command.

You must disable and then enable a virtual server for a modified SSL policy to take effect.

The device does not support specifying an SSL server policy that uses the following cipher suites:

- **exp_rsa_des_cbc_sha**.
- **exp_rsa_rc2_md5**.
- **exp_rsa_rc4_md5**.
- **rsa_des_cbc_sha**.

If you execute this command multiple times without the **sni** *server-name* option, the most recent configuration takes effect.

You can specify multiple SSL server policies with SSL server indications, and each SSL server policy must have a different SSL server indication.

If you specify multiple SSL server policies, only the SSL server policy without an SSL server indication takes effect.

Examples

Specify the SSL server policy **ssp** for the HTTP virtual server **vs2**.

```
<Sysname> system-view
[Sysname] virtual-server vs2 type http
[Sysname-vs-http-vs2] ssl-server-policy ssp
```

statistics-match url

Use **statistics-match url** to configure a URL match rule.

Use **undo statistics-match url** to delete a URL match rule.

Syntax

statistics-match [*rule-id*] **url** *url*

undo statistics-match *rule-id*

Default

No URL match rules exist.

Views

Statistics node view

Predefined user roles

network-admin

context-admin

Parameters

rule-id: Specifies the match rule ID in the range of 1 to 256. If you do not specify a match rule ID, the system assigns the smallest available rule ID to the match rule.

url: Specifies a URL regular expression, a case-sensitive string of 1 to 255 characters. The string cannot contain question marks (?).

Usage guidelines

You can configure a maximum of 256 URL match rules for one statistics node.

Examples

In statistics node **bank**, configure a string of **.html** to match URLs in HTTP packets.

```
<Sysname> system-view
[Sysname] parameter-profile http1 type http-statistics
[Sysname-para-http-statistics-http1] node bank
[Sysname-para-http-statistics-http1-node-bank] statistics-match url *.html
```

status-code

Use **status-code** to configure a response status code to check.

Use **undo status-code** to remove a response status code.

Syntax

status-code *code*

undo status-code *code*

Default

No response status code is configured for checking.

Views

HTTP passive LB probe template view

Predefined user roles

network-admin

context-admin

Parameters

code: Specifies a response status code, in the range of 100 to 599.

Usage guidelines

The device monitors the responses of HTTP requests with URLs specified in the **check-url** command. If the status code in an HTTP response is the same as the specified response status code, a URL error is recorded.

You can configure a maximum of 10 response status codes for one HTTP passive load balancing template.

Examples

Configure response status code 404 in HTTP passive load balancing template **tplt**.

```
<Sysname> system-view
```

```
[Sysname] loadbalance probe-template http-passive tplt
[Sysname-lbpt-http-passive-tplt] status-code 404
```

Related commands

check-url

sticky

Use **sticky** to specify a sticky group for a virtual server.

Use **undo sticky** to restore the default.

Syntax

sticky *sticky-name*

undo sticky

Default

No sticky group is specified for a virtual server.

Views

HTTP virtual server view

Predefined user roles

network-admin

context-admin

Parameters

sticky-name: Specifies a sticky group by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

You can also specify a sticky group by using the **default server-farm** and **server-farm** (LB action view) commands. The sticky group specified by using the **sticky** command has the highest priority.

This command allows you to specify only HTTP cookie sticky groups.

Examples

Specify the HTTP cookie sticky group **test** for HTTP virtual server **vs**.

```
<Sysname> system-view
[Sysname] virtual-server vs type http
[Sysname-vs-http-vs] sticky test
```

Related commands

default server-farm

server-farm (LB action view)

sticky-group

sticky-group

Use **sticky-group** to create a sticky group and enter its view, or enter the view of an existing sticky group.

Use **undo sticky-group** to delete the specified sticky group.

Syntax

sticky-group *group-name* [**type** { **address-port** | **http-content** | **http-cookie** | **http-header** | **http-passive** | **payload** | **radius**| **sip** | **ssl** | **tcp-payload** | **udp-passive** }]

undo sticky-group *group-name*

Default

No sticky groups exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a sticky group name, a case-insensitive string of 1 to 63 characters.

type { **address-port** | **http-content** | **http-cookie** | **http-header** | **http-passive** | **payload** | **radius** | **sip** | **ssl** | **tcp-payload** | **udp-passive** }: Specifies the sticky group type, address and port, HTTP entity, HTTP cookie, HTTP header, HTTP passive, HTTP or UDP payload, RADIUS, SIP, SSL, TCP payload, or UDP passive. When you create a sticky group, you must specify the sticky group type. You can enter an existing sticky group view without entering the type of the sticky group.

Usage guidelines

A sticky group uses a specific sticky method to distribute similar sessions to the same real server or link. The sticky method applies to the first packet of a session. Subsequent packets of the session are distributed to the same real server or link.

You can configure only the address- and port-type sticky groups if the device does not have any licenses installed. To configure sticky groups of any other type, you must install licenses. For information about licensing, see license management in *Fundamentals Configuration Guide*.

Examples

Create the address- and port-type sticky group **sg1** and enter sticky group view.

```
<Sysname> system-view
[Sysname] sticky-group sg1 type address-port
[Sysname-sticky-address-port-sg1]
```

sticky-over-busy enable

Use **sticky-over-busy enable** to enable stickiness-over-busyness.

Use **undo sticky-over-busy enable** to disable stickiness-over-busyness.

Syntax

sticky-over-busy enable

undo sticky-over-busy enable

Default

Stickiness-over-busyness is disabled.

Views

Sticky group view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command enables the device to assign client requests to real servers based on sticky entries, regardless of whether the real servers are busy.

When stickiness-over-busyness is disabled, the device assigns client requests to only the real servers in normal state.

Examples

In address- and port-type sticky group **sg1**, enable stickiness-over-busyness.

```
<Sysname> system-view
[Sysname] sticky-group sg1 type address-port
[Sysname-sticky-address-port-sg1] sticky-over-busy enable
```

sticky-sync enable (transparent DNS proxy view)

Use **sticky-sync enable** to enable sticky entry synchronization for a transparent DNS proxy.

Use **undo sticky-sync enable** to disable sticky entry synchronization for a transparent DNS proxy.

Syntax

sticky-sync enable [**global**]

undo sticky-sync enable

Default

Sticky entry synchronization is disabled for a transparent DNS proxy.

Views

Transparent DNS proxy view

Predefined user roles

network-admin

context-admin

Parameters

global: Enables global synchronization.

Usage guidelines

This command can back up sticky entry information to ensure service continuity during a master and backup switchover in hot backup mode.

In a VRRP network, you must specify the **global** keyword for the sticky entry synchronization feature to take effect.

The following configuration changes will cause the device to delete existing sticky entries and generate new ones based on subsequent traffic:

- Disable sticky entry synchronization.
- Change the sticky entry synchronization type.

Examples

Enable sticky entry synchronization for transparent DNS proxy **dns_proxy1**.

```
<Sysname>system-view
[Sysname] loadbalance dns-proxy dns_proxy1 type udp
[Sysname-lb-dp-udp-dns_proxy1] sticky-sync enable
```

sticky-sync enable (virtual server view)

Use **sticky-sync enable** to enable sticky entry synchronization for a virtual server.

Use **undo sticky-sync enable** to disable sticky entry synchronization for a virtual server.

Syntax

sticky-sync enable [**global**]

undo sticky-sync enable

Default

Sticky entry synchronization is disabled for a virtual server.

Views

Virtual server view

Predefined user roles

network-admin

context-admin

Parameters

global: Enables global synchronization.

Usage guidelines

For successful sticky entry synchronization, if you want to specify a sticky group, enable sticky entry synchronization before specifying a sticky group on both LB devices. You can specify a sticky group by using the **sticky** *sticky-name* option when you specify a primary server farm (see the default server-farm command).

In a VRRP network, you must specify the **global** keyword for the sticky entry synchronization feature to take effect.

The following configuration changes will cause the device to delete existing sticky entries and generate new ones based on subsequent traffic:

- Disable sticky entry synchronization.
- Change the sticky entry synchronization type.

Examples

Enable sticky entry synchronization for the IP-type virtual server **vs3**.

```
<Sysname>system-view
[Sysname] virtual-server vs3 type ip
[Sysname-vs-ip-vs3] sticky-sync enable
```

success-criteria (DNS server pool member view)

Use **success-criteria** to specify the health monitoring success criteria for a DNS server pool member.

Use **undo success-criteria** to restore the default.

Syntax

success-criteria { **all** | **at-least** *min-number* }

undo success-criteria

Default

Health monitoring succeeds only when all the specified health monitoring methods succeed.

Views

DNS server pool member view

Predefined user roles

network-admin

context-admin

Parameters

all: Specifies the health monitoring success criteria as all successful health monitoring methods.

at-least *min-number*: Specifies the health monitoring success criteria as the specified minimum number of successful health monitoring methods, in the range of 1 to 4294967295.

Usage guidelines

If the *min-number* setting exceeds the number of existing health monitoring methods on the device, the number of existing health monitoring methods applies.

The health monitoring success criteria configuration in DNS server pool member view takes precedence over the configuration in DNS server pool view.

The health monitoring result for a DNS server affects the availability of a DNS server pool member. The health monitoring result for a DNS server pool member does not affect the availability of a DNS server.

Examples

Configure the health monitoring success criteria for the DNS server pool member **ds1** as a minimum number of 2 successful health monitoring methods.

```
<Sysname> system-view
[Sysname] loadbalance dns-server-pool dsp1
[Sysname-lb-dsp-dsp1] dns-server ds1 port 10
[Sysname-lb-dsp-dsp1-#member#-ds1-port-10] success-criteria at-least 2
```

success-criteria (DNS server pool view)

Use **success-criteria** to specify the health monitoring success criteria for a DNS server pool.

Use **undo success-criteria** to restore the default.

Syntax

success-criteria { **all** | **at-least** *min-number* }

undo success-criteria

Default

Health monitoring succeeds only when all the specified health monitoring methods succeed.

Views

DNS server pool view

Predefined user roles

network-admin

context-admin

Parameters

all: Specifies the health monitoring success criteria as all successful health monitoring methods.

at-least *min-number*: Specifies the health monitoring success criteria as the specified minimum number of successful health monitoring methods, in the range of 1 to 4294967295.

Usage guidelines

If the *min-number* setting exceeds the number of existing health monitoring methods on the device, the number of existing health monitoring methods applies.

The health monitoring success criteria configuration in DNS server view takes precedence over the configuration in DNS server pool view.

Examples

Configure the health monitoring success criteria for the DNS server pool **dns-pool** as a minimum number of 2 successful health monitoring methods.

```
<Sysname> system-view
[Sysname] loadbalance dns-server-pool dns-pool
[Sysname-lb-dspool-dns-pool] success-criteria at-least 2
```

Related commands

success-criteria (DNS server view)

success-criteria (DNS server view)

Use **success-criteria** to specify the health monitoring success criteria for a DNS server.

Use **undo success-criteria** to restore the default.

Syntax

success-criteria { **all** | **at-least** *min-number* }

undo success-criteria

Default

Health monitoring succeeds only when all the specified health monitoring methods succeed.

Views

DNS server view

Predefined user roles

network-admin

context-admin

Parameters

all: Specifies the health monitoring success criteria as all successful health monitoring methods.

at-least *min-number*: Specifies the health monitoring success criteria as the specified minimum number of successful health monitoring methods, in the range of 1 to 4294967295.

Usage guidelines

If the *min-number* setting exceeds the number of existing health monitoring methods on the device, the number of existing health monitoring methods applies.

The health monitoring success criteria configuration in DNS server view takes precedence over the configuration in DNS server pool view.

Examples

Configure the health monitoring success criteria for DNS server **ds1** as a minimum number of 2 successful health monitoring methods.

```
<Sysname> system-view
[Sysname] loadbalance dns-server ds1
[Sysname-lb-ds-ds1] success-criteria at-least 2
```

Related commands

success-criteria (DNS server pool view)

success-criteria (link group member view)

Use **success-criteria** to specify the health monitoring success criteria for a link group member.

Use **undo success-criteria** to restore the default.

Syntax

success-criteria { **all** | **at-least** *min-number* }

undo success-criteria

Default

Health monitoring succeeds only when all the specified health monitoring methods succeed.

Views

Link group member view

Predefined user roles

network-admin

context-admin

Parameters

all: Specifies the health monitoring success criteria as all successful health monitoring methods.

at-least *min-number*: Specifies the health monitoring success criteria as the specified minimum number of successful health monitoring methods, in the range of 1 to 4294967295.

Usage guidelines

If the *min-number* setting exceeds the number of existing health monitoring methods on the device, the number of existing health monitoring methods applies.

The health monitoring success criteria configuration in link group member view takes precedence over the configuration in link group view.

The health monitoring result for a link affects the availability of a link group member. The health monitoring result for a link group member does not affect the availability of a link.

Examples

Configure the health monitoring success criteria for the link group member **lk1** as a minimum number of 2 successful health monitoring methods.

```
<Sysname> system-view
[Sysname] loadbalance link-group lg
[Sysname-lb-lgroup-lg] link lk1
[Sysname-lb-lgroup-lg-#member#-lk1] success-criteria at-least 2
```

success-criteria (link group view)

Use **success-criteria** to specify the health monitoring success criteria for a link group.

Use **undo success-criteria** to restore the default.

Syntax

success-criteria { **all** | **at-least** *min-number* }

undo success-criteria

Default

Health monitoring succeeds only when all the specified health monitoring methods succeed.

Views

Link group view

Predefined user roles

network-admin

context-admin

Parameters

all: Specifies the health monitoring success criteria as all successful health monitoring methods.

at-least *min-number*: Specifies the health monitoring success criteria as the specified minimum number of successful health monitoring methods, in the range of 1 to 4294967295.

Usage guidelines

If the *min-number* setting exceeds the number of existing health monitoring methods on the device, the number of existing health monitoring methods applies.

The health monitoring success criteria configuration in link view takes precedence over the configuration in link group view.

Examples

Configure the health monitoring success criteria for the link group **lg** as a minimum number of 2 successful health monitoring methods.

```
<Sysname> system-view
[Sysname] loadbalance link-group lg
[Sysname-lb-lgroup-lg] success-criteria at-least 2
```

Related commands

success-criteria (link view)

success-criteria (link view)

Use **success-criteria** to specify the health monitoring success criteria for an LB link.

Use **undo success-criteria** to restore the default.

Syntax

success-criteria { **all** | **at-least** *min-number* }

undo success-criteria

Default

Health monitoring succeeds only when all the specified health monitoring methods succeed.

Views

LB link view

Predefined user roles

network-admin

context-admin

Parameters

all: Specifies the health monitoring success criteria as all successful health monitoring methods.

at-least *min-number*: Specifies the health monitoring success criteria as the specified minimum number of successful health monitoring methods, in the range of 1 to 4294967295.

Usage guidelines

If the *min-number* setting exceeds the number of existing health monitoring methods on the device, the number of existing health monitoring methods applies.

Examples

Configure the health monitoring success criteria for the LB link **lk1** as a minimum number of 2 successful health monitoring methods.

```
<Sysname> system-view
[Sysname] loadbalance link lk1
[Sysname-lb-link-lk1] success-criteria at-least 2
```

Related commands

success-criteria (link group view)

success-criteria (real server view)

Use **success-criteria** to specify the health monitoring success criteria for a real server.

Use **undo success-criteria** to restore the default.

Syntax

success-criteria { **all** | **at-least** *min-number* }

undo success-criteria

Default

Health monitoring succeeds only when all the specified health monitoring methods succeed.

Views

Real server view

Predefined user roles

network-admin

context-admin

Parameters

all: Specifies the health monitoring success criteria as all successful health monitoring methods.

at-least *min-number*: Specifies the health monitoring success criteria as the specified minimum number of successful health monitoring methods, in the range of 1 to 4294967295.

Usage guidelines

If the *min-number* setting exceeds the number of existing health monitoring methods on the device, the number of existing health monitoring methods applies.

The health monitoring success criteria configuration in real server view takes precedence over the configuration in server farm view.

Examples

Configure the health monitoring success criteria for the real server **rs** as a minimum number of 2 successful health monitoring methods.

```
<Sysname> system-view
[Sysname] real-server rs
[Sysname-rserver-rs] success-criteria at-least 2
```

success-criteria (server farm member view)

Use **success-criteria** to specify the health monitoring success criteria for a server farm member.

Use **undo success-criteria** to restore the default.

Syntax

success-criteria { **all** | **at-least** *min-number* }

undo success-criteria

Default

Health monitoring succeeds only when all the specified health monitoring methods succeed.

Views

Server farm member view

Predefined user roles

network-admin

context-admin

Parameters

all: Specifies the health monitoring success criteria as all successful health monitoring methods.

at-least *min-number*: Specifies the health monitoring success criteria as the specified minimum number of successful health monitoring methods, in the range of 1 to 4294967295.

Usage guidelines

If the *min-number* setting exceeds the number of existing health monitoring methods on the device, the number of existing health monitoring methods applies.

The health monitoring success criteria configuration in server farm member view takes precedence over the configuration in server farm view.

The health monitoring result for a real server affects the availability of a server farm member. The health monitoring result for a server farm member does not affect the availability of a real server.

Examples

Configure the health monitoring success criteria for the server farm member **rs1** as a minimum number of 2 successful health monitoring methods.

```
<Sysname> system-view
[Sysname] server-farm sf
[Sysname-sfarm-sf] real-server rs1 port 80
[Sysname-sfarm-sf-#member#-rs1-port-80] success-criteria at-least 2
```

success-criteria (server farm view)

Use **success-criteria** to specify the health monitoring success criteria for a server farm.

Use **undo success-criteria** to restore the default.

Syntax

success-criteria { **all** | **at-least** *min-number* }

undo success-criteria

Default

Health monitoring succeeds only when all the specified health monitoring methods succeed.

Views

Server farm view

Predefined user roles

network-admin

context-admin

Parameters

all: Specifies the health monitoring success criteria as all successful health monitoring methods.

at-least *min-number*: Specifies the health monitoring success criteria as the specified minimum number of successful health monitoring methods, in the range of 1 to 4294967295.

Usage guidelines

If the *min-number* setting exceeds the number of existing health monitoring methods on the device, the number of existing health monitoring methods applies.

The health monitoring success criteria configuration in real server view takes precedence over the configuration in server farm view.

Examples

Configure the health monitoring success criteria for the server farm **sf** as a minimum number of 2 successful health monitoring methods.

```
<Sysname> system-view
[Sysname] server-farm sf
[Sysname-sfarm-sf] success-criteria at-least 2
```

syn retransmission-timeout

Use **syn retransmission-timeout** to set the retransmission timeout time for SYN packets.

Use **undo syn retransmission-timeout** to restore the default.

Syntax

syn retransmission-timeout *timeout-value*

undo syn retransmission-timeout

Default

The retransmission timeout time for SYN packets is 10 seconds.

Views

TCP parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

timeout-value: Specifies the retransmission timeout time for SYN packets, in the range of 1 to 75 seconds.

Usage guidelines

This command sets the amount of time the device waits for a SYN ACK before closing a TCP connection.

Examples

Set the retransmission timeout time for SYN packets to 5 seconds for TCP connections.

```
<Sysname> system-view
[Sysname] parameter-profile profile type tcp
[Sysname-para-tcp-profile] syn retransmission-timeout 5
```

Related commands

display parameter-profile

tcp connection idle-timeout

Use **tcp connection idle-timeout** to set the idle timeout for TCP connections.

Use **undo tcp connection idle-timeout** to restore the default.

Syntax

tcp connection idle-timeout *value*

undo tcp connection idle-timeout

Default

The idle timeout is 0 seconds for TCP connections, which means TCP connections never time out.

Views

TCP parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

value: Specifies the idle timeout in the range of 10 to 86400 seconds.

Usage guidelines

This command sets the idle timeout for TCP connections between the LB device and the clients and for TCP connections between the LB device and the servers. If no traffic is available on a TCP connection before the idle timeout expires, the LB device terminates the TCP connection.

Examples

Set the idle timeout to 60 seconds for TCP connections.

```
<Sysname> system-view
[Sysname] parameter-profile pp1 type tcp
[Sysname-para-tcp-pp1] tcp connection idle-timeout 60
```

tcp mss

Use **tcp mss** to set the MSS for the LB device.

Use **undo tcp mss** to restore the default.

Syntax

tcp mss *value*

undo tcp mss

Default

The MSS is not set for the LB device.

Views

TCP parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

value: Specifies the MSS value in the range of 128 to 1460 bytes.

Usage guidelines

This command takes effect only when the fast HTTP or HTTP virtual server has referenced a TCP parameter profile.

When the client establishes a TCP connection to the LB device, the client sends its own MSS value to the LB device. The LB device records the MSS value and sends the configured MSS value to the client. The client and the LB device use the smaller MSS value for communication.

When the LB device establishes a TCP connection to the server, the LB device sends the configured MSS value to the server. The server records the MSS value and sends its own MSS value to the LB device. The LB device and the server use the smaller MSS value for communication.

Examples

Set the MSS to 1300 bytes for the LB device.

```
<Sysname> system-view
[Sysname] parameter-profile tcp type tcp
[Sysname-para-tcp-tcp] tcp mss 1300
```

tcp option insert

Use **tcp option insert** to insert the client IP address into a TCP option.

Use **undo tcp option insert** to remove the configuration.

Syntax

tcp option insert *option-number* **src-addr** [**encode** { **binary** | **string** }]

undo tcp option insert *option-number*

Default

The client IP address is not inserted into any TCP options.

Views

TCP parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

option-number: Specifies a TCP option by its number. Valid values are 6, 7, 9 to 18, and 22 to 254.

encode { **binary** | **string** }: Specifies the binary or string encoding mode. The default is binary mode.

Usage guidelines

This command inserts the client's actual IP address as the source IP address into the specified option in headers of TCP packets sent to the server.

This command takes effect only on TCP parameter profiles referenced by the following virtual servers:

- HTTP virtual servers.
- TCP virtual servers configured with SSL server policies.
- TCP virtual servers operating at Layer 7.
- MySQL virtual servers.

You can execute this command multiple times to insert the client IP address to a maximum of five TCP options.

If you execute this command multiple times for the same TCP option, the most recent configuration takes effect.

Examples

In TCP parameter profile **para2**, insert the client IP address into TCP option 28.

```
<Sysname> system-view
[Sysname] parameter-profile para2 type tcp
[Sysname-para-tcp-para2] tcp option insert 28 src-addr
```

Related commands

parameter-profile

tcp option remove

Use **tcp option remove** to remove the specified TCP option from TCP packet headers.

Use **undo tcp option remove** to cancel the removal configuration.

Syntax

tcp option remove *option-number*

undo tcp option remove *option-number*

Default

No TCP option is removed from TCP packet headers.

Views

TCP parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

option-number: Specifies a TCP option by its number in the range of 3 to 254.

Usage guidelines

This command removes the specified TCP option from headers of TCP packets sent to the server.

You can execute this command multiple times to remove a maximum of five TCP options.

Examples

In TCP parameter profile **para2**, remove TCP option 8 from TCP packet headers.

```
<Sysname> system-view
[Sysname] parameter-profile para2 type tcp
[Sysname-para-tcp-para2] tcp option remove 8
```

Related commands

parameter-profile

tcp window-size

Use **tcp window-size** to configure the maximum local window size for TCP connections.

Use **undo tcp window-size** to restore the default.

Syntax

tcp window-size *size*

undo tcp window-size

Default

The maximum local window size for TCP connections is 65535.

Views

TCP parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

size: Specifies the maximum local window size for TCP connections, in the range of 8192 to 65535.

Examples

Set the maximum local window size for TCP connections to 8192 for the TCP parameter profile **pp3**.

```
<Sysname> system-view
[Sysname] parameter-profile pp3 type tcp
[Sysname-para-tcp-pp3] tcp window-size 8192
```

tcp-close

Use **tcp-close** to configure the method to close TCP connections.

Use **undo tcp-close** to restore the default.

Syntax

tcp-close { **fin** | **rst** }

undo tcp-close

Default

FIN packets are sent to close TCP connections.

Views

Generic/HTTP LB action view

Predefined user roles

network-admin

context-admin

Parameters

fin: Closes TCP connections by sending FIN packets.

rst: Closes TCP connections by sending RST packets.

Examples

In generic LB action **lba1**, configure the **rst** method to close TCP connections.

```
<Sysname> system-view
[Sysname] loadbalance action lba1 type generic
[Sysname-lba-generic-lba1] tcp-close rst
```

tcp-payload

Use **tcp-payload** to configure the TCP payload sticky method.

Use **undo tcp-payload** to delete the TCP payload sticky method.

Syntax

tcp-payload [**offset** *offset*] [**start** *start-string*] [**end** *end-string* | **length** *length*]

undo tcp-payload

Default

No TCP payload sticky methods exist.

Views

TCP payload sticky group view

Predefined user roles

network-admin

context-admin

Parameters

offset *offset*: Specifies the offset value of the TCP payload based on the start of the TCP packet, in the range of 0 to 1000 bytes. The default is 0.

start *start-string*: Specifies the regular expression that marks the start of the TCP payload, a case-sensitive string of 1 to 127 characters starting from the *offset* value. The string cannot contain question marks (?).

end *end-string*: Specifies the regular expression that marks the end of the TCP payload, a case-sensitive string of 1 to 127 characters starting from the *start-string* value. The string cannot contain question marks (?).

length *length*: Specifies the length of the TCP payload, in the range of 0 to 1000 bytes. The default is 0, which indicates all lengths.

Usage guidelines

Use this command to obtain the TCP payload information used to generate sticky entries based on the *offset*, *start-string*, *end-string*, and *length* values. The *start-string* and *end-string* values are not included in the sticky entry information.

If you do not specify any parameters in this command, the sticky entry is generated based on the whole TCP packet.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure the TCP payload sticky method for the TCP payload sticky group **sg**: Use the whole TCP packet to generate sticky entries.

```
<Sysname> system-view
[Sysname] sticky-group sg type tcp-payload
[Sysname-sticky-payload-sg] tcp-payload
```

timeout (LB probe template view)

Use **timeout** to set the timeout time for probe responses.

Use **undo timeout** to restore the default.

Syntax

timeout *timeout-value*

undo timeout

Default

The timeout time for probe responses is 3 seconds for ICMP probe packets and custom monitoring probe packets and is 5 seconds for HTTP passive probe packets.

Views

ICMP LB probe template view

HTTP passive LB probe template view

Custom-monitoring LB probe template view

Predefined user roles

network-admin

context-admin

Parameters

timeout-value: Specifies the timeout time for probe responses, in the range of 1 to 60 seconds for ICMP probe packets, 1 to 255 seconds for HTTP passive probe packets, and 1 to 86400 seconds for custom monitoring probe packets.

Usage guidelines

As a best practice, set the timeout time for probe responses to be smaller than the monitoring time (set by using the **monitor-interval** command).

After an HTTP passive LB probe template is referenced, the device monitors the responses of HTTP requests with URLs specified in the **check-url** command. If the response time for an HTTP request exceeds the specified timeout time, a URL error is recorded.

Examples

Set the timeout time for probe responses to 5 seconds in the ICMP template **icmptplt**.

```
<Sysname> system-view
[Sysname] loadbalance probe-template icmp icmptplt
[Sysname-lbpt-icmp-icmptplt] timeout 5
```

Related commands

check-url
monitor-interval

timeout (proximity view)

Use **timeout** to set the timeout timer for proximity entries.

Use **undo timeout** to restore the default.

Syntax

timeout *timeout-value*

undo timeout

Default

The timeout timer for proximity entries is 60 seconds.

Views

Proximity view

Predefined user roles

network-admin

context-admin

Parameters

timeout-value: Specifies the timeout timer in the range of 60 to 3600 seconds.

Examples

Set the timeout timer for proximity entries to 80 seconds.

```
<Sysname> system-view
[Sysname] loadbalance proximity
```

```
[Sysname-lb-proximity] timeout 80
```

timeout (sticky group view)

Use **timeout** to set the timeout timer for sticky entries.

Use **undo timeout** to restore the default.

Syntax

timeout { **indefinite** | *timeout-value* }

undo timeout

Default

The timeout timer for sticky entries is 86400 seconds for sticky groups of the HTTP cookie, HTTP passive, and UDP passive types and 60 seconds for sticky groups of other types.

Views

Sticky group view

Predefined user roles

network-admin

context-admin

Parameters

indefinite: Specifies an indefinite timeout timer for sticky entries so that the sticky entries never age out. Sticky groups of the HTTP cookie type, HTTP passive type, and UDP passive type do not support this keyword.

timeout-value: Specifies the timeout timer in the range of 0 to 31536000 seconds for sticky groups of the HTTP cookie type and in the range of 10 to 604800 seconds for sticky groups of other types.

Usage guidelines

For sticky groups of the HTTP cookie type, the following principles apply:

- If the sticky method is cookie insert or cookie rewrite, a timeout timer of 0 indicates session persistency.
- If the sticky method is cookie get, a timeout timer of 0 indicates the timeout time for the sticky entries is 0 seconds.

Examples

Set the timeout timer for sticky entries to 100 seconds in the address- and port-type sticky group **sg1**.

```
<Sysname> system-view
[Sysname] sticky-group sg1 type address-port
[Sysname-sticky-address-port-sg1] timeout 100
```

time-wait timeout

Use **time-wait timeout** to set the TIME_WAIT state timeout time for TCP connections.

Use **undo time-wait timeout** to restore the default.

Syntax

time-wait timeout *value*

undo time-wait timeout

Default

The TIME_WAIT state timeout time is 2 seconds for TCP connections.

Views

TCP parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

value: Specifies the TIME_WAIT state timeout time in the range of 1 to 65535 seconds.

Usage guidelines

A TCP connection cannot be released until the TIME_WAIT timer expires. To release TCP connections faster and improve load balancing efficiency, use this command to set a shorter TIME_WAIT state timeout time.

Examples

Set the TIME_WAIT state timeout time for TCP connections to 30 seconds in the TCP parameter profile **pa1**.

```
<Sysname> system-view
[Sysname] parameter-profile pa1 type tcp
[Sysname-para-tcp-pa1] time-wait timeout 30
```

topology region

Use **topology region** to configure a topology.

Use **undo topology region** to restore the default.

Syntax

topology region *region-name* { **ip** *ipv4-address* { *mask-length* | *mask* } | **ipv6** *ipv6-address prefix-length* } [**priority** *priority*]

undo topology region *region-name* [**ip** *ipv4-address* [*mask-length* | *mask*] | **ipv6** *ipv6-address* [*prefix-length*]]

Default

No topologies exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

region-name: Specifies a region by its name, a case-insensitive string of 1 to 63 characters.

ip *ipv4-address*: Specifies the IPv4 address of a virtual server.

mask-length: Specifies the mask length for the IPv4 address, in the range of 0 to 32. The default is 32.

mask: Specifies the mask for the IPv4 address. The default is 255.255.255.255.

ipv6 *ipv6-address prefix-length*: Specifies the IPv6 address of a virtual server.

prefix-length: Specifies the prefix length for the IPv6 address, in the range of 0 to 128. The default is 128.

priority *priority*: Specifies the priority of the topology, in the range of 1 to 255. The default weight is 100.

Usage guidelines

A topology associates the region where the local DNS server resides with the IP address of a virtual server.

When the static proximity algorithm (**topology**) is specified for the virtual server pool by using the **predictor** command, you must configure a topology.

When a DNS request matches multiple topology records, the topology record with the highest priority is selected.

You can execute this command multiple times to configure multiple IP address ranges for a region.

If you only specify a region when deleting a topology, all topologies for the region are deleted.

Examples

Configure a topology by associating the region **region-ct** with the IPv4 address **1.2.3.4**.

```
<Sysname> system-view
[Sysname] topology region region-ct ip 1.2.3.4 24 priority 200
```

Related commands

loadbalance region

predictor (virtual server pool view)

translation-mode

Use **translation-mode** to configure a translation mode for a SNAT global policy.

Use **undo translation-mode** to restore the default.

Syntax

translation-mode { **auto-map** | **snat-pool** *pool-name* }

undo translation-mode

Default

No translation mode is configured for a SNAT global policy.

Views

SNAT global policy view

Predefined user roles

network-admin

context-admin

Parameters

auto-map: Specifies the automatic mapping mode.

snat-pool *pool-name*: Specifies the SNAT address pool mode. The *pool-name* argument specifies the SNAT address pool name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

The device supports the following translation modes in a SNAT global policy:

- **Automatic mapping**—Translates the source IP address into the IP address of the interface connecting to the real servers.
- **SNAT address pool**—Translates the source IP address into an IP address in the specified SNAT address pool.

If SNAT is not configured for a server farm, the server farm uses SNAT global policies for address translation.

Examples

Specify SNAT address pool **sp** for address translation in SNAT global policy **sn1**.

```
<Sysname> system-view
[Sysname] loadbalance snat-global-policy sn1
[Sysname-lb-snat-gp-sn1] translation-mode snat-pool sp
```

transparent enable (link group view)

Use **transparent enable** to disable NAT for a link group.

Use **undo transparent enable** to enable NAT for a link group.

Syntax

transparent enable

undo transparent enable

Default

NAT is enabled for a link group.

Views

Link group view

Predefined user roles

network-admin

context-admin

Examples

Disable NAT for the link group **lg**.

```
<Sysname> system-view
[Sysname] loadbalance link-group lg
[Sysname-lb-lgroup-sinalab] transparent enable
```

transparent enable (server farm view)

Use **transparent enable** to disable NAT for a server farm.

Use **undo transparent enable** to enable NAT for a server farm.

Syntax

transparent enable

undo transparent enable

Default

NAT is enabled for a server farm.

Views

Server farm view

Predefined user roles

network-admin

context-admin

Usage guidelines

If the server farm is referenced by a virtual server of the HTTP type, the NAT feature takes effect even if it is disabled.

Examples

Disable NAT for the server farm **sf**.

```
<Sysname> system-view
[Sysname] server-farm sf
[Sysname-sfarm-sf] transparent enable
```

trusted-access-controller

Use **trusted-access-controller** to specify a trusted access controller for a virtual server.

Use **undo trusted-access-controller** to restore the default.

Syntax

trusted-access-controller iam *controller-name* **action** { **api-auth** | **app-auth** }

undo trusted-access-controller

Default

A virtual server does not reference any trusted access controller.

Views

HTTP virtual server view

Predefined user roles

network-admin

context-admin

Parameters

iam: Specifies the IAM-type trusted access controller.

controller-name: Specifies a trusted access controller by its name, a case-insensitive string of 1 to 63 characters.

action: Specifies an action to take.

api-auth: Performs API authentication.

app-auth: Performs application authentication.

Usage guidelines

The device performs authentication and authorization with the specified trusted access controller for matching requests on behalf of clients. If the authentication and authorization succeed, the device

forwards the requests. For more information about trusted access controllers, see trusted access controller in *Security Configuration Guide*.

Examples

Specify IAM trusted access controller **tac** for the HTTP virtual server **vs3** to perform application authentication.

```
<Sysname> system-view
[Sysname] virtual-server vs3 type http
[Sysname-vs-http-vs3]] trusted-access-controller iam tac action app-auth
```

Related commands

trusted-access controller (*Security Command Reference*)

ttl (DNS forward zone view)

Use **ttl** to set the TTL for resource records.

Use **undo ttl** to restore the default.

Syntax

ttl *ttl-value*

undo ttl

Default

The TTL for resource records is 3600 seconds.

Views

DNS forward zone view

Predefined user roles

network-admin

context-admin

Parameters

ttl-value: Specifies the TTL value in the range of 0 to 4294967295 seconds.

Examples

Set the TTL for resource records to 1 day for DNS forward zone **abc.com**.

```
<Sysname> system-view
[Sysname] loadbalance zone abc.com
[Sysname-lb-zone-abc.com] ttl 86400
```

Related commands

display loadbalance zone

ttl (DNS mapping view)

Use **ttl** to set the TTL for DNS records.

Use **undo ttl** to restore the default.

Syntax

ttl *ttl-value*

undo ttl

Default

The TTL for DNS records is 3600 seconds.

Views

DNS mapping view

Predefined user roles

network-admin

context-admin

Parameters

ttl-value: Specifies the TTL value in the range of 0 to 4294967295 seconds.

Usage guidelines

Use this command to set a proper TTL to cache DNS records for DNS responses.

- For the DNS client to get the updated DNS record when the LB policy or virtual server configuration changes, set a smaller TTL value, for example, 60 seconds.
- For stable, fast domain name resolution when the network is stable, set a larger TTL value, for example, 86400 seconds.

Examples

Set the TTL for DNS records to 4000 seconds for the DNS mapping **dm1**.

```
<Sysname> system-view
[Sysname] loadbalance dns-map dm1
[Sysname-lb-dm-dm1] ttl 4000
```

Related commands

display loadbalance dns-map

ttl weight

Use **ttl weight** to set the TTL weight for proximity calculation.

Use **undo ttl weight** to restore the default.

Syntax

ttl weight *ttl-weight*

undo ttl weight

Default

The TTL weight for proximity calculation is 100.

Views

Proximity view

Predefined user roles

network-admin

context-admin

Parameters

ttl-weight: Specifies the TTL weight for proximity calculation, in the range of 0 to 255. A larger value indicates a higher weight.

Examples

Set the TTL weight for proximity calculation to 200.

```
<Sysname> system-view
[Sysname] loadbalance proximity
[Sysname-lb-proximity] ttl weight 200
```

udp per-packet

Use **udp per-packet** to enable per-packet load balancing for UDP traffic for a virtual server.

Use **undo udp per-packet** to disable per-packet load balancing for UDP traffic for a virtual server.

Syntax

udp per-packet

undo udp per-packet

Default

Per-packet load balancing for UDP traffic is disabled for a virtual server.

Views

UDP virtual server view

UDP-based SIP virtual server view

Predefined user roles

network-admin

context-admin

Usage guidelines

When per-packet load balancing for UDP traffic is disabled, the LB device distributes traffic matching the virtual server according to application type. Traffic of the same application type is distributed to one real server.

When per-packet load balancing for UDP traffic is enabled, the following results apply:

- The LB device distributes traffic matching the virtual server on a per-packet basis.
- The LB device does not collect statistics of connections on the virtual server or real server.
- If NAT is not enabled for the referenced server farm, the LB device does not collect statistics of packets sent by the virtual server or real server.
- The following configurations are still effective:
  - Scheduling algorithm configured on the server farm referenced by the virtual server.
  - Sticky method of the sticky group when the virtual server references the server farm.

    Because packets of the same session have the same quintuple, the hash scheduling algorithm or the source IP address sticky method yields the same result for the packets. For example, if a server farm uses the hash scheduling algorithm or the source IP address sticky method, the LB device distributes UDP packets of the same session to one real server. In this case, the LB device cannot distribute UDP packets on a per-packet basis.

Examples

Enable per-packet load balancing for UDP traffic for the UDP virtual server **vs5**.

```
<Sysname> system-view
[Sysname] virtual-server vs5 type udp
[Sysname-vs-udp-vs5] udp per-packet
```

username

Use **username** to specify the login username and password of the MySQL database.

Use **undo username** to remove the login username and password of the MySQL database.

Syntax

username *username* [**password** { **cipher** | **simple** } *string*]

undo username *username*

Default

The login username and password of the MySQL database is not specified.

Views

MySQL virtual server view

Predefined user roles

network-admin

context-admin

Parameters

username: Specifies the username, a case-sensitive string of 1 to 63 characters.

password: Specifies the password. If you do not specify the password, the password is null.

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password string. Its plaintext form is a case-sensitive string of 1 to 127 characters. Its encrypted form is a case-sensitive string of 1 to 255 characters.

Usage guidelines

You can configure a maximum of 100 login users.

The specified login username and password must be the same as the actual login username and password of the MySQL database.

Examples

Specify the username and password as **root** and **123456**, respectively, for the MySQL virtual server **vs1**.

```
<Sysname> system-view
[Sysname] virtual-server vs1 type mysql
[Sysname-vs-mysql-vs1] username root password simple 123456
```

variable

Use **variable** to associate a variable with a server farm member.

Use **undo variable** to disassociate a variable from a server farm member.

Syntax

variable *variable-name* **value** *value*

undo variable *variable-name*

Default

No variable is associated with a server farm member.

Views

Server farm member view

Predefined user roles

network-admin

context-admin

Parameters

variable-name: Specifies a variable name, a case-sensitive string of 1 to 63 characters.

value *value*: Specifies the variable value, a case-sensitive string of 1 to 127 characters.

Examples

Associate a variable with variable name **var1** and variable value 1 with server farm member **rs**.

```
<Sysname> system-view
[Sysname] server-farm sf
[Sysname-sfarm-sf] real-server rs port 5001
[Sysname-sfarm-sf-#member#-rs-port-5001] variable var1 value _1
```

Related commands

payload rewrite

version

Use **version** to configure the MySQL database version.

Use **undo version** to restore the default.

Syntax

version { **5.0** | **5.1** | **5.5** | **5.6** | **5.7** }

undo version

Default

The MySQL database version is 5.6.

Views

MySQL virtual server view

Predefined user roles

network-admin

context-admin

Parameters

{ **5.0** | **5.1** | **5.5** | **5.6** | **5.7** }: Specifies the MySQL database version number.

Usage guidelines

The LB device performs authentication for clients on behalf of the MySQL server and sends database initialization packets of the specified MySQL version to clients.

Examples

Configure the MySQL database version as 5.7 for the MySQL virtual server **vs1**.

```
<Sysname> system-view
[Sysname] virtual-server vs1 type mysql
[Sysname-vs-mysql-vs1] version 5.7
```

virtual-ip

Use **virtual-ip** to add a virtual IPv4 address to a virtual server pool.

Use **undo virtual-ip** to delete a virtual IPv4 address from a virtual server pool.

Syntax

virtual-ip *ipv4-address* **link** *link-name* [**weight** *weight-value*]

undo virtual-ip *ipv4-address*

Default

No virtual IPv4 addresses are added to a virtual server pool.

Views

Virtual server pool view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-address: Specifies a virtual IPv4 address.

link *link-name*: Specifies an LB link by its name, a case-insensitive string of 1 to 63 characters.

weight *weight-value*: Specifies the weight for the virtual IPv4 address, in the range of 1 to 255. The default weight is 100.

Usage guidelines

In scenarios where server load balancing is not required, you can configure virtual IPv4 addresses instead of virtual servers to simplify configuration.

For the weighted round-robin scheduling algorithm, a virtual IPv4 address with a greater weight value are preferentially scheduled.

You can add multiple virtual IPv4 addresses to a virtual server pool, and a virtual IPv4 address can be associated with one link. If you execute this command multiple times for the same virtual IPv4 address, the most recent configuration takes effect.

Examples

Add virtual IPv4 address 10.0.0.1 associated with LB link **link1** to virtual server pool **local-pool**.

```
<Sysname> system-view
[Sysname] loadbalance virtual-server-pool local-pool
[Sysname-lb-vspool-local-pool] virtual-ip 10.0.0.1 link link1
```

Related commands

loadbalance link

loadbalance virtual-server-pool

virtual-ipv6

Use **virtual-ipv6** to add a virtual IPv6 address to a virtual server pool.

Use **undo virtual-ipv6** to delete a virtual IPv6 address from a virtual server pool.

Syntax

virtual-ipv6 *ipv6-address* **link** *link-name* [**weight** *weight-value*]

undo virtual-ipv6 *ipv6-address*

Default

No virtual IPv6 addresses are added to a virtual server pool.

Views

Virtual server pool view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address: Specifies a virtual IPv6 address.

link *link-name*: Specifies an LB link by its name, a case-insensitive string of 1 to 63 characters.

weight *weight-value*: Specifies the weight for the virtual IPv6 address, in the range of 1 to 255. The default weight is 100.

Usage guidelines

In scenarios where server load balancing is not required, you can configure virtual IPv6 addresses instead of virtual servers to simplify configuration.

For the weighted round-robin scheduling algorithm, a virtual IPv6 address with a greater weight value are preferentially scheduled.

You can add multiple virtual IPv6 addresses to a virtual server pool, and a virtual IPv6 address can be associated with one link. If you execute this command multiple times for the same virtual IPv6 address, the most recent configuration takes effect.

Examples

Add virtual IPv6 address 10::1 associated with LB link **link1** to virtual server pool **local-pool**.

```
<Sysname> system-view
[Sysname] loadbalance virtual-server-pool local-pool
[Sysname-lb-vspool-local-pool] virtual-ipv6 10::1 link link1
```

Related commands

loadbalance link

loadbalance virtual-server-pool

virtual ip address

Use **virtual ip address** to configure an IPv4 address (VSIP) for a virtual server.

Use **undo virtual ip address** to restore the default.

Syntax

virtual ip address *ipv4-address* [*mask-length* | *mask*]

undo virtual ip address

Default

No IPv4 address is configured for a virtual server.

Views

Virtual server view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-address: Specifies an IPv4 address. It cannot be a loopback address, multicast address, broadcast address, or an address in the format of 0.X.X.X (with a mask length of 32).

mask-length: Specifies a mask length in the range of 0 to 32. The default is 32. This argument is not supported by virtual servers of the fast HTTP type and HTTP type.

mask: Specifies a subnet mask. The default is 255.255.255.255. This argument is not supported by virtual servers of the fast HTTP type and HTTP type.

Usage guidelines

If the virtual server IP address is on the same network as the IP address of the device interface connected to the client, you must execute the **arp-nd interface** command for the virtual server. In the situation does not exist, you do not need to execute the **arp-nd interface** command.

Examples

Configure the IPv4 address for the IP-type virtual server **vs3** as 1.1.1.1/24.

```
<Sysname> system-view
[Sysname] virtual-server vs3 type ip
[Sysname-vs-ip-vs3] virtual ip address 1.1.1.1 24
```

Related commands

arp-nd interface (virtual server view)

virtual ipv6 address

Use **virtual ipv6 address** to configure an IPv6 address (VSIP) for a virtual server.

Use **undo virtual ipv6 address** to restore the default.

Syntax

virtual ipv6 address *ipv6-address* [*prefix-length*]

undo virtual ipv6 address

Default

No IPv6 address is configured for a virtual server.

Views

Virtual server view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address: Specifies an IPv6 address, which cannot be a loopback address, IPv6 multicast address, link-local address, or all-zero address (when the prefix length is not 0).

prefix-length: Specifies a prefix length in the range of 0 to 128. The default is 128. This argument is not supported by virtual servers of the fast HTTP type and HTTP type.

Usage guidelines

If the virtual server IP address is on the same network as the IP address of the device interface connected to the client, you must execute the **arp-nd interface** command for the virtual server. In the situation does not exist, you do not need to execute the **arp-nd interface** command.

Examples

Configure the IPv6 address for the IP-type virtual server **vs3** as 1001::1/64.

```
<Sysname> system-view
[Sysname] virtual-server vs3 type ip
[Sysname-vs-ip-vs3] virtual ipv6 address 1001::1 64
```

Related commands

arp-nd interface (virtual server view)

virtual-server (system view)

Use **virtual-server** to create a virtual server and enter its view, or enter the view of an existing virtual server.

Use **undo virtual-server** to delete the specified virtual server.

Syntax

virtual-server *virtual-server-name* [**type** { **fast-http** | **http** | **ip** | **link-ip** | | **mysql sip-tcp** | **sip-udp** | **radius** | **tcp** | **udp** }]

undo virtual-server *virtual-server-name*

Default

No virtual servers exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

virtual-server-name: Specifies the virtual server name, a case-insensitive string of 1 to 63 characters.

type { **fast-http** |**http** | **ip** | **link-ip** | **mysql** | **sip-tcp** | **sip-udp** | **radius** | **tcp** | **udp** }: Specifies the virtual server type as fast HTTP, HTTP, IP, link-IP, MySQL, RADIUS, TCP-based SIP, UDP-based SIP, TCP, or UDP. When you create a virtual server, you must specify

a virtual server type. You can enter an existing virtual server view without entering the type of the virtual server.

Usage guidelines

You can create fast HTTP, HTTP, MySQL, RADIUS, SIP, TCP, or UDP virtual servers only if the device has licenses installed. For information about licensing, see license management in *Fundamentals Configuration Guide*.

Examples

Create the virtual server **vs3** with the IP type, and enter virtual server view.

```
<Sysname> system-view
[Sysname] virtual-server vs3 type ip
[Sysname-vs-ip-vs3]
```

virtual-server (virtual server pool view)

Use **virtual-server** to add a virtual server to a virtual server pool.

Use **undo virtual-server** to delete a virtual server from a virtual server pool.

Syntax

virtual-server *virtual-server-name* **link** *link-name* [**weight** *weight-value*]

undo virtual-server *virtual-server-name*

Default

No virtual servers are added to a virtual server pool.

Views

Virtual server pool view

Predefined user roles

network-admin

context-admin

Parameters

virtual-server-name: Specifies a virtual server by its name, a case-insensitive string of 1 to 63 characters.

link *link-name*: Specifies an LB link by its name, a case-insensitive string of 1 to 63 characters.

weight *weight-value*: Specifies the weight for the virtual server, in the range of 1 to 255. The default weight is 100. For the weighted round robin algorithm, a greater value means a higher priority to be referenced. If you do not specify this option, the default weight 100 applies.

Usage guidelines

You can add multiple virtual servers to a virtual server pool.

To ensure correct operation of inbound link load balancing when server load balancing is also enabled, do not specify the virtual server's IP address as the DNS listener's IP address.

The virtual server's IP address for inbound link load balancing must be a unicast address with a 32-bit mask length. The IP address cannot be an all-zero address.

Examples

Add the virtual server **vs1** associated with the LB link **link1** to the virtual server pool **local-pool**.

```
<Sysname> system-view
[Sysname] loadbalance virtual-server-pool local-pool
```

```
[Sysname-lb-vspool-local-pool] virtual-server vs1 link link1
```

Related commands

loadbalance link

loadbalance virtual-server-pool

virtual-server-pool

Use **virtual-server-pool** to specify a virtual server pool for a DNS mapping.

Use **undo virtual-server-pool** to restore the default.

Syntax

virtual-server-pool *pool-name*

undo virtual-server-pool *pool-name*

Default

No virtual server pool is specified for a DNS mapping.

Views

DNS mapping view

Predefined user roles

network-admin

context-admin

Parameters

pool-name: Specifies the virtual server pool name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the virtual server pool **pool1** for the DNS mapping **dm1**.

```
<Sysname> system-view
[Sysname] loadbalance dns-map dm1
[Sysname-lb-dm-dm1] virtual-server-pool pool1
```

vpn-instance (DNS listener view)

Use **vpn-instance** to specify a VPN instance for a DNS listener.

Use **undo vpn-instance** to restore the default.

Syntax

vpn-instance *vpn-instance-name*

undo vpn-instance

Default

A DNS listener belongs to the public network.

Views

DNS listener view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance-name: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters.

Examples

Specify VPN instance **vpn1** for DNS listener **ct-listener**.

```
<Sysname> system-view
[Sysname] loadbalance dns-listener ct-listener
[Sysname-lb-dl-ct-listener] vpn-instance vpn1
```

Related commands

display loadbalance dns-listener

vpn-instance (DNS server view)

Use **vpn-instance** to specify a VPN instance for a DNS server.

Use **undo vpn-instance** to restore the default.

Syntax

vpn-instance *vpn-instance-name*

undo vpn-instance

Default

A DNS server belongs to the public network.

Views

DNS server view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance-name: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters.

Examples

Specify VPN instance **vpn1** for DNS server **ds1**.

```
<Sysname> system-view
[Sysname] loadbalance dns-server ds1
[Sysname-vs-http-vs] vpn-instance vpn1
```

Related commands

display loadbalance dns-server

vpn-instance (link view)

Use **vpn-instance** to specify a VPN instance for a link.

Use **undo vpn-instance** to restore the default.

Syntax

vpn-instance *vpn-instance-name*

undo vpn-instance

Default

A link belongs to the public network.

Views

Link view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance-name: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

Before executing this command, you must create the VPN instance by using the **ip vpn-instance** *vpn-instance-name* command. If the specified VPN instance has not been created, the link state will be unavailable.

Examples

Specify VPN instance **vpn1** for link **lk1**.

```
<Sysname> system-view
[Sysname] loadbalance link lk1
[Sysname-lb-link-lk1] vpn-instance vpn1
```

Related commands

ip vpn-instance (*MPLS Command Reference*)

vpn-instance (real server view)

Use **vpn-instance** to specify a VPN instance for a real server.

Use **undo vpn-instance** to restore the default.

Syntax

vpn-instance *vpn-instance-name*

undo vpn-instance

Default

A real server belongs to the public network if VPN instance inheritance is disabled.

A real server belongs to the VPN instance specified for its virtual server if VPN instance inheritance is enabled.

Views

Real server view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance-name: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters.

Examples

Specify VPN instance **vpn1** for real server **rs**.

```
<Sysname> system-view
[Sysname] real-server rs
[Sysname-rserver-rs] vpn-instance vpn1
```

Related commands

inherit vpn-instance disable

vpn-instance (SNAT address pool view)

Use **vpn-instance** to specify a VPN instance for a SNAT address pool.

Use **undo vpn-instance** to restore the default.

Syntax

vpn-instance *vpn-instance-name*

undo vpn-instance

Default

A SNAT address pool belongs to the public network.

Views

SNAT address pool view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance-name: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

Use this command to isolate SNAT address pools if they overlap.

As a best practice, specify the VPN instance of the associated real server for a SNAT address pool.

Examples

Specify VPN instance **vpn1** for SNAT address pool **sp1**.

```
<Sysname> system-view
[Sysname] loadbalance snat-global-policy sp1
[Sysname-lb-snat-gp-sp1] vpn-instance vpn1
```

Related commands

display loadbalance snat-pool

vpn-instance (SNAT global policy view)

Use **vpn-instance** to specify a VPN instance for a SNAT global policy.

Use **undo vpn-instance** to restore the default.

Syntax

vpn-instance *vpn-instance-name*

undo vpn-instance

Default

A SNAT global policy belongs to the public network.

Views

SNAT global policy view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance-name: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters.

Examples

Specify VPN instance **vpn1** for SNAT global policy **sn1**.

```
<Sysname> system-view
[Sysname] loadbalance snat-global-policy sn1
[Sysname-lb-snat-gp-sn1] vpn-instance vpn1
```

vpn-instance (transparent DNS proxy view)

Use **vpn-instance** to specify a VPN instance for a transparent DNS proxy.

Use **undo vpn-instance** to restore the default.

Syntax

vpn-instance *vpn-instance-name*

undo vpn-instance

Default

A transparent DNS proxy belongs to the public network.

Views

Transparent DNS proxy view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance-name: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters.

Examples

Specify VPN instance **vpn1** for transparent DNS proxy **dns-proxy1**.

```
<Sysname> system-view
[Sysname] loadbalance dns-proxy dns-proxy1
[Sysname-lb-dp-udp-dns-proxy1] vpn-instance vpn1
```

vpn-instance (virtual server view)

Use **vpn-instance** to specify a VPN instance for a virtual server.

Use **undo vpn-instance** to restore the default.

Syntax

vpn-instance *vpn-instance-name*

undo vpn-instance

Default

A virtual server belongs to the public network.

Views

Virtual server view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance-name: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters.

Examples

Specify VPN instance **vpn1** for the IP-type virtual server **vs3**.

```
<Sysname>system-view
[Sysname] virtual-server vs3 type ip
[Sysname-vs-ip-vs3] vpn-instance vpn1
```

vrrp vrid

Use **vrrp vrid** to bind a VRRP group to a virtual server.

Use **undo vrrp vrid** to unbind a VRRP group from a virtual server.

Syntax

vrrp [**ipv6**] **vrid** *virtual-router-id* **interface** *interface-type interface-number*

undo vrrp [**ipv6**]

Default

No VRRP group is bound to a virtual server.

Views

Virtual server view

Predefined user roles

network-admin

context-admin

Parameters

ipv6: Specifies an IPv6 VRRP group. If you do not specify this keyword, this command binds an IPv4 VRRP group to a virtual server.

virtual-router-id: Specifies a VRRP group by its virtual router ID in the range of 1 to 255.

interface-type interface-number: Specifies the interface on which the VRRP group was created.

Usage guidelines

In a VRRP hot backup system, execute this command if you configure server load balancing on the primary device in a remote backup group to make sure the return packets are processed on the same master device. For more information about remote backup groups, see RBM in *High Availability Configuration Guide*.

Multiple virtual servers bound to different VRRP groups cannot use the same SNAT address pool.

A virtual server can be bound to a maximum of one IPv4 or IPv6 VRRP group. You can bind an IPv4 VRRP group to only an IPv4 virtual server, or bind an IPv6 VRRP group to only an IPv6 virtual server.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Bind VRRP group 1 to TCP virtual server **vs**.

```
<Sysname> system-view
[Sysname] virtual-server vs type tcp
[Sysname-vs-tcp-vs] vrrp vrid 1 interface gigabitethernet 1/0/1
```

Related commands

virtual-server

vrrp vrid (*High Availability Command Reference*)

weight (DNS server pool member view)

Use **weight** to set the weight of a DNS server pool member.

Use **undo weight** to restore the default.

Syntax

weight *weight-value*

undo weight

Default

The weight of a DNS server pool member is 100.

Views

DNS server pool member view

Predefined user roles

network-admin

context-admin

Parameters

weight-value: Specifies the weight in the range of 1 to 255. A greater value means a higher priority in scheduling.

Usage guidelines

The weight configured in this command is used in the weighted round-robin algorithm.

Examples

Set the weight of the DNS server pool member **ds1** to **150**.

```
<Sysname> system-view
[Sysname] loadbalance dns-server-pool dsp1
[Sysname-lb-dspool-dsp1] dns-server ds1 port 10
[Sysname-lb-dspool-dsp1-#member#-ds1-port-10] weight 150
```

weight (DNS server view)

Use **weight** to set the weight of a DNS server to be used by the weighted round robin algorithm and bandwidth algorithm.

Use **undo weight** to restore the default.

Syntax

weight *weight-value*

undo weight

Default

The weight of a DNS server is 100.

Views

DNS server view

Predefined user roles

network-admin

context-admin

Parameters

weight-value: Specifies the weight in the range of 1 to 255. A greater value means a higher priority in scheduling.

Examples

Set the weight of the DNS server **ds1** to **150**.

```
<Sysname> system-view
[Sysname] loadbalance dns-server ds1
[Sysname-lb-ds-ds1] weight 150
```

weight (link group member view)

Use **weight** to set the weight of a link group member.

Use **undo weight** to restore the default.

Syntax

weight *weight-value*

undo weight

Default

The weight of a link group member is 100.

Views

Link group member view

Predefined user roles

network-admin

context-admin

Parameters

weight-value: Specifies the weight in the range of 1 to 255. A greater value means a higher priority in scheduling.

Usage guidelines

The weight configured in this command is used in the weighted least-connection algorithm and weighted round-robin algorithm.

Examples

Set the weight of the link group member **lk1** to **150**.

```
<Sysname> system-view
[Sysname] loadbalance link-group lg
[Sysname-lb-lgroup-lg] link lk1
[Sysname-lb-lgroup-lg-#member#-lk1] weight 150
```

weight (link view)

Use **weight** to set the weight of a link to be used by the weighted round robin and weighted least connection algorithms.

Use **undo weight** to restore the default.

Syntax

weight *weight-value*

undo weight

Default

The weight of a link is 100.

Views

Link view

Predefined user roles

network-admin

context-admin

Parameters

weight-value: Specifies the weight in the range of 1 to 255. For the weighted round robin or weighted least connection algorithm, a greater value means a higher priority to be referenced.

Examples

Set the weight of the link **lk1** to **150**.

```
<Sysname> system-view
[Sysname] loadbalance link lk1
[Sysname-lb-link-lk1] weight 150
```

weight (real server view)

Use **weight** to set the weight of a real server to be used by the weighted round robin and weighted least connection algorithms.

Use **undo weight** to restore the default.

Syntax

weight *weight-value*

undo weight

Default

The weight of a real server is 100.

Views

Real server view

Predefined user roles

network-admin

context-admin

Parameters

weight-value: Specifies the weight in the range of 1 to 255. For the weighted round robin or weighted least connection algorithm, a greater value means a higher priority to be referenced.

Examples

Set the weight of the real server **rs** to **150**.

```
<Sysname> system-view
[Sysname] real-server rs
[Sysname-rserver-rs] weight 150
```

weight (server farm member view)

Use **weight** to set the weight of a server farm member.

Use **undo weight** to restore the default.

Syntax

weight *weight-value*

undo weight

Default

The weight of a server farm member is 100.

Views

Server farm member view

Predefined user roles

network-admin

context-admin

Parameters

weight-value: Specifies the weight in the range of 1 to 255. A greater value means a higher priority in scheduling.

Usage guidelines

The weight configured in this command is used in the weighted least-connection algorithm and weighted round-robin algorithm.

Examples

Set the weight of the server farm member **rs1** to **150**.

```
<Sysname> system-view
[Sysname] server-farm sf
[Sysname-sfarm-sf] real-server rs1 port 80
[Sysname-sfarm-sf-#member#-rs1-port-80] weight 150
```

whois-mntner

Use **whois-mntner** to specify a whois maintainer object for an ISP.

Use **undo whois-mntner** to delete a whois maintainer object for an ISP.

Syntax

whois-mntner *mntner-name*

undo whois-mntner *mntner-name*

Default

No whois maintainer object is specified for an ISP.

Views

ISP view

Predefined user roles

network-admin

context-admin

Parameters

mntner-name: Specify a whois maintainer object by its name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

This command specifies the geographical area where ISP address information is to be updated by the whois server.

You can specify a maximum of 10 whois maintainer objects for an ISP.

A whois maintainer object is globally unique.

Examples

Specify whois maintainer object **MAINT-CHINANET** for ISP **isp1**.

```
<Sysname> system-view
[Sysname] loadbalance isp name isp1
[Sysname-lbisp-isp1] whois-mntner MAINT-CHINANET
```

window-size

Use **window-size** to set the window size used for compression.

Use **undo window-size** to restore the default.

Syntax

window-size *size*

undo window-size

Default

The window size used for compression is 16 KB.

Views

HTTP-compression parameter profile view

Predefined user roles

network-admin

context-admin

Parameters

size: Specifies the window size in KB used for compression. The value can only be 1, 2, 4, 8, 16, or 32.

Examples

Create the HTTP-compression parameter profile **pa1**, and set the window size used for compression to 32 KB.

```
<Sysname> system-view
[Sysname] parameter-profile pa1 type http-compress
[Sysname-para-http-compression-pa1] window-size 32
```

zero-window threshold

Use **zero-window threshold** to set the percentage threshold of zero-window packets for a TCP zero-window LB probe template.

Use **undo zero-window threshold** to restore the default.

Syntax

zero-window threshold *percentage*

undo packet-zero-window

Default

The percentage threshold of zero-window packets is 40%.

Views

TCP zero-window LB probe template view

Predefined user roles

network-admin

context-admin

Parameters

percentage: Specifies the percentage threshold of zero-window packets, in the range of 1 to 100.

Usage guidelines

When the percentage of zero-window packets sent by a real server reaches the threshold, the protection action specified in the **protect-action** command is taken.

Examples

In TCP zero-window LB probe template **zerotplt**, set the percentage threshold of zero-window packets to 20%.

```
<Sysname>system-view
[Sysname] loadbalance probe-template tcp-zero-window zerotplt
[Sysname-lbpt-tcp-zwnd-zerotplt] zero-window threshold 20
```

Related commands

protect-action

NSFOCUS Firewall Series

NF High Availability

Command Reference

NSFOCUS Technologies, Inc.

Document version: 6W600-20230221

Preface

This command reference describes the commands for configuring high availability features.

This preface includes the following topics about the documentation:

- Audience.
- Conventions.

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators.

Conventions

The following information describes the conventions used in the documentation.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select a minimum of one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
CAUTION:	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Contents

RBM-based hot backup commands

adjust-cost enable

Use **adjust-cost enable** to enable hot backup to adjust the link cost for the specified routing protocol on the standby device.

Use **undo adjust-cost enable** to disable hot backup from adjusting the link cost for the specified routing protocol on the standby device.

Syntax

adjust-cost { **bgp** | **isis** | **ospf** | **ospfv3** } **enable** { **absolute** [*absolute-cost*] | **increment** [*increment-cost*] }

undo adjust-cost { **bgp** | **isis** | **ospf** | **ospfv3** } **enable**

Default

The hot backup system does not adjust the link cost for the specified routing protocol on the standby device.

Views

RBM view

Predefined user roles

network-admin

Parameters

bgp: Specifies the BGP protocol.

isis: Specifies the IS-IS protocol.

ospf: Specifies the OSPF protocol.

ospfv3: Specifies the OSPFv3 protocol.

absolute [*absolute-cost*]: Specifies an absolute cost in the range of 1 to 65535. The default value is 65500. If you specify this option, the standby device will advertise an absolute link cost for the specified routing protocol.

increment [*increment-cost*]: Specifies an increment cost in the range of 1 to 65535. The default value is 100. If you specify this option, the standby device will advertise the original link cost plus this increment cost for the specified routing protocol.

Usage guidelines

In a hot backup system, the routing protocols on hot backup member devices advertise link cost according to their respective operation mechanisms. This command allows you to enable the routing protocols to advertise link cost modified as configured. The active device still uses the original link cost advertisement method.

To ensure switchover of both uplink and downlink traffic to the new active device, configure this command with the same parameters on both hot backup member devices.

In dual-active mode, both devices advertise link cost according to the operation mechanisms of the running routing protocols. When one device is faulty and becomes the standby device, it will advertise link cost modified as configured.

To enable the feature for multiple routing protocols, execute this command multiple times by specifying the protocols.

If you execute the command multiple times for a specific routing protocol, the most recent configuration takes effect.

Examples

Enable hot backup to adjust OSPF link cost on the standby device by specifying an absolute value of 6000.

```
<Sysname> system-view
[Sysname] remote-backup group
[Sysname-remote-backup-group] adjust-cost ospf enable absolute 6000
```

backup-mode

Use **backup-mode** to configure the hot backup mode.

Use **undo backup-mode** to restore the default.

Syntax

backup-mode dual-active

undo backup-mode

Default

The hot backup mode is active/standby.

Views

RBM view

Predefined user roles

network-admin

Usage guidelines

The hot backup system supports active/standby mode and dual-active mode. In active/standby mode, only the active device processes services. In dual-active mode, both devices process services.

Changing the dual-active mode to active/standby mode might affect services. Make sure you understand the potential impact before performing the operation.

Examples

Configure the dual-active mode.

```
<Sysname> system-view
[Sysname] remote-backup group
[Sysname-remote-backup-group] backup-mode dual-active
```

configuration auto-sync enable

Use **configuration auto-sync enable** to enable automatic configuration synchronization.

Use **undo configuration auto-sync enable** to disable automatic configuration synchronization.

Syntax

configuration auto-sync enable

undo configuration auto-sync enable

Default

Automatic configuration synchronization is enabled.

Views

RBM view

Predefined user roles

network-admin

Usage guidelines

The automatic configuration synchronization feature synchronizes existing configuration on the primary device in bulk to the secondary device. Consequent synchronization for added, deleted, or modified configuration will be performed in real time.

If the amount of configuration to be synchronized is large, bulk synchronization might take one to two hours.

Examples

Enable automatic configuration synchronization.

```
<Sysname> system-view
[Sysname] remote-backup group
[Sysname-remote-backup-group] configuration auto-sync enable
```

configuration manual-sync

Use **configuration manual-sync** to manually synchronize the configuration of the primary device to the secondary device.

Syntax

configuration manual-sync

Views

RBM view

Predefined user roles

network-admin

Usage guidelines

This command takes effect only on the primary device.

This command does not take effect when bulk configuration backup is in progress. To view the backup progress, execute the **display remote-backup-group status** command.

Examples

Manually synchronize the configuration of the primary device to the secondary device.

```
<Sysname> system-view
[Sysname] remote-backup group
[Sysname-remote-backup-group] configuration manual-sync
```

Related commands

display remote-backup-group status

configuration manual-sync-check

Use **configuration manual-syn-check** to perform a one-off configuration consistency check.

Syntax

configuration manual-sync-check

Views

RBM view

Predefined user roles

network-admin

Usage guidelines

This command allows you to perform a one-off configuration consistency check as needed. If the system detects configuration inconsistency, it generates a log for you to manually synchronize configuration. To view the check result, execute the **display remote-backup-group sync-check** command.

Examples

Perform a one-off configuration consistency check.

```
<Sysname> system-view
[Sysname] remote-backup group
[Sysname-remote-backup-group] configuration manual-sync-check
```

Related commands

configuration manual-sync

display remote-backup-group sync-check

configuration sync-check

Use **configuration sync-check** to enable configuration consistency check.

Use **undo configuration sync-check** to disable configuration consistency check.

Syntax

configuration sync-check [**interval** *interval*]

undo configuration sync-check

Default

Configuration consistency check is enabled.

Views

RBM view

Predefined user roles

network-admin

Parameters

interval *interval*: Specifies the configuration consistency check interval, in the range of 1 to 168 hours. The default value is 24.

Usage guidelines

The hot backup system verifies configuration consistency between the primary and secondary devices to avoid service interruption upon active/standby switchover. If a device detects configuration inconsistency, it generates a log for you to manually synchronize configuration.

Examples

Enable configuration consistency check and set the check interval to 120 hours.

```
<Sysname>system-view
[Sysname] remote-backup group
[Sysname-remote-backup-group] configuration sync-check interval 120
```

Related commands

configuration manual-sync

configuration manual-sync-check

data-channel

Use **data-channel** to configure a data channel.

Use **undo data-channel** to restore the default.

Syntax

data-channel interface *interface-type interface-number*

undo data-channel

Default

No data channel is configured.

Views

RBM view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number to set up a data channel between the primary and secondary devices.

Usage guidelines

The primary and secondary devices use the interface specified in the command to set up a data channel. The data channel transmits only backup packets and the packets that require transparent transmission.

The data channel is a Layer 2 channel that can transverse only Layer 2 switches.

Examples

Set up a data channel using interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] remote-backup group
[Sysname-remote-backup-group] data-channel interface gigabitethernet 1/0/1
```

delay-time

Use **delay-time** to enable traffic switchover upon failure recovery.

Use **undo delay-time** to disable traffic switchover upon failure recovery.

Syntax

delay-time *delay-time*

undo delay-time

Default

Traffic switchover upon failure recovery is disabled.

Views

RBM view

Predefined user roles

network-admin

Parameters

delay-time: Specifies the switchover delay time in the range of 1 to 1440 minutes.

Usage guidelines

After an active/standby switchover in a hot backup system, if the original active device recovers, traffic will not be switched back by default. Perform this task to enable traffic switchover to the original active device upon failure recovery. You can set a delay timer to ensure smooth service switchover.

In dual-active mode, you must configure this command to ensure that both devices can operate after the failure is recovered.

Examples

Enable traffic switchover upon failure recovery and set the switchover delay time to two minutes.

```
<Sysname>system-view
[Sysname] remote-backup group
[Sysname-remote-backup-group] delay-time 2
```

device-role

Use **device-role** to configure the hot backup role.

Use **undo device-role** to restore the default.

Syntax

device-role { **primary** | **secondary** }

undo device-role

Default

The hot backup role is not configured.

Views

RBM view

Predefined user roles

network-admin

Parameters

primary: Assigns the primary role to the device.

secondary: Assigns the secondary role to the device.

Usage guidelines

The hot backup system backs up important configuration from the primary device to the secondary device to prevent service interruption when an active/standby switchover occurs. The configuration on the secondary device is overwritten. The unidirectional backup mechanism avoids configuration conflicts, especially in dual-active mode, and ensures configuration consistency on the primary and secondary devices.

Each hot backup member device adds a prefix to the view prompt to identify its hot backup role.

- The primary device adds the **RBM_P** prefix, **RBM_P<Sysname>** for example.
- The secondary device adds the **RBM_S** prefix, **RBM_S<Sysname>** for example.

After you assign hot backup roles to hot backup member devices, both devices add the **RBM_P** prefix to their view prompts. The devices display view prompt prefixes according to their hot backup roles after they set up the control channel.

The hot backup system must contain one primary device and one secondary device.

As a best practice, configure service features on the primary device.

Examples

Assign the primary role to the device.

```
<Sysname> system-view
[Sysname] remote-backup group
[Sysname-remote-backup-group] device-role primary
RBM_P[Sysname-remote-backup-group]
```

display remote-backup-group status

Use **display remote-backup-group status** to display hot backup status information.

Syntax

display remote-backup-group status

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display hot backup status information on the default context.

```
<Sysname> display remote-backup-group status
Remote backup group information:
  Backup mode: Dual-active
  Device management role: Primary
  Device running status: Active
  Data channel interface: GigabitEthernet1/0/1
  Local IP: 1.1.1.1
  Remote IP: 1.1.1.2   Destination port: 1028
  Control channel status: Connected
```

```
  Keepalive interval: 1s
  Keepalive count: 10
  Configuration consistency check interval: 24 hour
  Configuration consistency check result: Consistent
  Configuration backup status: Batch backup (Do not operate
the device at will, such as board insertion and removal.)
  Session backup status: Hot backup enabled
  Delay-time: 1 min
  Remaining switchover delay time: 3 minutes, 32 seconds
  Uptime since last switchover: 0 days, 0 hours, 11 minutes
  Switchover records:
    Time                    Status change       Cause
    2021-06-22 13:33:33     Initial to Standby  Local device rebooted
    2021-06-22 14:34:34     Initial to Active   Peer device rebooted
```

Display hot backup status information on non-default contexts.

```
<Sysname> display remote-backup-group status
Remote backup group information:
  Backup mode: Dual-active
  Device management role: Primary
  Device running status: Active
  Control channel status: Connected
  Configure channel status: Disconnected
```

Table 1 Command output

Field	Description
Backup mode	Hot backup mode: • **Dual-active**. • **Active/standby**.
Device management role	Hot backup role of the device: • **Primary**. • **Secondary**.
Device running status	Running status of the device. • **Active**. • **Standby**. • **Initial**—The local IP address, peer IP address, or hot backup role is not configured.
Data channel interface	Interface used to set up the data channel.
Local IP	Local IP address used by control channel packets. This field is not displayed if the parameter is not configured.
Remote IP	Peer IP address used by control channel packets. This field is not displayed if the parameter is not configured.
Local IPv6	Local IPv6 address used by control channel packets. This field is not displayed if the parameter is not configured.
Remote IPv6	Peer IPv6 address used by control channel packets. This field is not displayed if the parameter is not configured.
Destination port	Peer port number used by control channel packets.
Control channel status	Control channel status:

Field	Description
	• **Connected**. • **Disconnected**.
Configure channel status: Disconnected	Status of the configuration information channel for non-default contexts: • **Connected**. • **Disconnected**. This filed is displayed only for non-default contexts. If the configuration information channel is disconnected, the device cannot synchronize configuration of non-default contexts.
Keepalive interval	Interval for sending keepalive packets.
Keepalive count	Maximum number of keepalive attempts.
Configuration consistency check interval	Configuration consistency check interval in hours. This field is displayed only when configuration consistency check is enabled.
Configuration consistency check result	Result of the configuration consistency check: • **Consistent**. • **Inconsistent**. • **Checking**. • **Not Performed**.
Configuration backup status	Status of configuration backup: • **Batch backup in progress (Do not operate the device at will, such as board insertion and removal.)**. • **Auto sync enabled**. • **Auto sync disabled**.
Session backup status	Status of session entry backup: • **Batch backup in progress**. • **Hot backup enabled**. • **Hot backup disabled**.
Delay-time	Delay time for traffic switchover back to the original active device in minutes. If the delay time is not configured, this switchover feature is disabled for the hot backup system.
Remaining switchover delay time	Remaining delay time for traffic switchover back to the original active device in minutes. This field is not displayed if traffic switchover is disabled.

display remote-backup-group sync-check

Use **`display remote-backup-group sync-check`** to display the configuration consistency check result for hot backup.

Syntax

`display remote-backup-group sync-check`

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

Use this command when the primary and secondary devices have inconsistent configuration. You can view the inconsistent configuration only after the configuration consistency check is finished.

The command displays detailed inconsistency information for only the service features supported by hot backup. For a feature not supported by hot backup, the command displays only the interface where configuration inconsistency exists.

Examples

Display the configuration consistency check result for hot backup. (The configuration consistency check has not been performed.)

```
<Sysname> display remote-backup-group sync-check
No configuration consistency checks have been performed.
```

Display the configuration consistency check result for hot backup. (No inconsistent configuration exists.)

```
<Sysname> display remote-backup-group sync-check
No inconsistent configuration exists.
```

Display the configuration consistency check result for hot backup. (Inconsistent configuration exists.)

```
<Sysname> display remote-backup-group sync-check
Inconsistent configuration exists.
Configuration on secondary device:
#
security-policy ip
 rule 0 name abc
  source-zone trust
  destination-zone untrust
#

Configuration on primary device:
#
security-policy ip
 rule 0 name abc
  source-zone dmz
  destination-zone trust
#
Context 2

Configuration on secondary device:
#
security-policy ip
 rule 0 name 10
#



Configuration on primary device:
#
security-policy ip
#
Context 3
```

```
Configuration on secondary device:
#
object-group ipv6 address d
#
security-policy ipv6
 rule 0 name d
  source-ip d
#


Configuration on primary device:
#
security-policy ipv6
 rule 0 name d
#
```

Related commands

configuration sync-check

configuration manual-syn-check

hot-backup enable

Use **hot-backup enable** to enable service entry hot backup.

Use **undo hot-backup enable** to disable service entry hot backup.

Syntax

hot-backup enable

undo hot-backup enable

Default

Service entry hot backup is enabled.

Views

RBM view

Predefined user roles

network-admin

Usage guidelines

This command enables the active device in the hot backup system to back up service entries to the standby device in real time. This prevents service interruption when an active/standby switchover occurs.

Examples

Enable service entry hot backup.

```
<Sysname> system-view
[Sysname] remote-backup group
[Sysname-remote-backup-group] hot-backup enable
```

hot-backup protocol enable

Use **hot-backup protocol enable** to enable hot backup for the session entries of application layer protocols.

Use **undo hot-backup protocol enable** to disable hot backup for the session entries of application layer protocols.

Syntax

hot-backup protocol { **dns** | **http** } * **enable**

undo hot-backup protocol { **dns** | **http** } * **enable**

Default

The hot backup system performs hot backup for the session entries of application layer protocols.

Views

RBM view

Predefined user roles

network-admin

Parameters

dns: Specifies DNS.

http: Specifies HTTP.

Usage guidelines

For this command to take effect, first execute the **hot-backup enable** command.

Enable HTTP and DNS backup if asymmetric-path traffic traverses the hot backup system. HTTP and DNS backup ensures that a flow and its return traffic are processed correctly on hot backup members.

If hot backup active/standby mode is used or only symmetric-path traffic traverses the hot backup system, disabling HTTP and DNS backup can improve performance of hot backup members at the expense of delayed data synchronization. When you disable HTTP and DNS backup, make sure you are fully aware of the impact on the network. A device removes a DNS or HTTP connection if packet exchange is inactive. When a switchover interrupts a connection, the DNS or HTTP client re-initiates the connection immediately, which has little impact on user services.

The hot backup system backs up the sessions created for other application protocols as long as service entry backup is enabled.

Examples

Disable hot backup for the session entries of application layer protocols.

```
<Sysname> system-view
[Sysname] remote-backup group
[Sysname-remote-backup-group] undo hot-backup protocol dns enable
```

Related commands

hot-backup enable

keepalive count

Use **keepalive count** to set the maximum number of keepalive attempts.

Use **undo keepalive count** to restore the default.

Syntax

keepalive count *counts*

undo keepalive count

Default

The maximum number of keepalive attempts is 10.

Views

RBM view

Predefined user roles

network-admin

Parameters

times: Sets the maximum number of keepalive attempts, in the range of 1 to 255.

Usage guidelines

If the value for the maximum number of keepalive attempts is too small, network latency will cause incorrect switchovers. If this issue occurs, increase the value of this parameter.

The device periodically sends keepalive packets to the peer over the control channel. If the device has not received any responses from the peer when the maximum number of keepalive attempts is reached, the control channel is disconnected.

Examples

Set the maximum number of keepalive attempts to 6.

```
<Sysname> system-view
[Sysname] remote-backup group
[Sysname-remote-backup-group] keepalive count 6
```

Related commands

keepalive interval

keepalive interval

Use **keepalive interval** to set the interval for sending keepalive packets.

Use **undo keepalive interval** to restore the default.

Syntax

keepalive interval *interval*

undo keepalive interval

Default

The device sends keepalive packets at one-second intervals.

Views

RBM view

Predefined user roles

network-admin

Parameters

interval: Sets the interval for sending keepalive packets in seconds, in the range of 1 to 60.

Usage guidelines

The device periodically sends keepalive packets to the peer over the control channel. If the device has not received any responses from the peer when the maximum number of keepalive attempts is reached, the control channel is disconnected.

Examples

Set the interval for sending keepalive packets to 2 seconds.

```
<Sysname> system-view
[Sysname] remote-backup group
[Sysname-remote-backup-group] keepalive interval 2
```

Related commands

keepalive count

local-ip

Use **local-ip** to configure the local IPv4 address for setting up the control channel.

Use **undo local-ip** to restore the default.

Syntax

local-ip *ipv4-address*

undo local-ip

Default

The local IPv4 address is not configured for setting up the control channel.

Views

RBM view

Predefined user roles

network-admin

Parameters

ipv4-address: Specifies the local IPv4 address for setting up the control channel. The IP address cannot be an all-zero, loopback, or multicast address.

Usage guidelines

The hot backup system compares the specified local and peer IP address to determine the device role for setting up the control channel. The device with higher IP address acts as the server to listen for TCP connection requests, and the other device acts as the client to initiate the TCP connection.

You can configure a local IPv4 address or a local IPv6 address, but not both.

Examples

Configure the local IPv4 address as 1.1.1.2 for setting up the control channel.

```
<Sysname> system-view
[Sysname] remote-backup group
[Sysname-remote-backup-group] local-ip 1.1.1.2
```

Related commands

local-ipv6

remote-ip

local-ipv6

Use **local-ipv6** to configure the local IPv6 address for setting up the control channel.

Use **undo local-ipv6** to restore the default.

Syntax

local-ipv6 *ipv6-address*

undo local-ipv6

Default

The local IPv6 address is not configured for setting up the control channel.

Views

RBM view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the local IPv6 address for setting up the control channel. The IP address cannot be an all-zero address, loopback address, multicast address, or IPv6 address with an embedded IPv4 address.

Usage guidelines

The hot backup system compares the specified local and peer IPv6 address to determine the device role for setting up the control channel. The device with higher IPv6 address acts as the server to listen for TCP connection requests, and the other device acts as the client to initiate the TCP connection.

You can configure a local IPv4 address or a local IPv6 address, but not both.

Examples

Configure the local IPv6 address as 2019::1 for setting up the control channel.

```
<Sysname> system-view
[Sysname] remote-backup group
[Sysname-remote-backup-group] local-ipv6 2019::1
```

Related commands

local-ip

remote-ipv6

remote-backup group

Use **remote-backup group** command to enter RBM view.

Use **undo remote-backup group** to remove all settings of hot backup.

Syntax

remote-backup group

undo remote-backup group

Views

System view

Predefined user roles

network-admin

Usage guidelines

The hot backup system provides backup for important configuration and service entries between devices. It collaborates with VRRP to implement hot backup that enables smooth master/backup switchover upon link failures for service continuity.

Examples

Enter RBM view.

```
<Sysname> system-view
[Sysname] remote-backup group
[Sysname-remote-backup-group]
```

remote-ip

Use **remote-ip** to configure the peer IPv4 address for setting up the control channel.

Use **undo remote-ip** to restore the default.

Syntax

remote-ip *ipv4-address* [**port** *port-number*]

undo remote-ip *ipv4-address*

Default

The peer IPv4 address is not configured for setting up the control channel.

Views

RBM view

Predefined user roles

network-admin

Parameters

ipv4-address: Specifies the peer IPv4 address for setting up the control channel. The IP address cannot be an all-zero, loopback, or multicast address.

port *port-number*: Specifies a port by its number used for establishing TCP connection. The value range for the *port-number* argument is 1024 to 65535, and the default value is 60064.

Usage guidelines

The control channel transmits data by using packets, including hot backup status packets, configuration consistency check packets, and configuration synchronization packets. Each member device compares the specified local and peer IP address to determine the device role for setting up the control channel. The device with higher IP address acts as the server to listen for TCP connection requests, and the other device acts as the client to initiate the TCP connection.

If the port number is configured on the server, the port provides services for the client. If the port number is configured on the client, the port serves as the destination port to establish TCP connection to the server. The source port is randomly generated on the client.

You can specify only one peer IP address with the same port number on the primary and secondary devices.

You can configure a remote IPv4 address or a remote IPv6 address, but not both.

Examples

Configure the peer IPv4 address and port number as 1.1.1.1 and 4456 for setting up the control channel.

```
<Sysname> system-view
[Sysname] remote-backup group
[Sysname-remote-backup-group] remote-ip 1.1.1.1 port 4456
```

Related commands

local-ip

remote-ipv6

remote-ipv6

Use **remote-ipv6** to configure the peer IPv6 address for setting up the control channel.

Use **undo remote-ipv6** to restore the default.

Syntax

remote-ipv6 *ipv6-address* [**port** *port-number*]

undo remote-ipv6 *ipv6-address*

Default

The peer IPv6 address is not configured for setting up the control channel.

Views

RBM view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the peer IPv6 address for setting up the control channel. The IP address cannot be an all-zero address, loopback address, multicast address, or IPv6 address with an embedded IPv4 address.

port *port-number*: Specifies a port by its number used for establishing TCP connection. The value range for the *port-number* argument is 1024 to 65535, and the default value is 60064. Make sure the port number is not in use.

Usage guidelines

The control channel transmits data by using packets, including hot backup status packets, configuration consistency check packets, and configuration synchronization packets. Each member device compares the specified local and peer IPv6 address to determine the device role for setting up the control channel. The device with higher IPv6 address acts as the server to listen for TCP connection requests, and the other device acts as the client to initiate the TCP connection.

If the port number is configured on the server, the port provides services for the client. If the port number is configured on the client, the port serves as the destination port to establish TCP connection to the server. The source port is randomly generated on the client.

You can specify only one peer IPv6 address with the same port number on the primary and secondary devices.

You can configure a remote IPv4 address or a remote IPv6 address, but not both.

Examples

Configure the peer IPv6 address and port number as 2018::1 and 4456 for setting up the control channel.

```
<Sysname> system-view
[Sysname] remote-backup group
[Sysname-remote-backup-group] remote-ipv6 2018::1 port 4456
```

Related commands

local-ipv6

remote-ip

silent-backup-interface

Use **silent-backup-interface** to disable the standby device from sending or receiving protocol packets of a dynamic routing protocol.

Use **undo silent-backup-interface** to enable the standby device to send and receive protocol packets of a dynamic routing protocol.

Syntax

silent-backup-interface { **ospf** | **ospfv3** }

undo silent-backup-interface { **ospf** | **ospfv3** }

Default

The standby device can send and receive protocol packets of a dynamic routing protocol.

Views

RBM view

Predefined user roles

network-admin

Parameters

ospf: Specifies OSPF.

ospfv3: Specifies OSPFv3.

Usage guidelines

This command disconnects the neighbor relationships for a dynamic routing protocol on the standby device. The active device can send and receive protocol packets of that dynamic routing protocol, and correctly process both uplink and downlink traffic.

You can execute this command multiple times to disable multiple dynamic routing protocols on the standby device.

You cannot use this command together with the **adjust-cost enable** command.

Examples

Disable the standby device from sending or receiving OSPF protocol packets.

```
<Sysname> system-view
[Sysname] remote-backup group
[Sysname-remote-backup-group] silent-backup-interface ospf
```

Related commands

adjust-cost enable

switchover request

Use **switchover request** to perform an active/standby switchover.

Syntax

switchover request

Views

RBM view

Predefined user roles

network-admin

Usage guidelines

If you want to replace components or upgrade software on the current active device, you can execute this command to switch services to the standby device.

This command applies only when hot backup operates in active/standby mode.

In a hot backup and VRRP associated network, executing this command might cause temporary virtual IP address conflict in the VRRP group, which is considered a normal condition.

For stable operation of hot backup, do not repeatedly execute this command within one minute.

Examples

Perform an active/standby switchover.

```
<Sysname> system-view
[Sysname] remote-backup group
[Sysname-remote-backup-group] switchover request
```

track

Use **track** to associate hot backup with Track.

Use **undo track** to remove the association.

Syntax

track *track-entry-number*

undo track *track-entry-number*

Default

The hot backup system is not associated with Track.

Views

RBM view

Predefined user roles

network-admin

Parameters

track-entry-number: Specifies a track entry by its ID in the range of 1 to 1024.

Usage guidelines

Use this command to associate hot backup with Track to monitor links. If one of the monitored track entries becomes Negative, hot backup performs an active/standby switchover and switches traffic

to the new active device to ensure service continuity. For more information about Track, see *Network Management and Monitoring Configuration Guide*.

You can use the **track interface** and **track** commands in conjunction, but you cannot use these commands to monitor the same interfaces.

The **track vlan** and **track** commands are mutually exclusive. You cannot configure both of them.

To associate hot backup with multiple track entries, execute this command multiple times.

Examples

Associate hot backup with track entries 1 and 2.

```
<Sysname> system-view
[Sysname] remote-backup group
[Sysname-remote-backup-group] track 1
[Sysname-remote-backup-group] track 2
```

Related commands

track (*Network Management and Monitoring Command Reference*)

track interface

Use **track interface** to enable hot backup to monitor an interface.

Use **undo track interface** to remove the configuration.

Syntax

track interface *interface-type interface-number*

undo track interface [*interface-type interface-number*]

Default

The hot backup system does not monitor any interfaces.

Views

RBM view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number. You can specify a Layer 2 or Layer 3 Ethernet interface in the current software version. If you do not specify this argument, the **undo** form of the command removes the monitoring for all interfaces.

Usage guidelines

Use this command to enable hot backup to monitor the interfaces connecting the uplink and downlink devices. The monitored interfaces can forward packets only when they are all up. If any of the monitored interfaces goes down, none of them will be able to forward packets.

If the uplink and downlink interfaces of the hot backup system are Layer 3 Ethernet interfaces and hot backup is used with static routes, use the **track interface** command to monitor those interfaces.

If the uplink and downlink interfaces of the hot backup system are Layer 2 Ethernet interfaces connected to peer Layer 3 interfaces, use the **track interface** command to monitor the Layer 2 Ethernet interfaces.

You can use the **track interface** and **track** commands in conjunction, but you cannot use these commands to monitor the same interfaces.

The **track vlan** and **track interface** commands are mutually exclusive. You cannot configure both of them.

To enable hot backup to monitor multiple interfaces, execute this command multiple times.

The hot backup system does not support monitoring member ports of aggregate interfaces.

Examples

Enable hot backup to monitor interfaces GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

```
<Sysname> system-view
[Sysname] remote-backup group
[Sysname-remote-backup-group] track interface gigabitethernet 1/0/1
[Sysname-remote-backup-group] track interface gigabitethernet 1/0/2
```

Related commands

track

track interface

track vlan

track vlan

Use **track vlan** to enable hot backup to monitor a VLAN.

Use **undo track vlan** to remove the configuration.

Syntax

track vlan *vlan-id*

undo track vlan [*vlan-id*]

Default

The hot backup system does not monitor any VLANs.

Views

RBM view

Predefined user roles

network-admin

Parameters

vlan-id: Specifies a VLAN by its ID in the range of 1 to 4094. If you do not specify this argument, the **undo** form of the command removes the monitoring for all VLANs.

Usage guidelines

Use this command to enable hot backup to monitor the VLANs of the uplink and downlink devices. The monitored VLANs are active and the member ports can forward packets only when the member ports are all up. If any of the member ports goes down, none of them will be able to forward packets, and all the monitored VLANs will become inactive.

In active/standby mode, the state of monitored VLANs is active on the primary device and inactive on the secondary device.

In dual-active mode, the state of monitored VLANs is active on both the primary and secondary devices.

Do not enable hot backup to monitor VLAN 1 (to which all access ports belong by default). This restriction prevents an unused interface in down state from interrupting operation of other interfaces in VLAN 1.

To enable hot backup to monitor multiple VLANs, execute this command multiple times.

The **track vlan** command is mutually exclusive with the **track interface** and **track** commands. You cannot use the **track vlan** command in conjunction with the **track interface** or **track** command.

Examples

Enable hot backup to monitor VLAN 10.

```
<Sysname> system-view
[Sysname] remote-backup group
[Sysname-remote-backup-group] track vlan 10
```

Related commands

track

track interface

track vlan

transparent-transmit enable

Use **transparent-transmit enable** to enable transparent service traffic transmission between the remote backup group members.

Use **undo transparent-transmit enable** to disable transparent service traffic transmission between the remote backup group members.

Syntax

transparent-transmit enable

undo transparent-transmit enable

Default

Transparent service traffic transmission is enabled.

Views

RBM view

Predefined user roles

network-admin

Usage guidelines

Enable transparent service traffic transmission only when asymmetric-path traffic traverses the hot backup system operating in dual-active mode.

If an asymmetric-path flow traverses the hot backup system operating in dual-active mode, the flow and its return traffic are processed by different remote backup group members. This will degrade the traffic processing performance of modules such as NBAR, DPI, and load balancing. For example, the packet recognition rate of NBAR might drop. For an asymmetric-path flow and its return traffic to be processed by the same remote backup group member, enable transparent service traffic transmission. Transparent service traffic transmission is resource-intensive. Make sure you are fully aware of the impact of this feature when you use it on a live network.

Examples

Enable transparent service traffic transmission between the remote backup group members.

```
<Sysname> system-view
[Sysname] remote-backup group
[Sysname-remote-backup-group] transparent-transmit enable
```

vrrp ipv6 vrid

Use **vrrp ipv6 vrid** to create an IPv6 VRRP group and assign a virtual IPv6 address to it, or to assign a virtual IPv6 address to an existing IPv6 VRRP group.

Use **undo vrrp ipv6 vrid** to remove all configurations of an IPv6 VRRP group, or to remove a virtual IPv6 address from an IPv6 VRRP group.

Syntax

vrrp ipv6 vrid *virtual-router-id* **virtual-ip** *virtual-address* [*prefix-length*] **link-local** { **active** | **standby** }

undo vrrp ipv6 vrid *virtual-router-id* [**virtual-ip** [*virtual-address* [**link-local**]]]

Default

No IPv6 VRRP groups exist.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

virtual-router-id: Specifies an IPv6 VRRP group by its virtual router ID in the range of 1 to 255.

virtual-ip *virtual-address*: Specifies a virtual IPv6 address. If you do not specify this option, the **undo vrrp ipv6 vrid** command removes all virtual IPv6 addresses from the specified IPv6 VRRP group.

prefix-length: Specifies the prefix length of the virtual IPv6 address, in the range of 1 to 128. If you do not specify this argument, the default value 128 applies.

link-local: Specifies a link-local address as the virtual IPv6 address.

active: Associates the IPv6 VRRP group with hot backup by adding the device to the IPv6 VRRP active group. The initial role of the device is master.

standby: Associates the IPv6 VRRP group with hot backup by adding the device to the IPv6 VRRP standby group. The initial role of the device is backup.

Usage guidelines

You can execute this command multiple times to assign multiple virtual IPv6 addresses to an IPv6 VRRP group. When you configure hot backup in collaboration with VRRP, you can assign a maximum of 4096 virtual IPv6 addresses to a VRRP group. If you specify the prefix length to assign a virtual IPv6 subnet, the subnet is recognized as one virtual IPv6 address.

The first virtual IPv6 address that you assign to an IPv6 VRRP group must be a link-local address, and it must be removed last.

An IPv6 VRRP group can have only one link-local address as its virtual IPv6 address. For an IPv6 VRRP group to work correctly, you must also assign it a global unicast address as a virtual IPv6 address.

The virtual IPv6 address of an IPv6 VRRP group and the downlink interface IPv6 address of the VRRP group members must be on the same subnet. Otherwise, the hosts on the subnet might fail to access external networks.

You cannot associate an IPv6 VRRP group operating in load balancing mode with hot backup.

When you configure hot backup in collaboration with VRRP, make sure the interfaces in an IPv6 VRRP group do not own the virtual IPv6 addresses.

You cannot associate an IPv6 VRRP group with both hot backup and Track.

You cannot use the **track vlan** command in conjunction with the **track interface** command.

To modify the settings for the command, first execute the **undo** form of the command, and then execute the **vrrp ipv6 vrid** command again.

Examples

Create IPv6 VRRP group 1, assign virtual IPv6 address fe80::10 to the VRRP group, and assign the device to the VRRP active group. Then assign virtual IPv6 address 1::10 to the VRRP group.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local active
[Sysname-GigabitEthernet1/0/1] vrrp ipv6 vrid 1 virtual-ip 1::10
```

vrrp vrid

Use **vrrp vrid** to create an IPv4 VRRP group and assign a virtual IP address to it, or to assign a virtual IP address to an existing IPv4 VRRP group.

Use **undo vrrp vrid** to remove all configurations of an IPv4 VRRP group, or to remove a virtual IP address from an IPv4 VRRP group.

Syntax

vrrp vrid *virtual-router-id* **virtual-ip** *virtual-address* [*mask* | *mask-length*] { **active** | **standby** }

undo vrrp vrid *virtual-router-id* [**virtual-ip** [*virtual-address*]]

Default

No IPv4 VRRP groups exist.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

virtual-ip *virtual-address*: Specifies a virtual IP address. You cannot specify the virtual IP address as any of the following IP addresses:

- All-zero address (0.0.0.0).
- Broadcast address (255.255.255.255).
- Loopback address.
- IP address of other than Class A, Class B, and Class C.

- Invalid IP address (for example, 0.0.0.1).

If you do not specify the *virtual-address* argument, the **undo vrrp vrid** command removes all virtual IP addresses from the specified IPv4 VRRP group.

mask-length: Specifies a mask length in the range of 1 to 32. If you do not specify a subnet mask or a mask length, the default mask length 32 applies.

active: Associates the VRRP group with hot backup by adding the device to the VRRP active group. The initial role of the device is master.

standby: Associates the VRRP group with hot backup by adding the device to the VRRP standby group. The initial role of the device is backup.

Usage guidelines

You can execute this command multiple times to assign multiple virtual IP addresses to an IPv4 VRRP group. When you configure hot backup in collaboration with VRRP, you can assign a maximum of 4096 virtual IPv4 addresses to a VRRP group. If you specify the mask or mask length to assign a virtual IPv4 subnet, the subnet is recognized as one virtual IPv4 address.

The virtual IP address of an IPv4 VRRP group and the downlink interface IP addresses of the VRRP group members must be on the same subnet. Otherwise, the hosts on the subnet might fail to access external networks.

You cannot associate a VRRP group operating in load balancing mode with hot backup.

For VRRP to operate correctly, make sure a virtual IP address of an IPv4 VRRP group is not the IP address of any interface in the VRRP group.

When you configure hot backup in collaboration with VRRP, make sure the interfaces in an IPv4 VRRP group do not own the virtual IPv4 addresses.

You cannot associate a VRRP group with both hot backup and Track.

You cannot use the **track vlan** command in conjunction with the **track interface** command.

To modify the settings for the command, first execute the **undo** form of the command, and then execute the **vrrp vrid** command again.

Examples

Create IPv4 VRRP group 1, assign virtual IP address 10.10.10.10 to the VRRP group, and assign the device to the VRRP active group.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] vrrp vrid 1 virtual-ip 10.10.10.10 active
```

Related commands

display vrrp

NSFOCUS Firewall Series

NF Interface Command Reference

NSFOCUS Technologies, Inc.

Document version: 6W600-20230221

Preface

This command reference describes the commands for configuring interfaces in bulk, Ethernet interfaces, loopback interfaces, null interfaces, and inloopback interfaces.

This preface includes the following topics about the documentation:

- Audience.
- Conventions.

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators.

Conventions

The following information describes the conventions used in the documentation.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select a minimum of one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
CAUTION:	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Contents

Bulk interface configuration commands

display interface range

Use **display interface range** to display information about named interface ranges created by using the **interface range name** command.

Syntax

display interface range [**name** *name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

name *name*: Specifies an interface range by its name, a case-sensitive string of 1 to 32 characters. If you do not specify an interface range name, this command displays information about all interface ranges created by using the **interface range name** command.

Examples

Display information about the interface ranges created by using the **interface range name** command.

```
<Sysname> display interface range
Interface range name t2 GigabitEthernet1/0/1 GigabitEthernet1/0/2
Interface range name test GigabitEthernet1/0/3 GigabitEthernet1/0/4
```

The output shows the following:

- Interfaces GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 are added to interface range **t2**.
- Interfaces GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 are added to interface range **test**.

Related commands

interface range name

interface range

Use **interface range** to create an interface range and enter the interface range view.

Syntax

interface range *interface-list*

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interface-list: Specifies a space-separated list of up to 24 interface items. Each item specifies an interface by its type and number or specifies a subrange of interfaces in the form of *interface-type interface-number1* **to** *interface-type interface-number2*.When you specify a subrange of interfaces, the interfaces must be all fixed interfaces or on the same interface module. The start interface number must be identical to or lower than the end interface number.

Usage guidelines

Use this command to bulk configure multiple interfaces with the same feature instead of configuring them one by one. For example, execute the **shutdown** command in interface range view to shut down a range of interfaces.

The interface range created by using this command is not saved to the running configuration. You cannot use the interface range repeatedly. To create an interface range that can be used repeatedly, use the **interface range name** command.

In interface range view, only the commands supported by the first interface in the specified interface list are available for configuration. To view available commands, enter a question mark (?) in interface range view.

After a command is executed in interface range view, one of the following situations might occur:

- The system displays an error message and stays in interface range view. It means that the execution failed on one or multiple member interfaces.
  - If the execution failed on the first member interface, the command is not executed on any member interfaces.
  - If the execution failed on a non-first member interface, the command takes effect on the remaining member interfaces.
- The system returns to system view. It means that:
  - The command is supported in both system view and interface view.
  - The execution failed on a member interface in interface range view and succeeded in system view.
  - The command is not executed on the subsequent member interfaces.

  You can use the **display this** command to verify the configuration in interface view of each member interface. In addition, if the configuration in system view is not needed, use the **undo** form of the command to remove the configuration.

To verify the configuration of the first member interface, you can execute the **display this** command in interface range view.

When you bulk configure interfaces, follow these guidelines:

- Before you configure an interface as the first interface in an interface range, make sure you can enter the view of the interface by using the **interface** *interface-type* { *interface-number* | *interface-number.subnumber* } command.
- Do not assign both an aggregate interface and any of its member interfaces to an interface range. Some commands, after being executed on both an aggregate interface and its member interfaces, can break up the aggregation.
- Understand that the more interfaces you specify, the longer the command execution time.

Examples

Shut down interfaces GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4.

```
<Sysname> system-view
[Sysname] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```

```
[Sysname-if-range] shutdown
```

interface range name

Use **interface range name** *name* **interface** *interface-list* to create a named interface range and enter the interface range view.

Use **interface range name** *name* without the **interface** keyword to enter the view of a named interface range.

Use **undo interface range name** to delete the interface range with the specified name.

Syntax

interface range name *name* [**interface** *interface-list*]

undo interface range name *name*

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

name: Specifies an interface range name, a case-sensitive string of 1 to 32 characters.

interface-list: Specifies a space-separated list of up to 24 interface items. Each item specifies an interface by its type and number or a subrange of interfaces in the form of *interface-type interface-number1* **to** *interface-type interface-number2*.When you specify a subrange of interfaces, the interfaces must be all fixed interfaces or on the same interface module. The start interface number must be identical to or lower than the end interface number.

Usage guidelines

A named interface range is saved in the running configuration and can be used repeatedly to bulk configure its member interfaces.

In interface range view, only the commands supported by the first interface in the specified interface list are available for configuration. To view available commands, enter a question mark (?) in interface range view.

After a command is executed in interface range view, one of the following situations might occur:

- The system displays an error message and stays in interface range view. It means that the execution failed on one or multiple member interfaces.
  - If the execution failed on the first member interface, the command is not executed on any member interfaces.
  - If the execution failed on a non-first member interface, the command takes effect on the remaining member interfaces.
- The system returns to system view. It means that:
  - The command is supported in both system view and interface view.
  - The execution failed on a member interface in interface range view and succeeded in system view.
  - The command is not executed on the subsequent member interfaces.

  You can use the **display this** command to verify the configuration in interface view of each member interface. In addition, if the configuration in system view is not needed, use the **undo** form of the command to remove the configuration.

To verify the configuration of the first interface, you can execute the **display this** command in interface range view.

To view the member interfaces of a named interface range, use the **display interface range** command.

When you bulk configure interfaces, follow these guidelines:

- Before you configure an interface as the first interface in an interface range, make sure you can enter the view of the interface by using the **interface** *interface-type* { *interface-number* | *interface-number.subnumber* } command.
- Do not assign both an aggregate interface and any of its member interfaces to an interface range. Some commands, after being executed on both an aggregate interface and its member interfaces, can break up the aggregation.
- Understand that the more interfaces you specify, the longer the command execution time.
- To guarantee bulk interface configuration performance, configure fewer than 1000 interface range names.

Examples

Add GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to interface range **myEthPort**, and enter the interface range view.

```
<Sysname> system-view
[Sysname] interface range name myEthPort interface gigabitethernet 1/0/1 to
gigabitethernet 1/0/4
[Sysname-if-range-myEthPort]
```

Enter the view of interface range **myEthPort**.

```
<Sysname> system-view
[Sysname] interface range name myEthPort
[Sysname-if-range-myEthPort]
```

Related commands

display interface range

Contents

Ethernet interface commands

Physical interfaces on firewall modules can only be used as IRF physical interfaces.

Common Ethernet interface commands

bandwidth

Use **bandwidth** to set the expected bandwidth of an interface.

Use **undo bandwidth** to restore the default.

Syntax

bandwidth *bandwidth-value*

undo bandwidth

Default

The expected bandwidth (in kbps) is the interface baud rate divided by 1000.

Views

Ethernet interface view

Ethernet subinterface view

Predefined user roles

network-admin

context-admin

Parameters

bandwidth-value: Specifies the expected bandwidth in the range of 1 to 400000000 kbps.

Usage guidelines

The expected bandwidth is an informational parameter used only by higher-layer protocols for calculation. You cannot adjust the actual bandwidth of an interface by using this command.

Examples

Set the expected bandwidth of GigabitEthernet 1/0/1 to 1000 kbps.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] bandwidth 1000
```

Set the expected bandwidth of GigabitEthernet 1/0/1.1 to 1000 kbps.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1.1
[Sysname-GigabitEthernet1/0/1.1] bandwidth 1000
```

Related commands

speed

broadcast-suppression

Use **broadcast-suppression** to enable broadcast suppression and set the broadcast suppression threshold.

Use **undo broadcast-suppression** to disable broadcast suppression.

Syntax

broadcast-suppression { *ratio* | **pps** *max-pps* | **kbps** *max-kbps* }

undo broadcast-suppression

Default

Ethernet interfaces do not suppress broadcast traffic.

Views

Ethernet interface view

Predefined user roles

network-admin

context-admin

Parameters

ratio: Sets the broadcast suppression threshold as a percentage of the interface bandwidth. The value range for this argument is 0 to 100. A smaller value means that less broadcast traffic is allowed to pass through.

pps *max-pps*: Specifies the maximum number of broadcast packets that the interface can forward per second. The value range for the *max-pps* argument (in pps) is 0 to 1.4881 × the interface bandwidth.

kbps *max-kbps*: Specifies the maximum number of kilobits of broadcast traffic that the Ethernet interface can forward per second. The value range for this argument (in kbps) is 0 to the interface bandwidth.

Usage guidelines

The broadcast storm suppression features limits the size of broadcast traffic to a threshold on an interface. When the broadcast traffic on the interface exceeds this threshold, the system drops packets until the traffic drops below this threshold.

Both the **storm-constrain** command and the **broadcast-suppression** command can suppress broadcast storms on a port. The **broadcast-suppression** command uses the chip to physically suppress broadcast traffic. It has less influence on the device performance than the **storm-constrain** command, which uses software to suppress broadcast traffic.

For the traffic suppression result to be determined, do not configure both the **storm-constrain broadcast** command and the **broadcast-suppression** command on an interface.

The configured suppression threshold value in pps or kbps might be converted into a multiple of a step supported by the chip. As a result, the effective suppression threshold might be different from the configured one. To determine the suppression threshold that takes effect, see the prompts on the device.

Examples

Set the broadcast suppression threshold to 10000 kbps on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] broadcast-suppression kbps 10000
```

Related commands

- **multicast-suppression**

  unicast-suppression

combo enable

> **CAUTION:**
>
> - In the BootWare menu, fiber combo ports are not available.
> - When the fiber combo port is active, it supports only the speeds autonegotiation and 1000 Mbps, and supports only duplex modes full and autonegotiation. If the copper combo port is configured with any other speed or duplex settings, the settings do not take effect after it is switched to the fiber combo port.

Use **combo enable** to activate the copper or fiber combo port of a combo interface.

Syntax

combo enable { **copper** | **fiber** }

The following matrixes show support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	Yes
NFNX3-HDB680, NFNX3-HDB1080	No

Default

The copper combo port of a combo interface is activated.

Views

Ethernet interface view

Predefined user roles

network-admin

context-admin

Parameters

copper: Activates the copper combo port. In this case, use twisted pairs to connect the port.

fiber: Activates the fiber combo port. In this case, use optical fibers to connect the port.

Usage guidelines

A combo interface is a logical interface that physically contains one fiber combo port and one copper combo port on the device panel. The two ports share one forwarding interface. As a result, they cannot work simultaneously. When you activate either port, the other port is automatically disabled. You can select to activate the copper combo port or fiber combo port.

Before using this command, perform the following tasks according to the marks on the device panel:

- Determine the combo interfaces on your device.
- Identify the two physical interfaces that belong to each combo interface.

Examples

Activate the copper combo port of combo interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] combo enable copper
```

Activate the fiber combo port of combo interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] combo enable fiber
```

dampening

Use **dampening** to enable the device to dampen an interface when the interface is flapping.

Use **undo dampening** to restore the default.

Syntax

dampening [*half-life reuse suppress max-suppress-time*]

undo dampening

Default

Interface dampening is disabled on Ethernet interfaces.

Views

Ethernet interface view

Predefined user roles

network-admin

context-admin

Parameters

half-life: Specifies the amount of time after which a penalty is decreased, in the range of 1 to 120 seconds. The default value is 54 seconds.

reuse: Specifies the reuse threshold in the range of 200 to 20000. The default value is 750. The reuse threshold must be less than the suppression threshold.

suppress: Specifies the suppression threshold in the range of 200 to 20000. The default value is 2000.

max-suppress-time: Specifies the maximum amount of time the interface can be dampened, in the range of 1 to 255 seconds. The default value is 162 seconds (three times the half-life timer).

Usage guidelines

When configuring the **dampening** command, follow these rules to set the values mentioned above:

- The ceiling is equal to 2 (Max-suppress-time/Decay) × reuse-limits. It is not user configurable.
- The configured suppress limit is lower than or equal to the ceiling.
- The ceiling is lower than or equal to the maximum suppress limit supported.

This command does not take effect on the administratively down events. When you execute the **shutdown** command, the penalty restores to 0, and the interface reports the down event to the higher layer protocols.

Do not enable the dampening function on an interface with spanning tree protocols enabled.

After an interface in down state is dampened, the interface state displayed through the **display interface** command, MIB, or Web is always down.

Examples

Enable interface dampening on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dampening
```

Enable interface dampening on GigabitEthernet 1/0/1, and set the following parameters:

- Half life time to 2 seconds.
- Reuse value to 800.
- Suppression threshold to 3000.
- Maximum suppression interval to 5 seconds.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dampening 2 800 3000 5
```

Related commands

display interface

default

Use **default** to restore the default settings for an interface.

Syntax

default

Views

Ethernet interface view

Ethernet subinterface view

Predefined user roles

network-admin

context-admin

Usage guidelines

CAUTION:

The **default** command might interrupt ongoing network services. Make sure you are fully aware of the impacts of this command when you use it in a live network.

This command might fail to restore the default settings for some commands because of command dependencies or system restrictions. You can use the **display this** command in interface view to identify these commands, and use their **undo** forms or follow the command reference to restore their default settings. If your restoration attempt still fails, follow the error message instructions to solve the problem.

Examples

Restore the default settings for GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] default
```

```
This command will restore the default settings. Continue? [Y/N]:y
```

Restore the default settings for GigabitEthernet 1/0/1.1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1.1
[Sysname-GigabitEthernet1/0/1.1] default
This command will restore the default settings. Continue? [Y/N]:y
```

description

Use **description** to configure the description of an interface.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

The description of an interface is the interface name plus **Interface** (for example, **GigabitEthernet1/0/1 Interface**).

Views

Ethernet interface view

Ethernet subinterface view

Predefined user roles

network-admin

context-admin

Parameters

text: Specifies the interface description, a case-sensitive string of 1 to 255 characters.

Examples

Set the description of GigabitEthernet 1/0/1 to **lan-interface**.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] description lan-interface
```

Set the description of GigabitEthernet 1/0/1.1 to **subinterface1/0/1.1**.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1.1
[Sysname-GigabitEthernet1/0/1.1] description subinterface1/0/1.1
```

display counters

Use **display counters** to display interface traffic statistics.

Syntax

display counters { **inbound** | **outbound** } **interface** [*interface-type* [*interface-number* | *interface-number.subnumber*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

inbound: Displays inbound traffic statistics.

outbound: Displays outbound traffic statistics.

interface-type: Specifies an interface type.

interface-number: Specifies an interface number.

interface-number.subnumber: Specifies a subinterface number. The *interface-number* argument is an interface number. The *subnumber* argument is the number of a subinterface created under the interface. The value range for the *subnumber* argument is 1 to 4094.

Usage guidelines

To clear the Ethernet interface traffic statistics, use the **reset counters interface** command.

If you do not specify an interface type, this command displays traffic statistics for all interfaces that have traffic counters.

If you specify an interface type but do not specify an interface number, this command displays traffic statistics for all interfaces of the specified type.

If you specify an interface type and number, this command displays traffic statistics for the specified interface.

Examples

Display inbound traffic statistics for all interfaces.

```
<Sysname> display counters inbound interface
Interface            Total (pkts)    Broadcast (pkts)    Multicast (pkts)  Err (pkts)
GE1/0/1                       100                 100                   0           0
GE1/0/2                  Overflow            Overflow            Overflow    Overflow

 Overflow: More than 14 digits (7 digits for column "Err").
       --: Not supported.
```

Table 1 Command output

Field	Description
Interface	Abbreviated interface name.
Total (pkts)	Total number of packets received or sent through the interface.
Broadcast (pkts)	Total number of broadcast packets received or sent through the interface.
Multicast (pkts)	Total number of multicast packets received or sent through the interface.
Err (pkts)	Total number of error packets received or sent through the interface.
Overflow: More than 14 digits (7 digits for column "Err")	The command displays **Overflow** when any of the following conditions exist: • The data length of an **Err** field value is greater than 7 decimal digits. • The data length of a non-Err field value is greater than 14 decimal digits.

Field	Description
--: Not supported	The statistical item is not supported.

Related commands

reset counters interface

display counters rate

Use **display counters rate** to display traffic rate statistics for interfaces in up state for the most recent statistics polling interval.

Syntax

display counters rate { **inbound** | **outbound** } **interface** [*interface-type* [*interface-number* | *interface-number.subnumber*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

inbound: Displays inbound traffic rate statistics.

outbound: Displays outbound traffic rate statistics.

interface-type: Specifies an interface type.

interface-number: Specifies an interface number.

interface-number.subnumber: Specifies a subinterface number. The *interface-number* argument is an interface number. The *subnumber* argument is the number of a subinterface created under the interface. The value range for the *subnumber* argument is 1 to 4094.

Usage guidelines

If you do not specify an interface type, this command displays traffic rate statistics for all up interfaces that have traffic counters.

If you specify an interface type but do not specify an interface number, this command displays traffic rate statistics for all up interfaces of the specified type.

If you specify an interface type and an interface, this command displays traffic rate statistics for the specified interface.

If an interface that you specify is always down for the most recent statistics polling interval, the system prompts that the interface does not support the command.

You can use the **flow-interval** command to set the statistics polling interval.

Examples

Display the inbound traffic rate statistics for all interfaces.

```
<Sysname> display counters rate inbound interface
Usage: Bandwidth utilization in percentage
```

```
Interface            Usage (%)   Total (pps)   Broadcast (pps)   Multicast (pps)
GE1/0/1                      0             0                --                --

 Overflow: More than 14 digits.
       --: Not supported.
```

Table 2 Command output

Field	Description
Interface	Abbreviated interface name.
Usage (%)	Bandwidth usage (in percentage) of the interface for the last statistics polling interval.
Total (pps)	Average receiving or sending rate (in pps) for unicast packets for the last statistics polling interval.
Broadcast (pps)	Average receiving or sending rate (in pps) for broadcast packets for the last statistics polling interval.
Multicast (pps)	Average receiving or sending rate (in pps) for multicast packets for the last statistics polling interval. .
Overflow: more than 14 decimal digits	The command displays **Overflow** if the data length of a statistical item is greater than 14 decimal digits.
--: not supported	The statistical item is not supported.

Related commands

`flow-interval`

`reset counters interface`

display ethernet statistics

Use **`display ethernet statistics`** to display the Ethernet module statistics.

Syntax

`display ethernet statistics slot` *`slot-number`*

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

`slot` *`slot-number:`* Specifies an IRF member device by its member ID.

Examples

Display the Ethernet module statistics for the specified slot.

```
<Sysname> display ethernet statistics slot 1
ETH receive packet statistics:
    Totalnum        : 10447          ETHIINum     : 4459
```

```
    SNAPNum          : 0              RAWNum        : 0
    LLCNum           : 0              UnknownNum    : 0
    ForwardNum       : 4459           ARP           : 0
    MPLS             : 0              ISIS          : 0
    ISIS2            : 0              IP            : 0
    IPV6             : 0
ETH receive error statistics:
    NullPoint        : 0              ErrIfindex    : 0
    ErrIfcb          : 0              IfShut        : 0
    ErrAnalyse       : 5988           ErrSrcMAC     : 5988
    ErrHdrLen        : 0

ETH send packet statistics:
    L3OutNum         : 211            VLANOutNum    : 0
    FastOutNum       : 155            L2OutNum      : 0
ETH send error statistics:
    MbufRelayNum     : 0              NullMbuf      : 0
    ErrAdjFwd        : 0              ErrPrepend    : 0
    ErrHdrLen        : 0              ErrPad        : 0
    ErrQoSTrs        : 0              ErrVLANTrs    : 0
    ErrEncap         : 0              ErrTagVLAN    : 0
    IfShut           : 0              IfErr         : 0
```

Table 3 Output description

Field	Description
ETH receive packet statistics	Statistics about the Ethernet packets received by the Ethernet module: • **Totalnum**—Total number of received packets. • **ETHIINum**—Number of packets encapsulated by using Ethernet II. • **SNAPNum**—Number of packets encapsulated by using SNAP. • **RAWNum**—Number of packets encapsulated by using RAW. • **ISISNum**—Number of packets encapsulated by using ISIS. • **LLCNum**—Number of packets encapsulated by using LLC. • **UnknownNum**—Number of packets encapsulated by using unknown methods. • **ForwardNum**—Number of packets forwarded at Layer 2 or sent to the CPU. • **ARP**—Number of ARP packets. • **ISIS**—Number of IS-IS packets. • **ISIS2**—Number of large 802.3/802.2 frames encapsulated by using IS-IS. • **IP**—Number of IP packets. • **IPv6**—Number of IPv6 packets.

Field	Description
ETH receive error statistics	Statistics about the error Ethernet packets in the inbound direction on the Ethernet module. Errors might be included in packets or occur during the receiving process. The items include: • **NullPoint**—Number of packets that include null pointers. • **ErrIfindex**—Number of packets that include incorrect interface indexes. • **ErrIfcb**—Number of packets that include incorrect interface control blocks. • **IfShut**—Number of packets that are being received when the interface is shut down. • **ErrAnalyse**—Number of packets that include packet parsing errors. • **ErrSrcMAC**—Number of packets that include incorrect source MAC addresses. • **ErrHdrLen**—Number of packets that include header length errors.
ETH send packet statistics	Statistics about the Ethernet packets sent by the Ethernet module: • **L3OutNum**—Number of packets sent out of Layer 3 Ethernet interfaces. • **VLANOutNum**—Number of packets sent out of VLAN interfaces. • **FastOutNum**—Number of packets fast forwarded. • **L2OutNum**—Number of packets sent out of Layer 2 Ethernet interfaces.
ETH send error statistics	Statistics about the error Ethernet packets in the outbound direction on the Ethernet module: • **MbufRelayNum**—Number of packets transparently sent. • **NullMbuf**—Number of packets with null pointers. • **ErrAdjFwd**—Number of packets with adjacency table errors. • **ErrPrepend**—Number of packets with extension errors. • **ErrHdrLen**—Number of packets with header length errors. • **ErrPad**—Number of packets with padding errors. • **ErrQoSTrs**—Number of packets that failed to be sent by QoS. • **ErrVLANTrs**—Number of packets that failed to be sent in VLANs. • **ErrEncap**—Number of packets that failed to be sent due to link header encapsulation failures. • **ErrTagVLAN**—Number of packets that failed to be sent due to VLAN tag encapsulation failures. • **IfShut**—Number of packets that are being sent when the interface is shut down. • **IfErr**—Number of packets with incorrect outgoing interfaces.

Related commands

`reset ethernet statistics`

display interface

Use **`display interface`** to display interface information.

Syntax

`display interface` [*`interface-type`* [*`interface-number`* | *`interface-number.subnumber`*]] [**`brief`** [**`description`** | **`down`**]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface-type: Specifies an interface type.

interface-number: Specifies an interface number.

interface-number.subnumber: Specifies a subinterface number. The *interface-number* argument is an interface number. The *subnumber* argument is the number of a subinterface created under the interface. The value range for the *subnumber* argument is 1 to 4094.

brief: Displays brief interface information. If you do not specify this keyword, the command displays detailed interface information.

description: Displays complete interface descriptions. If you do not specify this keyword, the command displays only the first 27 characters of each interface description.

down: Displays information about interfaces in down state and the causes. If you do not specify this keyword, the command displays information about interfaces in all states.

Usage guidelines

If you do not specify an interface type, this command displays information about all interfaces except VA interfaces. For more information about VA interfaces, see PPP in *Layer 2—WAN Access Configuration Guide*.

If you specify an interface type but do not specify an interface number, this command displays information about all interfaces of the specified type.

Examples

Display information about Layer 3 interface GigabitEthernet 1/0/1.

```
<Sysname> display interface gigabitethernet 1/0/1
GigabitEthernet1/0/1
Current state: Administratively DOWN
Line protocol state: DOWN
Description: GigabitEthernet1/0/1 Interface
Bandwidth: 1000000 kbps
Maximum transmission unit: 1500
Allow jumbo frames to pass
Broadcast max-ratio: 100%
Multicast max-ratio: 100%
Unicast max-ratio: 100%
Internet protocol processing: Disabled
IP packet frame type: Ethernet II, hardware address: 3822-d666-bd0c
IPv6 packet frame type: Ethernet II, hardware address: 3822-d666-bd0c
Media type is twisted pair, loopback not set, promiscuous mode set
Speed Negotiation, Duplex Negotiation, link type is autonegotiation
Output flow-control is disabled, input flow-control is disabled
Last link flapping: Never
Last clearing of counters: Never
Current system time:2078-11-09 17:58:38
```

```
Last time when physical state changed to up:-
Last time when physical state changed to down:2078-11-01 21:21:23
 Peak input rate: 0 bytes/sec, at 00-00-00 00:00:00
 Peak output rate: 0 bytes/sec, at 00-00-00 00:00:00
 Last 300 second input: 0 packets/sec 0 bytes/sec -%
 Last 300 second output: 0 packets/sec 0 bytes/sec -%
 Input (total):  0 packets, 0 bytes
          0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Input (normal):  0 packets, 0 bytes
          0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Input:  0 input errors, 0 runts, 0 giants, - throttles
          0 CRC, 0 frame, 0 overruns, 0 aborts
          0 ignored, - parity errors
 Output (total): 0 packets, 0 bytes
          0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Output (normal): 0 packets, 0 bytes
          0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Output: 0 output errors, 0 underruns, - buffer failures
          0 aborts, 0 deferred, 0 collisions, 0 late collisions
          0 lost carrier, 0 no carrier
IPv4 traffic statistics:
Last 300 seconds input rate: 300 packets/sec, 230000 bytes/sec
Last 300 seconds output rate: 200 packets/sec, 220000 bytes/sec
Input: 12 packets, 1968 bytes
Output: 0 packets, 0 bytes
IPv6 traffic statistics:
 Last 300 seconds input rate: 300 packets/sec, 230000bytes/sec
 Last 300 seconds output rate: 200 packets/sec,220000 bytes/sec
 Input: 12 packets, 1968 bytes
 Output: 0 packets, 0 bytes
```

Display detailed information about Layer 2 interface GigabitEthernet 1/0/1.

```
<Sysname> display interface gigabitethernet 1/0/1
GigabitEthernet1/0/1
Current state: DOWN
Line protocol state: DOWN
IP packet frame type: Ethernet II, hardware address: 000c-2963-b767
Description: GigabitEthernet1/0/1 Interface
Bandwidth: 100000 kbps
Loopback is not set
Media type is twisted pair, port hardware type is 1000_BASE_T_AN_SFP
Unknown-speed mode, unknown-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
Flow-control is not enabled
Maximum frame length: 9216
Allow jumbo frame to pass
Broadcast max-ratio: 100%
Multicast max-ratio: 100%
Unicast max-ratio: 100%
```

```
PVID: 1
MDI type: Automdix
Port link-type: Access
 Tagged VLANs:   None
 UnTagged VLANs: 1
Port priority: 2
Last link flapping: 6 hours 39 minutes 25 seconds
Last clearing of counters:  14:34:09 Tue 11/01/2011
Current system time:2017-12-09 10:59:08
Last time when physical state changed to up:-
Last time when physical state changed to down:2017-12-09 10:59:07
 Peak input rate: 0 bytes/sec, at 2013-07-17 22:06:19
 Peak output rate: 0 bytes/sec, at 2013-07-17 22:06:19
 Last 300 second input:  0 packets/sec 0 bytes/sec -%
 Last 300 second output:  0 packets/sec 0 bytes/sec -%
 Input (total):  0 packets, 0 bytes
          0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Input (normal):  0 packets, 0 bytes
          0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Input:  0 input errors, 0 runts, 0 giants, 0 throttles
          0 CRC, 0 frame, 0 overruns, 0 aborts
          0 ignored, 0 parity errors
 Output (total): 0 packets, 0 bytes
          0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Output (normal): 0 packets, 0 bytes
          0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Output: 0 output errors, 0 underruns, 0 buffer failures
          0 aborts, 0 deferred, 0 collisions, 0 late collisions
          0 lost carrier, 0 no carrier
```

Table 4 Command output

Field	Description
Current state	Physical link state of the interface: • **Administratively DOWN**—The interface has been shut down by using the **shutdown** command. • **DOWN**—The interface is administratively up, but its physical state is down (possibly because no physical link exists or the link has failed). • **DOWN (Link-Aggregation interface down)**—The aggregate interface to which the interface belongs has been shut down by using the **shutdown** command. • **DOWN (Monitor-Link uplink down)**—The interface has been shut down by Monitor Link. • **ETH-rddc Shutdown**—The interface has been shut down by the Reth module. • **mac-address moving down**—The interface has been shut down by the MAC address move suppression feature. • **MAD ShutDown**—The interface has been shut down by IRF MAD. This state occurs if the interface is on an IRF fabric placed in Recovery state after an IRF split. • **Storm-Constrain**—The interface has been shut down because the storm control feature detected that multicast or broadcast traffic exceeded the upper threshold. • **STP DOWN**—The interface has been shut down by the BPDU guard feature. • **UP**—The interface is both administratively and physically up.

Line protocol state	Data link layer state of the interface. The state is determined through automatic parameter negotiation at the data link layer.
	• **UP**—The data link layer protocol is up.
	• **UP (spoofing)**—The data link layer protocol is up, but the link is an on-demand link or does not exist. This attribute is typical of null interfaces and loopback interfaces.
	• **DOWN**—The data link layer protocol is down.
	• **DOWN (***protocols***)**—The data link layer has been shut down by protocols included in the parentheses. Available protocols include:
	  ○ **LAGG**—Shuts down the data link layer when it detects that the aggregate interface does not have Selected ports.
	  ○ **BFD**—Shuts down the data link layer when it detects a link failure.

The peer line protocol state is DOWN(Bit-error down)	Bit errors occur on the peer interface, so the data link layer state of the interface is down. This field is displayed when the local interface receives bit error messages from the peer interface.
Bandwidth	Expected bandwidth of the interface.
Maximum transmission unit	MTU of the interface.
Internet protocol processing: Disabled	The interface is not assigned an IP address and cannot process IP packets.

Field	Description
Internet address: *ip-address*/*mask-length* (*Type*)	IP address of the interface and type of the address in parentheses. Possible IP address types include: • **Primary**—Manually configured primary IP address. • **Sub**—Manually configured secondary IP address. If the interface has both primary and secondary IP addresses, the primary IP address is displayed. If the interface has only secondary IP addresses, the lowest secondary IP address is displayed. • **DHCP-allocated**—DHCP allocated IP address. For more information, see DHCP client configuration in *Layer 3—IP Services Configuration Guide*. • **BOOTP-allocated**—BOOTP allocated IP address. For more information, see BOOTP client configuration in *Layer 3—IP Services Configuration Guide*. • **PPP-negotiated**—IP address assigned by a PPP server during PPP negotiation. For more information, see PPP configuration in *Layer 2—WAN Access Configuration Guide*. • **Unnumbered**—IP address borrowed from another interface. • **Cellular-allocated**—IP address allocated through the modem-manufacturer's proprietary protocol. For more information, see mobile communication modem management in *Layer 2—WAN Access Configuration Guide*. • **MAD**—IP address assigned to an IRF member device for MAD on the interface. For more information, see IRF configuration in *Virtual Technologies Configuration Guide*.
IP packet frame type	IPv4 packet framing format.
hardware address	MAC address of the interface.
IPv6 packet frame type	IPv6 packet framing format.
FEC mode	FEC mode. This field depends on your configuration.
Port priority	Port priority of the interface.
Loopback is set internal	An internal loopback test is running on the interface. This field depends on your configuration.
Loopback is set external	An external loopback test is running on the interface. This field depends on your configuration.
Loopback is not set	No loopback test is running on the interface. This field depends on your configuration.
10Mbps-speed mode	The interface is operating at 10 Mbps. This field depends on your configuration and the link parameter negotiation result.
100Mbps-speed mode	The interface is operating at 100 Mbps. This field depends on your configuration and the link parameter negotiation result.
1000Mbps-speed mode	The interface is operating at 1000 Mbps. This field depends on your configuration and the link parameter negotiation result.
10Gbps-speed mode	The interface is operating at 10 Gbps. This field depends on your configuration and the link parameter negotiation result.
Unknown-speed mode	The speed of the interface is unknown because the speed negotiation fails or the interface is physically disconnected.

Field	Description
half-duplex mode	The interface is operating in half duplex mode. This field depends on your configuration and the link parameter negotiation result.
full-duplex mode	The interface is operating in full duplex mode. This field depends on your configuration and the link parameter negotiation result.
unknown-duplex mode	The duplex mode of the interface is unknown because the duplex mode negotiation fails or the interface is physically disconnected.
Link speed type is autonegotiation	The interface is configured with the **speed auto** command.
Link speed type is force link	The interface is manually configured with a speed (for example, 1000 Mbps) by using the **speed** command.
link duplex type is autonegotiation	The interface is configured with the **duplex auto** command.
link duplex type is force link	The interface is manually configured with a duplex mode (for example, half or full) by using the **duplex** command.
Flow-control is not enabled	Generic flow control is disabled on the interface. This field depends on your configuration and the link parameter negotiation result.
Maximum frame length	Maximum length of Ethernet frames allowed to pass through the interface.
Allow jumbo frame to pass	The interface allows jumbo frames to pass through.
Broadcast max-	Broadcast storm suppression threshold in ratio, pps, or kbps. The unit of the threshold depends on your configuration.
Multicast max-	Multicast storm suppression threshold in ratio, pps, or kbps. The unit of the threshold depends on your configuration.
Unicast max-	Unknown unicast storm suppression threshold in ratio, pps, or kbps. The unit of the threshold depends on your configuration.
PVID	Port VLAN ID (PVID) of the interface.
MDI type	MDIX mode of the interface. Options include automdix, mdi, and mdix.
Port link-type	Link type of the interface: • access. • trunk. • hybrid.
Tagged VLANs	VLANs for which the interface sends packets without removing VLAN tags.
Untagged VLANs	VLANs for which the interface sends packets after removing VLAN tags.
VLAN Passing	VLANs whose packets can be forwarded by the port. The VLANs must have been created.
VLAN permitted	VLANs whose packets are permitted by the port.
Trunk port encapsulation	Encapsulation protocol type for the trunk port.
Last link flapping	The amount of time that has elapsed since the most recent physical state change of the interface. This field displays **Never** if the interface has been physically down since device startup.

Field	Description
Last clearing of counters	Time when the **reset counters interface** command was last used to clear the interface statistics. This field displays **Never** if the **reset counters interface** command has never been used on the interface since device startup.
Current system time	Current system time in the YYYY/MM/DD HH:MM:SS format. If the time zone is configured, this field is in the YYYY/MM/DD HH:MM:SS UTC±HH:MM:SS format.
Last time when physical state changed to up	Last time when physical state of the interface changed to up. A hyphen (-) indicates that the physical state of the interface has not changed to up.
Last time when physical state changed to down	Last time when physical state of the interface changed to down. A hyphen (-) indicates that the physical state of the interface has not changed to down.
Last 300 second input: 0 packets/sec 0 bytes/sec 0% Last 300 second output: 0 packets/sec 0 bytes/sec 0%	Average inbound or outbound traffic rate (in pps and Bps) in the last 300 seconds, and the ratio of the actual rate to the interface bandwidth. A hyphen (-) indicates that the statistical item is not supported.
Input(total): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	The two fields on the first line represent the inbound traffic statistics (in packets and bytes) for the interface. All inbound normal packets, abnormal packets, and normal pause frames were counted. The four fields on the second line represent: • Number of inbound unicast packets. • Number of inbound broadcasts. • Number of inbound multicasts. • Number of inbound pause frames. A hyphen (-) indicates that the statistical item is not supported.
Input(normal): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	The two fields on the first line represent the inbound normal traffic and pause frame statistics (in packets and bytes) for the interface. The four fields on the second line represent: • Number of inbound normal unicast packets. • Number of inbound normal broadcasts. • Number of inbound normal multicasts. • Number of inbound normal pause frames. A hyphen (-) indicates that the statistical item is not supported.
input errors	Statistics of incoming error packets.
runts	Number of inbound frames meeting the following conditions: • Shorter than 64 bytes. • In correct format. • Containing valid CRCs.

Field	Description
giants	Number of inbound giants. Giants refer to frames larger than the maximum frame length supported on the interface. For an Ethernet interface that does not permit jumbo frames, the maximum frame length is as follows: • 1518 bytes (without VLAN tags). • 1522 bytes (with VLAN tags). For an Ethernet interface that permits jumbo frames, the maximum Ethernet frame length is set when you configure jumbo frame support on the interface.
throttles	Number of inbound frames that had a non-integer number of bytes.
CRC	Total number of inbound frames that had a normal length, but contained CRC errors.
frame	Total number of inbound frames that contained CRC errors and a non-integer number of bytes.
overruns	Number of packets dropped because the input rate of the port exceeded the queuing capability.

aborts	Total number of illegal inbound packets:
	• **Fragment frames**—CRC error frames shorter than 64 bytes. The length (in bytes) can be an integral or non-integral value.
	• **Jabber frames**—CRC error frames greater than the maximum frame length supported on the Ethernet interface (with an integral or non-integral length).
	  ○ For an Ethernet interface that does not permit jumbo frames, the maximum frame length is 1518 bytes (without VLAN tags) or 1522 bytes (with VLAN tags).
	  ○ For an Ethernet interface that permits jumbo frames, the maximum Ethernet frame length is set when you configure jumbo frame support on the interface.
	• **Symbol error frames**—Frames that contained a minimum of one undefined symbol.
	• **Unknown operation code frames**—Non-pause MAC control frames.
	• **Length error frames**—Frames whose 802.3 length fields did not match the actual frame length (46 to 1500 bytes).

ignored	Number of inbound frames dropped because the receiving buffer of the port ran low.
parity errors	Total number of frames with parity errors.
Output(total): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	The two fields on the first line represent the outbound traffic statistics (in packets and bytes) for the interface. All outbound normal packets, abnormal packets, and normal pause frames were counted. The four fields on the second line represent: • Number of outbound unicast packets. • Number of outbound broadcasts. • Number of outbound multicasts. • Number of outbound pause frames. A hyphen (-) indicates that the statistical item is not supported.

Field	Description
Output(normal): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	The two fields on the first line represent the outbound normal traffic and pause frame statistics (in packets and bytes) for the interface. The four fields on the second line represent: • Number of outbound normal unicast packets. • Number of outbound normal broadcasts. • Number of outbound normal multicasts. • Number of outbound normal pause frames. A hyphen (-) indicates that the statistical item is not supported.
output errors	Number of outbound packets with errors.
underruns	Number of packets dropped because the output rate of the interface exceeded the output queuing capability. This is a low-probability hardware anomaly.
buffer failures	Number of packets dropped because the transmitting buffer of the interface ran low.
aborts	Number of packets that failed to be transmitted, for example, because of Ethernet collisions.
deferred	Number of frames that the interface deferred to transmit because of detected collisions.
collisions	Number of frames that the interface stopped transmitting because Ethernet collisions were detected during transmission.
late collisions	Number of frames that the interface deferred to transmit after transmitting their first 512 bits because of detected collisions.
lost carrier	This field is not supported in the current software version. Number of carrier losses during transmission. This counter increases by one when a carrier is lost, and applies to serial WAN interfaces.
no carrier	This field is not supported in the current software version. Number of times that the port failed to detect the carrier when attempting to send frames. This counter increases by one when a port failed to detect the carrier, and applies to serial WAN interfaces.
Peak input rate	Peak rate of inbound traffic in Bps, and the time when the peak inbound traffic rate occurred.
Peak output rate	Peak rate of outbound traffic in Bps, and the time when the peak outbound traffic rate occurred.

Display brief information about all interfaces.

```
<Sysname> display interface brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) – spoofing

Interface            Link Protocol Primary IP      Description
GE1/0/1              DOWN DOWN     --
Loop0                UP   UP(s)    2.2.2.9
NULL0                UP   UP(s)    --
Vlan1                UP   UP       --
Vlan999              UP   UP       192.168.1.42
```

```
Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Speed: (a) - auto
Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface            Link Speed   Duplex Type PVID Description
GE1/0/2              DOWN auto    A      A    1
GE1/0/3              UP   1G(a)   F(a)   A    1    aaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Display brief information about GigabitEthernet 1/0/1, including the complete description of the interface.

```
<Sysname> display interface gigabitethernet 1/0/1 brief description
Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Speed: (a) - auto
Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface            Link Speed   Duplex Type PVID Description
GE1/0/1              UP   1G(a)   F(a)   A    1    aaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Display information about interfaces in DOWN state and the causes.

```
<Sysname> display interface brief down
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Interface            Link Cause
GE1/0/1              DOWN Not connected
Vlan2                DOWN Not connected

Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Interface            Link Cause
GE1/0/2              DOWN Not connected
```

Table 5 Command output

Field	Description
Brief information on interfaces in route mode:	Brief information about Layer 3 interfaces.
Interface	Interface name.
Link	Physical link state of the interface: • **UP**—The interface is physically up. • **DOWN**—The interface is physically down. • **ADM**—The interface has been shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command. • **Stby**—The interface is a backup interface in standby state. To see the primary interface, use the **display interface-backup state** command.

Field	Description
Protocol	Data link layer protocol state of the interface: • **UP**—The data link layer protocol of the interface is up. • **DOWN**—The data link layer protocol of the interface is down. • **UP(s)**—The data link layer protocol of the interface is up, but the link is an on-demand link or does not exist. The **(s)** attribute represents the spoofing flag. This value is typical of null interfaces and loopback interfaces.
Primary IP	Primary IP address of the interface. This field displays two hyphens (**--**) if the interface does not have an IP address.
Description	Description of the interface.
Brief information of interfaces in bridge mode:	Brief information about Layer 2 interfaces.
Type: A - access; T - trunk; H – hybrid	Link type options for interfaces.
Speed	Speed of the interface, in bps. This field displays the **(a)** flag next to the speed if the speed is automatically negotiated. This field displays **auto** if the interface is configured to autonegotiate its speed but the autonegotiation has not started.
Duplex	Duplex mode of the interface: • **A**—Autonegotiation. The interface is configured to autonegotiate its duplex mode but the autonegotiation has not started. • **F**—Full duplex. • **F(a)**—Autonegotiated full duplex. • **H**—Half duplex. • **H(a)**—Autonegotiated half duplex.
Type	Link type of the interface: • **A**—Access. • **H**—Hybrid. • **T**—Trunk.
PVID	Port VLAN ID.
Cause	Cause for the physical link state of an interface to be **DOWN**: • **Administratively**—The interface has been manually shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command. • **DOWN (Link-Aggregation interface down)**—The interface is a member port of an aggregate interface, and the aggregate interface is down. • **DOWN (Monitor-Link uplink down)**—The monitor link module has detected that the uplink is down. • **MAD ShutDown**—The interface is on an IRF fabric placed by IRF MAD in Recovery state after an IRF split. • **Not connected**—No physical connection exists (possibly because the network cable is disconnected or faulty). • **Storm-Constrain**—The storm control feature has detected that multicast or broadcast traffic exceeded the upper threshold. • **STP DOWN**—The interface has been shut down by the BPDU guard feature. • **Standby**—The interface is a backup interface in standby state.

Related commands

reset counters interface

display interface link-info

Use **display interface link-info** to display the status and packet statistics of interfaces.

Syntax

display interface link-info [**main**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

main: Specifies all interfaces except subinterfaces. If you do not specify this keyword, this command displays status and packet statistics of all interfaces.

Examples

Display status and statistics of all interfaces.

```
<Sysname> display interface link-info
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface                   Link Protocol  InUsage OutUsage   InErrs  OutErrs
GE1/0/1                     UP   UP         10.09%       0%        0        0
NULL0                       UP   UP(s)          0%       0%        0        0
BAGG11                      ADM  DOWN           --       --       --       --
  GE1/0/2                   DOWN DOWN           --       --       --       --
RAGG11                      ADM  DOWN           --       --       --       --
  GE1/0/3                   DOWN DOWN           --       --       --       --

 Overflow: More than 7 digits.
       --: Not supported.
```

Table 6 Command output

Field	Description
Link: ADM - administratively down; Stby - standby	Physical link state of the interface: • **ADM**—The interface has been shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command. • **Stby**—The interface is a backup interface in standby state. To see the primary interface, use the **display interface-backup state** command.
Protocol: (s) – spoofing	The data link layer protocol of the interface is up, but the link is an on-demand link or does not exist. The **(s)** attribute represents the spoofing

Field	Description
	flag. This value is typical of null interfaces, loopback interfaces, and InLoopback interfaces.
Interface	Abbreviated interface name.
Link	Physical link state of the interface: • **UP**—The interface is physically up. • **DOWN**—The interface is physically down. • **ADM**—The interface has been shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command. • **Stby**—The interface is a backup interface in standby state.
Protocol	Data link layer protocol state of the interface: • **UP**—The data link layer protocol of the interface is up. • **DOWN**—The data link layer protocol of the interface is down. • **UP(s)**—The data link layer protocol of the interface is up, but the link is an on-demand link or does not exist. The **(s)** attribute represents the spoofing flag. This value is typical of null interfaces, loopback interfaces, and InLoopback interfaces.
InUsage	Inbound bandwidth usage within the most recent statistics polling interval. It is calculated by this formula: Average inbound speed of the interface within the most recent statistics polling interval/interface bandwidth. When the usage is smaller than 0.01%, 0.01% is displayed. To set the statistics polling interval, use the **flow-interval** command.
OutUsage	Outbound bandwidth usage within the most recent statistics polling interval. It is calculated by this formula: Average outbound speed of the interface within the most recent statistics polling interval/interface bandwidth. When the usage is smaller than 0.01%, 0.01% is displayed. To set the statistics polling interval, use the **flow-interval** command.
InErrs	Number of error packets received.
OutErrs	Number of error packets sent.
Overflow: More than 7 digits.	The data length of a statistical item value is greater than 7 decimal digits.
--: Not supported.	A hyphen (-) indicates that the corresponding statistical item is not supported.

Related commands

flow-interval

display interface main

Use **display interface main** to display operating status and information of all interfaces except subinterfaces.

Syntax

display interface [*interface-type*] [**brief** [**description** | **down**]] **main**

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface-type: Specifies an interface type. If you do not specify this argument, the command displays information about interfaces of all types.

brief: Displays brief interface information. If you do not specify this keyword, the command displays detailed interface information.

description: Displays complete interface descriptions. If you do not specify this keyword, the command displays only the first 27 characters of each interface description.

down: Displays information about interfaces in down state and the causes. If you do not specify this keyword, the command displays information about interfaces in all states.

Examples

Display operating status and information of all interfaces except subinterfaces.

```
<Sysname> display interface main
GigabitEthernet1/0/1
Current state: UP
Line protocol state: UP
Description: Port 5 on the card
Bandwidth: 100000 kbps
Maximum transmission unit: 1500
Allow jumbo frames to pass
Broadcast max-ratio: 100%
Multicast max-ratio: 100%
Unicast max-ratio: 100%
Internet address: 192.168.100.110/24 (Primary)
IP packet frame type: Ethernet II, hardware address: 2222-4444-2226
IPv6 packet frame type: Ethernet II, hardware address: 2222-4444-2226
Media type is twisted pair, loopback not set, promiscuous mode not set
100Mb/s, Full-duplex, link type is autonegotiation
Output flow-control is disabled, input flow-control is disabled
Last link flapping: 1 days 1 hours 22 minutes
Last clearing of counters: Never
Current system time:2021-01-22 16:43:57
Last time when physical state changed to up:2021-01-21 15:21:22
Last time when physical state changed to down:2021-01-21 15:20:28
 Peak input rate: 4040494 bytes/sec, at 2021-01-21 16:34:59
 Peak output rate: 3401055 bytes/sec, at 2021-01-21 16:54:44
 Last 300 second input: 12 packets/sec 1258 bytes/sec 0%
 Last 300 second output: 7 packets/sec 472 bytes/sec 0%
 Input (total):  2856977 packets, 228635952 bytes
          2281642 unicasts, 221205 broadcasts, 354130 multicasts, 0 pauses
 Input (normal):  2856977 packets, 228635952 bytes
          2281642 unicasts, 221205 broadcasts, 354130 multicasts, 0 pauses
 Input:  0 input errors, 0 runts, 0 giants, - throttles
          0 CRC, 0 frame, 0 overruns, 0 aborts
          0 ignored, - parity errors
```

```
 Output (total): 2302787 packets, 128916144 bytes
          2302781 unicasts, 6 broadcasts, 0 multicasts, 0 pauses
 Output (normal): 2302787 packets, 128916144 bytes
          2302781 unicasts, 6 broadcasts, 0 multicasts, 0 pauses
 Output: 0 output errors, 0 underruns, - buffer failures
          0 aborts, 0 deferred, 0 collisions, 0 late collisions
          0 lost carrier, 0 no carrier

GigabitEthernet1/0/2
Current state: DOWN
Line protocol state: DOWN
Description: 123456
Maximum transmission unit: 1500
Allow jumbo frames to pass
Broadcast max-ratio: 100%
Multicast max-ratio: 100%
Unicast max-ratio: 100%
Dampening enabled:
 Penalty: 0 (not suppressed)
 Ceiling: 4525
 Reuse: 800
 Suppress: 3000
 Half-life: 2 seconds
 Max-suppress-time: 5 seconds
 Flap count: 0
Internet protocol processing: Disabled
IP packet frame type: Ethernet II, hardware address: 2222-4444-2227
IPv6 packet frame type: Ethernet II, hardware address: 2222-4444-2227
Media type is twisted pair, loopback not set, promiscuous mode not set
Speed Negotiation, Duplex Negotiation, link type is autonegotiation
Output flow-control is disabled, input flow-control is disabled
Last link flapping: Never
Last clearing of counters: Never
Current system time:2021-01-22 16:43:57
Last time when physical state changed to up:-
Last time when physical state changed to down:2021-01-22 15:42:07
 Peak input rate: 0 bytes/sec, at 00-00-00 00:00:00
 Peak output rate: 0 bytes/sec, at 00-00-00 00:00:00
 Last 30 second input: 0 packets/sec 0 bytes/sec -%
 Last 30 second output: 0 packets/sec 0 bytes/sec -%
 Input (total):  0 packets, 0 bytes
          0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Input (normal):  0 packets, 0 bytes
          0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Input:  0 input errors, 0 runts, 0 giants, - throttles
          0 CRC, 0 frame, 0 overruns, 0 aborts
          0 ignored, - parity errors
 Output (total): 0 packets, 0 bytes
```

```
          0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Output (normal): 0 packets, 0 bytes
          0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Output: 0 output errors, 0 underruns, - buffer failures
          0 aborts, 0 deferred, 0 collisions, 0 late collisions
          0 lost carrier, 0 no carrier
```

Display brief information of all interfaces except subinterfaces.

```
<Sysname> display interface brief main
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) – spoofing

Interface            Link Protocol Primary IP      Description
GE1/0/1              DOWN DOWN     --
Loop0                UP   UP(s)    2.2.2.9
NULL0                UP   UP(s)    --
Vlan1                UP   DOWN     --
Vlan999              UP   UP       192.168.1.42

Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Speed: (a) - auto
Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface            Link Speed   Duplex Type PVID Description
GE1/0/2              DOWN auto    A      A    1
```

Display brief information about all interfaces except subinterfaces, including the complete interface descriptions.

```
<Sysname> display interface  brief description main
Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Speed: (a) - auto
Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface            Link Speed   Duplex Type PVID Description
GE1/0/3              UP   auto    F(a)   A    1    aaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Display information about interfaces (except subinterfaces) in DOWN state and the causes.

```
<Sysname> display interface brief down main
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Interface            Link Cause
GE1/0/1              DOWN Not connected
Vlan2                DOWN Not connected

Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Interface            Link Cause
```

```
GE1/0/2              DOWN Not connected
```

For description on the **display interface main** command output, see Table 4 and Table 5.

display packet-drop

Use **display packet-drop** to display information about packets dropped on an interface.

Syntax

display packet-drop { **interface** [*interface-type* [*interface-number*]] | **summary** }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface-type: Specifies an interface type.

interface-number: Specifies an interface number.

summary: Displays the summary of dropped packets on all interfaces.

Usage guidelines

If you do not specify an interface type, this command displays information about dropped packets on all interfaces on the device.

If you specify an interface type but do not specify an interface number, this command displays information about dropped packets on all interfaces of the specified type.

Examples

Display information about dropped packets on GigabitEthernet 1/0/1.

```
<Sysname> display packet-drop interface gigabitethernet 1/0/1
GigabitEthernet1/0/1:
Packets dropped due to full GBP or insufficient bandwidth: 301
Packets dropped due to Fast Filter Processor (FFP): 261
Packets dropped due to STP non-forwarding state: 0
Packets dropped due to rate-limit: 143
Packets dropped due to broadcast-suppression: 301
Packets dropped due to unicast-suppression: 215
Packets dropped due to multicast-suppression: 241
Packets dropped due to Tx packet aging: 246
```

Display the summary of dropped packets on all interfaces.

```
<Sysname> display packet-drop summary
All interfaces:
Packets dropped due to full GBP or insufficient bandwidth: 301
Packets dropped due to Fast Filter Processor (FFP): 261
Packets dropped due to STP non-forwarding state: 0
```

```
Packets dropped due to rate-limit: 143
Packets dropped due to broadcast-suppression: 301
Packets dropped due to unicast-suppression: 215
Packets dropped due to multicast-suppression: 241
Packets dropped due to Tx packet aging: 246
```

Table 7 Command output

Field	Description
Packets dropped due to full GBP or insufficient bandwidth	Packets that are dropped because the buffer is used up or the bandwidth is insufficient.
Packets dropped due to Fast Filter Processor (FFP)	Packets that are filtered out.
Packets dropped due to STP non-forwarding state	Packets that are dropped because STP is in the non-forwarding state.
Packets dropped due to rate-limit	Packets that are dropped due to the rate limit set on the device.
Packets dropped due to broadcast-suppression	Packets that are dropped due to broadcast suppression.
Packets dropped due to unicast-suppression	Packets that are dropped due to unknown unicast suppression.
Packets dropped due to multicast-suppression	Packets that are dropped due to multicast suppression.
Packets dropped due to Tx packet aging	Outbound packets that are timed out.

duplex

Use **duplex** to set the duplex mode for an Ethernet interface.

Use **undo duplex** to restore the default.

Syntax

duplex { **auto** | **full** | **half** }

undo duplex

Default

Ethernet interfaces operate in autonegotiation mode.

Views

Ethernet interface view

Predefined user roles

network-admin

context-admin

Parameters

auto: Configures the interface to autonegotiate the duplex mode with the peer.

full: Configures the interface to operate in full duplex mode. In this mode, the interface can receive and transmit packets simultaneously.

half: Configures the interface to operate in half duplex mode. In this mode, the interface can only receive or transmit packets at a given time.

Examples

Configure GigabitEthernet 1/0/1 to operate in full duplex mode.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] duplex full
```

flow-control

Use **flow-control** to enable TxRx-mode generic flow control on an Ethernet interface.

Use **undo flow-control** to disable TxRx-mode generic flow control on the Ethernet interface.

Syntax

flow-control

undo flow-control

Default

TxRx-mode generic flow control is disabled on an Ethernet interface.

Views

Ethernet interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

With TxRx-mode generic flow control configured, an interface can both send and receive flow control frames:

- When congested, the interface sends a flow control frame to its peer.
- Upon receiving a flow control frame from the peer, the interface suspends sending packets.

To implement flow control on a link, enable generic flow control at both ends of the link.

Examples

Enable TxRx-mode generic flow control on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] flow-control
```

flow-interval

Use **flow-interval** to set the statistics polling interval.

Use **undo flow-interval** to restore the default.

Syntax

flow-interval *interval*

undo flow-interval

Default

The statistics polling interval is 300 seconds.

Views

System view

Ethernet interface view

The following compatibility matrix shows the support of hardware platforms for views:

Models	Views
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280	System view and Ethernet interface view
NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	Ethernet interface view
NFNX3-HDB680, NFNX3-HDB1080	System view and Ethernet interface view

Predefined user roles

network-admin

context-admin

Parameters

interval: Sets the statistics polling interval in seconds. The interval is in the range of 5 to 300 and must be a multiple of 5.

Usage guidelines

The statistics polling interval configured in system view takes effect on all Ethernet interface.

The statistics polling interval configured in Ethernet interface view takes effect only on the current interface.

For an interface, the configuration in its Ethernet interface view takes priority. The configuration in system view is used when the configuration in Ethernet interface view is the default.

This command is not applicable to interfaces assigned to contexts in shared mode.

Examples

Set the statistics polling interval to 100 seconds on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] flow-interval 100
```

interface

Use **interface** to enter interface view, create a subinterface and enter its view, or enter the view of an existing subinterface.

Syntax

interface *interface-type* { *interface-number* | *interface-number.subnumber* }

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interface-type: Specifies an interface type.

interface-number: Specifies an interface number.

interface-number.subnumber: Specifies a subinterface number. The *interface-number* argument is an interface number. The *subnumber* argument is the number of a subinterface created under the interface. The value range for the *subnumber* argument is 1 to 4094.

Examples

Enter the view of GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1]
```

Create Ethernet subinterface GigabitEthernet 1/0/1.1 and enter its view.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1.1
[Sysname-GigabitEthernet1/0/1.1]
```

jumboframe enable

Use **jumboframe enable** to allow jumbo frames within the specified length to pass through.

Use **undo jumboframe enable** to prevent jumbo frames from passing through.

Use **undo jumboframe enable** *size* to restore the default.

Syntax

jumboframe enable [*size*]

undo jumboframe enable [*size*]

Default

The device allows jumbo frames within a specific length to pass through. The length of jumbo frames that are allowed to pass through varies by device model.

Models	Default
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080	9216
NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	1600

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Predefined user roles

network-admin

context-admin

Parameters

size: Sets the maximum length (in bytes) of Ethernet frames that are allowed to pass through.

The following compatibility matrix shows the value ranges for the maximum jumbo frame size:

Models	Value range
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080	9216
NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	1600

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Allow jumbo frames to pass through GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] jumboframe enable
```

loopback

CAUTION:

After you enable loopback testing on an Ethernet interface, the interface does not forward data traffic.

Use **loopback** to enable loopback testing on an Ethernet interface.

Use **undo loopback** to disable loopback testing on an Ethernet interface.

Syntax

loopback { **external** | **internal** }

undo loopback

Default

Loopback testing is disabled on an Ethernet interface.

Views

Ethernet interface view

Predefined user roles

network-admin

context-admin

Parameters

external: Enables external loopback testing on the Ethernet interface.

internal: Enables internal loopback testing on the Ethernet interface.

Usage guidelines

After you enable loopback testing on an Ethernet interface, the Ethernet interface switches to full duplex mode. After you disable loopback testing, the Ethernet interface restores to its duplex setting.

The **shutdown** and **loopback** commands are mutually exclusive.

Examples

Enable internal loopback testing on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] loopback internal
```

multicast-suppression

Use **multicast-suppression** to enable multicast storm suppression and set the multicast storm suppression threshold.

Use **undo multicast-suppression** to disable multicast storm suppression.

Syntax

multicast-suppression { *ratio* | **pps** *max-pps* | **kbps** *max-kbps* }

undo multicast-suppression

Default

Ethernet interfaces do not suppress multicast traffic.

Views

Ethernet interface view

Predefined user roles

network-admin

context-admin

Parameters

ratio: Sets the multicast suppression threshold as a percentage of the interface bandwidth. The value range for this argument (in percentage) is 0 to 100. A smaller value means that less multicast traffic is allowed to pass through.

pps *max-pps*: Specifies the maximum number of multicast packets that the interface can forward per second. The value range for the *max-pps* argument (in pps) is 0 to 1.4881 × the interface bandwidth.

kbps *max-kbps*: Specifies the maximum number of kilobits of multicast traffic that the Ethernet interface can forward per second. The value range for this argument (in kbps) is 0 to the interface bandwidth.

Usage guidelines

The multicast storm suppression feature limits the size of multicast traffic to a threshold on an interface. When the multicast traffic on the interface exceeds this threshold, the system drops packets until the traffic drops below this threshold.

Both the **storm-constrain** command and the **multicast-suppression** command can suppress multicast storms on a port. The **multicast-suppression** command uses the chip to physically suppress multicast traffic. It has less influence on the device performance than the **storm-constrain** command, which uses software to suppress multicast traffic.

For the traffic suppression result to be determined, do not configure both the **storm-constrain multicast** command and the **multicast-suppression** command on an interface.

The configured suppression threshold value in pps or kbps might be converted into a multiple of a step supported by the chip. As a result, the effective suppression threshold might be different from the configured one. To determine the suppression threshold that takes effect, see the prompts on the device.

Examples

Set the multicast storm suppression threshold to 10000 kbps on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] multicast-suppression kbps 10000
```

Related commands

broadcast-suppression

unicast-suppression

port link-mode

Use **port link-mode** to change the link mode of an Ethernet interface.

Use **undo port link-mode** to restore the default.

Syntax

port link-mode { **bridge** | **route** }

undo port link-mode

Default

An Ethernet interface operates in Layer 3 mode.

Views

Ethernet interface view

Predefined user roles

network-admin

context-admin

Parameters

bridge: Specifies the Layer 2 mode.

route: Specifies the Layer 3 mode.

Usage guidelines

CAUTION:

Changing the link mode of an Ethernet interface also restores all commands (except **shutdown** and **combo enable**) on the Ethernet interface to their defaults in the new link mode.

Interfaces operate differently depending on the hardware structure of interface cards. For a device:

- Some Ethernet interfaces can operate only as Layer 2 Ethernet interfaces (in bridge mode).
- Some Ethernet interfaces can operate only as Layer 3 Ethernet interfaces (in route mode).
- Some Ethernet interfaces can operate either as Layer 2 or Layer 3 Ethernet interfaces. You can use this command to set the link mode to bridge or route for these Ethernet interfaces.

Examples

Configure GigabitEthernet 1/0/1 to operate in Layer 2 mode.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-mode bridge
```

reset counters interface

Use **reset counters interface** to clear the interface statistics.

Syntax

reset counters interface [*interface-type* [*interface-number* | *interface-number.subnumber*]]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

interface-type: Specifies an interface type.

interface-number: Specifies an interface number.

interface-number.subnumber: Specifies a subinterface number. The *interface-number* argument is an interface number. The *subnumber* argument is the number of a subinterface created under the interface. The value range for the *subnumber* argument is 1 to 4094.

Usage guidelines

Use this command to clear history statistics if you want to collect traffic statistics for a specific time period.

If you do not specify an interface type, this command clears statistics for all interfaces except VA interfaces. For more information about VA interfaces, see PPPoE in *Layer 2—WAN Access Configuration Guide*.

If you specify an interface type but do not specify an interface number, this command clears statistics for all interfaces of the specified type.

Examples

Clear the statistics for GigabitEthernet 1/0/1.

```
<Sysname> reset counters interface gigabitethernet 1/0/1
```

Related commands

display counters interface

display counters rate interface

display interface

reset ethernet statistics

Use **reset ethernet statistics** to clear the Ethernet module statistics.

Syntax

reset ethernet statistics [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

slot *slot-number:* Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears statistics for all IRF member devices.

Examples

Clear the Ethernet module statistics for the specified slot.

```
<Sysname> reset ethernet statistics slot 1
```

Related commands

display ethernet statistics

reset packet-drop interface

Use **reset packet-drop interface** to clear the dropped packet statistics for an interface.

Syntax

reset packet-drop interface [*interface-type* [*interface-number*]]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

interface-type: Specify an interface type.

interface-number: Specify an interface number.

Usage guidelines

If you do not specify an interface type, this command clears dropped packet statistics for all interfaces on the device.

If you specify an interface type but do not specify an interface number, the command clears dropped packet statistics for all interfaces of the specified type.

Examples

Clear dropped packet statistics for GigabitEthernet 1/0/1.

```
<Sysname> reset packet-drop interface gigabitethernet 1/0/1
```

Clear dropped packet statistics for all interfaces.

```
<Sysname> reset packet-drop interface
```

Related commands

display packet-drop

shutdown

Use **shutdown** to shut down an Ethernet interface or subinterface.

Use **undo shutdown** to bring up an Ethernet interface or subinterface.

Syntax

shutdown

undo shutdown

Default

An Ethernet interface or subinterface is up.

Views

Ethernet interface view

Ethernet subinterface view

Predefined user roles

network-admin

context-admin

Usage guidelines

CAUTION:

Executing the **shutdown** command on an interface will disconnect the link of the interface and interrupt communication. Use this command with caution.

Some interface configurations might require an interface restart before taking effect.

The **shutdown** and **loopback** commands are mutually exclusive.

Examples

Shut down and then bring up GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] shutdown
[Sysname-GigabitEthernet1/0/1] undo shutdown
```

Shut down and then bring up GigabitEthernet 1/0/1.1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1.1
[Sysname-GigabitEthernet1/0/1.1] shutdown
[Sysname-GigabitEthernet1/0/1.1] undo shutdown
```

speed

Use **speed** to set the speed of an Ethernet interface.

Use **undo speed** to restore the default.

Syntax

speed { **10** | **100** | **1000** | **auto** }

undo speed

Default

An Ethernet interface autonegotiates its speed.

Views

Ethernet interface view

Predefined user roles

network-admin

context-admin

Parameters

10: Sets the interface speed to 10 Mbps.

100: Sets the interface speed to 100 Mbps.

1000: Sets the interface speed to 1000 Mbps.

auto: Enables the interface to negotiate a speed with its peer.

Usage guidelines

For an Ethernet copper port, use the **speed** command to set its speed to match the speed of the peer interface. Support of copper ports for keywords of this command varies by copper port type. For more information, use the **speed ?** command in interface view. If the system does not prompt that operation failed when you configure a speed for a copper port, the copper port supports this speed. Otherwise, the copper port does not support this speed.

For a fiber port, use the **speed** command to set its speed to match the rate of a transceiver module. Support of fiber ports for keywords of this command varies by fiber port type. For more information, use the **speed ?** command in interface view. If the system does not prompt that operation failed when you configure a speed for a fiber port, the fiber port supports this speed. Otherwise, the fiber port does not support this speed.

Additionally, you must select a speed for a fiber port according to the transceiver module installed to ensure that the transceiver module can be used properly. If the transceiver module installed in a fiber port does not support the speed for the fiber port, the transceiver module cannot be used. For example, the transceiver module cannot be used if the following conditions exist:

- The transceiver module installed in an SFP+ fiber port is an SFP GE transceiver module and the **speed 10000** command is executed on the fiber port.
- The transceiver module installed in an SFP+ fiber port is an SFP 10-GE transceiver module and the **speed 1000** command is executed on the fiber port.

Examples

Configure GigabitEthernet 1/0/1 to autonegotiate the speed.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] speed auto
```

sub-interface rate-statistic

Use **sub-interface rate-statistic** to enable rate statistics collection for the subinterfaces of an Ethernet interface.

Use **undo sub-interface rate-statistic** to disable rate statistics collection for the subinterfaces of an Ethernet interface.

Syntax

sub-interface rate-statistic

undo sub-interface rate-statistic

Default

The system does not collect rate statistics for the subinterfaces of an Ethernet interface.

Views

Ethernet interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command is resource intensive. When you use this command, make sure you fully understand its impact on system performance.

Examples

Enable rate statistics collection for the subinterfaces of GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] sub-interface rate-statistic
This configuration may make a negative effect on the performance. Are you sure to continue?
[Y/N]:y
```

unicast-suppression

Use **unicast-suppression** to enable unknown unicast storm suppression and set the unknown unicast storm suppression threshold.

Use **undo unicast-suppression** to disable unknown unicast storm suppression.

Syntax

unicast-suppression { *ratio* | **pps** *max-pps* | **kbps** *max-kbps* }

undo unicast-suppression

Default

Ethernet interfaces do not suppress unknown unicast traffic.

Views

Ethernet interface view

Predefined user roles

network-admin

context-admin

Parameters

ratio: Sets the unknown unicast suppression threshold as a percentage of the interface bandwidth. The value range for this argument (in percentage) is 0 to 100. A smaller value means that less unknown unicast traffic is allowed to pass through.

pps *max-pps*: Specifies the maximum number of unknown unicast packets that the interface can forward per second. The value range for the *max-pps* argument (in pps) is 0 to 1.4881 × the interface bandwidth.

kbps *max-kbps*: Specifies the maximum number of kilobits of unknown unicast traffic that the Ethernet interface can forward per second. The value range for this argument (in kbps) is 0 to the interface bandwidth.

Usage guidelines

The unknown unicast storm suppression feature limits the size of unknown unicast traffic to a threshold on an interface. When the unknown unicast traffic on the interface exceeds this threshold, the system discards packets until the unknown unicast traffic drops below this threshold.

The configured suppression threshold value in pps or kbps might be converted into a multiple of a step supported by the chip. As a result, the effective suppression threshold might be different from the configured one. To determine the suppression threshold that takes effect, see the prompts on the device.

Examples

Set the unknown unicast storm suppression threshold to 10000 kbps on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] unicast-suppression kbps 10000
```

Related commands

broadcast-suppression

- **multicast-suppression**

Layer 2 Ethernet interface commands

display storm-constrain

Use **display storm-constrain** to display storm control settings and statistics.

Syntax

display storm-constrain [**broadcast** | **multicast**] [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

broadcast: Displays broadcast storm control settings and statistics.

multicast: Displays multicast storm control settings and statistics.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify this option, the command displays storm control settings and statistics for all storm control-enabled interfaces.

Usage guidelines

If you do not specify the **broadcast** or **multicast** keyword, this command displays all storm control settings on all storm control-enabled interfaces.

Examples

Display the storm control settings on all storm control-enabled ports.

```
<Sysname> display storm-constrain
Abbreviation: BC - broadcast; MC - multicast; UC - unicast;
              FW - forwarding
Flow Statistic Interval: 5 (in seconds)
Port          Type Lower     Upper     Unit  Mode     Status   Trap Log StateChg
------------------------------------------------------------------------------
GE1/0/1       MC   100       200       kbps  shutdown shutdown off  on  10
```

Table 8 Command output

Field	Description
Flow Statistic Interval	Traffic polling interval (in seconds) of the storm control module.
Port	Abbreviated interface name.
Type	Type of traffic subjected to storm control: • **BC**—Broadcast packets. • **MC**—Multicast packets. • **UC**—Unicast packets. This field is not supported in the current software version.
Lower	Lower storm control threshold.
Upper	Upper storm control threshold.
Unit	Storm control threshold unit, in pps, kbps, or percentage.
Mode	Action (block or shutdown) taken on the interface when the upper threshold is reached. N/A indicates that no action is configured.
Status	Packet forwarding status: • **FW**—The port is forwarding traffic correctly. • **shutdown**—The port has been shut down. • **block**—The port drops the type of traffic.
Trap	Status of the storm control threshold event trap switch: • **on**—The port sends threshold event traps. • **off**—The port does not send threshold event traps.
Log	Status of the storm control threshold event log switch: • **on**—The port sends threshold event log messages. • **off**—The port does not send threshold event log messages.
StateChg	Number of forwarding state changes of the interface. When the **StateChg** field reaches 65535, it resets automatically.

mdix-mode

IMPORTANT:
Fiber ports do not support this command.

Use **mdix-mode** to configure the Medium Dependent Interface Cross-Over (MDIX) mode of an Ethernet interface.

Use **undo mdix-mode** to restore the default.

Syntax

mdix-mode { **automdix** | **mdi**| **mdix** }

undo mdix-mode

Default

Ethernet interfaces operate in **automdix** mode.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

context-admin

Parameters

automdix: Specifies that the interface negotiates pin roles with its peer.

mdi: Specifies that pins 1 and 2 are transmit pins and pins 3 and 6 are receive pins.

mdix: Specifies that pins 1 and 2 are receive pins and pins 3 and 6 are transmit pins.

Examples

Configure GigabitEthernet 1/0/1 to operate in **automdix** mode.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mdix-mode automdix
```

storm-constrain

Use **storm-constrain** to enable storm control and set thresholds for broadcast, multicast, or unknown unicast packets on an Ethernet interface.

Use **undo storm-constrain** to disable storm control for broadcast, multicast, unknown unicast, or all types of traffic.

Syntax

storm-constrain { **broadcast** | **multicast** } **pps** *upperlimit lowerlimit*

undo storm-constrain { **all** | **broadcast** | **multicast** }

Default

Traffic storm control is disabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

context-admin

Parameters

all: Disables storm control for all types of traffic: multicast and broadcast.

broadcast: Enables or disables broadcast storm control.

multicast: Enables or disables multicast storm control.

pps: Sets storm control thresholds in pps.

upperlimit: Sets the upper threshold. If you specify the **pps** keyword, the value range for the *upperlimit* argument is 0 to 1.4881 × the interface bandwidth.

lowerlimit: Sets the lower threshold. If you specify the **pps** keyword, the value range for the *lowerlimit* argument is 0 to 1.4881 × the interface bandwidth.

Usage guidelines

After you configure storm control for a type of traffic, the device collects the statistics for the type of traffic at the interval configured by using the **storm-constrain interval** command. When the type of traffic exceeds its upper threshold, the interface takes an action configured by using the **storm-constrain control** command.

The **storm-constrain**, **broadcast-suppression**, **multicast-suppression**, and **unicast-suppression** commands can suppress storms on an interface. The **broadcast-suppression**, **multicast-suppression**, and **unicast-suppression** commands use the chip to physically suppress traffic. They have less influence on the device performance than the **storm-constrain** command, which uses software to suppress traffic.

For the traffic suppression result to be determined, do not configure both storm control and storm suppression for the same type of traffic.

When configuring this command, make sure *upperlimit* is greater than *lowerlimit*.

Examples

Enable broadcast storm control on GigabitEthernet 1/0/1 and set the upper and lower thresholds to 200 pps and 150 pps, respectively.

<Sysname> system-view

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] storm-constrain broadcast pps 200 150
```

Related commands

storm-constrain control

storm-constrain interval

storm-constrain control

Use **storm-constrain control** to set the action to take on an Ethernet interface when a type of traffic (multicast or broadcast) exceeds the upper storm control threshold.

Use **undo storm-constrain control** to restore the default.

Syntax

storm-constrain control { **block** | **shutdown** }

undo storm-constrain control

Default

No action is taken on an Ethernet interface when a type of traffic exceeds the upper storm control threshold.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

context-admin

Parameters

block: Blocks the type of traffic exceeding the upper threshold and forwards other types of traffic. Even though the interface does not forward the blocked type of traffic, it still counts the traffic. When the blocked type of traffic drops below the lower threshold, the port begins to forward the traffic.

shutdown: Goes down automatically and stops forwarding any traffic. When the type of traffic exceeding the upper threshold drops below the lower threshold, the interface does not forward traffic. To bring up the interface, use the **undo shutdown** command or disable storm control on the interface.

Examples

Configure GigabitEthernet 1/0/1 to block a specific type of traffic when the type of traffic exceeds the upper storm control threshold.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] storm-constrain control block
```

Related commands

storm-constrain

storm-constrain control

storm-constrain enable log

Use **storm-constrain enable log** to enable an Ethernet interface to output log messages when it detects storm control threshold events.

Use **undo storm-constrain enable log** to disable an Ethernet interface from outputting log messages for storm control threshold events.

Syntax

storm-constrain enable log

undo storm-constrain enable log

Default

An Ethernet interface outputs log messages when monitored traffic exceeds the upper threshold or drops below the lower threshold from a value above the upper threshold.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

context-admin

Examples

Enable GigabitEthernet 1/0/1 to output log messages when it detects storm control threshold events.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] storm-constrain enable log
```

storm-constrain enable trap

Use **storm-constrain enable trap** to enable an Ethernet interface to send storm control threshold event traps.

Use **undo storm-constrain enable trap** to disable an Ethernet interface from sending storm control threshold event traps.

Syntax

storm-constrain enable trap

undo storm-constrain enable trap

Default

An interface sends out storm control threshold event traps when monitored traffic exceeds the upper threshold or drops below the lower threshold from a value above the upper threshold.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

context-admin

Examples

Enable GigabitEthernet 1/0/1 to send traps when it detects storm control threshold events.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] storm-constrain enable trap
```

storm-constrain interval

Use **storm-constrain interval** to set the traffic polling interval of the storm control module.

Use **undo storm-constrain interval** to restore the default.

Syntax

storm-constrain interval *interval*

undo storm-constrain interval

Default

The storm control module polls traffic statistics every 10 seconds.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interval: Sets the traffic polling interval of the storm control module. The value range is 1 to 300 seconds. To ensure network stability, as a best practice, do not use a traffic polling interval shorter than 10 seconds.

Usage guidelines

The traffic polling interval set by using the **storm-constrain interval** command is specific to storm control. To set the statistics polling interval of an interface, use the **flow-interval** command.

Examples

Set the traffic statistics polling interval of the storm control module to 60 seconds.

```
<Sysname> system-view
[Sysname] storm-constrain interval 60
```

Related commands

storm-constrain

storm-constrain control

Layer 3 Ethernet interface or subinterface commands

mac-address

Use **mac-address** to set the MAC address of an Ethernet interface.

Use **undo mac-address** to restore the default.

Syntax

mac-address *mac-address*

undo mac-address

Default

The MAC address of a Layer 3 Ethernet interface varies by device model. The MAC address of a Layer 3 Ethernet subinterface is that of the main interface.

Views

Layer 3 Ethernet interface view

Layer 3 Ethernet subinterface view

Predefined user roles

network-admin

context-admin

Parameters

mac-address: Specifies a MAC address in the format of H-H-H.

Examples

Set the MAC address of GigabitEthernet 1/0/1 to 0001-0001-0001.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-address 1-1-1
```

mac-address-filter enable

Use **mac-address-filter enable** to enable destination MAC filtering.

Use **undo mac-address-filter enable** to disable destination MAC filtering.

Syntax

mac-address-filter enable

undo mac-address-filter enable

Views

System view

Default

Destination MAC filtering is enabled.

Predefined user roles

network-admin

Usage guidelines

This feature takes effect only on Layer 3 Ethernet interfaces/subinterfaces, Layer 3 aggregate interfaces, and Layer 3 Reth interfaces. These interfaces are referred to as interfaces in this command.

Typically, use the default settings.

With this feature enabled, when an interface receives a packet, the interface operates as follows:

- If the destination MAC address of the packet is the MAC address of the interface, the interface accepts and processes the packet.
- If the destination MAC address of the packet is not the MAC address of the interface, the interface drops the packet.

With this feature disabled, an interface accepts and processes a packet, without checking the destination MAC address of the packet.

Examples

Enable destination MAC filtering.

```
<Sysname> system-view
[Sysname] mac-address-filter enable
```

mtu

Use **mtu** to set the MTU for an Ethernet interface or subinterface.

Use **undo mtu** to restore the default.

Syntax

mtu *size*

undo mtu

Default

The MTU of an Ethernet interface or subinterface is 1500 bytes.

Views

Layer 3 Ethernet interface view

Layer 3 Ethernet subinterface view

Predefined user roles

network-admin

context-admin

Parameters

size: Sets the MTU in bytes. The value range for this argument is 46 to 1560.

Usage guidelines

A smaller MTU size results in more fragments. When you set the MTU for an interface, consider QoS queue lengths, for example, consider that the default FIFO queue length is 75. To prevent a too small MTU from causing packet drops in QoS queuing, you can perform one of the following configurations:

- Tune the MTU with the **mtu** command.
- Tune QoS queue lengths with the **qos fifo queue-length** command.

For more information about the **qos fifo queue-length** command, see *ACL and QoS Command Reference*.

Examples

Set the MTU to 1430 bytes for GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mtu 1430
```

Set the MTU to 1430 bytes for GigabitEthernet 1/0/1.1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1.1
[Sysname-GigabitEthernet1/0/1.1] mtu 1430
```

traffic-statistic enable

Use **traffic-statistic enable** to enable subinterface rate statistics collection for a Layer 3 Ethernet subinterface.

Use **undo traffic-statistic enable** to disable subinterface rate statistics collection for a Layer 3 Ethernet subinterface.

Syntax

traffic-statistic enable

undo traffic-statistic enable

Default

Subinterface rate statistics collection is disabled for a Layer 3 Ethernet subinterface.

Views

Layer 3 Ethernet subinterface view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command is resource intensive. The system becomes busy and the CPU usage increases when you enable this feature on a large number of Ethernet subinterfaces or set a shorter interval by using the **flow-interval** command.

You can use the **display interface** or **display counters** command to display the subinterface rate statistics.

Examples

Enable subinterface rate statistics collection for GigabitEthernet 1/0/1.1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1.1
[Sysname-GigabitEthernet1/0/1.1] traffic-statistic enable
```

Related commands

display counters

display interface

flow-interval

Contents

Loopback, null, and inloopback interface commands

bandwidth

Use **bandwidth** to set the expected bandwidth for an interface.

Use **undo bandwidth** to restore the default.

Syntax

bandwidth *bandwidth-value*

undo bandwidth

Default

The expected bandwidth of a loopback interface is 0 kbps.

Views

Loopback interface view

Predefined user roles

network-admin

context-admin

Parameters

bandwidth-value: Specifies the expected bandwidth in the range of 1 to 400000000 kbps.

Usage guidelines

The expected bandwidth is an informational parameter used only by higher-layer protocols for calculation. You cannot adjust the actual bandwidth of an interface by using this command.

Examples

Set the expected bandwidth of Loopback 0 to 1000 kbps.

```
<Sysname> system-view
[Sysname] interface loopback 0
[Sysname-LoopBack0] bandwidth 1000
```

default

Use **default** to restore the default settings for an interface.

Syntax

default

Views

Loopback interface view

Null interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

CAUTION:

The **default** command might interrupt ongoing network services. Make sure you are fully aware of the impact of this command before using it on a live network.

This command might fail to restore the default settings for some commands for reasons such as command dependencies and system restrictions. Use the **display this** command in interface view to identify these commands, and then use their **undo** forms or follow the command reference to restore their default settings. If your restoration attempt still fails, follow the error message instructions to resolve the problem.

Examples

Restore the default settings for Loopback 0.

```
<Sysname> system-view
[Sysname] interface loopback 0
[Sysname-LoopBack0] default
```

description

Use **description** to configure the description of an interface.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

The interface description uses the *interface name* **Interface** format, for example, LoopBack0 **Interface**.

Views

Loopback interface view

Null interface view

Predefined user roles

network-admin

context-admin

Parameters

text: Specifies the description, a case-sensitive string of 1 to 255 characters.

Usage guidelines

Configure a description for an interface for easy identification and management purposes.

You can use the **display interface** command to view the configured description.

Examples

Configure the description of Loopback 0 as **for RouterID**.

```
<Sysname> system-view
[Sysname] interface loopback 0
[Sysname-LoopBack0] description for RouterID
```

display interface inloopback

Use **display interface inloopback** to display information about the inloopback interface.

Syntax

display interface [**inloopback** [**0**]] [**brief** [**description** | **down**]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

inloopback [**0**]: Specifies an inloopback interface by its number. If you do not specify the **inloopback** keyword, the command displays information about all interfaces except VA interfaces. For more information about VA interfaces, see PPP in *Layer 2—WAN Access Configuration Guide*.

brief: Displays brief interface information. If you do not specify this keyword, the command displays detailed interface information.

description: Displays complete interface descriptions. If you do not specify this keyword, the command displays only the first 27 characters of interface descriptions. The description of an inloopback interface is always **InLoopBack0 Interface** and cannot be configured.

down: Displays information about interfaces in down state and the causes. If you do not specify this keyword, the command displays information about interfaces in all states.

Usage guidelines

The device has only one inloopback interface Inloopback 0. If you specify the **inloopback** keyword, the command displays information about the interface Inloopback 0 regardless of whether you specify the **0** keyword.

Examples

Display detailed information about Inloopback 0.

```
<Sysname> display interface inloopback
InLoopBack0
Current state: UP
Line protocol state: UP(spoofing)
Description: InLoopBack0 Interface
Maximum transmission unit: 1536
Physical: InLoopBack
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

Table 1 Command output

Field	Description
Current state	Physical link state of the interface, which is always **UP**, meaning that the inloopback interface can receive and transmit packets.
Line protocol state	Data link layer state of the interface, which is always **UP(spoofing)**. **UP(spoofing)** represents that the data link layer protocol of the interface is up, but the link is an on-demand link or does not exist. This attribute is typical of null interfaces and loopback interfaces.
Description	Description of the interface, which is always **InLoopBack0 Interface** and cannot be configured.
Maximum transmission unit	MTU of the interface.
Physical: InLoopBack	The physical type of the interface is inloopback.
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec	Average input rate during the last 300 seconds (displayed when the interface supports traffic statistics collection): • **bytes/sec**—Average number of bytes received per second. • **bits/sec**—Average number of bits received per second. • **packets/sec**—Average number of packets received per second.
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec	Average output rate over the last 300 seconds (displayed when the interface supports traffic statistics collection): • **bytes/sec**—Average number of bytes sent per second. • **bits/sec**—Average number of bits sent per second. • **packets/sec**—Average number of packets sent per second.
Input: 0 packets, 0 bytes, 0 drops	Total number and size (in bytes) of incoming packets of the interface and the number of dropped packets (displayed when the interface supports traffic statistics collection).
Output: 0 packets, 0 bytes, 0 drops	Total number and size (in bytes) of outgoing packets of the interface and the number of dropped packets (displayed when the interface supports traffic statistics collection).

Display brief information about Inloopback 0.

```
<Sysname> display interface inloopback 0 brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP         Description
InLoop0              UP   UP(s)    --
```

Table 2 Command output

Field	Description
Link	Physical link state of the interface, which is always **UP**, meaning that the link is physically up.
Protocol	Data link layer protocol state of the interface, which is always **UP(s)**. **UP(s)** represents that the data link layer protocol of the interface is up, but the link is an on-demand link or does not exist. The **(s)** attribute represents the spoofing flag. This value is typical of null interfaces and loopback interfaces.

Field	Description
Primary IP	IP address of the interface. Because inloopback interfaces do not support CLI configuration, this field does not display a value.
Description	Description of the interface. Because inloopback interfaces do not support CLI configuration, this field does not display a value.

display interface loopback

Use **display interface loopback** to display information about the specified or all existing loopback interfaces.

Syntax

display interface [**loopback** [*interface-number*]] [**brief** [**description** | **down**]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

loopback [*interface-number*]: Specifies a loopback interface by its number, which can be the number of any existing loopback interface. If you do not specify the **loopback** keyword, the command displays information about all interfaces except VA interfaces. If you specify the **loopback** keyword but do not specify the *interface-number* argument, the command displays information about all existing loopback interfaces on the device. For more information about VA interfaces, see PPP in *Layer 2—WAN Access Configuration Guide*.

brief: Displays brief interface information. If you do not specify this keyword, the command displays detailed interface information.

description: Displays complete interface descriptions. If you do not specify this keyword, the command displays only the first 27 characters of interface descriptions.

down: Displays information about interfaces in down state and the causes. If you do not specify this keyword, the command displays information about interfaces in all states.

Usage guidelines

This command is supported only after a loopback interface is created.

Examples

Display detailed information about Loopback 0.

```
<Sysname> display interface loopback 0
LoopBack0
Current state: UP
Line protocol state: UP(spoofing)
```

```
Description: LoopBack0 Interface
Bandwidth: 1000 kbps
Maximum transmission unit: 1536
Internet protocol processing: Disabled
Physical: Loopback
Last clearing of counters:  Never
Last 300 seconds input rate:  0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate:  0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

Table 3 Command output

Field	Description
Current state	Physical link state of the interface: • **UP**—The loopback interface can receive and transmit packets. • **Administratively DOWN**—The interface has been shut down by using the **shutdown** command.
Line protocol state	Data link layer state of the interface. **UP (spoofing)** means that the data link layer protocol of the interface is up, but the link is an on-demand link or does not exist. This attribute is typical of null interfaces and loopback interfaces.
Description	Description of the interface.
Bandwidth	Expected bandwidth of the interface. This field is not displayed when the value is 0.
Maximum transmission unit	MTU of the interface.
Internet protocol processing: Disabled	The interface is not assigned an IP address and cannot process IP packets.
Internet address: *ip-address*/*mask-length* (*Type*)	IP address of the interface and type of the address in parentheses. Possible IP address types include: • **Primary**—Manually configured primary IP address. • **Sub**—Manually configured secondary IP address. If the interface has both primary and secondary IP addresses, the primary IP address is displayed. If the interface has only secondary IP addresses, the lowest secondary IP address is displayed. • **DHCP-Allocated**—DHCP allocated IP address. For more information, see DHCP client configuration in *Layer 3—IP Services Configuration Guide*. • **BOOTP-Allocated**—BOOTP allocated IP address. For more information, see BOOTP client configuration in *Layer 3—IP Services Configuration Guide*. • **PPP-Negotiated**—IP address assigned by a PPP server during PPP negotiation. For more information, see PPP configuration in *Layer 2—WAN Access Configuration Guide*. • **Unnumbered**—IP address borrowed from another interface. • **Cellular-Allocated**—IP address allocated through the modem manufacturer's proprietary protocol. For more information, see mobile communication modem management in *Layer 2—WAN Access Configuration Guide*. • **MAD**—IP address assigned to an IRF member device for MAD on the interface. For more information, see IRF configuration in *Virtual Technologies Configuration Guide*.

Field	Description
Physical: Loopback	The physical type of the interface is loopback.
baudrate	Baud rate in Kbps.
Last clearing of counters	Time when statistics on the logical interface were last cleared by using the **reset counters interface** command. If the statistics of the interface have never been cleared by using the **reset counters interface** command since the device started, this field displays **Never**.
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec	Average input rate during the last 300 seconds (displayed when the interface supports traffic statistics collection): • **bytes/sec**—Average number of bytes received per second. • **bits/sec**—Average number of bits received per second. • **packets/sec**—Average number of packets received per second.
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec	Average output rate over the last 300 seconds (displayed when the interface supports traffic statistics collection): • **bytes/sec**—Average number of bytes sent per second. • **bits/sec**—Average number of bits sent per second. • **packets/sec**—Average number of packets sent per second.
Input: 0 packets, 0 bytes, 0 drops	Total number and size (in bytes) of incoming packets of the interface and the number of dropped packets (displayed when the interface supports traffic statistics collection).
Output: 0 packets, 0 bytes, 0 drops	Total number and size (in bytes) of outgoing packets of the interface and the number of dropped packets (displayed when the interface supports traffic statistics collection).

Display brief information about all loopback interfaces.

```
<Sysname> display interface loopback brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP      Description
Loop0                UP   UP(s)    --              forLAN1
```

Display information about all loopback interfaces in down state and the causes.

```
<Sysname> display interface loopback brief down
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Interface            Link Cause
Loop0                ADM  Administratively
```

Table 4 Command output

Field	Description
Link	Physical link state of the interface: • **UP**—The interface is physically up. • **DOWN**—The interface is physically down. • **ADM**—The interface has been shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command. • **Stby**—The interface is a backup interface in standby state.

Field	Description
Protocol	Data link layer protocol state of the interface, which is always **UP(s)**. **UP(s)** represents that the data link layer protocol of the interface is up, but the link is an on-demand link or does not exist. The **(s)** attribute represents the spoofing flag. This value is typical of null interfaces and loopback interfaces.
Primary IP	Primary IP address of the interface.
Description	Description of the interface.
Cause	Cause for the physical link state of the interface to be **DOWN**. **Administratively** represents that the interface has been manually shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command.

Related commands

interface loopback

reset counters interface loopback

display interface null

Use **display interface null** to display information about the null interface.

Syntax

display interface [**null** [**0**]] [**brief** [**description** | **down**]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

null [**0**]: Specifies a null interface by its number. If you do not specify the **null** keyword, the command displays information about all interfaces except VA interfaces. For more information about VA interfaces, see PPP in *Layer 2—WAN Access Configuration Guide*.

brief: Displays brief interface information. If you do not specify this keyword, the command displays detailed interface information.

description: Displays complete interface descriptions. If you do not specify this keyword, the command displays only the first 27 characters of interface descriptions.

down: Displays information about interfaces in down state and the causes. If you do not specify this keyword, the command displays information about interfaces in all states.

Usage guidelines

The device has only one null interface Null 0. If you specify the **null** keyword, the command displays information about the interface Null 0 regardless of whether you specify the **0** keyword.

Examples

Display detailed information about Null 0.

```
<Sysname> display interface null 0
NULL0
Current state: UP
Line protocol state: UP(spoofing)
Description: NULL0 Interface
Bandwidth: 1000000 kbps
Maximum transmission unit: 1500
Internet protocol processing: Disabled
Physical: NULL DEV, baudrate: 1000000 kbps
Last clearing of counters: Never
Last 300 seconds input rate:  0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate:  0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

Display brief information about Null 0.

```
<Sysname> display interface null 0 brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP         Description
NULL0                UP   UP(s)    --
```

For the command output, see Table 3 and Table 4.

Related commands

`interface null`

`reset counters interface null`

interface loopback

Use **`interface loopback`** to create a loopback interface and enter its view, or enter the view of an existing loopback interface.

Use **`undo interface loopback`** to remove a loopback interface.

Syntax

`interface loopback` *`interface-number`*

`undo interface loopback` *`interface-number`*

Default

No loopback interfaces exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interface-number: Specifies a loopback interface by its number. The value range for this argument is 0 to 1023.

Usage guidelines

The physical layer state and link layer protocols of a loopback interface are always up unless the loopback interface is manually shut down. You can use a loopback interface to achieve the following purposes:

- Prevent the connection from being affected by the physical state of the interface.
- Improve the reliability of the connection.

For example, you can configure a loopback interface as the source interface for establishing an FTP connection, or use the loopback interface address as the Router ID in BGP.

Examples

Create Loopback 0.

```
<Sysname> system-view
[Sysname] interface loopback 0
[Sysname-LoopBack0]
```

interface null

Use **interface null** to enter null interface view.

Syntax

interface null 0

Default

A device has only one null interface (Null 0), which cannot be created or deleted.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

0: Specifies Null 0. The null interface number is always 0.

Examples

Enter Null 0 interface view.

```
<Sysname> system-view
[Sysname] interface null 0
[Sysname-NULL0]
```

reset counters interface loopback

Use **reset counters interface loopback** to clear the statistics on the specified or all loopback interfaces.

Syntax

reset counters interface [**loopback** [*interface-number*]]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

loopback [*interface-number*]: Specifies a loopback interface by its number. If you do not specify the **loopback** keyword, the command clears the statistics on all interfaces except VA interfaces. If you specify the **loopback** keyword but do not specify the *interface-number* argument, the command clears the statistics on all loopback interfaces.

Usage guidelines

To determine whether a loopback interface works correctly within a period by collecting the traffic statistics within that period, first use the **reset counters interface** [**loopback** [*interface-number*]] command to clear the statistics. Then have the interface automatically collect the statistics.

This command is available only if a minimum of one loopback interface has been created.

Examples

Clear the statistics on Loopback 0.

```
<Sysname> reset counters interface loopback 0
```

Related commands

display interface loopback

reset counters interface null

Use **reset counters interface null** to clear the statistics on the null interface.

Syntax

reset counters interface [**null** [**0**]]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

null [**0**]: Specifies a null interface by its number. If you do not specify the **null** keyword, the command clears the statistics on all interfaces except VA interfaces.

Usage guidelines

To determine whether the null interface works correctly within a period by collecting the traffic statistics within that period, first use the **reset counters interface** [**null** [**0**]] command to clear the statistics. Then have the interface automatically collect the statistics.

Examples

Clear the statistics on Null 0.

```
<Sysname> reset counters interface null 0
```

Related commands

display interface null

shutdown

Use **shutdown** to shut down a loopback interface.

Use **undo shutdown** to bring up a loopback interface.

Syntax

shutdown

undo shutdown

Default

A loopback interface is up.

Views

Loopback interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

CAUTION:

Use the **shutdown** command with caution, because the command disconnects the connection of the interface and disables the interface from communicating.

Examples

Shut down Loopback 0.

```
<Sysname> system-view
[Sysname] interface loopback 0
[Sysname-LoopBack0] shutdown
```

NSFOCUS Firewall Series

NF Layer 2—LAN Switching Command Reference

NSFOCUS Technologies, Inc.

Document version: 6W600-20230221

Preface

This command reference describes the commands for configuring LAN switching features, including MAC address table, Ethernet link aggregation, spanning tree, VLANs, VLAN termination, LLDP, and Layer 2 forwarding.

This preface includes the following topics about the documentation:

- Audience.
- Conventions.

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators.

Conventions

The following information describes the conventions used in the documentation.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select a minimum of one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
CAUTION:	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Contents

MAC address table commands

display mac-address

Use **display mac-address** to display MAC address entries.

Syntax

display mac-address [*mac-address* [**vlan** *vlan-id*] | [[**dynamic** | **static**] [**interface** *interface-type interface-number*] | **blackhole**] [**vlan** *vlan-id*] [**count**]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

mac-address: Specifies a MAC address in the format of H-H-H. When entering a MAC address, you can omit the leading zeros in each H section. For example, enter f-e2-1 for 000f-00e2-0001.

vlan *vlan-id*: Specifies a VLAN by its ID in the range of 1 to 4094.

dynamic: Displays dynamic MAC address entries.

static: Displays static MAC address entries.

interface *interface-type interface-number*: Specifies an interface by its type and number.

blackhole: Displays blackhole MAC address entries.

count: Displays only the number of MAC address entries that match all entry attributes you specify in the command. Detailed information about MAC address entries is not displayed. For example, you can use the **display mac-address vlan 20 dynamic count** command to display the number of dynamic entries for VLAN 20. If you do not specify an entry attribute, the command displays the number of entries in the MAC address table. If you do not specify this keyword, the command displays detailed information about the specified MAC address entries.

Usage guidelines

Use this command to display static, dynamic, or blackhole MAC address entries. A MAC address entry includes a destination MAC address, an outgoing interface, and a VLAN ID.

If you do not specify any parameters, the command displays all MAC address entries.

This command displays dynamic MAC address entries for an aggregate interface only when the aggregate interface has a minimum of one Selected member port.

Examples

Display MAC address entries for VLAN 100.

```
<Sysname> display mac-address vlan 100
MAC Address      VLAN ID    State           Port/Nickname           Aging
```

```
0033-0033-0033   100        Blackhole        N/A                  N
0000-0000-0002   100        Static           GE1/0/3              N
00e0-fc00-5829   100        Learned          GE1/0/4              Y
```

Display the number of MAC address entries.

```
<Sysname> display mac-address count
1 mac address(es) found.
```

Table 1 Command output

Field	Description
VLAN ID	ID of the VLAN to which the outgoing interface of the MAC address entry belongs.
State	MAC address entry state: • **Static**—Static MAC address entry. • **Learned**—Dynamic MAC address entry. Dynamic entries can be learned or manually configured. • **Blackhole**—Blackhole MAC address entry. • **Drop aging**—MAC address entry that can age out. Packets from this MAC address are dropped. • **Drop no-aging**—MAC address entry that cannot age out. Packets from this MAC address are dropped. • **Vlan-interface**—MAC address entry of a VLAN interface.
Port/Nickname	When the field displays an interface name, the field indicates the outgoing interface for packets that are destined for the MAC address. This field displays **N/A** for a blackhole MAC address entry. The **Nickname** field is not supported in the current software version.
Aging	Whether the entry can age out: • **Y**—The entry can age out. • **N**—The entry never ages out.
mac address(es) found	Number of matching MAC address entries.

Related commands

mac-address

mac-address timer

display mac-address aging-time

Use **display mac-address aging-time** to display the aging timer for dynamic MAC address entries.

Syntax

display mac-address aging-time

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display the aging timer for dynamic MAC address entries.

```
<Sysname> display mac-address aging-time
MAC address aging time: 300s.
```

Related commands

mac-address timer

display mac-address mac-learning

Use **display mac-address mac-learning** to display the global MAC address learning status and the MAC learning status of the specified interface or all interfaces.

Syntax

display mac-address mac-learning [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, the command displays the global MAC address learning status and the MAC address learning status of all interfaces.

Examples

Display the global MAC address learning status and the MAC learning status of all interfaces.

```
<Sysname> display mac-address mac-learning
Global MAC address learning status: Enabled.

Port                         Learning Status
GE1/0/1                      Enabled
GE1/0/2                      Enabled
```

Table 2 Command output

Field	Description
Global MAC address learning status	Global MAC address learning status: • Enabled. • Disabled.
Learning Status	MAC address learning status of an interface: • Enabled. • Disabled.

Related commands

mac-address mac-learning enable

mac-address (interface view)

Use **mac-address** to add or modify a MAC address entry on an interface.

Use **undo mac-address** to delete a MAC address entry on an interface.

Syntax

mac-address { **dynamic** | **static** } *mac-address* **vlan** *vlan-id*

undo mac-address { **dynamic** | **static** } *mac-address* **vlan** *vlan-id*

Default

An interface is not configured with MAC address entries.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

context-admin

Parameters

dynamic: Specifies dynamic MAC address entries.

static: Specifies static MAC address entries.

mac-address: Specifies a MAC address in the format of H-H-H, excluding multicast, all-zero, and all-F MAC addresses. When entering a MAC address, you can omit the leading zeros in each H section. For example, enter f-e2-1 for 000f-00e2-0001.

vlan *vlan-id*: Specifies an existing VLAN to which the specified interface belongs. The value range for the *vlan-id* argument is 1 to 4094.

Usage guidelines

Typically, the device automatically builds the MAC address table by learning the source MAC addresses of incoming frames on each interface. However, you can manually configure static MAC address entries. For a MAC address, a manually configured static entry takes precedence over a dynamically learned entry. To improve the security for the user device connected to an interface, manually configure a static entry to bind the user device to the interface. Then, the frames destined for the user device (for example, Host A) are always sent out of the interface. Other hosts using the forged MAC address of Host A cannot obtain the frames destined for Host A.

The MAC address entry configuration cannot survive a reboot unless you save it. The dynamic MAC address entries, however, are lost upon reboot whether or not you save the configuration.

Examples

Add a static entry for MAC address 000f-e201-0101 on GigabitEthernet 1/0/1 that belongs to VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-address static 000f-e201-0101 vlan 2
```

Add a static entry for MAC address 000f-e201-0101 on Bridge-Aggregation 1 that belongs to VLAN 1.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] mac-address static 000f-e201-0102 vlan 1
```

Related commands

display mac-address

mac-address (system view)

mac-address (system view)

Use **mac-address** to add or modify a MAC address entry.

Use **undo mac-address** to delete one or all MAC address entries.

Syntax

mac-address { **dynamic** | **static** } *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*

mac-address blackhole *mac-address* **vlan** *vlan-id*

undo mac-address [[**dynamic** | **static**] *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*]

undo mac-address [**blackhole** | **dynamic** | **static**] [*mac-address*] **vlan** *vlan-id*

undo mac-address [**dynamic** | **static**] **interface** *interface-type interface-number*

Default

The system is not configured with MAC address entries.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

dynamic: Specifies dynamic MAC address entries.

static: Specifies static MAC address entries.

blackhole: Specifies blackhole MAC address entries. Packets whose source or destination MAC addresses match blackhole MAC address entries are dropped.

mac-address: Specifies a MAC address in the format of H-H-H, excluding multicast, all-zero, and all-F MAC addresses. When entering a MAC address, you can omit the leading zeros in each H section. For example, enter f-e2-1 for 000f-00e2-0001.

vlan *vlan-id*: Specifies an existing VLAN to which the interface belongs. The value range for the *vlan-id* argument is 1 to 4094.

interface *interface-type interface-number*: Specifies an outgoing interface by its type and number.

Usage guidelines

You can use this command to configure the following types of MAC address entries:

- Dynamic entries.

Dynamic entries include manually configured dynamic entries and automatically learned dynamic entries.

- Static entries.

  For a MAC address, a manually configured static entry takes precedence over a dynamic entry. To improve the security for the user device connected to an interface, manually configure a static entry to bind the user device to the interface. Then, the frames destined for the user device (for example, Host A) are always sent out of the interface. Other hosts using the forged MAC address of Host A cannot obtain the frames destined for Host A.

- Blackhole entries.

  To drop frames with the specified source MAC addresses or destination MAC addresses, you can configure blackhole entries.

A static or blackhole entry can overwrite a dynamic entry, but not vice versa.

If you execute the **undo mac-address** command without specifying any parameters, this command deletes all unicast MAC address entries and static multicast MAC address entries.

You can delete all the MAC address entries (including unicast and static multicast MAC address entries) from the specified VLAN. You can also delete only one type (dynamic, static, or blackhole) of MAC address entries. You can single out an interface and delete the unicast MAC address entries on it, but not the static multicast MAC address entries.

The MAC address entry configuration cannot survive a reboot unless you save it. The dynamic MAC address entries, however, are lost upon reboot whether or not you save the configuration.

Examples

Add a static entry for MAC address 000f-e201-0101. Then, all frames that are destined for this MAC address are sent out of GigabitEthernet 1/0/1, which belongs to VLAN 2.

```
<Sysname> system-view
[Sysname] mac-address static 000f-e201-0101 interface gigabitethernet 1/0/1 vlan 2
```

Related commands

display mac-address

mac-address (interface view)

mac-address mac-learning enable

Use **mac-address mac-learning enable** to enable MAC address learning globally, on an interface, or on a VLAN.

Use **undo mac-address mac-learning enable** to disable MAC address learning globally or on an interface.

Syntax

mac-address mac-learning enable

undo mac-address mac-learning enable

Default

MAC address learning is enabled.

Views

System view

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

VLAN view

Predefined user roles

network-admin

context-admin

Usage guidelines

To prevent the MAC address table from becoming saturated, you can disable MAC address learning.

For example, a number of packets with different source MAC addresses reaching a device can affect the MAC address table update. To avoid such attacks, you can disable MAC address learning by following these guidelines:

- You can disable MAC address learning on a per-interface basis. If you disable MAC address learning globally, MAC address learning is disabled for all interfaces. The device then stops learning MAC addresses and cannot dynamically update the MAC address table.
- Because disabling MAC address learning can result in broadcast storms, enable broadcast storm suppression after you disable MAC address learning on an interface. For more information about broadcast storm suppression, see *Interface Configuration Guide*.
- With MAC address learning enabled globally, you can disable MAC address learning for an interface.
- After MAC address learning is disabled, existing dynamic MAC address entries can age out.

Examples

Disable MAC address learning globally.

```
<Sysname> system-view
[Sysname] undo mac-address mac-learning enable
```

Disable MAC address learning on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo mac-address mac-learning enable
```

Related commands

display mac-address mac-learning

mac-address mac-learning priority

Use **mac-address mac-learning priority** to assign MAC learning priority to an interface.

Use **undo mac-address mac-learning priority** to restore the default.

Syntax

mac-address mac-learning priority { **high** | **low** }

undo mac-address mac-learning priority

Default

Low MAC address learning priority is used.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

context-admin

Parameters

high: Assigns high MAC learning priority.

low: Assigns low MAC learning priority.

Usage guidelines

The MAC address learning priority values can be high and low. An interface with high MAC address learning priority can learn any MAC address. An interface with low MAC address learning priority can learn only the MAC addresses that have not been learned by high-priority interfaces.

The MAC learning priority mechanism can help defend your network against MAC address spoofing attacks. To prevent the downlink interface from learning the MAC address of an upper layer device (for example, the gateway), you can perform the following tasks:

- Assign high MAC learning priority to an uplink interface.
- Assign low MAC learning priority to a downlink interface.

Examples

Assign high MAC learning priority to GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-address mac-learning priority high
```

Assign high MAC learning priority to Bridge-Aggregation 1.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] mac-address mac-learning priority high
```

mac-address max-mac-count

Use **mac-address max-mac-count** to set the MAC learning limit on an interface.

Use **undo mac-address max-mac-count** to restore the default.

Syntax

mac-address max-mac-count *count*

undo mac-address max-mac-count

Default

The maximum number of MAC addresses that an interface can learn is restricted by hardware capability of the device.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

context-admin

Parameters

count: Specifies the maximum number of MAC addresses that can be learned on an interface. When the argument is set to 0, the interface is not allowed to learn MAC addresses.

The following compatibility matrixes show the value ranges for this argument:

Models	Value range
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080	0 to 4096
NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	0 to 1024

Usage guidelines

This command helps limit the MAC address table size. When the number of MAC address entries learned by an interface reaches the limit, the interface stops learning MAC address entries.

Examples

Configure GigabitEthernet 1/0/1 to learn a maximum of 200 MAC address entries.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-address max-mac-count 200
```

Related commands

mac-address

mac-address max-mac-count enable-forwarding

mac-address max-mac-count enable-forwarding

Use **mac-address max-mac-count enable-forwarding** to enable the device to forward unknown frames received on an interface after the MAC learning limit on the interface is reached. Unknown frames refer to frames whose source MAC addresses are not in the MAC address table.

Use **undo mac-address max-mac-count enable-forwarding** to disable the device from forwarding unknown frames received on an interface after the MAC learning limit on the interface is reached.

Syntax

mac-address max-mac-count enable-forwarding

undo mac-address max-mac-count enable-forwarding

Default

When the MAC learning limit on an interface is reached, the device can forward unknown frames received on the interface.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

context-admin

Examples

Configure GigabitEthernet 1/0/1 to learn a maximum of 200 MAC address entries.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-address max-mac-count 200
```

Disable the device from forwarding unknown frames received on GigabitEthernet 1/0/1 after the MAC learning limit on GigabitEthernet 1/0/1 is reached.

```
[Sysname-GigabitEthernet1/0/1] undo mac-address max-mac-count enable-forwarding
```

Related commands

mac-address

mac-address max-mac-count

mac-address timer

Use **mac-address timer** to set the aging timer for dynamic MAC address entries.

Use **undo mac-address timer** to restore the default.

Syntax

mac-address timer { **aging** *seconds* | **no-aging** }

undo mac-address timer

Default

The aging timer is 300 seconds for dynamic MAC address entries.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

aging *seconds*: Specifies an aging timer for dynamic MAC address entries, in seconds. The value range for the *seconds* argument is 10 to 1400.

no-aging: Configures dynamic MAC address entries not to age.

Usage guidelines

To set the aging timer appropriately, follow these guidelines:

- A long aging interval causes the MAC address table to retain outdated entries and fail to accommodate the most recent network changes.
- A short aging interval results in removal of valid entries. Then, unnecessary broadcast packets appear and affect device performance.

Examples

Set the aging time to 500 seconds for dynamic MAC address entries.

```
<Sysname> system-view
[Sysname] mac-address timer aging 500
```

Related commands

display mac-address aging-time

snmp-agent trap enable mac-address

Use **snmp-agent trap enable mac-address** to enable SNMP notifications for the MAC address table.

Use **undo snmp-agent trap enable mac-address** to disable SNMP notifications for the MAC address table.

Syntax

snmp-agent trap enable mac-address

undo snmp-agent trap enable mac-address

Default

SNMP notifications are enabled for the MAC address table.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

To report critical MAC address move events to an NMS, enable SNMP notifications for the MAC address table. For MAC address move event notifications to be sent correctly, you must also configure SNMP on the device.

When SNMP notifications are disabled for the MAC address table, the device sends the generated logs to the information center. To display the logs, configure the log destination and output rule configuration in the information center.

For information about SNMP and information center configuration, see the network management and monitoring configuration guide for the device.

The MAC address table supports only SNMP notifications about MAC address moves. When you enable or disable SNMP notifications about MAC address moves, you enable or disable all types of SNMP notifications for the MAC address table.

Examples

Disable SNMP notifications for the MAC address table.

```
<Sysname> system-view
[Sysname] undo snmp-agent trap enable mac-address
```

Contents

Ethernet link aggregation commands

bandwidth

Use **bandwidth** to set the expected bandwidth for an interface.

Use **undo bandwidth** to restore the default.

Syntax

bandwidth *bandwidth-value*

undo bandwidth

Default

The expected bandwidth (in kbps) is the interface baud rate divided by 1000.

Views

Layer 2 aggregate interface view

Layer 3 aggregate interface view

Layer 3 aggregate subinterface view

Predefined user roles

network-admin

context-admin

Parameters

bandwidth-value: Specifies the expected bandwidth in the range of 1 to 400000000 kbps.

Usage guidelines

The expected bandwidth is an informational parameter used only by higher-layer protocols for calculation. You cannot adjust the actual bandwidth of an interface by using this command.

Examples

Set the expected bandwidth to 10000 kbps for Layer 2 aggregate interface Bridge-Aggregation 1.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] bandwidth 10000
```

Set the expected bandwidth to 10000 kbps for Layer 3 aggregate interface Route-Aggregation 1.

```
<Sysname> system-view
[Sysname] interface route-aggregation 1
[Sysname-Route-Aggregation1] bandwidth 10000
```

default

Use **default** to restore the default settings for an aggregate interface.

Syntax

default

Views

Layer 2 aggregate interface view

Layer 3 aggregate interface view

Layer 3 aggregate subinterface view

Predefined user roles

network-admin

context-admin

Usage guidelines

CAUTION:

The **default** command might interrupt ongoing network services. Make sure you are fully aware of the impacts of this command when you execute it on a live network.

This command might fail to restore the default settings for some commands for reasons such as command dependencies and system restrictions. Use the **display this** command in interface view to identify these commands, and then use their **undo** forms or follow the command reference to restore their default settings. If your restoration attempt still fails, follow the error message instructions to resolve the problem.

Examples

Restore the default settings for Layer 2 aggregate interface 1.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] default
```

Restore the default settings for Layer 3 aggregate interface 1.

```
<Sysname> system-view
[Sysname] interface route-aggregation 1
[Sysname-Route-Aggregation1] default
```

description

Use **description** to configure the description of an interface.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

The description of an interface is *interface-name* **Interface**. For example, the default description of Bridge-Aggregation 1 is **Bridge-Aggregation1 Interface**.

Views

Layer 2 aggregate interface view

Layer 3 aggregate interface view

Layer 3 aggregate subinterface view

Predefined user roles

network-admin

context-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 255 characters.

Examples

Configure the description as **connect to the lab** for Layer 2 aggregate interface Bridge-Aggregation 1.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] description connect to the lab
```

Configure the description as **connect to the lab** for Layer 3 aggregate interface Route-Aggregation 1.

```
<Sysname> system-view
[Sysname] interface route-aggregation 1
[Sysname-Route-Aggregation1] description connect to the lab
```

display interface

Use **display interface** to display aggregate interface information.

Syntax

display interface [{ **bridge-aggregation** | **route-aggregation** } [*interface-number*]] [**brief** [**description** | **down**]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

bridge-aggregation: Specifies Layer 2 aggregate interfaces.

route-aggregation: Specifies Layer 3 aggregate interfaces.

interface-number: Specifies an existing aggregate interface number.

brief: Displays brief interface information. If you do not specify this keyword, the command displays detailed interface information.

description: Displays complete interface descriptions. If you do not specify this keyword, the command displays only the first 27 characters of each interface description.

down: Displays information about interfaces in down state and the causes for the down state. If you do not specify this keyword, the command displays information about interfaces in all states.

Usage guidelines

If you do not specify an aggregate interface type, this command displays information about all interfaces except VA interfaces. For more information about VA interfaces, see PPP configuration in *Layer 2—WAN Access Configuration Guide*.

If you specify an aggregate interface type but do not specify an interface number, this command displays information about all aggregate interfaces of the specified type.

Examples

Display detailed information about Layer 2 aggregate interface Bridge-Aggregation 1.

```
<Sysname> display interface bridge-aggregation 1
Bridge-Aggregation1
Current state: UP
IP packet frame type: Ethernet II, hardware address: 000f-e207-f2e0
Description: Bridge-Aggregation1 Interface
Bandwidth: 1000 kbps
2Gbps-speed mode, full-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
PVID: 1
Port link-type: Access
 Tagged VLANs:   None
 UnTagged VLANs: 1
Last clearing of counters: Never
  Last 300 seconds input:  6900 packets/sec 885160 bytes/sec    0%
  Last 300 seconds output:  3150 packets/sec 404430 bytes/sec    0%
  Input (total):  5364747 packets, 686688416 bytes
         2682273 unicasts, 1341137 broadcasts, 1341337 multicasts, 0 pauses
  Input (normal):  5364747 packets, 686688416 bytes
         2682273 unicasts, 1341137 broadcasts, 1341337 multicasts, 0 pauses
  Input:  0 input errors, 0 runts, 0 giants, 0 throttles
         0 CRC, 0 frame, 0 overruns, - aborts
         - ignored, - parity errors
  Output (total): 1042508 packets, 133441832 bytes
         1042306 unicasts, 0 broadcasts, 202 multicasts, - pauses
  Output (normal): 1042508 packets, 133441832 bytes
         1042306 unicasts, 0 broadcasts, 202 multicasts, 0 pauses
  Output: 0 output errors, - underruns, - buffer failures
         0 aborts, 0 deferred, 0 collisions, 0 late collisions
         - lost carrier, - no carrier
```

Display detailed information about Layer 3 aggregate interface Route-Aggregation 1.

```
<Sysname> display interface route-aggregation 1
Route-Aggregation1
Current state: UP
Line protocol state: UP
Description: Route-Aggregation1 Interface
Bandwidth: 1000 kbps
Maximum transmission unit: 1500
Internet protocol processing: Disabled
IP packet frame type: Ethernet II, hardware address: 0000-0000-0000
IPv6 packet frame type: Ethernet II, hardware address: 0000-0000-0000
Link speed type is autonegotiation, link duplex type is autonegotiation
Last clearing of counters: Never
 Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
 Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
 Input: 0 packets, 0 bytes, 0 drops
 Output: 0 packets, 0 bytes, 0 drops
```

Display brief information about Layer 2 aggregate interface Bridge-Aggregation 1.

```
<Sysname> display interface bridge-aggregation 1 brief
Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Speed: (a) – auto
Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface            Link Speed   Duplex Type PVID Description
BAGG1                UP   auto    A      A    1
```

Display brief information about Layer 3 aggregate interface Route-Aggregation 1.

```
<Sysname> display interface route-aggregation 1 brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP         Description
RAGG1                UP   UP       --
```

Table 1 Command output

Field	Description
Bridge-Aggregation1	Layer 2 aggregate interface name.
Route-Aggregation1	Layer 3 aggregate interface name.
Current state	Physical link state of the interface: • **Administratively DOWN**—The interface has been shut down by using the **shutdown** command. • **DOWN**—The interface is administratively up, but its physical state is down (possibly because no physical link exists or the link has failed). • **UP**—The interface is both administratively and physically up.
IP packet frame type	IPv4 packet framing format.
Description	Description of the interface.
Bandwidth	Expected bandwidth of the interface. This field is not displayed when the bandwidth is 0 kbps.
Port priority	Port priority of the interface.
Unknown-speed mode, unknown-duplex mode	The interface speed and duplex mode are unknown.
Port link-type	Port link type: • Access. • Trunk. • Hybrid.
Tagged VLANs	VLAN whose packets are sent out of this interface with a tag.
Untagged VLANs	VLAN whose packets are sent out of this interface without a tag.
Last clearing of counters	Time when the **reset counters interface** command was last used to clear the interface statistics. This field displays **Never** if the **reset counters interface** command has never been used on the interface since device startup.
Last 300 seconds input/output rate	Average input or output rate over the last 300 seconds.

Field	Description
Input/Output (total)	Statistics of all packets received or sent on the interface.
Input/Output (normal)	Statistics of all normal packets received or sent on the interface.
Line protocol state	Data link layer state of the interface: • **UP**. • **DOWN**.
Maximum transmission unit	MTU of the interface.
Internet protocol processing: Disabled	The interface is not assigned an IP address and cannot process IP packets.
Internet address: *ip-address*/*mask-length* (*Type*)	IP address of the interface and type of the address in parentheses. Possible IP address types include: • **Primary**—Manually configured primary IP address. • **Sub**—Manually configured secondary IP address. If the interface has both primary and secondary IP addresses, the primary IP address is displayed. If the interface has only secondary IP addresses, the lowest secondary IP address is displayed. • **DHCP-Allocated**—DHCP allocated IP address. For more information, see DHCP client configuration in *Layer 3—IP Services Configuration Guide*. • **BOOTP-Allocated**—BOOTP allocated IP address. For more information, see BOOTP client configuration in *Layer 3—IP Services Configuration Guide*. • **PPP-Negotiated**—IP address assigned by a PPP server during PPP negotiation. For more information, see PPP configuration in *Layer 2—WAN Access Configuration Guide*. • **Unnumbered**—IP address borrowed from another interface. • **MAD**—IP address assigned to an IRF member device for MAD on the interface. For more information, see IRF configuration in *Virtual Technologies Configuration Guide*.
Brief information on interfaces in route mode	Brief information about Layer 3 interfaces.
Brief information on interfaces in bridge mode	Brief information about Layer 2 interfaces.
Interface	Abbreviated interface name.
Link	Physical link state of the interface: • **UP**—The interface is physically up. • **DOWN**—The interface is physically down. • **ADM**—The interface has been shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command. • **Stby**—The interface is a backup interface in standby state.
Speed	Speed of the interface, in bps. This field displays the **(a)** flag next to the speed if the speed is automatically negotiated. This field displays **auto** if the interface is configured to autonegotiate its speed but the autonegotiation has not started.
Duplex	Duplex mode of the interface: • **A**—Autonegotiation. The interface is configured to autonegotiate its duplex mode but the autonegotiation has

Field	Description
	not started. • **F**—Full duplex. • **F(a)**—Autonegotiated full duplex. • **H**—Half duplex. • **H(a)**—Autonegotiated half duplex.
Type	Link type of the interface: • **A**—Access. • **H**—Hybrid. • **T**—Trunk.
Protocol	Data link layer protocol state of the interface: • **UP**—The data link layer protocol of the interface is up. • **DOWN**—The data link layer protocol of the interface is down. • **UP(s)**—The data link layer protocol of the interface is up, but the link is an on-demand link or does not exist. The **(s)** attribute represents the spoofing flag. This value is typical of null interfaces and loopback interfaces.
Primary IP	Primary IP address of the interface. This field displays two hyphens (**--**) if the interface does not have an IP address.
Cause	Cause for the physical link state of an interface to be **DOWN**.

display lacp system-id

Use **display lacp system-id** to display the local system ID.

Syntax

display lacp system-id

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Usage guidelines

You can use the **lacp system-priority** command to change the LACP priority of the local system. The LACP priority value is specified in decimal format in the **lacp system-priority** command. However, it is displayed in hexadecimal format in the output from the **display lacp system-id** command.

Examples

Display the local system ID.

```
<Sysname> display lacp system-id
Actor System ID: 0x8000, 0000-fc00-6504
```

Table 2 Command output

Field	Description
Actor System ID: 0x8000, 0000-fc00-6504	Local system ID, which contains the system LACP priority (0x8000 in this sample output) and the system MAC address (0000-FC00-6504 in this sample output).

Related commands

lacp system-priority

display link-aggregation load-sharing mode

Use **display link-aggregation load-sharing mode** to display global or group-specific link-aggregation load sharing modes.

Syntax

display link-aggregation load-sharing mode [**interface** [{ **bridge-aggregation** | **route-aggregation** } *interface-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

bridge-aggregation: Specifies Layer 2 aggregate interfaces.

route-aggregation: Specifies Layer 3 aggregate interfaces.

interface-number: Specifies an existing aggregate interface number.

Usage guidelines

If you do not specify the **interface** keyword, the command displays the global link-aggregation load sharing modes.

If you specify the **interface** keyword, but do not specify an interface, the command displays all group-specific load sharing modes.

The **bridge-aggregation** or **route-aggregation** keyword is available only when aggregate interfaces of the corresponding type exist on the device.

Examples

Display the global link-aggregation load sharing mode. This example displays the default settings.

```
<Sysname> display link-aggregation load-sharing mode
MAC-in-MAC traffic load-sharing mode:
Default
Link-aggregation load-sharing algorithm:
Default
Link-aggregation load-sharing seed:
Default
```

```
Link-aggregation load-sharing mode:
Layer 2 traffic: packet type-based sharing
Layer 3 traffic: packet type-based sharing
```

Display the global link-aggregation load sharing mode. This example displays user-configured settings.

```
<Sysname> display link-aggregation load-sharing mode
MAC-in-MAC traffic load-sharing mode:
Inner
Link-aggregation load-sharing algorithm:
4
Link-aggregation load-sharing seed:
0x3ff
Link-aggregation load-sharing mode:
destination-mac address, source-mac address
```

Display the link-aggregation load sharing mode of Layer 2 aggregation group 1. This example displays the default settings.

```
<Sysname> display link-aggregation load-sharing mode interface bridge-aggregation 1
Bridge-Aggregation1 load-sharing mode:
Layer 2 traffic: packet type-based sharing
Layer 3 traffic: packet type-based sharing
```

Display the link-aggregation load sharing mode of Layer 2 aggregation group 1. This example displays user-configured settings.

```
<Sysname> display link-aggregation load-sharing mode interface bridge-aggregation 1
Bridge-Aggregation1 load-sharing mode:
destination-mac address, source-mac address
```

Display the link-aggregation load sharing mode of Layer 3 aggregation group 1. This example displays the default settings.

```
<Sysname> display link-aggregation load-sharing mode interface route-aggregation 1
Route-Aggregation1 load-sharing mode:
Layer 2 traffic: packet type-based sharing
Layer 3 traffic: packet type-based sharing
```

Display the link-aggregation load sharing mode of Layer 3 aggregation group 1. This example displays user-configured settings.

```
<Sysname> display link-aggregation load-sharing mode interface route-aggregation 1
Route-Aggregation1 load-sharing mode:
destination-mac address, source-mac address
```

Table 3 Command output

Field	Description
Link-aggregation load-sharing mode	Global link-aggregation load sharing mode. By default, this field displays the link-aggregation load sharing modes for Layer 2 and Layer 3 traffic. If you have configured the global link-aggregation load sharing mode, this field displays the configured mode.
Bridge-Aggregation1 load-sharing mode	Link-aggregation load sharing mode of Layer 2 aggregation group 1. By default, this field displays the global link-aggregation load sharing modes.

Field	Description
	If you have configured a link-aggregation load sharing mode for this aggregation group, this field displays the configured mode.
Route-Aggregation1 load-sharing mode	Link-aggregation load sharing mode of Layer 3 aggregation group 1. By default, this field displays the global link-aggregation load sharing modes. If you have configured a link-aggregation load sharing mode for this aggregation group, this field displays the configured mode.
Layer 2 traffic: destination-mac address, source-mac address	Default link-aggregation load sharing mode for Layer 2 traffic. In this sample output, Layer 2 traffic is load shared based on source and destination MAC addresses.
Layer 2 traffic: packet type-based sharing	Default link-aggregation load sharing mode for Layer 2 traffic. In this sample output, the system automatically selects a load sharing mode for Layer 2 traffic.
Layer 3 traffic: destination-ip address, source-ip address	Default link-aggregation load sharing mode for Layer 3 traffic. In this sample output, Layer 3 traffic is load shared based on source and destination IP addresses.
Layer 3 traffic: packet type-based sharing	Default link-aggregation load sharing mode for Layer 3 traffic. In this sample output, the system automatically selects a load sharing mode for Layer 3 traffic.
destination-mac address, source-mac address	User-configured link-aggregation load sharing mode. In this sample output, traffic is load shared based on source and destination MAC addresses.

display link-aggregation load-sharing path

Use **display link-aggregation load-sharing path** to display forwarding information about the specified traffic flow.

Syntax

display link-aggregation load-sharing path interface { **bridge-aggregation** | **route-aggregation** } *interface-number* **ingress-port** *interface-type interface-number* [**route**] { { **destination-ip** *ip-address* | **destination-ipv6** *ipv6-address* } | { **source-ip** *ip-address* | **source-ipv6** *ipv6-address* } | **destination-mac** *mac-address* | **destination-port** *port-id* | **ethernet-type** *type-number* | **ip-protocol** *protocol-id* | **source-mac** *mac-address* | **source-port** *port-id* | **vlan** *vlan-id* } * **slot** *slot-number*

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

bridge-aggregation: Specifies Layer 2 aggregate interfaces.

route-aggregation: Specifies Layer 3 aggregate interfaces.

interface-number: Specifies an existing aggregate interface by its number.

ingress-port *interface-type interface-number*: Specifies an ingress port by its type and number. The ingress port must be a physical port.

route: Displays forwarding information about Layer 3 traffic. If you do not specify this keyword, the command displays forwarding information about Layer 2 traffic.

destination-ip *ip-address*: Specifies a destination IPv4 address.

destination-ipv6 *ipv6-address*: Specifies a destination IPv6 address.

source-ip *ip-address*: Specifies a source IPv4 address.

source-ipv6 *ipv6-address*: Specifies a source IPv6 address.

destination-mac *mac-address*: Specifies a destination MAC address in H-H-H format.

destination-port *port-id*: Specifies a destination port number in the range of 1 to 65535.

ethernet-type *type-number*: Specifies an Ethernet type code in the range of 1 to 65535.

ip-protocol *protocol-id*: Specifies an IP protocol by its ID in the range of 0 to 255.

source-mac *mac-address*: Specifies a source MAC address in H-H-H format.

source-port *port-id*: Specifies a source port number in the range of 1 to 65535.

vlan *vlan-id*: Specifies a VLAN by its ID in the range of 1 to 4094.

slot *slot-number*: Specifies an IRF member device by its member ID.

Usage guidelines

A parameter specified in the command might not be used for selecting the egress port. The **Load sharing parameters** field displays the parameters that are used in egress port selection. For example, you can specify both the **destination-mac** *mac-address* and **destination-ip** *ip-address* options. If only the destination MAC address is used for selecting the egress port, the **Load sharing parameters** field does not display the **destination-ip** parameter.

If a parameter required for selecting the egress port is not specified, the default value of the parameter is used. If the parameter does not have any default values, the parameter is set to 0.

This command takes effect only on per-flow load sharing and automatic load sharing. As a best practice, do not use this command for per-packet load sharing.

Examples

Display forwarding information about the specified traffic flow to be sent out of Layer 2 aggregate interface Bridge-Aggregation 1.

```
<Sysname> display link-aggregation load-sharing path interface bridge-aggregation 1
ingress-port gigabitethernet 1/0/1 destination-mac 0000-fc00-0001 source-mac
0000-fc00-0002 source-ip 10.100.0.2 destination-ip 10.100.0.1 slot 1
Load sharing mode: destination-mac, source-mac, source-ip, destination-ip
Unspecified parameters are set to 0.
Load-sharing parameters:
  Ingress port：GigabitEthernet1/0/1
  Destination MAC: 0000-fc00-0001
  Source MAC: 0000-fc00-0002
  Destination IP: 10.100.0.1
  Source IP: 10.100.0.2
Egress port: GigabitEthernet1/0/3
```

Table 4 Command output

Field	Description
Load sharing mode:	Load sharing mode set for the aggregation group: • **destination-mac**—Traffic is load shared based on destination MAC addresses. • **source-mac**—Traffic is load shared based on source MAC addresses. • **destination-ip**—Traffic is load shared based on destination IP addresses. • **source-ip**—Traffic is load shared based on source IP addresses. • **destination-port**—Traffic is load shared based on destination ports. • **source-port**—Traffic is load shared based on source ports. • **ip-protocol**—Traffic is load shared based on IP protocol types. • **ingress-port**—Traffic is load shared based on ingress ports. • **vlan**—Traffic is load shared based on VLAN IDs. • **packet type-based sharing**—Traffic is load shared automatically based on packet types. If no load sharing mode is set, this field also displays **packet type-based sharing**.
Load sharing parameters	Parameters that are used in egress port selection.
Egress port	Egress port of the specified traffic flow. If no egress port is found, this field displays **N/A**.

display link-aggregation member-port

Use **display link-aggregation member-port** to display detailed link aggregation information about the specified member ports.

Syntax

display link-aggregation member-port [*interface-list* | **auto**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface-list: Specifies a list of link aggregation member ports, in the format *interface-type interface-number1* [**to** *interface-type interface-number2*]. The value for the *interface-number2* argument must be equal to or greater than the value for the *interface-number1* argument.

auto: Specifies all link aggregation member ports that are enabled with automatic assignment.

Usage guidelines

A member port in a static aggregation group cannot obtain information about the peer group. For such member ports, the command displays the port number, port priority, and operational key of only the local end.

Examples

Display detailed information about GigabitEthernet 1/0/1, which is a member port of a static aggregation group.

```
<Sysname> display link-aggregation member-port gigabitethernet 1/0/1
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
       D -- Synchronization, E -- Collecting, F -- Distributing,
       G -- Defaulted, H -- Expired

GigabitEthernet1/0/1:
Aggregate Interface: Bridge-Aggregation1
Port Number: 1
Port Priority: 32768
Oper-Key: 1
```

Display detailed information about GigabitEthernet 1/0/2, which is a member port of a dynamic aggregation group.

```
<Sysname> display link-aggregation member-port gigabitethernet 1/0/2
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
       D -- Synchronization, E -- Collecting, F -- Distributing,
       G -- Defaulted, H -- Expired

GigabitEthernet1/0/2:
Aggregate Interface: Bridge-Aggregation2
Local:
    Port Number: 2
    Port Priority: 32768
    Oper-Key: 2
    Flag: {ACDEF}
Remote:
    System ID: 0x8000, 000f-e267-6c6a
    Port Number: 26
    Port Priority: 32768
    Oper-Key: 2
    Flag: {ACDEF}
Received LACP Packets: 5 packet(s)
Illegal: 0 packet(s)
Sent LACP Packets: 7 packet(s)
```

Table 5 Command output

Field	Description
Flags	LACP state flags. This field is one byte long, represented by ABCDEFGH from the least significant bit to the most significant bit. A letter appears when its bit is 1 and does not appear when its bit is 0. • **A**—Indicates whether LACP is active on the port. 1 indicates active. 0 indicates passive. • **B**—Indicates the LACP timeout interval. 1 indicates the short timeout

Field	Description
	interval. 0 indicates the long timeout interval. • **C**—Indicates whether the sending system considers that the link is aggregatable. 1 indicates yes. 0 indicates no. • **D**—Indicates whether the sending system considers that the link has been aggregated. 1 indicates yes. 0 indicates no. • **E**—Indicates whether the sending system considers that the link can collect frames. 1 indicates yes. 0 indicates no. • **F**—Indicates whether the sending system considers that the link can distribute frames. 1 indicates yes. 0 indicates no. • **G**—Indicates whether the RX state machine of the sending system is in default state. 1 indicates yes. 0 indicates no. • **H**—Indicates whether the RX state machine of the sending system is in expired state. 1 indicates yes. 0 indicates no.
Aggregate Interface	Aggregate interface to which the member port belongs.
Local	Information about the local end.
Oper-key	Operational key.
Flag	LACP protocol state flag.
Remote	Information about the peer end.
System ID	Peer system ID, containing the system LACP priority and the system MAC address.
Received LACP Packets	Total number of LACP packets received.
Illegal	Total number of illegal packets.
Sent LACP Packets	Total number of LACP packets sent.

display link-aggregation summary

Use **`display link-aggregation summary`** to display brief information about all aggregation groups.

Syntax

`display link-aggregation summary`

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Usage guidelines

Static link aggregation groups cannot obtain information about the peer groups. As a result, the **Partner ID** field displays **None** or nothing for a static link aggregation group.

Examples

Display brief information about all aggregation groups.

```
<Sysname> display link-aggregation summary
Aggregate Interface Type:
BAGG -- Bridge-Aggregation, BLAGG –- Blade-Aggregation, RAGG -- Route-Aggregation, SCH-B
– Schannel-Bundle
Aggregation Mode: S -- Static, D -- Dynamic
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Actor System ID: 0x8000, 000f-e267-6c6a

AGG         AGG   Partner ID              Selected  Unselected  Individual  Share
Interface   Mode                          Ports     Ports       Ports       Type
--------------------------------------------------------------------------------
RAGG1       S     None                    1         0           0           NonS
BAGG2       D     0x8000,00e0-fcff-ff01   2         0           0           Shar
```

Table 6 Command output

Field	Description
Aggregate Interface Type	Aggregate interface type: • **BAGG**—Layer 2. • **RAGG**—Layer 3. • **BLAGG**—Blade. This type is not supported in the current software version. • **SCH-B**—S-channel bundle. This type is not supported in the current software version.
Aggregation Mode	Aggregation group type: • **S**—Static. • **D**—Dynamic.
Loadsharing Type	Load sharing type: • **Shar**—Load-sharing. • **NonS**—Non-load-sharing.
Actor System ID	Local system ID, which contains the local system LACP priority and the local system MAC address.
AGG Interface	Type and number of the aggregate interface.
AGG Mode	Aggregation group type.
Partner ID	System ID of the peer system, which contains the peer system LACP priority and the peer system MAC address.
Selected Ports	Total number of Selected ports.
Unselected Ports	Total number of Unselected ports.
Individual Ports	Total number of Individual ports.
Share Type	Load sharing type.

display link-aggregation verbose

Use **display link-aggregation verbose** to display detailed information about the aggregation groups that correspond to the specified aggregate interfaces.

Syntax

display link-aggregation verbose [{ **bridge-aggregation** | **route-aggregation** } [*interface-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

bridge-aggregation: Specifies Layer 2 aggregate interfaces.

route-aggregation: Specifies Layer 3 aggregate interfaces.

interface-number: Specifies an existing aggregate interface by its number.

Usage guidelines

If you do not specify an aggregate interface type, the command displays detailed information about all aggregation groups.

If you specify an aggregate interface type but do not specify an interface number, the command displays detailed information about all aggregation groups of the specified type.

The **bridge-aggregation** or **route-aggregation** keyword is available only when aggregate interfaces of the corresponding type exist on the device.

Examples

Display detailed information about Layer 2 aggregation group 1, which is a dynamic aggregation group.

```
<Sysname> display link-aggregation verbose bridge-aggregation 1
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation1
Creation Mode: Manual
Aggregation Mode: Dynamic
Loadsharing Type: Shar
System ID: 0x8000, 000f-e267-6c6a
Local:
  Port             Status  Priority Oper-Key  Flag
--------------------------------------------------------------------------------
  GE1/0/1          S       32768    2         {ACDEF}
  GE1/0/2          S       32768    2         {ACDEF}
  GE1/0/3          S       32768    2         {ACDEF}
Remote:
```

```
  Actor            Partner Priority Oper-Key  SystemID               Flag
--------------------------------------------------------------------------------
  GE1/0/1          1       32768    2         0x8000, 000f-e267-57ad {ACDEF}
  GE1/0/2          1       32768    2         0x8000, 000f-e267-57ad {ACDEF}
  GE1/0/3          1       32768    2         0x8000, 000f-e267-57ad {ACDEF}
```

Display detailed information about Layer 3 aggregation group 1, which is a dynamic aggregation group.

```
<Sysname> display link-aggregation verbose route-aggregation 1
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Route-Aggregation1
Creation Mode: Manual
Aggregation Mode: Dynamic
Loadsharing Type: Shar
System ID: 0x8000, 000f-e267-6c6a
Local:
  Port             Status  Priority Oper-Key  Flag
--------------------------------------------------------------------------------
  GE1/0/1          S       32768    2         {ACDEF}
  GE1/0/2          S       32768    2         {ACDEF}
  GE1/0/3          S       32768    2         {ACDEF}
Remote:
  Actor            Partner Priority Oper-Key  SystemID               Flag
--------------------------------------------------------------------------------
  GE1/0/1          1       32768    2         0x8000, 000f-e267-57ad {ACDEF}
  GE1/0/2          1       32768    2         0x8000, 000f-e267-57ad {ACDEF}
  GE1/0/3          1       32768    2         0x8000, 000f-e267-57ad {ACDEF}
```

Display detailed information about Layer 2 aggregation group 2, which is a static aggregation group.

```
<Sysname> display link-aggregation verbose bridge-aggregation 2
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation2
Aggregation Mode: Static
Loadsharing Type: Shar
  Port             Status  Priority Oper-Key
--------------------------------------------------------------------------------
  GE1/0/1          S       32768    1
```

```
  GE1/0/2          S       32768    1
  GE1/0/3          S       32768    1
```

Display detailed information about Layer 3 aggregation group 2, which is a static aggregation group.

```
<Sysname> display link-aggregation verbose route-aggregation 2
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Route-Aggregation2
Aggregation Mode: Static
Loadsharing Type: Shar
  Port             Status  Priority Oper-Key
--------------------------------------------------------------------------------
  GE1/0/1          S       32768    1
  GE1/0/2          S       32768    1
  GE1/0/3          S       32768    1
```

Table 7 Command output

Field	Description
Loadsharing Type	Load sharing type: • **Shar**—Load-sharing. • **NonS**—Non-load-sharing.
Port Status	Port state: • **Selected**. • **Unselected**. • **Individual**.
Port	Port type. **Auto port** indicates that the port is enabled with automatic assignment.
Flags	LACP state flags. This field is one byte long, represented by ABCDEFGH from the least significant bit to the most significant bit. A letter appears when its bit is 1 and does not appear when its bit is 0. • **A**—Indicates whether LACP is active on the port. 1 indicates active. 0 indicates passive. • **B**—Indicates the LACP timeout interval. 1 indicates the short timeout interval. 0 indicates the long timeout interval. • **C**—Indicates whether the sending system considers that the link is aggregatable. 1 indicates yes. 0 indicates no. • **D**—Indicates whether the sending system considers that the link has been aggregated. 1 indicates yes. 0 indicates no. • **E**—Indicates whether the sending system considers that the link can collect frames. 1 indicates yes. 0 indicates no. • **F**—Indicates whether the sending system considers that the link can distribute frames. 1 indicates yes. 0 indicates no. • **G**—Indicates whether the RX state machine of the sending system is in default state. 1 indicates yes. 0 indicates no. • **H**—Indicates whether the RX state machine of the sending system is in expired state. 1 indicates yes. 0 indicates no.

Field	Description
Aggregate Interface	Name of the aggregate interface.
Creation Mode	Creation mode of the dynamic aggregate interface: • **Auto**. • **Manual**.
Aggregation Mode	Aggregation group type: • **S**—Static. • **D**—Dynamic.
System ID	Local system ID, containing the local system LACP priority and the local system MAC address.
Local	Information about the local end: • **Port**—Port type and number. • **Status**—Port state, which can be Selected, Unselected, or Individual. • **Priority**—Port priority. • **Oper-Key**—Operational key. • **Flag**—LACP state flag. **NOTE:** For static aggregation groups, the **Flag** field is not displayed.
Remote	Information about the peer end: • **Actor**—Type and number of the local port. This field displays the **(R)** flag next to the port if its peer port is the reference port. • **Partner**—Index of the peer port. • **Priority**—Priority of the peer port. • **Oper-Key**—Operational key of the peer port. • **System ID**—System ID of the peer end. • **Flag**—LACP state flag of the peer end.

interface bridge-aggregation

Use **`interface bridge-aggregation`** to create a Layer 2 aggregate interface and enter its view, or enter the view of an existing Layer 2 aggregate interface.

Use **`undo interface bridge-aggregation`** to delete a Layer 2 aggregate interface.

Syntax

`interface bridge-aggregation` *`interface-number`*

`undo interface bridge-aggregation` *`interface-number`*

Default

No Layer 2 aggregate interfaces exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interface-number: Specifies a Layer 2 aggregate interface number. The value range for the *interface-number* argument is 1 to 64.

Usage guidelines

When you create a Layer 2 aggregate interface, the system automatically creates a Layer 2 aggregation group with the same number. The aggregation group operates in static aggregation mode by default.

Deleting a Layer 2 aggregate interface also deletes the Layer 2 aggregation group. At the same time, the member ports of the aggregation group, if any, leave the aggregation group.

Examples

Create Layer 2 aggregate interface Bridge-Aggregation 1, and enter its view.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1]
```

interface route-aggregation

Use **interface route-aggregation** to create a Layer 3 aggregate interface or subinterface and enter its view, or enter the view of an existing Layer 3 aggregate interface or subinterface.

Use **undo interface route-aggregation** to delete a Layer 3 aggregate interface or subinterface.

Syntax

interface route-aggregation { *interface-number* | *interface-number.subnumber* }

undo interface route-aggregation { *interface-number* | *interface-number.subnumber* }

Default

No Layer 3 aggregate interfaces or subinterfaces exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interface-number: Specifies a Layer 3 aggregate interface number. The value range for the *interface-number* argument is 1 to 64.

interface-number.subnumber: Specifies a subinterface of a Layer 3 aggregate interface. The *interface-number* argument specifies the main interface number. The *subnumber* argument specifies the subinterface number and is separated from the main interface number by a dot (.). The value range for the *interface-number* argument is 1 to 4094.

Usage guidelines

When you create a Layer 3 aggregate interface, the system automatically creates a Layer 3 aggregation group with the same number. The Layer 3 aggregation group operates in static aggregation mode by default.

Deleting a Layer 3 aggregate interface also deletes the Layer 3 aggregation group and all its aggregate subinterfaces. At the same time, the member ports of the aggregation group, if any, leave the aggregation group.

Deleting a Layer 3 aggregate subinterface does not affect the state of the main interface and the corresponding aggregation group.

Examples

Create Layer 3 aggregate interface Route-Aggregation 1 and enter its view.

```
<Sysname> system-view
[Sysname] interface route-aggregation 1
[Sysname-Route-Aggregation1]
```

Create Layer 3 aggregate subinterface Route-Aggregation 1.1 and enter its view.

```
<Sysname> system-view
[Sysname] interface route-aggregation 1.1
[Sysname-Route-Aggregation1.1]
```

jumboframe enable

Use **jumboframe enable** to allow the jumbo frames on an interface to pass through.

Use **undo jumboframe enable** to deny jumbo frames on an interface.

Use **undo jumboframe enable** *size* to restore the default.

Syntax

jumboframe enable [*size*]

undo jumboframe enable [*size*]

Default

An aggregate interface allows jumbo frames within a specific length to pass through. The following compatibility matrixes show the default maximum jumbo frame length on each hardware model:

Models	Default
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	9216 bytes
NFNX3-HDB680, NFNX3-HDB1080	1524 bytes

Views

Layer 2 aggregate interface view

Layer 3 aggregate interface view

Predefined user roles

network-admin

context-admin

Parameters

size: Specifies the maximum length of jumbo frames, in bytes.

The following compatibility matrix shows the value ranges for this argument:

Hardware	Value range
NFNX3-HDB680, NFNX3-HDB1080	Fixed at 1524 bytes

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Allow jumbo frames to pass through on Layer 2 aggregate interface Bridge-Aggregation 1.

```
<Sysname> System-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] jumboframe enable
```

Allow jumbo frames to pass through on Layer 3 aggregate interface Route-Aggregation 1.

```
<Sysname> System-view
[Sysname] interface route-aggregation 1
[Sysname-Route-Aggregation1] jumboframe enable
```

lacp default-selected-port disable

Use **lacp default-selected-port disable** to disable the default port selection action for dynamic aggregation groups.

Use **undo lacp default-selected-port disable** to enable the default port selection action for dynamic aggregation groups.

Syntax

lacp default-selected-port disable

undo lacp default-selected-port disable

Default

The default port selection action is enabled for dynamic aggregation groups.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

The default port selection action applies to dynamic aggregation groups.

This action automatically chooses the port with the lowest ID from among all up member ports as a Selected port if none of them has received LACPDUs before the LACP timeout interval expires.

After this action is disabled, a dynamic aggregation group will not have any Selected ports to forward traffic if it has not received LACPDUs before the LACP timeout interval expires.

Examples

Disable the default port selection action.

```
<Sysname> system-view
[Sysname] lacp default-selected-port disable
```

lacp edge-port

Use **lacp edge-port** to configure an aggregate interface as an edge aggregate interface.

Use **undo lacp edge-port** to restore the default.

Syntax

lacp edge-port

undo lacp edge-port

Default

An aggregate interface does not operate as an edge aggregate interface.

Views

Layer 2 aggregate interface view

Layer 3 aggregate interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

Use this command on the aggregate interface that connects the device to a server if dynamic link aggregation is configured only on the device. This feature improves link reliability by enabling all member ports of the aggregation group to forward packets.

This command takes effect only on an aggregate interface corresponding to a dynamic aggregation group.

Link-aggregation traffic redirection cannot operate correctly on an edge aggregate interface.

Examples

Configure Layer 2 aggregate interface Bridge-Aggregation 1 as an edge aggregate interface.

```
<Sysname> System-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] lacp edge-port
```

Configure Layer 3 aggregate interface Route-Aggregation 1 as an edge aggregate interface.

```
<Sysname> System-view
[Sysname] interface route-aggregation 1
[Sysname-Route-Aggregation1] lacp edge-port
```

lacp mode

Use **lacp mode passive** to configure LACP to operate in passive mode on a port.

Use **undo lacp mode** to restore the default.

Syntax

lacp mode passive

undo lacp mode

Default

LACP operates in active mode on a port.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command takes effect only on member ports of dynamic aggregation groups.

When LACP is operating in passive mode on a local member port and its peer port, both ports cannot send LACPDUs. When LACP is operating in active mode on either end of a link, both ports can send LACPDUs.

Examples

Configure LACP to operate in passive mode on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lacp mode passive
```

lacp period short

Use **lacp period short** to enable the short LACP timeout interval (3 seconds) on an interface.

Use **undo lacp period** to restore the default.

Syntax

lacp period short

undo lacp period

Default

The LACP timeout interval is the long timeout interval (90 seconds) on an interface.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

To avoid traffic interruption during an ISSU, do not enable the short LACP timeout interval before performing the ISSU. For more information about ISSU, see *Fundamentals Configuration Guide*.

Examples

Enable the short LACP timeout interval (3 seconds) on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lacp period short
```

lacp system-priority

Use **lacp system-priority** to set the system LACP priority.

Use **undo lacp system-priority** to restore the default.

Syntax

lacp system-priority *priority*

undo lacp system-priority

Default

The system LACP priority is 32768.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

priority: Specifies the system LACP priority in the range of 0 to 65535. The smaller the value, the higher the system LACP priority.

Examples

Set the system LACP priority to 64.

```
<Sysname> system-view
[Sysname] lacp system-priority 64
```

Related commands

link-aggregation port-priority

link-aggregation forwarding-acceleration enable

Use **link-aggregation forwarding-acceleration enable** to enable forwarding acceleration on an aggregate interface.

Use **undo link-aggregation forwarding-acceleration enable** to disable forwarding acceleration on an aggregate interface.

Syntax

link-aggregation forwarding-acceleration enable

undo link-aggregation forwarding-acceleration enable

Default

Forwarding acceleration is enabled on aggregate interfaces.

Views

Layer 2 aggregate interface view

Layer 3 aggregate interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

Forwarding acceleration takes effect on an aggregate interface only when it is enabled both globally and on the aggregate interface.

This feature accelerates traffic forwarding on an aggregate interface whose member ports are located on multiple slots.

Examples

Enable forwarding acceleration on Bridge-Aggregation 1.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] link-aggregation forwarding-acceleration enable
```

Enable forwarding acceleration on Route-Aggregation 1.

```
<Sysname> system-view
[Sysname] interface route-aggregation 1
[Sysname-Route-Aggregation1] link-aggregation forwarding-acceleration enable
```

Related commands

link-aggregation global forwarding-acceleration enable

link-aggregation global forwarding-acceleration enable

Use **link-aggregation global forwarding-acceleration enable** to enable forwarding acceleration globally.

undo link-aggregation global forwarding-acceleration enable to disable forwarding acceleration globally.

Syntax

link-aggregation global forwarding-acceleration enable

undo link-aggregation global forwarding-acceleration enable

Default

Forwarding acceleration is disabled globally.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

Forwarding acceleration takes effect on an aggregate interface only when it is enabled both globally and on the aggregate interface.

This feature accelerates traffic forwarding on an aggregate interface whose member ports are located on multiple slots.

Examples

Enable forwarding acceleration globally.

```
<Sysname> system-view
[Sysname] link-aggregation global forwarding-acceleration enable
```

Related commands

link-aggregation forwarding-acceleration enable

link-aggregation global load-sharing mode

Use **link-aggregation global load-sharing mode** to set the global link-aggregation load sharing mode.

Use **undo link-aggregation global load-sharing mode** to restore the default.

Syntax

link-aggregation global load-sharing mode { **destination-ip** | **destination-mac** | **destination-port** | **ingress-port** | **source-ip** | **source-mac** | **source-port** } *

undo link-aggregation global load-sharing mode

Default

The system automatically chooses a load sharing mode depending on the packet type.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

destination-ip: Distributes traffic based on destination IP addresses.

destination-mac: Distributes traffic based on destination MAC addresses.

destination-port: Distributes traffic based on destination ports.

ingress-port: Distributes traffic based on ingress ports.

source-ip: Distributes traffic based on source IP addresses.

source-mac: Distributes traffic based on source MAC addresses.

source-port: Distributes traffic based on source ports.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

If an unsupported load sharing mode is set, the device displays an error message.

Examples

Set the global load sharing mode to load share packets based on destination MAC addresses.

```
<Sysname> system-view
[Sysname] link-aggregation global load-sharing mode destination-mac
```

Related commands

bandwidth

link-aggregation load-sharing mode

link-aggregation ignore vlan

Use **link-aggregation ignore vlan** to configure a Layer 2 aggregate interface to ignore the specified VLANs.

Use **undo link-aggregation ignore vlan** to remove the specified ignored VLANs for a Layer 2 aggregate interface.

Syntax

link-aggregation ignore vlan *vlan-id-list*

undo link-aggregation ignore vlan *vlan-id-list*

Default

A Layer 2 aggregate interface does not ignore any VLANs.

Views

Layer 2 aggregate interface view

Predefined user roles

network-admin

context-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN ID or a range of VLAN IDs in the form of *vlan-id1* to *vlan-id2*. The value range for VLAN IDs is 1 to 4094. The value for the *vlan-id2* argument must be equal to or greater than the value for the *vlan-id1* argument.

Usage guidelines

This command takes effect only when the link type of the Layer 2 aggregate interface is hybrid or trunk.

With this command configured, a Layer 2 aggregate interface ignores the permitted VLAN and VLAN tagging mode configuration of the specified VLANs when choosing Selected ports.

Examples

Configure Layer 2 aggregate interface **bridge-aggregation 1** to ignore VLAN 50.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] link-aggregation ignore vlan 50
```

link-aggregation load-sharing mode

Use **link-aggregation load-sharing mode** to set the link-aggregation load sharing mode for an aggregation group.

Use **undo link-aggregation load-sharing mode** to restore the default.

Syntax

link-aggregation load-sharing mode { **destination-ip** | **destination-mac** | **destination-port** | **source-ip** | **source-mac** | **source-port** } *

undo link-aggregation load-sharing mode

Default

An aggregation group uses the global link-aggregation load sharing mode.

Views

Layer 2 aggregate interface view

Layer 3 aggregate interface view

Predefined user roles

network-admin

context-admin

Parameters

destination-ip: Distributes traffic based on destination IP addresses.

destination-mac: Distributes traffic based on destination MAC addresses.

destination-port: Distributes traffic based on destination ports.

source-ip: Distributes traffic based on source IP addresses.

source-mac: Distributes traffic based on source MAC addresses.

source-port: Distributes traffic based on source ports.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

If an unsupported load sharing mode is set, the device displays an error message.

Examples

Configure Layer 2 aggregation group 1 to load share packets based on destination MAC addresses.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] link-aggregation load-sharing mode destination-mac
```

Configure Layer 3 aggregation group 1 to load share packets based on destination MAC addresses.

```
<Sysname> system-view
[Sysname] interface route-aggregation 1
[Sysname-Route-Aggregation1] link-aggregation load-sharing mode destination-mac
```

Related commands

bandwidth

link-aggregation global load-sharing mode

link-aggregation load-sharing mode local-first

Use **link-aggregation load-sharing mode local-first** to enable local-first load sharing for link aggregation globally.

Use **undo link-aggregation load-sharing mode local-first** to disable local-first load sharing for link aggregation globally.

Syntax

link-aggregation load-sharing mode local-first

undo link-aggregation load-sharing mode local-first

Default

Local-first load sharing is enabled for link aggregation globally.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

Use local-first load sharing in a multichassis link aggregation scenario to distribute traffic preferentially across member ports on the ingress device.

If you disable local-first load sharing, packets of an aggregate interface are load shared among all Selected ports on IRF member devices.

You can configure local-first load sharing globally or on a per-interface basis. An aggregate interface preferentially uses the interface-specific setting. If no interface-specific setting is available, the aggregate interface uses the global setting.

Examples

Disable local-first load sharing for link aggregation globally.

```
<Sysname> system-view
[Sysname] undo link-aggregation load-sharing mode local-first
```

Related commands

link-aggregation group load-sharing mode local-first

link-aggregation mode

Use **link-aggregation mode dynamic** to configure an aggregation group to operate in dynamic aggregation mode and enable LACP.

Use **undo link-aggregation mode** to restore the default.

Syntax

link-aggregation mode dynamic

undo link-aggregation mode

Default

An aggregation group operates in static aggregation mode.

Views

Layer 2 aggregate interface view

Layer 3 aggregate interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

Aggregation mode change might cause Selected member ports to become Unselected.

When you change the aggregation mode, make sure you understand the impact of the change on services.

Examples

Configure Layer 2 aggregation group 1 to operate in dynamic aggregation mode.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] link-aggregation mode dynamic
```

Configure Layer 3 aggregation group 1 to operate in dynamic aggregation mode.

```
<Sysname> system-view
[Sysname] interface route-aggregation 1
[Sysname-Route-Aggregation1] link-aggregation mode dynamic
```

link-aggregation port-priority

Use **link-aggregation port-priority** to set the port priority of an interface.

Use **undo link-aggregation port-priority** to restore the default.

Syntax

link-aggregation port-priority *priority*

undo link-aggregation port-priority

Default

The port priority of an interface is 32768.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Predefined user roles

network-admin

context-admin

Parameters

priority: Specifies the port priority in the range of 0 to 65535. The smaller the value, the higher the port priority.

Examples

Set the port priority to 64 for Layer 2 Ethernet interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] link-aggregation port-priority 64
```

Set the port priority to 64 for Layer 3 Ethernet interface GigabitEthernet 1/0/2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] link-aggregation port-priority 64
```

Related commands

lacp system-priority

link-aggregation selected-port maximum

Use **link-aggregation selected-port maximum** to set the maximum number of Selected ports allowed in an aggregation group.

Use **undo link-aggregation selected-port maximum** to restore the default.

Syntax

link-aggregation selected-port maximum *max-number*

undo link-aggregation selected-port maximum

Default

The maximum number of Selected ports allowed in an aggregation group depends on hardware limitation.

Views

Layer 2 aggregate interface view

Layer 3 aggregate interface view

Predefined user roles

network-admin

context-admin

Parameters

max-number: Specifies the maximum number of Selected ports allowed in an aggregation group. The value range for this argument is 1 to 16.

Usage guidelines

Executing this command might cause some of the Selected ports in an aggregation group to become Unselected ports.

The maximum number of Selected ports allowed in the aggregation groups must be the same for the local and peer ends.

For an aggregation group, the maximum number of Selected ports must be equal to or higher than the minimum number of Selected ports.

The maximum number of Selected ports allowed in an aggregation group is limited by one of the following values, whichever value is smaller:

- Maximum number set by using the **link-aggregation selected-port maximum** command.
- Maximum number of Selected ports allowed by the link aggregation capability.

You can implement backup between two ports by performing the following tasks:

- Assigning two ports to an aggregation group.
- Setting the maximum number of Selected ports to 1 for the aggregation group.

Then, only one Selected port is allowed in the aggregation group at any point in time, while the Unselected port acts as a backup port.

Examples

Set the maximum number of Selected ports to 5 for Layer 2 aggregation group 1.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] link-aggregation selected-port maximum 5
```

Set the maximum number of Selected ports to 5 for Layer 3 aggregation group 1.

```
<Sysname> system-view
[Sysname] interface route-aggregation 1
[Sysname-Route-Aggregation1] link-aggregation selected-port maximum 5
```

Related commands

link-aggregation selected-port minimum

link-aggregation selected-port minimum

Use **link-aggregation selected-port minimum** to set the minimum number of Selected ports in an aggregation group.

Use **undo link-aggregation selected-port minimum** to restore the default.

Syntax

link-aggregation selected-port minimum *min-number*

undo link-aggregation selected-port minimum

Default

The minimum number of Selected ports in an aggregation group is not specified.

Views

Layer 2 aggregate interface view

Layer 3 aggregate interface view

Predefined user roles

network-admin

context-admin

Parameters

min-number: Specifies the minimum number of Selected ports in an aggregation group required to bring up the aggregate interface. The value range for this argument is 1 to 16.

Usage guidelines

Executing this command might cause all member ports in the aggregation group to become Unselected ports.

The minimum number of Selected ports allowed in the aggregation groups must be the same for the local and peer ends.

For an aggregation group, the minimum number of Selected ports must be equal to or lower than the maximum number of Selected ports.

Examples

Set the minimum number of Selected ports to 3 for Layer 2 aggregation group 1.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] link-aggregation selected-port minimum 3
```

Set the minimum number of Selected ports to 3 for Layer 3 aggregation group 1.

```
<Sysname> system-view
[Sysname] interface route-aggregation 1
[Sysname-Route-Aggregation1] link-aggregation selected-port minimum 3
```

Related commands

link-aggregation selected-port maximum

link-delay

Use **link-delay** to set the physical state change suppression interval on an aggregate interface.

Use **undo link-delay** to restore the default.

Syntax

link-delay [**msec**] *delay-time* [**mode** { **up** | **updown** }]

undo link-delay [**msec**] *delay-time* [**mode** { **up** | **updown** }]

Default

Each time the physical link of an aggregate interface goes up or comes down, the system immediately reports the change to the CPU.

Views

Layer 2 aggregate interface view

Layer 3 aggregate interface view

Predefined user roles

network-admin

context-admin

Parameters

msec: Sets the physical state change suppression interval in milliseconds. If you do not specify this keyword, the suppression interval is in seconds.

delay-time: Sets the physical state change suppression interval. To report a physical state change immediately to the CPU, set the interval to 0.

- If you do not specify the **msec** keyword, the value range is 0 to 30 seconds.
- If you specify the **msec** keyword, the value range is 0 to 10000 milliseconds, and the value must be a multiple of 100.

mode up: Suppresses link-up events.

mode updown: Suppresses both link-up and link-down events.

Usage guidelines

You can configure this feature to suppress only link-down events, only link-up events, or both. If an event of the specified type persists when the suppression interval expires, the system reports the event.

When you configure this feature, follow these guidelines:

- To suppress only link-down events, use the **link-delay** [**msec**] *delay-time* command.
- To suppress only link-up events, use the **link-delay** [**msec**] *delay-time* **mode up** command.
- To suppress both link-down and link-up events, use the **link-delay** [**msec**] *delay-time* **mode updown** command.

On an interface, you can configure different suppression intervals for link-up and link-down events. If you execute the **link-delay** command multiple times for link-up or link-down events, the most recent configuration takes effect.

Examples

Set the link-down event suppression interval to 8 seconds on Bridge-Aggregation 1.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] link-delay down 8
```

Set the link-down event suppression interval to 8 seconds on Route-Aggregation 1.

```
<Sysname> system-view
[Sysname] interface route-aggregation 1
[Sysname-Route-Aggregation1] link-delay 8
```

mtu

Use **mtu** to set the MTU of a Layer 3 aggregate interface or subinterface.

Use **undo mtu** to restore the default.

Syntax

mtu *size*

undo mtu

Default

The MTU of Layer 3 aggregate interfaces and subinterfaces is 1500 bytes.

Views

Layer 3 aggregate interface view

Layer 3 aggregate subinterface view

Predefined user roles

network-admin

context-admin

Parameters

size: Specifies an MTU in bytes. The value range for this argument is 46 to 1560..

Examples

Set the MTU of interface Route-Aggregation 1 to 1430 bytes.

```
<Sysname> system-view
[Sysname] interface route-aggregation 1
[Sysname-Route-Aggregation1] mtu 1430
```

Related commands

display interface

port link-aggregation group

Use **port link-aggregation group** to assign an interface to an aggregation group.

Use **undo port link-aggregation group** to remove an interface from the aggregation group to which it belongs.

Syntax

port link-aggregation group *group-id*

undo port link-aggregation group

Default

An interface does not belong to any aggregation group.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Layer 3 Ethernet subinterface view

Predefined user roles

network-admin

context-admin

Parameters

group-id: Specifies an aggregation group by its aggregate interface number. The value range for the *number* argument is 1 to 64.

Usage guidelines

You can assign a Layer 2 or Layer 3 Ethernet interface only to a Layer 2 or Layer 3 aggregation group, respectively.

An interface can belong to only one aggregation group.

The following restrictions apply if you have not enabled multi-VLAN termination on an aggregate interface by using the **link-aggregation multivlan-termination** command:

- You cannot assign both Ethernet interfaces and Ethernet subinterfaces to the aggregation group.
- You cannot create subinterfaces on an Ethernet interface that is in the aggregation group.
- You cannot assign an Ethernet interface that has subinterfaces to the aggregation group.

You cannot create aggregate subinterfaces on an aggregate interface if its aggregation group contains Ethernet subinterfaces. You cannot assign Ethernet subinterfaces to an aggregation group if its aggregate interface has aggregate subinterfaces.

Before you assign an Ethernet subinterface to an aggregation group, perform the following tasks:

- If multi-VLAN termination is not enabled on the aggregate interface, configure VLAN termination on the Ethernet subinterface. You will be unable to modify the VLAN termination configuration after you assign the subinterface to the aggregation group. To configure VLAN termination, use the following commands:
  - **vlan-type dot1q default**.
  - **vlan-type dot1q untagged**.
  - **vlan-type dot1q vid**.
- To assign Ethernet subinterfaces that terminate different VLANs to the same aggregation group, enable multi-VLAN termination on the aggregate interface. If multi-VLAN termination is not enabled on the aggregate interface, you must make sure the Ethernet subinterfaces to be assigned to its aggregation group terminate the same VLAN.
- If you are assigning the Ethernet subinterface to a dynamic aggregation group, specify only one VLAN ID when you execute the **vlan-type dot1q vid** *vlan-id-list* [**loose**] command.

You cannot assign the following interfaces to an aggregation group:

- Member interfaces of redundant Ethernet interfaces.
- Member interfaces of redundancy group nodes.

For more information about redundant Ethernet interfaces and redundancy group nodes, see *Virtual Technologies Configuration Guide*.

Examples

Assign Layer 2 Ethernet interface GigabitEthernet 1/0/1 to Layer 2 aggregation group 1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-aggregation group 1
```

Assign Layer 3 Ethernet interface GigabitEthernet 1/0/2 to Layer 3 aggregation group 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] port link-aggregation group 2
```

Related commands

link-aggregation multivlan-termination

vlan-type dot1q default

vlan-type dot1q untagged

vlan-type dot1q vid

reset counters interface

Use **reset counters interface** to clear statistics about the specified aggregate interfaces.

Syntax

reset counters interface [{ **bridge-aggregation** | **route-aggregation** } [*interface-number*]]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

bridge-aggregation: Specifies Layer 2 aggregate interfaces.

route-aggregation: Specifies Layer 3 aggregate interfaces.

interface-number: Specifies an existing aggregate interface number.

Usage guidelines

Use this command to clear history statistics before you collect traffic statistics for a time period.

If you do not specify an aggregate interface type, the command clears statistics about all interfaces in the system except VA interfaces.

If you specify only an aggregate interface type, the command clears statistics about all aggregate interfaces of the specified type.

The **bridge-aggregation** or **route-aggregation** keyword is available only when aggregate interfaces of the corresponding type exist on the device.

Examples

Clear the statistics about interface Bridge-Aggregation 1.

```
<Sysname> reset counters interface bridge-aggregation 1
```

reset lacp statistics

Use **reset lacp statistics** to clear LACP statistics about the specified link aggregation member ports.

Syntax

reset lacp statistics [**interface** *interface-list*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

interface *interface-list*: Specifies a list of link aggregation member ports, in the format *interface-type interface-number1* [**to** *interface-type interface-number2*]. The value for the *interface-number1* argument must be equal to or greater than the value for the *interface-number2* argument. If you do not specify any member ports, the command clears LACP statistics about all member ports.

Examples

Clear LACP statistics about all link aggregation member ports.

```
<Sysname> reset lacp statistics
```

Related commands

display link-aggregation member-port

shutdown

Use **shutdown** to shut down an aggregate interface or subinterface.

Use **undo shutdown** to bring up an aggregate interface or subinterface.

Syntax

shutdown

undo shutdown

Default

An interface is not manually shut down.

Views

Layer 2 aggregate interface view

Layer 3 aggregate interface view

Layer 3 aggregate subinterface view

Predefined user roles

network-admin

context-admin

Usage guidelines

CAUTION:

The **shutdown** command will disconnect all links established on an interface. Make sure you are fully aware of the impacts of this command when you use it on a live network.

Shutting down or bringing up a Layer 3 aggregate interface shuts down or brings up its subinterfaces. Shutting down or bringing up a Layer 3 aggregate subinterface does not affect its main interface.

Examples

Bring up Layer 2 aggregate interface Bridge-Aggregation 1.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] undo shutdown
```

Bring up Layer 3 aggregate interface Route-Aggregation 1.

```
<Sysname> system-view
[Sysname] interface route-aggregation 1
[Sysname-Route-Aggregation1] undo shutdown
```

Contents

VLAN commands

Basic VLAN commands

bandwidth

Use **bandwidth** to set the expected bandwidth of an interface.

Use **undo bandwidth** to restore the default.

Syntax

bandwidth *bandwidth-value*

undo bandwidth

Default

The expected bandwidth (in kbps) is the interface baud rate divided by 1000.

Views

VLAN interface view

Predefined user roles

network-admin

context-admin

Parameters

bandwidth-value: Specifies the expected bandwidth in the range of 1 to 400000000 kbps.

Usage guidelines

The expected bandwidth is an informational parameter used only by higher-layer protocols for calculation. You cannot adjust the actual bandwidth of an interface by using this command.

Examples

Set the expected bandwidth to 10000 kbps for VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] bandwidth 10000
```

default

Use **default** to restore the default settings for a VLAN interface.

Syntax

default

Views

VLAN interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

CAUTION:

The **default** command might interrupt ongoing network services. Make sure you are fully aware of the impact of this command when you use it on a live network.

This command might fail to restore the default settings for some commands for reasons such as command dependencies or system restrictions. Use the **display this** command in interface view to identify these commands, and then use their **undo** forms or follow the command reference to restore their default settings. If your restoration attempt still fails, follow the error message instructions to resolve the problem.

Examples

Restore the default settings for VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] default
```

description

Use **description** to configure the description of a VLAN or VLAN interface.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

For a VLAN, the description is **VLAN** *vlan-id*. The *vlan-id* argument specifies the VLAN ID in a four-digit format. If the VLAN ID has fewer than four digits, leading zeros are added. For example, the default description of VLAN 100 is **VLAN 0100**.

For a VLAN interface, the description is the name of the interface. For example, **Vlan-interface1 Interface**.

Views

VLAN view

VLAN interface view

Predefined user roles

network-admin

context-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 255 characters.

Usage guidelines

To manage VLANs and VLAN interfaces efficiently, configure descriptions for them based on their functions or connections.

Examples

Configure the description of VLAN 2 as **sales-private**.

```
<Sysname> system-view
```

```
[Sysname] vlan 2
[Sysname-vlan2] description sales-private
```

Configure the description of VLAN-interface 2 as **linktoPC56**.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] quit
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] description linktoPC56
```

Related commands

display interface vlan-interface

display vlan

display interface vlan-interface

Use **display interface vlan-interface** to display VLAN interface information.

Syntax

display interface [**vlan-interface** [*interface-number*]] [**brief**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vlan-interface *interface-number*: Specifies a VLAN interface number. If you do not specify this option, the command displays information about all interfaces except VA interfaces. If you specify the **vlan-interface** keyword without specifying an interface, the command displays information about all VLAN interfaces. For more information about VA interfaces, see PPP in *Layer 2—WAN Access Configuration Guide*.

brief: Displays brief interface information. If you do not specify this keyword, the command displays detailed interface information.

Examples

Display information about VLAN-interface 2.

```
<Sysname> display interface vlan-interface 2
Vlan-interface2
Current state: DOWN
Line protocol state: DOWN
Description: Vlan-interface2 Interface
Bandwidth: 100000 kbps
Maximum transmission unit: 1500
Internet protocol processing : Disabled
IP packet frame type: Ethernet II, hardware address: 000f-e249-8050
IPv6 packet frame type: Ethernet II, hardware address: 000f-e249-8050
```

```
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

Display brief information about VLAN-interface 2.

```
<Sysname> display interface vlan-interface 2 brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP         Description
Vlan2                DOWN DOWN     --
```

Table 1 Command output

Field	Description
Vlan-interface2	VLAN interface name.
Current state	Physical link state of the VLAN interface: • **Administratively DOWN**—The interface has been shut down by using the **shutdown** command. • **DOWN**—The interface is administratively up, but its physical state is down. The VLAN of this VLAN interface does not contain any physical ports in up state. The ports might not be connected correctly or the links might have failed. • **UP**—The interface is both administratively and physically up.
Line protocol state	Data link layer state of the VLAN interface: • **DOWN**—The link layer protocol state of the interface is down. • **UP**—The link layer protocol state of the interface is up.
Description	Description of the VLAN interface.
Bandwidth	Expected bandwidth of the VLAN interface.
Maximum transmission unit	MTU of the VLAN interface.
Internet protocol processing : Disabled	The VLAN interface is not assigned an IP address and cannot process IP packets.
IP packet frame type	IPv4 packet framing format.
hardware address	MAC address of the VLAN interface.
IPv6 packet frame type	IPv6 packet framing format.
Last clearing of counters	The most recent time that the **reset counters interface vlan-interface** command was executed. This field displays **Never** if you have never executed this command.
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec	Average rates of input packets and output packets in the last 300 seconds (in Bps, bps, and pps).
Input: 0 packets, 0 bytes, 0 drops	Total number and size (in bytes) of the received packets of the interface and the number of the dropped packets.

Field	Description
Output: 0 packets, 0 bytes, 0 drops	Total number and size (in bytes) of the sent packets of the interface and the number of the dropped packets.
Brief information on interfaces in route mode	Brief information about Layer 3 interfaces.
Interface	Abbreviated interface name.
Link	Physical link state of the interface: • **UP**—The interface is physically up. • **DOWN**—The interface is physically down. • **ADM**—The interface has been shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command. • **Stby**—The interface is a backup interface in standby state. To see the primary interface, use the **display interface-backup state** command.
Protocol	Data link layer protocol state of the interface: • **UP**—The data link layer protocol state of the interface is up. • **DOWN**—The data link layer protocol state of the interface is down. • **UP(s)**—The data link layer protocol of the interface is up, but the link is an on-demand link or does not exist. The **(s)** attribute represents the spoofing flag.
Primary IP	Primary IP address of the interface.

Related commands

reset counters interface vlan-interface

display vlan

Use **display vlan** to display VLAN information.

Syntax

display vlan [*vlan-id1* [**to** *vlan-id2*] | **all** | **dynamic** | **static**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vlan-id1: Specifies a VLAN by its ID in the range of 1 to 4094.

vlan-id1 **to** *vlan-id2*: Specifies a VLAN ID range. Both the *vlan-id1* and the *vlan-id2* arguments are in the range of 1 to 4094. The value for the *vlan-id2* argument must be equal to or greater than the value for the *vlan-id1* argument.

all: Specifies all VLANs.

dynamic: Specifies dynamic VLANs. If you specify this keyword, the command displays the total number of dynamic VLANs and each dynamic VLAN ID. Dynamic VLANs are assigned by a RADIUS server.

static: Specifies static VLANs. If you specify this keyword, the command displays the total number of static VLANs and each static VLAN ID. Static VLANs are manually created.

Examples

Display information about VLAN 2.

```
<Sysname> display vlan 2
 VLAN ID: 2
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0002
 Name: VLAN 0002
 Tagged ports:   None
 Untagged ports:
    GigabitEthernet1/0/1  GigabitEthernet1/0/2  GigabitEthernet1/0/3
```

Display information about VLAN 3.

```
<Sysname> display vlan 3
 VLAN ID: 3
 VLAN type: static
 Route interface: Configured
 IPv4 address: 1.1.1.1
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0003
 Name: VLAN 0003
 Tagged ports:   None
 Untagged ports: None
```

Table 2 Command output

Field	Description
VLAN type	VLAN type, static or dynamic.
Route interface	Whether the VLAN interface is configured for the VLAN. • Not configured. • Configured.
Description	Description of the VLAN.
Name	VLAN name.
IP address	Primary IPv4 address of the VLAN interface. This field is displayed only when an IPv4 address is configured for the VLAN interface. When the VLAN interface is also configured with secondary IPv4 addresses, you can view them by using one of the following commands: • **display interface vlan-interface**. • **display this** (VLAN interface view).
Subnet mask	Subnet mask of the primary IP address. This field is available only when an IP address is configured for the VLAN interface.

Field	Description
Tagged ports	Tagged members of the VLAN.
Untagged ports	Untagged members of the VLAN.

Related commands

vlan

display vlan brief

Use **display vlan brief** to display brief VLAN information.

Syntax

display vlan brief

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display brief VLAN information.

```
<Sysname> display vlan brief
Brief information about all VLANs:
Supported Minimum VLAN ID: 1
Supported Maximum VLAN ID: 4094
Default VLAN ID: 1
VLAN ID   Name                            Port
1         VLAN 0001                       GE1/0/1  GE1/0/2  GE1/0/3
2         VLAN 0002
3         VLAN 0003
```

Table 3 Command output

Field	Description
Default VLAN ID	System default VLAN ID.
Name	VLAN name.
Port	Ports that allow packets from the VLAN to pass through.

interface vlan-interface

Use **interface vlan-interface** to create a VLAN interface and enter its view, or enter the view of an existing VLAN interface.

Use **undo interface vlan-interface** to delete a VLAN interface.

Syntax

interface vlan-interface *interface-number*

undo interface vlan-interface *interface-number*

Default

No VLAN interfaces exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interface-number: Specifies a VLAN interface number in the range of 1 to 4094.

Usage guidelines

Create the VLAN before you create the VLAN interface for a VLAN.

Examples

Create VLAN-interface 2, and enter its view.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] quit
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2]
```

Related commands

display interface vlan-interface

mtu

Use **mtu** to set the MTU for a VLAN interface.

Use **undo mtu** to restore the default.

Syntax

mtu *size*

undo mtu

Default

The MTU of a VLAN interface is 1500 bytes.

Views

VLAN interface view

Predefined user roles

network-admin

context-admin

Parameters

size: Sets the MTU .

The following matrix shows the value ranges for the MTU:

Models	Value range
NFNX3-HDB680, NFNX3-HDB1080	46 to 1500
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	46 to 1500

Usage guidelines

If you configure both the **mtu** and **ip mtu** commands on a VLAN interface, the MTU set by the **ip mtu** command is used for fragmentation. For more information about the **ip mtu** command, see *Layer 3—IP Services Command Reference*.

Examples

Set the MTU to 1492 bytes for VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] mtu 1492
```

Related commands

display interface vlan-interface

name

Use **name** to assign a name to a VLAN.

Use **undo name** to restore the default.

Syntax

name *text*

undo name

Default

The name of a VLAN is **VLAN** *vlan-id.* The *vlan-id* argument specifies the VLAN ID in a four-digit format. If the VLAN ID has fewer than four digits, leading zeros are added. For example, the name of VLAN 100 is **VLAN 0100**.

Views

VLAN view

Predefined user roles

network-admin

context-admin

Parameters

text: Specifies a VLAN name, a case-sensitive string of 1 to 32 characters.

Usage guidelines

If a large number of VLANs are configured, use VLAN names to identify them.

Examples

Assign the name **test vlan** to VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] name test vlan
```

Related commands

display vlan

reset counters interface vlan-interface

Use **reset counters interface vlan-interface** to clear statistics on a VLAN interface.

Syntax

reset counters interface [**vlan-interface** [*interface-number*]]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

vlan-interface *interface-number*: Specifies a VLAN interface by its number. If you do not specify this option, this command clears statistics on all interfaces except VA interfaces. If you specify the **vlan-interface** keyword without specifying an interface, this command clears statistics on all VLAN interfaces.

Usage guidelines

Use this command to clear the history statistics before you collect statistics within a time period.

Examples

Clear statistics on VLAN-interface 2.

```
<Sysname> reset counters interface vlan-interface 2
```

Related commands

display interface vlan-interface

shutdown

Use **shutdown** to shut down a VLAN interface.

Use **undo shutdown** to bring up a VLAN interface.

Syntax

shutdown

undo shutdown

Default

A VLAN interface is not manually shut down.

Views

VLAN interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

CAUTION:

Executing the **shutdown** command on a VLAN interface will disconnect the link of the VLAN interface and interrupt communication. Use this command with caution.

When a VLAN interface is not manually shut down, the following guidelines apply to the interface state:

- The VLAN interface is down if all ports in the VLAN are down.
- The VLAN interface is up if one or more ports in the VLAN are up.

When you use this command to shut down a VLAN interface, the VLAN interface remains in DOWN (Administratively) state. In this case, the VLAN interface state is not affected by the state of the ports in the VLAN.

Before you configure parameters for a VLAN interface, use this command to shut it down to prevent the configuration from affecting the network. After you complete the VLAN interface configuration, use the **undo shutdown** command to make the settings take effect.

To troubleshoot a failed VLAN interface, you can use the **shutdown** command and then the **undo shutdown** command on the interface to see whether it recovers.

In a VLAN, the state of each Ethernet port is independent of the state of the VLAN interface.

Examples

Shut down VLAN-interface 2, and then bring it up.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] shutdown
[Sysname-Vlan-interface2] undo shutdown
```

vlan

Use **vlan** *vlan-id* to create a VLAN and enter its view, or enter the view of an existing VLAN.

Use **vlan** *vlan-id1* **to** *vlan-id2* to create VLANs *vlan-id1* through *vlan-id2*, except reserved VLANs.

Use **vlan all** to create VLANs 1 through 4094.

Use **undo vlan** to delete the specified VLANs.

Syntax

vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

undo vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

Default

VLAN 1 (system default VLAN) exists.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

vlan-id1: Specifies a VLAN ID in the range of 1 to 4094.

vlan-id1 **to** *vlan-id2*: Specifies a VLAN range. The *vlan-id1* and *vlan-id2* arguments specify VLAN IDs. The value range for each of the two arguments is 1 to 4094. The value for the *vlan-id2* argument must be equal to or greater than the value for the *vlan-id1* argument.

all: Specifies all VLANs except reserved VLANs. The keyword is not supported when the maximum number of VLANs that can be created on a device is less than 4094.

Usage guidelines

You cannot create or delete the system default VLAN (VLAN 1) or reserved VLANs.

Before you delete a dynamic VLAN or a VLAN locked by an application, you must first remove the configuration from the VLAN.

Examples

Create VLAN 2 and enter its view.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2]
```

Create VLANs 4 through 100.

```
<Sysname> system-view
[Sysname] vlan 4 to 100
```

Related commands

display vlan

Port-based VLAN commands

display port

Use **display port** to display information about hybrid or trunk ports.

Syntax

display port { **hybrid** | **trunk** }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

hybrid: Specifies hybrid ports.

trunk: Specifies trunk ports.

Examples

Display information about hybrid ports.

```
<Sysname> display port hybrid
Interface            PVID  VLAN Passing
GE1/0/1              100   Tagged:  1000, 1002, 1500, 1600-1611, 2000,
                                    2555-2558, 3000, 4000
                           Untagged:1, 10, 15, 18, 20-30, 44, 55, 67, 100,
                                    150-160, 200, 255, 286, 300-302
```

Display information about trunk ports.

```
<Sysname> display port trunk
Interface            PVID  VLAN Passing
GE1/0/2              2     1-4, 6-100, 145, 177, 189-200, 244, 289, 400,
                           555, 600-611, 1000, 2006-2008
```

Table 4 Command output

Field	Description
Interface	Interface name.
PVID	Port VLAN ID.
VLAN Passing	Existing VLANs allowed on the port.
Tagged	VLANs from which the port sends packets without removing VLAN tags.
Untagged	VLANs from which the port sends packets after removing VLAN tags.

port

Use **port** to assign the specified access ports to a VLAN.

Use **undo port** to remove the specified access ports from a VLAN.

Syntax

port *interface-list*

undo port *interface-list*

Default

All ports are in VLAN 1.

Views

VLAN view

Predefined user roles

network-admin

context-admin

Parameters

interface-list: Specifies a space-separated list of up to 10 Ethernet interface items. Each item specifies an Ethernet interface or a range of Ethernet interfaces in the form of *interface-type interface-number1* **to** *interface-type interface-number2*. The value for the

interface-number2 argument must be equal to or greater than the value for the *interface-number1* argument.

Usage guidelines

This command is applicable only to access ports. This command cannot assign access ports to or remove access ports from VLAN 1.

By default, all ports are access ports. You can manually configure the port link type. For more information, see "port link-type."

Examples

Assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/2 to VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] port gigabitethernet 1/0/1 to gigabitethernet 1/0/2
```

Related commands

display vlan

port access vlan

Use **port access vlan** to assign an access port to the specified VLAN.

Use **undo port access vlan** to restore the default.

Syntax

port access vlan *vlan-id*

undo port access vlan

Default

All access ports belong to VLAN 1.

Views

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

context-admin

Parameters

vlan-id: Specifies a VLAN by its ID in the range of 1 to 4094.

Usage guidelines

By default, all access ports belong to VLAN 1. Therefore, this command cannot be used to assign access ports to VLAN 1. To move an access port to VLAN 1, execute the **undo port access vlan** command on the access port.

Before assigning an access port to a VLAN, make sure the VLAN has been created.

Examples

Assign GigabitEthernet 1/0/1 to VLAN 3.

```
<Sysname> system-view
[Sysname] vlan 3
[Sysname-vlan3] quit
```

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port access vlan 3
```

port hybrid pvid

Use **port hybrid pvid** to set the PVID of a hybrid port.

Use **undo port hybrid pvid** to set the PVID of a hybrid port to 1.

Syntax

port hybrid pvid vlan *vlan-id*

undo port hybrid pvid

Default

The PVID of a hybrid port is the ID of the VLAN to which the port belongs when its link type is **access**.

Views

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

context-admin

Parameters

vlan-id: Specifies a VLAN by its ID in the range of 1 to 4094.

Usage guidelines

You can use a nonexistent VLAN as the PVID of a hybrid port. When you delete the PVID of a hybrid port by using the **undo vlan** command, the PVID setting of the port does not change.

For correct packet transmission, set the same PVID for a local hybrid port and its peer.

To enable a hybrid port to transmit packets from its PVID, you must assign the hybrid port to the PVID by using the **port hybrid vlan** command.

Examples

Configure GigabitEthernet 1/0/1 as a hybrid port, set its PVID to VLAN 100, and assign it to VLAN 100 as an untagged member.

```
<Sysname> system-view
[Sysname] vlan 100
[Sysname-vlan100] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type hybrid
[Sysname-GigabitEthernet1/0/1] port hybrid pvid vlan 100
[Sysname-GigabitEthernet1/0/1] port hybrid vlan 100 untagged
```

Related commands

port hybrid vlan

port link-type

port hybrid vlan

Use **port hybrid vlan** to assign a hybrid port to the specified VLANs.

Use **undo port hybrid vlan** to remove a hybrid port from the specified VLANs.

Syntax

port hybrid vlan *vlan-id-list* { **tagged** | **untagged** }

undo port hybrid vlan *vlan-id-list*

Default

A hybrid port is an untagged member of the VLAN to which the port belongs when its link type is **access**.

Views

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

context-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN ID or a range of VLAN IDs in the form of *vlan-id1* **to** *vlan-id2*. The value range for VLAN IDs is 1 to 4094. The value for the *vlan-id2* argument must be equal to or greater than the value for the *vlan-id1* argument. The specified VLANs must already exist on the device.

tagged: Configures the port as a tagged member of the specified VLANs. A tagged member of a VLAN sends packets from the VLAN without removing VLAN tags.

untagged: Configures the port as an untagged member of the specified VLANs. An untagged member of a VLAN sends packets from the VLAN after removing VLAN tags.

Usage guidelines

A hybrid port can allow multiple VLANs. If you execute this command multiple times on a hybrid port, the hybrid port allows all the specified VLANs.

Examples

Configure GigabitEthernet 1/0/1 as a hybrid port, and assign it to VLAN 2, VLAN 4, and VLAN 50 through VLAN 100 as a tagged member.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type hybrid
[Sysname-GigabitEthernet1/0/1] port hybrid vlan 2 4 50 to 100 tagged
```

Related commands

port link-type

port link-type

Use **port link-type** to set the link type of a port.

Use **undo port link-type** to restore the default link type of a port.

Syntax

port link-type { **access** | **hybrid** | **trunk** }

undo port link-type

Default

Each port is an access port.

Views

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

context-admin

Parameters

access: Sets the port link type to access.

hybrid: Sets the port link type to hybrid.

trunk: Sets the port link type to trunk.

Usage guidelines

To change the link type of a port from trunk to hybrid or vice versa, first set the link type to access.

Examples

Configure GigabitEthernet 1/0/1 as a trunk port.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk
```

port trunk permit vlan

Use **port trunk permit vlan** to assign a trunk port to the specified VLANs.

Use **undo port trunk permit vlan** to remove a trunk port from the specified VLANs.

Syntax

port trunk permit vlan { *vlan-id-list* | **all** }

undo port trunk permit vlan { *vlan-id-list* | **all** }

Default

A trunk port allows packets only from VLAN 1 to pass through.

Views

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

context-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN ID or a range of VLAN IDs in the form of *vlan-id1* **to** *vlan-id2*. The value range for VLAN IDs is 1 to 4094. The value for the *vlan-id2* argument must be equal to or greater than the value for the *vlan-id1* argument.

all: Specifies all VLANs. To prevent unauthorized VLAN users from accessing restricted resources through the port, use the **port trunk permit vlan all** command with caution.

Usage guidelines

A trunk port can allow multiple VLANs. If you execute this command multiple times on a trunk port, the trunk port allows all the specified VLANs.

On a trunk port, packets only from the PVID can pass through untagged.

Examples

Configure GigabitEthernet 1/0/1 as a trunk port, and assign it to VLAN 2, VLAN 4, and VLAN 50 through VLAN 100.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk
[Sysname-GigabitEthernet1/0/1] port trunk permit vlan 2 4 50 to 100
```

Related commands

port link-type

port trunk pvid

Use **port trunk pvid** to set the PVID for a trunk port.

Use **undo port trunk pvid** to restore the default.

Syntax

port trunk pvid vlan *vlan-id*

undo port trunk pvid

Default

The PVID of a trunk port is VLAN 1.

Views

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

context-admin

Parameters

vlan-id: Specifies a VLAN by its ID in the range of 1 to 4094.

Usage guidelines

You can use a nonexistent VLAN as the PVID for a trunk port. When you delete the PVID of a trunk port by using the **undo vlan** command, the PVID setting of the port does not change.

For correct packet transmission, set the same PVID for a local trunk port and its peer.

To enable a trunk port to transmit packets from its PVID, you must assign the trunk port to the PVID by using the **port trunk permit vlan** command.

Examples

Configure GigabitEthernet 1/0/1 as a trunk, set its PVID to VLAN 100, and assign it to VLAN 100.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk
[Sysname-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Sysname-GigabitEthernet1/0/1] port trunk permit vlan 100
```

Related commands

port link-type

port trunk permit vlan

VLAN group commands

display vlan-group

Use **display vlan-group** to display VLAN group information.

Syntax

display vlan-group [*group-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

group-name: Specifies a VLAN group by its name, a case-sensitive string of 1 to 31 characters. The first character must be an alphabetical character. If you do not specify this argument, the command displays information about all VLAN groups.

Examples

Display information about VLAN group **test001**.

```
<Sysname> display vlan-group test001
VLAN group: test001
     VLAN list: 2-4 100 200
```

Display information about all VLAN groups.

```
<Sysname> display vlan-group
VLAN group: rnd
     VLAN list: Null
VLAN group: test001
     VLAN list: 2-4 100 200
```

Table 5 Command output

Field	Description
VLAN group	Name of the VLAN group.
VLAN list	VLAN list in the VLAN group.

Related commands

vlan-group

vlan-list

vlan-group

Use **vlan-group** to create a VLAN group and enter its view, or enter the view of an existing VLAN group.

Use **undo vlan-group** to delete a VLAN group.

Syntax

vlan-group *group-name*

undo vlan-group *group-name*

Default

No VLAN groups exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a VLAN group by its name, a case-sensitive string of 1 to 31 characters. The first character must be an alphabetical character.

Usage guidelines

A VLAN group includes a set of VLANs. You can add multiple VLAN lists to a VLAN group.

Examples

Create a VLAN group named **test001** and enter VLAN group view.

```
<Sysname> system-view
[Sysname] vlan-group test001
[Sysname-vlan-group-test001]
```

Related commands

vlan-list

vlan-list

Use **vlan-list** to add VLANs to a VLAN group.

Use **undo vlan-list** to remove VLANs from a VLAN group.

Syntax

vlan-list *vlan-id-list*

undo vlan-list *vlan-id-list*

Default

No VLANs exist in a VLAN group.

Views

VLAN group view

Predefined user roles

network-admin

context-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN ID or a range of VLAN IDs in the form of *vlan-id1* **to** *vlan-id2*. The value range for VLAN IDs is 1 to 4094. The value for the *vlan-id2* argument must be equal to or greater than the value for the *vlan-id1* argument.

Examples

Add VLAN 2 through VLAN 4, VLAN 100, and VLAN 200 to VLAN group **test001**.

```
<Sysname> system-view
[Sysname] vlan-group test001
[Sysname-vlan-group-test001] vlan-list 2 to 4 100 200
```

Related commands

vlan-group

Contents

VLAN termination commands

dot1q ethernet-type

Use **dot1q ethernet-type** to set the TPID value in the outermost VLAN tag of packets received and sent by an interface.

Use **undo dot1q ethernet-type** to restore the default.

Syntax

dot1q ethernet-type *hex-value*

undo dot1q ethernet-type

Default

The TPID value for the outermost VLAN tag of a VLAN-tagged packet received and sent by the interface is 0x8100.

Views

Layer 3 aggregate/Ethernet interface view

Reth interface view

Predefined user roles

network-admin

context-admin

Parameters

hex-value: Sets a hexadecimal TPID value in the range of 600 to ffff, excluding the common protocol type values listed in Table 1.

Table 1 Common protocol type values

Protocol	Value
ARP	0x0806
PUP	0x0200
RARP	0x8035
IP	0x0800
IPv6	0x86DD
PPPoE	0x8863/0x8864
IPX/SPX	0x8137
IS-IS	0x8000
LACP	0x8809
LLDP	0x88CC
802.1ag	0x8902
Cluster	0x88A7
Reserved on the device	0xFFFD/0xFFFE/0xFFFF

Usage guidelines

After you execute this command, only packets whose TPID in the outermost VLAN tag is 0x8100 or the configured value are processed as VLAN-tagged packets. When sending a packet, the interface sets the TPID value in the outermost VLAN tag to the configured value. If the packet includes two or more layers of VLAN tags, the interface sets the TPID values in the other VLAN tags to 0x8100.

Do not use this command in subinterface view.

Configurations made in interface view take effect on all subinterfaces of the interface.

Examples

Set the TPID value to 0x9100 in the outermost VLAN tag of VLAN-tagged packets received and sent by the subinterfaces of GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1q ethernet-type 9100
```

vlan-termination broadcast enable

Use **vlan-termination broadcast enable** to enable an interface to transmit broadcasts and multicasts.

Use **undo vlan-termination broadcast enable** to disable an interface from transmitting broadcasts and multicasts.

Syntax

vlan-termination broadcast enable

undo vlan-termination broadcast enable

Default

An ambiguous Dot1q termination-enabled interface drops broadcast and multicast packets.

Views

Layer 3 Ethernet subinterface view

Layer 3 aggregate subinterface view

Reth subinterface view

Predefined user roles

network-admin

context-admin

Usage guidelines

IMPORTANT:

This command affects system performance. If system performance is seriously affected by this command, execute the **undo** form of this command to remove the command configuration.

.To transmit a broadcast or multicast packet, the interface starts a traversal over the VLAN IDs specified for ambiguous termination. It copies the packet and tags each copy with a VLAN ID, until all VLAN IDs in the specified range are traversed.

Use this command when ambiguous Dot1q termination is enabled on an interface.

Examples

Configure GigabitEthernet 1/0/1.10 to tag a multicast or broadcast packet with each VLAN tag in the range of 10 to 20.

Enable Dot1q termination on GigabitEthernet 1/0/1.10 to terminate VLAN-tagged packets with outermost VLAN IDs in the range of 10 to 20.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1.10
[Sysname-GigabitEthernet1/0/1.10] vlan-type dot1q vid 10 to 20
```

Enable GigabitEthernet 1/0/1.10 to transmit broadcast and multicast packets.

```
[Sysname-GigabitEthernet1/0/1.10] vlan-termination broadcast enable
```

vlan-termination broadcast ra

Use **vlan-termination broadcast ra** to enable an interface to transmit router advertisement (RA) multicast packets.

Use **undo vlan-termination broadcast ra** to disable an interface from transmitting RA multicast packets.

Syntax

vlan-termination broadcast ra

undo vlan-termination broadcast ra

Default

An ambiguous Dot1q termination-enabled interface drops broadcast and multicast packets.

Views

Layer 3 Ethernet subinterface view

Layer 3 aggregate subinterface view

Reth subinterface view

Predefined user roles

network-admin

context-admin

Usage guidelines

To transmit an RA multicast packet, the interface starts a traversal over the VLAN IDs specified for ambiguous termination. It copies the packet and tags each copy with a VLAN ID, until all VLAN IDs in the specified range are traversed.

As a best practice, use this command to enable an ambiguous Dot1q termination-enabled interface to transmit RA multicast packets on an IPv6 network. This command prohibits transmission of broadcast packets and other types of multicast packets, and consumes less CPU resources than the **vlan-termination broadcast enable** command.

Examples

Configure GigabitEthernet 1/0/1.10 to tag RA multicast packets with each VLAN tag in the range of 10 to 20.

Enable Dot1q termination on GigabitEthernet 1/0/1.10 to terminate VLAN-tagged packets with outermost VLAN IDs in the range of 10 to 20.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1.10
[Sysname-GigabitEthernet1/0/1.10] vlan-type dot1q vid 10 to 20
```

Enable GigabitEthernet 1/0/1.10 to transmit RA multicast packets.

```
[Sysname-GigabitEthernet1/0/1.10] vlan-termination broadcast ra
```

vlan-type dot1q default

Use **vlan-type dot1q default** to enable default termination on a subinterface.

Use **undo vlan-type dot1q default** to disable default termination on a subinterface.

Syntax

vlan-type dot1q default

undo vlan-type dot1q default

Default

Default termination is disabled on a subinterface.

Views

Layer 3 Ethernet subinterface view

Layer 3 aggregate subinterface view

Reth subinterface view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command enables the subinterface to process packets that cannot be terminated by other subinterfaces on the same main interface.

Examples

Enable default termination on GigabitEthernet 1/0/1.1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1.1
[Sysname-GigabitEthernet1/0/1.1] vlan-type dot1q default
[Sysname-GigabitEthernet1/0/1.1] quit
```

vlan-type dot1q untagged

Use **vlan-type dot1q untagged** to enable untagged termination on a subinterface.

Use **undo vlan-type dot1q untagged** to disable untagged termination on a subinterface.

Syntax

vlan-type dot1q untagged

undo vlan-type dot1q untagged

Default

Untagged termination is disabled on a subinterface.

Views

Layer 3 Ethernet subinterface view

Layer 3 aggregate subinterface view

Reth subinterface view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command enables the subinterface to process untagged packets.

Examples

Enable untagged termination on GigabitEthernet 1/0/1.1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1.1
[Sysname-GigabitEthernet1/0/1.1] vlan-type dot1q untagged
[Sysname-GigabitEthernet1/0/1.1] quit
```

vlan-type dot1q vid

Use **vlan-type dot1q vid** to enable Dot1q termination on a subinterface, and specify the outermost VLAN IDs in the VLAN-tagged packets that can be terminated by the subinterface.

Use **undo vlan-type dot1q vid** to disable Dot1q termination on a subinterface.

Syntax

vlan-type dot1q vid *vlan-id-list*

undo vlan-type dot1q vid *vlan-id-list*

Default

Dot1q termination is disabled on a subinterface.

Views

Layer 3 Ethernet subinterface view

Layer 3 aggregate subinterface view

Reth subinterface view

Predefined user roles

network-admin

context-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 10 outermost VLAN ID items. Each item specifies an outermost VLAN ID or a range of outermost VLAN IDs in the form of *vlan-id1* **to** *vlan-id2*. The value range for VLAN IDs is 1 to 4094. The value for the *vlan-id2* argument must be equal to or greater than the value for the *vlan-id1* argument.

Usage guidelines

The VLAN ID ranges specified by the *vlan-id-list* argument for different subinterfaces of a main interface cannot overlap.

Examples

Configure GigabitEthernet 1/0/1.1 to terminate VLAN-tagged packets with outermost VLAN IDs in the range of 2 to 100.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1.1
```

```
[Sysname-GigabitEthernet1/0/1.1] vlan-type dot1q vid 2 to 100
```

Contents

Spanning tree commands

active region-configuration

Use **active region-configuration** to activate your MST region configuration.

Syntax

active region-configuration

Views

MST region view

Predefined user roles

network-admin

context-admin

Usage guidelines

When you configure MST region parameters, MSTP launches a new spanning tree calculation process that might cause network topology instability. This is most likely to occur when you configure the VLAN-to-instance mapping table. The launch occurs after you execute the **active region-configuration** command or the **stp global enable** command.

As a best practice, use the **check region-configuration** command to determine whether the MST region configurations to be activated are correct. Run this command only when they are correct.

Examples

Map VLAN 2 to MSTI 1 and activate the MST region configuration.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] instance 1 vlan 2
[Sysname-mst-region] active region-configuration
```

Related commands

check region-configuration

instance

region-name

revision-level

stp global enable

vlan-mapping modulo

check region-configuration

Use **check region-configuration** to display MST region pre-configuration information.

Syntax

check region-configuration

Views

MST region view

Predefined user roles

network-admin

context-admin

Usage guidelines

Spanning tree devices belong to the same MST region only when they are connected through a physical link and configured with the same details as follows:

- Format selector (0 by default and not configurable).
- MST region name.
- MST region revision level.
- VLAN-to-instance mapping entries in the MST region.

As a best practice, use this command to determine whether the MST region configurations to be activated are correct. Activate them only when they are correct.

Examples

Display MST region pre-configurations.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] check region-configuration
 Admin Configuration
   Format selector      : 0
   Region name          : 001122334400
   Revision level       : 0
   Configuration digest : 0x3ab68794d602fdf43b21c0b37ac3bca8

   Instance  VLANs Mapped
   0         1, 3 to 4094
   15        2
```

Table 1 Command output

Field	Description
Format selector	Format selector of the MST region, which is 0 (not configurable).
Region name	MST region name.
Revision level	Revision level of the MST region.
Instance VLANs Mapped	VLAN-to-instance mappings in the MST region.

Related commands

active region-configuration

instance

region-name

revision-level

vlan-mapping modulo

display stp

Use **display stp** to display spanning tree status and statistics.

Syntax

display stp [**instance** *instance-list* | **vlan** *vlan-id-list*] [**interface** *interface-list* | **slot** *slot-number*] [**brief**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

instance *instance-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

interface *interface-list*: Specifies a space-separated list of up to 10 interface items. Each item specifies an interface or a range of interfaces in the form of *interface-type interface-number 1* [**to** *interface-type interface-number 2*]. The interface number for *interface-number 2* must be equal to or greater than the interface number for *interface-number 1*.

brief: Displays brief spanning tree status and statistics. If this keyword is not specified, the command displays detailed spanning tree status and statistics.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all member devices.

Usage guidelines

In STP or RSTP mode, the command output is sorted by port name.

- If you do not specify a port, this command applies to all ports.
- If you specify a port list, this command applies to the specified ports.

In PVST mode, the command output is sorted by VLAN ID and by port name in each VLAN.

- If you do not specify a VLAN or port, this command applies to all ports in all VLANs.
- If you only specify a VLAN list but not a port, this command applies to all ports in the specified VLANs.
- If you only specify a port list but not a VLAN, this command applies to the specified ports in all VLANs.
- If you specify both a VLAN list and a port list, this command applies to the ports in the specified VLANs.

In MSTP mode, the command output is sorted by MSTI ID and by port name in each MSTI.

- If you do not specify an MSTI or port, this command applies to all MSTIs on all ports.
- If you specify an MSTI list but not a port, this command applies to all ports in the specified MSTIs.

- If you specify a port list but not an MSTI, this command applies to all MSTIs on the specified ports.
- If you specify both an MSTI list and a port list, this command applies to the specified ports in the specified MSTIs.

Examples

In MSTP mode, display the brief spanning tree status and statistics for MSTI 0 on port GigabitEthernet 1/0/1.

```
<Sysname> display stp instance 0 interface GigabitEthernet 1/0/1 brief
 MST ID      Port                        Role  STP State     Protection
 0           0           GigabitEthernet1/0/1         ALTE  DISCARDING    LOOP
```

In PVST mode, display the brief spanning tree status and statistics for VLAN 2 on port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] stp mode pvst
[Sysname] display stp vlan 2 interface gigabitethernet 1/0/1 brief
 VLAN ID     Port                        Role  STP State     Protection
 2           GigabitEthernet1/0/1        ALTE  DISCARDING    LOOP
```

Table 2 Command output

Field	Description
MST ID	MSTI ID in the MST region.
Port	Port name, corresponding to each MSTI or VLAN.
Role	Port role: • **ALTE**—The port is an alternate port. • **BACK**—The port is a backup port. • **ROOT**—The port is a root port. • **DESI**—The port is a designated port. • **MAST**—The port is a master port. • **DISA**—The port is disabled.
STP State	Spanning tree status on the port: • **FORWARDING**—The port can receive and send BPDUs and also forward user traffic. • **DISCARDING**—The port can receive and send BPDUs but cannot forward user traffic. • **LEARNING**—The port is in a transitional state. It can receive and send BPDUs but cannot forward user traffic.
Protection	Effective spanning tree protection feature on the port: • **ROOT**—Root guard. • **LOOP**—Loop guard. • **BPDU**—BPDU guard. If no spanning tree protection feature is configured or spanning tree protection is not triggered, this field displays **NONE**.

In MSTP mode, display the detailed spanning tree status and statistics for all MSTIs on all ports.

```
<Sysname> display stp
-------[CIST Global Info][Mode MSTP]-------
 Bridge ID           : 32768.0001-0000-0000
 Bridge times        : Hello 2s MaxAge 20s FwdDelay 15s MaxHops 20
 Root ID/ERPC        : 32768.0001-0000-0000, 0
```

```
 RegRoot ID/IRPC     : 32768.0001-0000-0000, 0
 RootPort ID         : 0.0
 BPDU-Protection     : Disabled
 Bridge Config-
 Digest-Snooping     : Disabled
 TC or TCN received  : 2
 Time since last TC  : 0 days 0h:0m:58s

----[Port1(GigabitEthernet1/0/1)][FORWARDING]----
 Port protocol       : Enabled
 Port role           : Designated Port (Boundary)
 Port ID             : 128.3
 Port cost(Legacy)   : Config=auto, Active=200
 Desg.bridge/port    : 32768.0001-0000-0000, 128.3
 Port edged          : Config=disabled, Active=disabled
 Point-to-Point      : Config=auto, Active=true
 Transmit limit      : 10 packets/hello-time
 TC-Restriction      : Disabled
 Role-Restriction    : Disabled
 Protection type     : Config=none, Active=none
 MST BPDU format     : Config=auto, Active=802.1s
 Port Config-
 Digest-Snooping     : Disabled
 Rapid transition    : True
 Num of VLANs mapped : 0
 Port times          : Hello 2s MaxAge 20s FwdDelay 15s MsgAge 0s RemHops 20
 BPDU sent           : 32
          TCN: 0, Config: 0, RST: 0, MST: 32
 BPDU received       : 2
          TCN: 0, Config: 0, RST: 0, MST: 2

-------[MSTI 1 Global Info]-------
 Bridge ID           : 32768.0001-0000-0000
 RegRoot ID/IRPC     : 32768.0001-0000-0000, 0
 RootPort ID         : 0.0
 Master bridge       : 32768.0001-0000-0000
 Cost to master      : 0
 TC received         : 0

----[Port1(GigabitEthernet1/0/1)][FORWARDING]----
 Port protocol       : Enabled
 Port role           : Designated Port (Boundary)
 Port ID             : 128.3
 Port cost(Legacy)   : Config=auto, Active=200
 Desg.bridge/port    : 32768.0001-0000-0000, 128.3
 Protection type     : Config=none, Active=none
 Rapid transition    : True
 Num of VLANs mapped : 64
```

```
 Port times          : RemHops 20
```

In PVST mode, display the spanning tree status and statistics for all ports in all VLANs.

```
<Sysname> system-view
[Sysname] stp mode pvst
[Sysname] display stp
-------[VLAN 1 Global Info]-------
Protocol status     : Enabled
Bridge ID           : 32768.000f-e200-2200
Bridge times        : Hello 2s MaxAge 20s FwdDelay 15s
VlanRoot ID/RPC     : 0.00e0-fc0e-6554, 200200
RootPort ID         : 128.48
BPDU-Protection     : Disabled
TC or TCN received  : 2
Time since last TC  : 0 days 0h:5m:42s

 ----[Port1(GigabitEthernet1/0/1)][FORWARDING]----
 Port protocol       : Enabled
 Port role           : Designated Port
 Port ID             : 128.153
 Port cost(Legacy)   : Config=auto, Active=200
 Desg. bridge/port   : 32768.000f-e200-2200, 128.2
 Port edged          : Config=disabled, Active=disabled
 Point-to-Point      : Config=auto, Active=true
 Transmit limit      : 10 packets/hello-time
 Protection type     : Config=none, Active=none
 Rapid transition    : False
 Port times          : Hello 2s MaxAge 20s FwdDelay 15s MsgAge 2s

-------[VLAN 2 Global Info]-------
Protocol status      : Enabled
Bridge ID            : 32768.000f-e200-2200
Bridge times         : Hello 2s MaxAge 20s FwDly 15s
VlanRoot ID/RPC      : 0.00e0-fc0e-6554, 200200
RootPort ID          : 128.48
BPDU-Protection      : Disabled
TC or TCN received   : 2
Time since last TC   : 0 days 0h:5m:42s
```

In MSTP mode, display the spanning tree status and statistics when the spanning tree feature is disabled.

```
<Sysname> display stp
 Protocol status    : Disabled
 Protocol Std.      : IEEE 802.1s
 Version            : 3
 Bridge-Prio.       : 32768
 MAC address        : 000f-e200-8048
 Max age(s)         : 20
 Forward delay(s)   : 15
 Hello time(s)      : 2
```

```
 Max hops           : 20
 TC Snooping        : Disabled
```

In PVST mode, display the spanning tree status and statistics when the spanning tree feature is disabled.

```
<Sysname> display stp
 Protocol status    : Disabled
 Protocol Std.      : IEEE 802.1w (pvst)
 Version            : 2
 Bridge-Prio.       : 32768
 MAC address        : 3822-d69f-0800
 Max age(s)         : 20
 Forward delay(s)   : 15
 Hello time(s)      : 2
 TC Snooping        : Disabled
```

Table 3 Command output

Field	Description
Bridge ID	Bridge ID, which contains the device's priority and its MAC address. For example, in output 32768.000f-e200-2200, the value preceding the dot is the device's priority. The value following the dot is the device's MAC address.
Bridge times	Major parameters for the bridge: • **Hello**—Hello timer. • **MaxAge**—Maximum age timer. • **FwdDelay**—Forward delay timer. • **MaxHops**—Maximum hops within the MST region.
Root ID/ERPC	CIST root ID and external path cost (the path cost from the device to the CIST root).
RegRoot ID/IRPC	CIST regional root ID and internal path cost (the path cost from the device to the CIST regional root).
VlanRoot ID/RPC	VLAN root ID and root path cost (the path cost from the device to the VLAN root bridge).
RootPort ID	Root port ID. The value **0.0** indicates that the device is the root and there is no root port.
BPDU-Protection	Global status of the BPDU guard feature.
Bridge Config-Digest-Snooping	Global status of Digest Snooping.
TC or TCN received	Number of TC/TCN BPDUs received in the MSTI or VLAN.
Time since last TC	Time since the latest topology change in the MSTI or VLAN.
Port protocol	Status of the spanning tree feature on the port.
Port role	Port role: • Alternate. • Backup. • Root. • Designated. • Master. • Disabled.
(Boundary)	The port is a regional boundary port.

Field	Description
Port cost(Legacy)	Path cost of the port. The field in parentheses indicates the standard (legacy, dot1d-1998, or dot1t) used for port path cost calculation. • **Config**—Configured value. • **Active**—Actual value.
Desg.bridge/port	Designated bridge ID and port ID of the port. The port ID displayed is insignificant for a port which does not support port priority.
Port edged	The port is an edge port or non-edge port. • **Config**—Configured value. • **Active**—Actual value.
Point-to-Point	The port is connected to a point-to-point link or not. • **Config**—Configured value. • **Active**—Actual value.
Transmit limit	Maximum number of BPDUs sent by a port within each hello time.
Protection type	Whether spanning tree protection is configured on the port: • **Config**—Configured spanning tree protection feature. • **Active**—Effective spanning tree protection feature. Spanning tree protection features are as follows: • **ROOT**—Root guard. • **LOOP**—Loop guard. • **BPDU**—BPDU guard. • **PVST BPDU**—PVST BPDU guard. If no spanning tree protection feature is configured or spanning tree protection is not triggered, this field displays **NONE**.
TC-Restriction	Status of TC transmission restriction on the port.
Role-Restriction	Status of port role restriction on the port.
MST BPDU format	Format of the MST BPDUs that the port can send: • **Config**—Configured value (legacy or 802.1s). • **Active**—Actual value (legacy or 802.1s).
Port Config-Digest-Snooping	Status of Digest Snooping on the port.
Rapid transition	Indicates whether the port rapidly transits to the forwarding state in the MSTI or VLAN.
Num of VLANs mapped	Number of VLANs that are mapped to the MSTI.
Port times	Major parameters for the port: • **Hello**—Hello timer. • **MaxAge**—Maximum age timer. • **FwdDelay**—Forward delay timer. • **MsgAge**—Message age timer. • **RemHops**—Remaining hops.
BPDU sent	Statistics on sent BPDUs.
BPDU received	Statistics on received BPDUs.
RegRoot ID/IRPC	MSTI regional root/internal path cost.
Root Type	MSTI root type:

Field	Description
	• **Primary root**. • **Secondary root**.
Master bridge	MSTI root bridge ID.
Cost to master	Path cost from the MSTI to the master bridge.
TC received	Number of received TC BPDUs.
Protocol status	Spanning tree protocol status.
Protocol Std.	Spanning tree protocol standard.
Version	Spanning tree protocol version.
Bridge-Prio.	In MSTP mode: Device's priority in the CIST. In PVST mode: Device's priority in VLAN 1.
Max age(s)	Aging timer for BPDUs (in seconds, which is the same as the aging timer for VLAN 1 in PVST mode).
Forward delay(s)	Port state transition delay (in seconds, which is the same as the port state transition delay for VLAN 1 in PVST mode).
Hello time(s)	Interval for the root bridge to send BPDUs (in seconds, which is the same as the interval for VLAN 1 in PVST mode).
Max hops	Maximum hops in the MSTI.
TC Snooping	Status of TC Snooping: **Enabled** or **Disabled**.

Related commands

`reset stp`

display stp abnormal-port

Use **`display stp abnormal-port`** to display information about ports that are blocked by spanning tree protection features.

Syntax

`display stp abnormal-port`

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

In MSTP mode, display information about ports that are blocked by spanning tree protection features.

```
<Sysname> display stp abnormal-port
 MST ID      Blocked Port                Reason
 1           GigabitEthernet1/0/1        Root-Protected
```

```
 2           GigabitEthernet1/0/2         Loop-Protected
 12          GigabitEthernet1/0/3         Loopback-Protected
```

In PVST mode, display information about ports that are blocked by spanning tree protection features.

```
<Sysname> system-view
[Sysname] stp mode pvst
[Sysname] display stp abnormal-port
 VLAN ID      Blocked Port                 Reason
 1            GigabitEthernet1/0/1         Root-Protected
 2            GigabitEthernet1/0/2         Loop-Protected
 2            GigabitEthernet1/0/3         Loopback-Protected
```

Table 4 Command output

Field	Description
MST ID	MSTI of a blocked port.
VLAN ID	VLAN of a blocked port.
Blocked Port	Name of a blocked port.
BlockReason	Reason that the port was blocked: • **Root-Protected**—Root guard feature. • **Loop-Protected**—Loop guard feature. • **Loopback-Protected**—Self-loop protection. A port in the MSTI receives a BPDU sent by itself. • **Disputed**—Dispute guard. A port receives a low-priority BPDU from a non-blocked designated port in forwarding or learning state. • **InconsistentPortType-Protected**—Inconsistent port type protection. • **InconsistentPvid-Protected**—Inconsistent PVID protection.

display stp bpdu-statistics

Use **display stp bpdu-statistics** to display the BPDU statistics for ports.

Syntax

display stp bpdu-statistics [**interface** *interface-type interface-number* [**instance** *instance-list*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number.

instance *instance-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

Usage guidelines

In MSTP mode, the command output is sorted by port name and by MSTI ID on each port.

- If you do not specify an MSTI or port, this command applies to all MSTIs on all ports.
- If you specify a port but not an MSTI, this command applies to all MSTIs on the port.
- If you specify both an MSTI ID and a port, this command applies to the specified MSTI on the port.

In STP, PVST, or RSTP mode, the command output is sorted by port name.

- If you do not specify a port, this command applies to all ports.
- If you specify a port, this command applies to the port.

Examples

In MSTP mode, display the BPDU statistics for all MSTIs on GigabitEthernet 1/0/1.

```
<Sysname> display stp bpdu-statistics interface gigabitethernet 1/0/1
 Port: GigabitEthernet1/0/1

 Instance-Independent:

 Type                        Count      Last Updated
 --------------------------- ---------- -----------------
 Invalid BPDUs               0
 Looped-back BPDUs           0
 Max-aged BPDUs              0
 TCN sent                    0
 TCN received                0
 TCA sent                    0
 TCA received                2          10:33:12 01/13/2011
 Config sent                 0
 Config received             0
 RST sent                    0
 RST received                0
 MST sent                    4          10:33:11 01/13/2011
 MST received                151        10:37:43 01/13/2011

 Instance 0:
 Type                        Count      Last Updated
 --------------------------- ---------- -----------------
 Timeout BPDUs               0
 Max-hoped BPDUs             0
 TC detected                 1          10:32:40 01/13/2011
 TC sent                     3          10:33:11 01/13/2011
 TC received                 0
```

In PVST mode, display the BPDU statistics for GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] stp mode pvst
```

```
[Sysname] display stp bpdu-statistics interface gigabitethernet 1/0/1
 Port: GigabitEthernet1/0/1

 Type                        Count      Last Updated
 --------------------------- ---------- -----------------
 Invalid BPDUs               0
 Looped-back BPDUs           0
 Max-aged BPDUs              0
 TCN sent                    0
 TCN received                0
 TCA sent                    0
 TCA received                2           10:33:12 01/13/2010
 Config sent                 0
 Config received             0
 RST sent                    0
 RST received                0
 MST sent                    4           10:33:11 01/13/2010
 MST received                151         10:37:43 01/13/2010
 Timeout BPDUs               0
 Max-hoped BPDUs             0
 TC detected                 511         10:32:40 01/13/2010
 TC sent                     8844        10:33:11 01/13/2010
 TC received                 1426        10:33:32 01/13/2010
 PVID inconsistency BPDUs    0
```

Table 5 Command output

Field	Description
Port	Port name.
Instance-Independent	Statistics not related to a specific MSTI.
Type	Statistical item.
Looped-back BPDUs	Number of BPDUs sent and then received by the same port.
Max-aged BPDUs	Number of BPDUs whose max age was exceeded.
TCN sent	Number of sent TCN BPDUs.
TCN received	Number of received TCN BPDUs.
TCA sent	Number of sent TCA BPDUs.
TCA received	Number of received TCA BPDUs.
Config sent	Number of sent configuration BPDUs.
Config received	Number of received configuration BPDUs.
RST sent	Number of sent RSTP BPDUs.
RST received	Number of received RSTP BPDUs.
MST sent	Number of sent MSTP BPDUs.
MST received	Number of received MSTP BPDUs.
Instance	Statistics for a specific MSTI.

Field	Description
Timeout BPDUs	Number of expired BPDUs.
Max-hoped BPDUs	Number of BPDUs whose maximum hops were exceeded.
TC detected	Number of detected topology changes.
TC sent	Number of sent TC BPDUs.
TC received	Number of received TC BPDUs.
PVID inconsistency BPDUs	Number of received PVST BPDUs with a PVID inconsistent with the incoming port.

display stp down-port

Use **display stp down-port** to display information about ports that were shut down by spanning tree protection features.

Syntax

display stp down-port

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display information about ports that were shut down by spanning tree protection features.

```
<Sysname> display stp down-port
 Down Port                      Reason
 GigabitEthernet1/0/1           BPDU protection
```

Table 6 Command output

Field	Description
Down Port	Name of a port that was shut down by the spanning tree protection features.
Reason	Reason that the port was shut down: • **BPDU protection**—Indicates the BPDU guard feature. • **PVST BPDU protection**—Indicates the PVST BPDU guard feature.

display stp history

Use **display stp history** to display port role calculation history.

Syntax

display stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **history** [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

instance *instance-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all member devices.

Usage guidelines

In STP or RSTP mode, the command output is sorted by port role calculation time.

In PVST mode, the command output is sorted by VLAN ID and by port role calculation time in each VLAN.

- If you do not specify a VLAN, this command applies to all VLANs.
- If you specify a VLAN list, this command applies to the specified VLANs.

In MSTP mode, the command output is sorted by MSTI ID and by port role calculation time in each MSTI.

- If you do not specify an MSTI, this command applies to all MSTIs.
- If you specify an MSTI list, this command applies to the specified MSTIs.

Examples

In STP mode, display the port role calculation history on the specified slot.

```
<Sysname> display stp history slot 1
 --------------- STP slot 1 history trace ---------------
 -------------------  Instance 0   ---------------------

 Port GigabitEthernet1/0/2
   Role change         : DESI->ALTE
   Time                : 2022/08/09 17:44:06
   Port priority       : 32768.36b5-6d1a-0300 0 32768.36b5-7829-0400 0
                         32768.36b5-6d1a-0300 128.3 128.3
   Designated priority : 32768.36b5-6d1a-0300 20 32768.36b5-7829-0400 0
                         32768.36b5-7829-0400 128.3 128.3

 Port GigabitEthernet1/0/1
   Role change         : DESI->ROOT
   Time                : 2022/08/09 17:44:06
```

```
   Port priority       : 32768.36b5-6d1a-0300 0 32768.36b5-7829-0400 0
                         32768.36b5-6d1a-0300 128.2 128.2
   Designated priority : 32768.36b5-6d1a-0300 20 32768.36b5-7829-0400 0
                         32768.36b5-7829-0400 128.2 128.2
```

In MSTP mode, display the port role calculation history on the specified slot in MSTI 2.

```
<Sysname> display stp instance 2 history slot 1
 -------------- STP slot 1 history trace ---------------
 ------------------  Instance 2   ---------------------

Port GigabitEthernet1/0/2
   Role change         : DESI->ALTE
   Time                : 2022/08/09 16:26:01
   Port priority       : 0.3085-b8b5-0100 0 0.3085-b8b5-0100 128.3 128.3
   Designated priority : 0.3085-b8b5-0100 20 32768.3085-bc3a-0200 128.3 128.3

Port GigabitEthernet1/0/1
   Role change         : DESI->ROOT
   Time                : 2022/08/09 16:26:01
   Port priority       : 0.3085-b8b5-0100 0 0.3085-b8b5-0100 128.2 128.2
   Designated priority : 0.3085-b8b5-0100 20 32768.3085-bc3a-0200 128.2 128.2
```

In PVST mode, display the port role calculation history on the specified slot in VLAN 2.

```
<Sysname> display stp vlan 2 history slot 1
 -------------- STP slot 1 history trace ---------------
 ------------------  VLAN 2   ---------------------

Port GigabitEthernet1/0/2
   Role change         : DESI->ALTE
   Time                : 2022/08/09 17:33:39
   Port priority       : 0.36b5-6d1a-0300 0 0.36b5-6d1a-0300 128.3 128.3
   Designated priority : 0.36b5-6d1a-0300 20 32768.36b5-7829-0400 128.3 128.3

 Port GigabitEthernet1/0/1
   Role change         : DESI->ROOT
   Time                : 2022/08/09 17:33:23
   Port priority       : 0.36b5-6d1a-0300 0 0.36b5-6d1a-0300 128.2 128.2
   Designated priority : 0.36b5-6d1a-0300 20 32768.36b5-7829-0400 128.2 128.2
```

Table 7 Command output

Field	Description
Port	Port name.
Role change	Role change of the port (**Aged** means that the change was caused by expiration of the received configuration BPDU).
Time	Time of port role calculation.
Port priority	Current priority of the port: • For STP mode, RSTP mode, and ISTs (MSTI 0) in MSTP mode, port priority includes common root bridge ID, cost of the path to the common root bridge, regional root bridge ID, cost of the path to the regional root bridge, designated bridge ID, designated port ID, and ID of the port that receives

Field	Description
	messages from the designated port, which are separated with spaces. • For PVST mode and CSTs in MSTP mode, port priority includes regional root bridge ID, cost of the path to the regional root bridge, designated bridge ID, designated port ID, and ID of the port that receives messages from the designated port, which are separated with spaces.
Designated priority	Priority information reported by the current port as a designated port: • For STP mode, RSTP mode, and ISTs (MSTI 0) in MSTP mode, port priority includes common root bridge ID, cost of the path to the common root bridge, regional root bridge ID, cost of the path to the regional root bridge, device bridge ID, designated port ID, and current port ID, which are separated with spaces. • For PVST mode and CSTs in MSTP mode, port priority includes regional root bridge ID, cost of the path to the regional root bridge, device bridge ID, designated port ID, and current port ID, which are separated with spaces.

display stp region-configuration

Use **display stp region-configuration** to display effective MST region configuration.

Syntax

display stp region-configuration

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

In MSTP mode, display effective MST region configuration.

```
<Sysname> display stp region-configuration
 Oper Configuration
   Format selector      : 0
   Region name          : hello
   Revision level       : 0
   Configuration digest : 0x5f762d9a46311effb7a488a3267fca9f

   Instance   VLANs Mapped
   0          21 to 4094
   1          1 to 10
   2          11 to 20
```

Table 8 Command output

Field	Description
Format selector	Format selector that is defined by the spanning tree protocol. The default value is 0, and the selector cannot be configured.

Field	Description
Region name	MST region name.
Revision level	Revision level of the MST region. The default value is 0, and the level can be configured by using the **revision-level** command.
VLANs Mapped	VLANs mapped to the MSTI.

Related commands

instance

region-name

revision-level

vlan-mapping modulo

display stp root

Use **display stp root** to display the root bridge information of spanning trees.

Syntax

display stp root

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

In MSTP mode, display the root bridge information of all spanning trees.

```
<Sysname> display stp root
 MST ID  Root Bridge ID        ExtPathCost IntPathCost Root Port
 0       0.00e0-fc0e-6554      200200      0           GigabitEthernet1/0/1
```

In PVST mode, display the root bridge information of all spanning trees.

```
<Sysname> display stp root
 VLAN ID  Root Bridge ID        ExtPathCost IntPathCost Root Port
 1        0.00e0-fc0e-6554      200200      0           GigabitEthernet1/0/1
```

Table 9 Command output

Field	Description
ExtPathCost	External path cost. The path cost of a port is either automatically calculated by the device or manually configured by using the **stp cost** command.
IntPathCost	Internal path cost. The path cost of a port is either automatically calculated by the device or manually configured by using the **stp cost** command.
Root Port	Root port name (displayed only if a port of the device is the root port of the MSTI).

display stp tc

Use **display stp tc** to display the incoming and outgoing TC/TCN BPDU statistics for ports.

Syntax

display stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **tc** [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

instance *instance-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all member devices.

Usage guidelines

In STP or RSTP mode, the command output is sorted by port name.

In PVST mode, the command output is sorted by VLAN ID and by port name in each VLAN.

- If you do not specify a VLAN, this command applies to all VLANs.
- If you specify a VLAN list, this command applies to the specified VLANs.

In MSTP mode, the command output is sorted by MSTI ID and by port name in each MSTI.

- If you do not specify an MSTI, this command applies to all MSTIs.
- If you specify an MSTI list, this command applies to the specified MSTIs.

Examples

In MSTP mode, display the incoming and outgoing TC/TCN BPDU statistics for all ports on slot 1 in MSTI 0.

```
<Sysname> display stp instance 0 tc slot 1
 -------------- STP slot 1 TC or TCN count -------------
 MST ID      Port                        Receive      Send
 0           GigabitEthernet1/0/1        6            4
 0           GigabitEthernet1/0/2        0            2
```

In PVST mode, display the incoming and outgoing TC/TCN BPDU statistics for all ports on slot 1 in VLAN 2.

```
<Sysname> display stp vlan 2 tc slot 1
 -------------- STP slot 1 TC or TCN count -------------
 VLAN ID     Port                        Receive      Send
 2           GigabitEthernet1/0/1        6            4
 2           GigabitEthernet1/0/2        0            2
```

Table 10 Command output

Field	Description
Port	Port name.
Receive	Number of TC/TCN BPDUs received on a port.
Send	Number of TC/TCN BPDUs sent by a port.

instance

Use **instance** to map a list of VLANs to an MSTI.

Use **undo instance** to remap the specified VLAN or all VLANs to the CIST (MSTI 0).

Syntax

instance *instance-id* **vlan** *vlan-id-list*

undo instance *instance-id* [**vlan** *vlan-id-list*]

Default

All VLANs are mapped to the CIST.

Views

MST region view

Predefined user roles

network-admin

context-admin

Parameters

instance-id: Specifies an MSTI ID in the range of 0 to 4094. A value of 0 represents the CIST. The value range for the *instance-id* argument is 1 to 4094 for the **undo instance** command.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

Usage guidelines

CAUTION:

Use caution with global Digest Snooping in the following situations:

- When you modify the VLAN-to-instance mappings.
- When you restore the default MST region configuration.

If the local device has different VLAN-to-instance mappings than its neighboring devices, loops or traffic interruption will occur.

If you do not specify any VLANs in the **undo instance** command, all VLANs mapped to the specified MSTI are remapped to the CIST.

You cannot map a VLAN to different MSTIs. If you map a VLAN that has been mapped to an MSTI to a new MSTI, the old mapping is automatically deleted.

You can configure VLAN-to-instance mapping for up to 65 MSTIs.

After configuring this command, run the **active region-configuration** command to activate the VLAN-to-instance mapping.

Examples

Map VLAN 2 to MSTI 1.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] instance 1 vlan 2
```

Related commands

active region-configuration

check region-configuration

display stp region-configuration

region-name

Use **region-name** to configure the MST region name.

Use **undo region-name** to restore the default MST region name.

Syntax

region-name *name*

undo region-name

Default

The MST region name of the device is its MAC address.

Views

MST region view

Predefined user roles

network-admin

context-admin

Parameters

name: Specifies the MST region name, a string of 1 to 32 characters.

Usage guidelines

The MST region name, the VLAN-to-instance mapping table, and the MSTP revision level of a device determine the device's MST region.

After configuring this command, execute the **active region-configuration** command to activate the configured MST region name.

Examples

Set the MST region name of the device to **hello**.

```
<Sysname> system-view
[Sysname] stp region-configuration
```

```
[Sysname-mst-region] region-name hello
```

Related commands

active region-configuration

check region-configuration

display stp region-configuration

instance

revision-level

vlan-mapping modulo

reset stp

Use **reset stp** to clear the spanning tree statistics.

Syntax

reset stp [**interface** *interface-list*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

interface *interface-list*: Specifies a space-separated list of up to 10 interface items. Each item specifies an interface or a range of interfaces in the form of *interface-type interface-number 1* [**to** *interface-type interface-number 2*]. The interface number for *interface-number 2* must be equal to or greater than the interface number for *interface-number 1*. If you do not specify this option, this command clears the spanning tree statistics on all ports.

Examples

Clear the spanning tree statistics on ports GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3.

```
<Sysname> reset stp interface gigabitethernet 1/0/1 to gigabitethernet 1/0/3
```

Related commands

display stp

revision-level

Use **revision-level** to configure the MSTP revision level.

Use **undo revision-level** to restore the default MSTP revision level.

Syntax

revision-level *level*

undo revision-level

Default

The MSTP revision level is 0.

Views

MST region view

Predefined user roles

network-admin

context-admin

Parameters

level: Specifies an MSTP revision level in the range of 0 to 65535.

Usage guidelines

The MSTP revision level, the MST region name, and the VLAN-to-instance mapping table of a device determine the device's MST region.

After configuring this command, execute the **active region-configuration** command to activate the configured MST region level.

Examples

Set the MSTP revision level of the MST region to 5.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] revision-level 5
```

Related commands

active region-configuration

check region-configuration

display stp region-configuration

instance

region-name

vlan-mapping modulo

snmp-agent trap enable stp

Use **snmp-agent trap enable stp** to enable SNMP notifications for new-root election events or spanning tree topology changes.

Use **undo snmp-agent trap enable stp** to disable SNMP notifications for new-root election events or spanning tree topology changes.

Syntax

snmp-agent trap enable stp [**new-root** | **tc**]

undo snmp-agent trap enable stp [**new-root** | **tc**]

Default

SNMP notifications are disabled for new-root election events.

In MSTP mode, SNMP notifications are enabled in MSTI 0 and disabled in other MSTIs for spanning tree topology changes.

In PVST mode, SNMP notifications are disabled for spanning tree topology changes in all VLANs.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

new-root: Enables the device to send notifications if the device is elected as a new root bridge. This keyword applies only to STP, MSTP, and RSTP modes.

tc: Enables the device to send notifications if the device receives TCN BPDUs. This keyword applies only to PVST mode.

Usage guidelines

If no keyword is specified, the **snmp-agent trap enable stp** command applies to SNMP notifications for different events as follows:

- In STP, MSTP, and RSTP modes, the command applies to SNMP notifications for new-root election events.
- In PVST mode, the command applies to SNMP notifications for spanning tree topology changes.

Examples

Enable SNMP notifications for new-root election events.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable stp new-root
```

stp bpdu-protection

Use **stp bpdu-protection** to enable BPDU guard globally.

Use **undo stp bpdu-protection** to disable BPDU guard globally.

Syntax

stp bpdu-protection

undo stp bpdu-protection

Default

BPDU guard is globally disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

With BPDU guard enabled, the device shuts down an edge port and notifies the NMS of the shutdown event when the edge port receives configuration BPDUs.

The device reactivates the ports that have been shut down when the port status detection timer expires. You can set this timer by using the **shutdown-interval** command. For more information about this command, see device management commands in *Fundamentals Command Reference*.

The **stp bpdu-protection** command takes effect only on the edge ports configured by using the **stp edged-port** command.

Examples

Enable BPDU guard globally.

```
<Sysname> system-view
[Sysname] stp bpdu-protection
```

Related commands

shutdown-interval (*Fundamentals Command Reference*)

stp edged-port

stp bridge-diameter

Use **stp bridge-diameter** to set the network diameter. The switched network diameter refers to the maximum number of devices on the path for an edge device to reach another through the root bridge.

Use **undo stp bridge-diameter** to restore the default.

Syntax

stp [**vlan** *vlan-id-list*] **bridge-diameter** *diameter*

undo stp [**vlan** *vlan-id-list*] **bridge-diameter**

Default

The network diameter of the switched network is 7.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094. If you set the STP, RSTP, or MSTP switched network diameter, do not specify this option.

diameter: Specifies the switched network diameter in the range of 2 to 7.

Usage guidelines

An appropriate setting of hello time, forward delay, and max age can speed up network convergence. The values of these timers are related to the network size, and you can set the timers by setting the network diameter. With the network diameter set to 7 (the default), the three timers are also set to their defaults.

In STP, RSTP, or MSTP mode, each MST region is considered as a device. The configured network diameter of the switched network takes effect only on the CIST (or the common root bridge).

In PVST mode, the configured network diameter takes effect only on the root bridges of the specified VLANs.

Examples

In MSTP mode, set the network diameter of the switched network to 5.

```
<Sysname> system-view
```

```
[Sysname] stp bridge-diameter 5
```

In PVST mode, set the network diameter of VLAN 2 in the switched network to 5.

```
<Sysname> system-view
[Sysname] stp vlan 2 bridge-diameter 5
```

Related commands

stp timer forward-delay

stp timer hello

stp timer max-age

stp compliance

Use **stp compliance** to configure the mode a port uses to recognize and send MSTP BPDUs.

Use **undo stp compliance** to restore the default.

Syntax

stp compliance { **auto** | **dot1s** | **legacy** }

undo stp compliance

Default

A port automatically recognizes the formats of received MSTP packets and determines the formats of MSTP packets to be sent based on the recognized formats.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

context-admin

Parameters

auto: Configures the port to recognize the MSTP BPDU format automatically and determine the format of MSTP BPDUs to send.

dot1s: Configures the port to receive and send only standard-format (802.1s-compliant) MSTP BPDUs.

legacy: Configures the port to receive and send only compatible-format MSTP BPDUs.

Usage guidelines

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Configure GigabitEthernet 1/0/1 to send only standard-format (802.1s) MSTP packets.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp compliance dot1s
```

stp config-digest-snooping

Use **stp config-digest-snooping** to enable Digest Snooping.

Use **undo stp config-digest-snooping** to disable Digest Snooping.

Syntax

stp config-digest-snooping

undo stp config-digest-snooping

Default

Digest Snooping is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

For Digest Snooping to take effect, you must enable Digest Snooping both globally and on associated ports. As a best practice, first enable Digest Snooping on ports connected to third-party vendor devices and then enable the feature globally. Digest Snooping takes effect on the ports simultaneously, which reduces impact on the network.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Enable Digest Snooping on GigabitEthernet 1/0/1 and then globally.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp config-digest-snooping
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] stp global config-digest-snooping
```

Related commands

display stp

stp global config-digest-snooping

stp cost

Use **stp cost** to set the path cost of a port.

Use **undo stp cost** to restore the default.

Syntax

stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **cost** *cost-value*

undo stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **cost**

Default

The device automatically calculates the path costs of ports in each spanning tree based on the corresponding standard.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

context-admin

Parameters

instance *instance-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

cost-value: Specifies the path cost of the port, with an effective range that varies by path cost calculation standard that is used.

- When the IEEE 802.1d-1998 standard is selected for path cost calculation, the value range for the *cost* argument is 1 to 65535.
- When the IEEE 802.1t standard is selected for path cost calculation, the value range for the *cost* argument is 1 to 200000000.
- When the private standard is selected for path cost calculation, the value range for the *cost* argument is 1 to 200000.

Usage guidelines

Path cost is an important factor in spanning tree calculation. Setting different path costs for a port in MSTIs allows VLAN traffic flows to be forwarded along different physical links. This results in VLAN-based load balancing.

The path cost setting of a port can affect the role selection of the port. When the path cost of a port is changed, the system calculates the role of the port and initiates a state transition.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, is takes effect only after the port leaves the aggregation group.

If you do not specify an MSTI or VLAN, this command sets the path cost of a port in the MSTP CIST or in the STP or RSTP spanning tree.

Examples

In MSTP mode, set the path cost to 200 for GigabitEthernet 1/0/1 in MSTI 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp instance 2 cost 200
```

In PVST mode, set the path cost to 200 for GigabitEthernet 1/0/1 in VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp vlan 2 cost 200
```

Related commands

display stp

stp pathcost-standard

stp edged-port

Use **stp edged-port** to configure a port as an edge port.

Use **undo stp edged-port** to restore the default.

Syntax

stp edged-port

undo stp edged-port

Default

All ports are non-edge ports.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

A port directly connecting to a user terminal rather than another device or a shared LAN segment can be configured as an edge port. In case the network topology changes, an edge port does not cause a temporary loop. You can enable the port to transit to the forwarding state rapidly by configuring it as an edge port. As a best practice, configure ports that directly connect to user terminals as edge ports.

Typically, configuration BPDUs from other devices cannot reach an edge port, because the edge port does not connect to any other device. When BPDU guard is disabled on a port configured as an edge port, the port acts as a non-edge port if it receives configuration BPDUs.

On a port, the loop guard feature and the edge port setting are mutually exclusive.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Configure GigabitEthernet 1/0/1 as an edge port.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp edged-port
```

Related commands

stp bpdu-protection

stp loop-protection

stp port bpdu-protection

stp enable

Use **stp enable** to enable the spanning tree feature.

Use **undo stp enable** to disable the spanning tree feature.

Syntax

stp enable

undo stp enable

Default

The spanning tree feature is enabled on all ports.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

When you enable the spanning tree feature, the device operates in STP, RSTP, PVST, or MSTP mode, depending on the spanning tree mode setting.

When you enable the spanning tree feature, the device dynamically maintains the spanning tree status of VLANs, based on received configuration BPDUs. When you disable the spanning tree feature, the device stops maintaining the spanning tree status.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

In MSTP mode, disable the spanning tree feature on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo stp enable
```

Related commands

stp global enable

stp mode

stp vlan enable

stp global config-digest-snooping

Use **stp global config-digest-snooping** to enable Digest Snooping globally.

Use **undo stp global config-digest-snooping** to disable Digest Snooping globally.

Syntax

stp global config-digest-snooping

undo stp global config-digest-snooping

Default

Digest Snooping is disabled globally.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

For Digest Snooping to take effect, you must enable Digest Snooping both globally and on associated ports. As a best practice, first enable Digest Snooping on ports connected to third-party vendor devices and then enable the feature globally. Digest Snooping takes effect on the ports simultaneously, which reduces impact on the network.

Examples

Enable Digest Snooping on GigabitEthernet 1/0/1 and then globally.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp config-digest-snooping
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] stp global config-digest-snooping
```

Related commands

display stp

stp config-digest-snooping

stp global enable

Use **stp global enable** to enable the spanning tree feature globally.

Use **undo stp global enable** to disable the spanning tree feature globally.

Syntax

stp global enable

undo stp global enable

Default

The spanning tree feature is disabled globally.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

When you enable the spanning tree feature, the device operates in STP, RSTP, PVST, or MSTP mode, depending on the spanning tree mode setting.

When the spanning tree feature is enabled, the device dynamically maintains the spanning tree status of VLANs based on received configuration BPDUs. When the spanning tree feature is disabled, the device stops maintaining the spanning tree status.

Examples

Enable the spanning tree feature globally.

```
<Sysname> system-view
[Sysname] stp global enable
```

Related commands

stp enable

stp mode

stp global mcheck

Use **stp global mcheck** to perform mCheck globally.

Syntax

stp global mcheck

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

When a port on an MSTP, RSTP, or PVST device connects to an STP device and receives STP BPDUs, the port automatically transits to the STP mode. However, the port cannot automatically transit back to the original mode when the following conditions exist:

- The peer STP device is shut down or removed.
- The port cannot detect the change.

In this case, you can perform an mCheck operation to forcibly transit the port to operate in the original mode.

The device operates in STP, RSTP, PVST, or MSTP mode, depending on the spanning tree mode setting.

The **stp global mcheck** command takes effect only when the device operates in MSTP, RSTP, or PVST mode.

Examples

Perform mCheck globally.

```
<Sysname> system-view
[Sysname] stp global mcheck
```

Related commands

stp mcheck

stp mode

stp ignore-pvid-inconsistency

Use **stp ignore-pvid-inconsistency** to disable inconsistent PVID protection.

Use **undo stp ignore-pvid-inconsistency** to enable inconsistent PVID protection.

Syntax

stp ignore-pvid-inconsistency

undo stp ignore-pvid-inconsistency

Default

Inconsistent PVID protection is enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command takes effect only when the device is operating in PVST mode.

Disabling inconsistent PVID protection might cause spanning tree calculation errors. To avoid such errors, make sure the following requirements are met:

- Make sure the VLANs on one device do not use the same ID as the PVID of its peer port (except the default VLAN) on another device.
- If the local port or its peer is a hybrid port, do not configure the local and peer ports as untagged members of the same VLAN.
- Disable inconsistent PVID protection on both the local device and the peer device.

Examples

In PVST mode, disable the inconsistent PVID protection feature.

```
<Sysname> system-view
[Sysname] stp mode pvst
[Sysname] stp ignore-pvid-inconsistency
```

stp loop-protection

Use **stp loop-protection** to enable loop guard on a port.

Use **undo stp loop-protection** to disable loop guard on a port.

Syntax

stp loop-protection

undo stp loop-protection

Default

Loop guard is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

On a port, the loop guard feature is mutually exclusive with the root guard feature or the edge port setting.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Enable loop guard on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp loop-protection
```

Related commands

stp edged-port

stp root-protection

stp max-hops

Use **stp max-hops** to set the maximum number of hops for an MST region.

Use **undo stp max-hops** to restore the default.

Syntax

stp max-hops *hops*

undo stp max-hops

Default

The maximum number of hops for an MST region is 20.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

hops: Specifies the maximum hops in the range of 1 to 40.

Examples

Set the maximum hops of the MST region to 35.

```
<Sysname> system-view
[Sysname] stp max-hops 35
```

Related commands

display stp

stp mcheck

Use **stp mcheck** to perform mCheck on a port.

Syntax

stp mcheck

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

When a port on an MSTP, RSTP, or PVST device connects to an STP device and receives STP BPDUs, the port automatically transits to the STP mode. However, the port cannot automatically transit back to the original mode when the following conditions exist:

- The peer STP device is shut down or removed.
- The port cannot detect the change.

In this case, you can perform an mCheck operation to forcibly transit the port to operation in the original mode.

For example, Device A, Device B, and Device C are connected in sequence. Device A runs STP, Device B does not run any spanning tree protocol, and Device C runs RSTP, MSTP, or PVST. When Device C receives an STP BPDU transparently transmitted by Device B, the receiving port transits to the STP mode. If you configure Device B to run RSTP, MSTP, or PVST with Device C, perform mCheck operations on the ports that connect Device B and Device C.

The device operates in STP, RSTP, PVST, or MSTP mode, depending on the spanning tree mode setting.

The **stp mcheck** command takes effect only when the device operates in MSTP, RSTP, or PVST mode.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Perform mCheck on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp mcheck
```

Related commands

stp global mcheck

stp mode

stp mode

Use **stp mode** to configure the spanning tree operating mode.

Use **undo stp mode** to restore the default.

Syntax

stp mode { **mstp** | **pvst** | **rstp** | **stp** }

undo stp mode

Default

A spanning tree device operates in MSTP mode.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

mstp: Configures the spanning tree device to operate in MSTP mode.

pvst: Configures the spanning tree device to operate in PVST mode.

rstp: Configures the spanning tree device to operate in RSTP mode.

stp: Configures the spanning tree device to operate in STP mode.

Usage guidelines

The MSTP mode is compatible with the RSTP mode, and the RSTP mode is compatible with the STP mode.

The PVST mode's compatibility with other modes is as follows:

- **Access port**—The PVST mode is compatible with other modes in any VLAN.
- **Trunk or hybrid port**—The PVST mode is compatible with other modes only in the default VLAN.

Examples

Configure the spanning tree device to operate in STP mode.

```
<Sysname> system-view
[Sysname] stp mode stp
```

Related commands

stp enable

stp global enable

stp global mcheck

stp mcheck

stp vlan enable

stp no-agreement-check

Use **stp no-agreement-check** to enable No Agreement Check on a port.

Use **undo stp no-agreement-check** to disable No Agreement Check on a port.

Syntax

stp no-agreement-check

undo stp no-agreement-check

Default

No Agreement Check is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command takes effect only after you enable it on the root port.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Enable No Agreement Check on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp no-agreement-check
```

stp pathcost-standard

Use **stp pathcost-standard** to specify a standard for the device to use when calculating the default path costs for ports.

Use **undo stp pathcost-standard** to restore the default.

Syntax

stp pathcost-standard { **dot1d-1998** | **dot1t** | **legacy** }

undo stp pathcost-standard

Default

The default standard is **legacy**.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

dot1d-1998: Configures the device to calculate the default path cost for ports based on IEEE 802.1d-1998.

dot1t: Configures the device to calculate the default path cost for ports based on IEEE 802.1t.

legacy: Configures the device to calculate the default path cost for ports based on a private standard.

Usage guidelines

If you change the standard that the device uses in calculating the default path costs, you restore the path costs to the default.

Examples

Configure the device to calculate the default path cost for ports based on IEEE 802.1d-1998.

```
<Sysname> system-view
[Sysname] stp pathcost-standard dot1d-1998
```

Related commands

display stp

stp cost

stp point-to-point

Use **stp point-to-point** to configure the link type of a port.

Use **undo stp point-to-point** to restore the default.

Syntax

stp point-to-point { **auto** | **force-false** | **force-true** }

undo stp point-to-point

Default

The default setting is **auto,** and the spanning tree device automatically detects whether a port connects to a point-to-point link.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

context-admin

Parameters

auto: Specifies automatic detection of the link type.

force-false: Specifies the non-point-to-point link type.

force-true: Specifies the point-to-point link type.

Usage guidelines

When connecting to a non-point-to-point link, a port is incapable of rapid state transition.

You can configure the link type as point-to-point for a Layer 2 aggregate interface or a port that operates in full duplex mode. As a best practice, use the default setting to let the device automatically detect the port link type.

In MSTP or PVST mode, the **stp point-to-point force-false** or **stp point-to-point force-true** command configured on a port takes effect on all MSTIs or VLANs.

Before you set the link type of a port to point-to-point, make sure the port is connected to a point-to-point link. Otherwise, a temporary loop might occur.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Configure the link type of GigabitEthernet 1/0/1 as point-to-point.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp point-to-point force-true
```

Related commands

display stp

stp port priority

Use **stp port priority** to set the priority of a port. The port priority affects the role of a port in a spanning tree.

Use **undo stp port priority** to restore the default.

Syntax

stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **port priority** *priority*

undo stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **port priority**

Default

The port priority is 128.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

context-admin

Parameters

instance *instance-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

priority: Specifies the port priority in the range of 0 to 240 in increments of 16 (as in 0, 16, 32).

Usage guidelines

The smaller the value, the higher the port priority. If all ports on your device use the same priority value, the port priority depends on the port index. The smaller the index, the higher the priority.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

If you do not specify an MSTI or VLAN, this command configures the priority of the ports in the MSTP CIST or in the STP or RSTP spanning tree.

Examples

In MSTP mode, set the port priority of GigabitEthernet 1/0/1 to 16 in MSTI 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp instance 2 port priority 16
```

In PVST mode, set the port priority of GigabitEthernet 1/0/1 to 16 in VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp vlan 2 port priority 16
```

Related commands

display stp

stp port-log

Use **stp port-log** to enable outputting port state transition information.

Use **undo stp port-log** to disable outputting port state transition information.

Syntax

stp port-log { **all** | **instance** *instance-list* | **vlan** *vlan-id-list* }

undo stp port-log { **all** | **instance** *instance-list* | **vlan** *vlan-id-list* }

Default

Outputting port state transition information is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

all: Specifies all MSTIs or VLANs.

instance *instance-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

Examples

In MSTP mode, enable outputting port state transition information for MSTI 2.

```
<Sysname> system-view
[Sysname] stp port-log instance 2
%Aug 16 00:49:41:856 2011 Sysname STP/3/STP_DISCARDING: Instance 2's port
GigabitEthernet1/0/1 has been set to discarding state.
%Aug 16 00:49:41:856 2011 Sysname STP/3/STP_FORWARDING: Instance 2's port
GigabitEthernet1/0/2 has been set to forwarding state.
```

The output shows that GigabitEthernet 1/0/1 in MSTI 2 transited to the discarding state and GigabitEthernet 1/0/2 in MSTI 2 transited to the forwarding state.

In PVST mode, enable outputting port state transition information for VLAN 1 through VLAN 4094.

```
<Sysname> system-view
[Sysname] stp port-log vlan 1 to 4094
%Aug 16 00:49:41:856 2006 Sysname STP/3/STP_DISCARDING: VLAN 2's GigabitEthernet1/0/1 has
been set to discarding state.
%Aug 16 00:49:41:856 2006 Sysname STP/3/STP_FORWARDING: VLAN 2's GigabitEthernet1/0/2 has
been set to forwarding state.
```

The output shows that GigabitEthernet 1/0/1 in VLAN 2 transited to the discarding state and GigabitEthernet 1/0/2 in VLAN 2 transited to the forwarding state.

stp priority

Use **stp priority** to set the priority of the device.

Use **undo stp priority** to restore the default.

Syntax

stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **priority** *priority*

undo stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **priority**

Default

The device priority is 32768.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

instance *instance-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The

value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

priority: Specifies the device priority in the range of 0 to 61440 in increments of 4096 (as in 0, 4096, 8192). You can set up to 16 priority values on the device. The smaller the value, the higher the device priority.

Usage guidelines

If you do not specify an MSTI or VLAN, this command configures the priority of the device in the MSTP CIST or in the STP or RSTP spanning tree.

Examples

In MSTP mode, set the device priority to 4096 in MSTI 1.

```
<Sysname> system-view
[Sysname] stp instance 1 priority 4096
```

In PVST mode, set the device priority to 4096 in VLAN 1.

```
<Sysname> system-view
[Sysname] stp vlan 1 priority 4096
```

stp pvst-bpdu-protection

Use **stp pvst-bpdu-protection** to enable PVST BPDU guard.

Use **undo stp pvst-bpdu-protection** to disable PVST BPDU guard.

Syntax

stp pvst-bpdu-protection

undo stp pvst-bpdu-protection

Default

PVST BPDU guard is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

PVST BPDU guard enables an MSTP-enabled device to shut down a port if the port receives PVST BPDUs. The shutdown port is brought up after a detection timer expires. To set the detection timer, use the **shutdown-interval** command.

Examples

In MSTP mode, enable PVST BPDU guard.

```
<Sysname> system-view
[Sysname] stp pvst-bpdu-protection
```

Related commands

shutdown-interval (For more information, see *Fundamentals Command Reference*.)

stp region-configuration

Use **stp region-configuration** to enter MST region view.

Use **undo stp region-configuration** to restore the default MST region configurations.

Syntax

stp region-configuration

undo stp region-configuration

Default

The default settings for an MST region are as follows:

- The MST region name of the device is its MAC address.
- All VLANs are mapped to the CIST.
- The MSTP revision level is 0.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

After you enter MST region view, you can configure MST region parameters, including the region name, VLAN-to-instance mappings, and revision level.

Examples

Enter MST region view.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region]
```

stp role-restriction

Use **stp role-restriction** to enable port role restriction.

Use **undo stp role-restriction** to disable port role restriction.

Syntax

stp role-restriction

undo stp role-restriction

Default

Port role restriction is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

When port role restriction is enabled on a port, the port cannot become a root port.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Enable port role restriction on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp role-restriction
```

stp root primary

Use **stp root primary** to configure the device as the root bridge.

Use **undo stp root** to restore the default.

Syntax

stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **root primary**

undo stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **root**

Default

The device is not a root bridge.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

instance *instance-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

Usage guidelines

Once you specify the device as the root bridge, you cannot change the priority of the device.

If you do not specify an MSTI or VLAN, this command configures the device as the root bridge of the MSTP CIST or of the STP or RSTP spanning tree.

Examples

In MSTP mode, specify the device as the root bridge of MSTI 1.

```
<Sysname> system-view
[Sysname] stp instance 1 root primary
```

In PVST mode, specify the device as the root bridge of VLAN 1.

```
<Sysname> system-view
[Sysname] stp vlan 1 root primary
```

Related commands

stp priority

stp root secondary

stp root secondary

Use **stp root secondary** to configure the device as a secondary root bridge.

Use **undo stp root** to restore the default.

Syntax

stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **root secondary**

undo stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **root**

Default

The device is not a secondary root bridge.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

instance *instance-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

Usage guidelines

Once you specify the device as a secondary root bridge, you cannot change the priority of the device.

If you do not specify an MSTI or VLAN, this command configures a secondary root bridge for the MSTP CIST or the STP or RSTP spanning tree.

Examples

In MSTP mode, specify the device as a secondary root bridge in MSTI 1.

```
<Sysname> system-view
[Sysname] stp instance 1 root secondary
```

In PVST mode, specify the device as a secondary root bridge in VLAN 1.

```
<Sysname> system-view
[Sysname] stp vlan 1 root secondary
```

Related commands

stp priority

stp root primary

stp root-protection

Use **stp root-protection** to enable root guard on a port.

Use **undo stp root-protection** to disable root guard on a port.

Syntax

stp root-protection

undo stp root-protection

Default

Root guard is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

On a port, the loop guard feature and the root guard feature are mutually exclusive.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Enable root guard on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp root-protection
```

Related commands

stp edged-port

stp loop-protection

stp tc-protection

Use **stp tc-protection** to enable TC-BPDU attack guard for the device.

Use **undo stp tc-protection** to disable TC-BPDU attack guard for the device.

Syntax

stp tc-protection

undo stp tc-protection

Default

TC-BPDU attack guard is enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

With TC-BPDU guard, you can set the maximum number of immediate forwarding address entry flushes that the device can perform every 10 seconds. For TC-BPDUs received that exceed the limit, the device performs a forwarding address entry flush when the interval elapses. This prevents frequent flushing of forwarding address entries.

Examples

Disable TC-BPDU attack guard for the device.

```
<Sysname> system-view
[Sysname] undo stp tc-protection
```

Related commands

stp tc-protection threshold

stp tc-protection threshold

Use **stp tc-protection threshold** to set the maximum number of forwarding address entry flushes that the device can perform every 10 seconds.

Use **undo stp tc-protection threshold** to restore the default.

Syntax

stp tc-protection threshold *number*

undo stp tc-protection threshold

Default

By default, the device can perform a maximum of 6 forwarding address entry flushes every 10 seconds.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

number: Specifies the maximum number of immediate forwarding address entry flushes that the device can perform every 10 seconds. The value is in the range of 1 to 255.

Examples

Configure the device to perform up to 10 forwarding address entry flushes every 10 seconds.

```
<Sysname> system-view
[Sysname] stp tc-protection threshold 10
```

Related commands

stp tc-protection

stp tc-restriction

Use **stp tc-restriction** to enable TC-BPDU transmission restriction.

Use **undo stp tc-restriction** to disable TC-BPDU transmission restriction.

Syntax

stp tc-restriction

undo stp tc-restriction

Default

TC-BPDU transmission restriction is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

When TC-BPDU transmission restriction is enabled on a port, the port does not send TC-BPDUs to other ports. It also does not delete MAC address entries.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Enable TC-BPDU transmission restriction on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp tc-restriction
```

stp tc-snooping

Use **stp tc-snooping** to enable TC Snooping.

Use **undo stp tc-snooping** to disable TC Snooping.

Syntax

stp tc-snooping

undo stp tc-snooping

Default

TC Snooping is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

TC Snooping and the spanning tree feature are mutually exclusive. You must globally disable the spanning tree feature before enabling TC Snooping.

Examples

Globally disable the spanning tree feature and enable TC Snooping.

```
<Sysname> system-view
[Sysname] undo stp global enable
[Sysname] stp tc-snooping
```

Related commands

stp global enable

stp timer forward-delay

Use **stp timer forward-delay** to set the forward delay timer.

Use **undo stp timer forward-delay** to restore the default.

Syntax

stp [**vlan** *vlan-id-list*] **timer forward-delay** *time*

undo stp [**vlan** *vlan-id-list*] **timer forward-delay**

Default

The forward delay timer is 1500 centiseconds.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094. If you set the STP, RSTP, or MSTP forward delay, do not specify this option.

time: Specifies the forward delay in centiseconds, in the range of 400 to 3000 in increments of 100 (as in 400, 500, 600).

Usage guidelines

The forward delay timer determines the time interval of state transition. To prevent temporary loops, a spanning tree port goes through the learning (intermediate) state before it transits from the discarding state to the forwarding state. To stay synchronized with the remote device, the port has a wait period that is determined by the forward delay timer between transition states.

As a best practice, do not set the forward delay with this command. Instead, you can specify the network diameter of the switched network by using the **stp bridge-diameter** command. This command makes the spanning tree protocols automatically calculate the optimal settings for the forward delay timer. If the network diameter uses the default value, the forward delay timer also uses the default value.

Examples

In MSTP mode, set the forward delay timer to 2000 centiseconds.

```
<Sysname> system-view
[Sysname] stp timer forward-delay 2000
```

In PVST mode, set the forward delay timer for VLAN 2 to 2000 centiseconds.

```
<Sysname> system-view
[Sysname] stp vlan 2 timer forward-delay 2000
```

Related commands

stp bridge-diameter

stp timer hello

stp timer max-age

stp timer hello

Use **stp timer hello** to set the hello time.

Use **undo stp timer hello** to restore the default.

Syntax

stp [**vlan** *vlan-id-list*] **timer hello** *time*

undo stp [**vlan** *vlan-id-list*] **timer hello**

Default

The hello time is 200 centiseconds.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094. If you set the STP, RSTP, or MSTP hello time, do not specify this option.

time: Specifies the hello time in centiseconds, in the range of 100 to 1000 in increments of 100 (as in 100, 200, 300).

Usage guidelines

Hello time is the interval at which spanning tree devices send configuration BPDUs to maintain the spanning tree. If a device fails to receive configuration BPDUs within the set period of time, a new spanning tree calculation process is triggered.

As a best practice, do not set the hello time with this command. Instead, you can specify the network diameter of the switched network by using the **stp bridge-diameter** command. This command makes the spanning tree protocols automatically calculate the optimal settings for the hello timer. If the network diameter uses the default value, the hello timer also uses the default value.

Examples

In MSTP mode, set the hello time to 400 centiseconds.

```
<Sysname> system-view
[Sysname] stp timer hello 400
```

In PVST mode, set the hello time for VLAN 2 to 400 centiseconds.

```
<Sysname> system-view
[Sysname] stp vlan 2 timer hello 400
```

Related commands

stp bridge-diameter

stp timer forward-delay

stp timer max-age

stp timer max-age

Use **stp timer max-age** to set the max age timer.

Use **undo stp timer max-age** to restore the default.

Syntax

stp [**vlan** *vlan-id-list*] **timer max-age** *time*

undo stp [**vlan** *vlan-id-list*] **timer max-age**

Default

The max age is 2000 centiseconds.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094. If you set the STP, RSTP, or MSTP max age, do not specify this option.

time: Specifies the max age in centiseconds, in the range of 600 to 4000 in increments of 100 (as in 600, 700, 800).

Usage guidelines

In the CIST of an MSTP network, the device determines whether a configuration BPDU received on a port has expired based on the max age timer. If the configuration BPDU has expired, a new spanning tree calculation process starts. The max age timer takes effect only on the CIST (or MSTI 0).

As a best practice, do not set the max age timer with this command. Instead, you can specify the network diameter of the switched network by using the **stp bridge-diameter** command. This command makes the spanning tree protocols automatically calculate the optimal settings for the max age timer. If the network diameter uses the default value, the max age timer also uses the default value.

Examples

In MSTP mode, set the max age timer to 1000 centiseconds.

```
<Sysname> system-view
[Sysname] stp timer max-age 1000
```

In PVST mode, set the max age timer for VLAN 2 to 1000 centiseconds.

```
<Sysname> system-view
[Sysname] stp vlan 2 timer max-age 1000
```

Related commands

stp bridge-diameter

stp timer forward-delay

stp timer hello

stp timer-factor

Use **stp timer-factor** to configure the timeout period by setting the timeout factor.

Timeout period = timeout factor × 3 × hello time.

Use **undo stp timer-factor** to restore the default.

Syntax

stp timer-factor *factor*

undo stp timer-factor

Default

The timeout factor of the device is set to 3.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

factor: Specifies the timeout factor in the range of 1 to 20.

Usage guidelines

In a stable network, each non-root-bridge forwards configuration BPDUs to surrounding devices at the interval of hello time to determine whether any link fails. If a device does not receive a BPDU from the upstream device within nine times of the hello time, it assumes that the upstream device has failed. Then it will start a new spanning tree calculation process.

As a best practice, set the timeout factor to 5, 6, or 7 in the following situations:

- To prevent undesired spanning tree calculations. An upstream device might be too busy to forward configuration BPDUs in time, for example, many Layer 2 interfaces are configured on the upstream device. In this case, the downstream device fails to receive a BPDU within the timeout period and then starts an undesired spanning tree calculation.
- To save network resources on a stable network.

Examples

Set the timeout factor of the device to 7.

```
<Sysname> system-view
[Sysname] stp timer-factor 7
```

Related commands

stp timer hello

stp transmit-limit

Use **stp transmit-limit** to set the BPDU transmission rate of a port.

Use **undo stp transmit-limit** to restore the default.

Syntax

stp transmit-limit *limit*

undo stp transmit-limit

Default

The BPDU transmission rate of all ports is 10.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

context-admin

Parameters

limit: Specifies the BPDU transmission rate in the range of 1 to 255.

Usage guidelines

The maximum number of BPDUs a port can send within each hello time equals the BPDU transmission rate plus the hello timer value.

A larger BPDU transmission rate value requires more system resources. An appropriate BPDU transmission rate setting can prevent spanning tree protocols from using excessive bandwidth resources during network topology changes. As a best practice, use the default value.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Set the BPDU transmission rate of GigabitEthernet 1/0/1 to 5.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp transmit-limit 5
```

stp vlan enable

Use **stp vlan enable** to enable the spanning tree feature for VLANs.

Use **undo stp enable** to disable the spanning tree feature for VLANs.

Syntax

stp vlan *vlan-id-list* **enable**

undo stp vlan *vlan-id-list* **enable**

Default

The spanning tree feature is enabled in VLANs.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

Usage guidelines

When you enable the spanning tree feature, the device operates in STP, RSTP, PVST, or MSTP mode, depending on the spanning tree mode setting.

When you enable the spanning tree feature, the device dynamically maintains the spanning tree status of VLANs, based on received configuration BPDUs. When you disable the spanning tree feature, the device stops maintaining the spanning tree status.

Examples

In PVST mode, globally enable the spanning tree feature and then enable the spanning tree feature for VLAN 2.

```
<Sysname> system-view
[Sysname] stp mode pvst
```

```
[Sysname] stp global enable
[Sysname] stp vlan 2 enable
```

Related commands

stp enable

stp global enable

stp mode

vlan-mapping modulo

Use **vlan-mapping modulo** to map VLANs in an MST region to MSTIs according to the specified modulo value and quickly create a VLAN-to-instance mapping table.

Syntax

vlan-mapping modulo *modulo*

Default

All VLANs are mapped to the CIST (MSTI 0).

Views

MST region view

Predefined user roles

network-admin

context-admin

Parameters

modulo: Specifies the modulo value. The value range for this argument is 1 to 64.

Usage guidelines

You cannot map a VLAN to different MSTIs. If you map a VLAN that has been mapped to an MSTI to a new MSTI, the old mapping is automatically deleted.

This command maps each VLAN to the MSTI with ID (VLAN ID – 1) % *modulo* + 1. (VLAN ID – 1) % *modulo* is the modulo operation for (VLAN ID – 1). If the modulo value is 15, then VLAN 1 is mapped to MSTI 1, VLAN 2 to MSTI 2, …, VLAN 15 to MSTI 15, VLAN 16 to MSTI 16, and so on.

Examples

Map VLANs to MSTIs as per modulo 8.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] vlan-mapping modulo 8
```

Related commands

active region-configuration

check region-configuration

display stp region-configuration

region-name

revision-level

Contents

LLDP commands

display lldp local-information

Use **display lldp local-information** to display local LLDP information.

Syntax

display lldp local-information [**global** | **interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

global: Displays the global local LLDP information.

interface *interface-type interface-number*: Specifies a port by its type and number.

Usage guidelines

If you do not specify any keywords or arguments, the command displays all local LLDP information, which includes the following:

- The global LLDP information.
- The LLDP information about the LLDP-enabled ports in up state.

Examples

Display all local LLDP information.

```
<Sysname> display lldp local-information
Global LLDP local-information:
 Chassis ID          : 88df-9e71-5e2d
 System name         : NSFOCUS
 System description  :
   NSFOCUS Software. Software Version 7.1.064, Ess 9536P05
   NSFOCUS NFNX3-HDB680
   Copyright (c) 2004-2019 NSFOCUS. All rights reserved.
 System capabilities supported : Bridge, Router, Customer Bridge, Service Bridge
 System capabilities enabled   : Bridge, Router, Customer Bridge

 MED information:
 Device class               : Connectivity device
 MED inventory information of master board:
 HardwareRev                : Ver.A
 FirmwareRev                : Basic Version:  1.02
Extend Version:  1.02
```

```
 SoftwareRev                : Version 7.10
 SerialNum                  : 219801A1KB9185Q00010
 Manufacturer name          : NSFOCUS
 Model name                 : NFNX3-HDB680
 Asset tracking identifier  : Unknown

LLDP local-information of port 1[GigabitEthernet1/0/0]:
 Port ID type        : Interface name
 Port ID             : GigabitEthernet1/0/0
 Port description    : GigabitEthernet1/0/0 Interface
 LLDP agent nearest-bridge management address:
 Management address type           : IPv4
 Management address                : 192.168.100.120
 Management address interface type : IfIndex
 Management address interface ID   : 1
 Management address OID            : 0
 LLDP agent nearest-nontpmr management address:
 Management address type           : IPv4
 Management address                : 192.168.100.120
 Management address interface type : IfIndex
 Management address interface ID   : 1
 Management address OID            : 0
 LLDP agent nearest-customer management address:
 Management address type           : IPv4
 Management address                : 192.168.100.120
 Management address interface type : IfIndex
 Management address interface ID   : 1
 Management address OID            : 0
 Link aggregation supported : Yes
 Link aggregation enabled   : No
 Aggregation port ID        : 0
 Auto-negotiation supported : Yes
 Auto-negotiation enabled   : No
 OperMau                    : Speed(1000)/Duplex(Full)
 Power port class           : PD
 PSE power supported        : No
 PSE power enabled          : No
 PSE pairs control ability  : No
 Power pairs                : Signal
 Port power classification  : Class 0
 Maximum frame size         : 1600
 Transmit Tw                : 0 us
 Receive Tw                 : 0 us
 Fallback Tw                : 0 us
 Echo Transmit Tw           : 0 us
 Echo Receive Tw            : 0 us
```

Table 1 Command output

Field	Description
Chassis ID	Bridge MAC address of the device.
System capabilities supported	Supported capabilities: • **Bridge**—Switching is supported. • **Router**—Routing is supported. • **Customer Bridge**—The customer bridge feature is supported. • **Service Bridge**—The service bridge feature is supported.
System capabilities enabled	Enabled capabilities: • **Bridge**—Switching is enabled. • **Router**—Routing is enabled. • **Customer Bridge**—The customer bridge feature is enabled. • **Service Bridge**—The service bridge feature is enabled.
Device class	MED device class: • **Connectivity device**—Network device. • **Class I**—Normal terminal device. It requires the basic LLDP discovery services. • **Class II**—Media terminal device. It supports media streams, and can also act as a normal terminal device. • **Class III**—Communication terminal device. It supports the IP communication systems of end users, and can also act as a normal terminal device or media terminal device.
MED inventory information of master board	MED inventory information about the MPU.
HardwareRev	Hardware version.
FirmwareRev	Firmware version.
SoftwareRev	Software version.
SerialNum	Serial number.
Manufacturer name	Device manufacturer.
Model name	Device model.
Port ID type	Port ID type: • MAC address. • Interface name.
Port ID	Port ID, the value of which depends on the port ID type.
Management address interface type	Numbering type of the interface identified by the management address.
Management address interface ID	Index of the interface identified by the management address.
Management address OID	Management address object ID.
Link aggregation supported	Indicates whether link aggregation is supported on the port.
Link aggregation enabled	Indicates whether link aggregation is enabled on the port.
Aggregation port ID	Member port ID, which is 0 when link aggregation is disabled.
Auto-negotiation supported	Indicates whether autonegotiation is supported on the port.
Auto-negotiation enabled	Indicates whether autonegotiation is enabled on the port.

Field	Description
OperMau	Speed and duplex state of the port.
Power port class	This field is not supported in the current software version. PoE port class: • **PSE**—Power sourcing equipment. • **PD**—Powered device.
PSE power supported	Indicates whether the device can operate as a PSE.
PSE power enabled	Indicates whether the device is operating as a PSE.
PSE pairs control ability	Indicates whether the pair selection ability is available.
Power pairs	This field is not supported in the current software version. Power supply mode: • **Signal**—Uses data pairs to supply power. • **Spare**—Uses spare pairs to supply power.
Transmit Tw	Sleep time of the local client, in μs.
Receive Tw	Sleep time of the peer client expected by the local client, in μs.
Fallback Tw	Candidate sleep time of the peer client expected by the local client, in μs.
Echo Transmit Tw	Sleep time of the peer client, in μs. This field displays zero when one of the following cases occurs: • The local client has not received the sleep time of the peer client. • The sleep time of the peer client is 0 μs.
Echo Receive Tw	Sleep time of the local client expected by the peer client, in μs. This field displays zero when one of the following cases occurs: • The local client has not received the expected sleep time from the peer client. • The sleep time of the local client expected by the peer client is 0 μs.

display lldp neighbor-information

Use **display lldp neighbor-information** to display the LLDP information received from the neighboring devices.

Syntax

display lldp neighbor-information [[[**interface** *interface-type interface-number*] [**agent** { **nearest-bridge** | **nearest-customer** | **nearest-nontpmr** }] [**verbose**]] | **list** [**system-name** *system-name*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify this option, the command displays the LLDP information that all ports receive from the neighboring devices.

agent: Specifies an agent type. If you do not specify an agent type, the command displays the LLDP information that all LLDP agents receive from the neighboring devices.

nearest-bridge: Specifies nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

nearest-nontpmr: Specifies nearest non-TPMR bridge agents.

verbose: Displays the detailed LLDP information that the local device receives from the neighboring devices. If you do not specify this keyword, the command displays the brief LLDP information that the local device receives from the neighboring devices.

list: Displays the LLDP information that the local device receives from the neighboring devices in the form of a list.

system-name *system-name*: Displays the LLDP information that the local device receives from a neighboring device specified by its system name. The *system-name* argument is a string of 1 to 255 characters. If you do not specify this option, the command displays the LLDP information that the local device receives from all neighboring devices in a list.

Examples

Display detailed LLDP information that the nearest bridge agents on all ports received from the neighboring devices.

```
<Sysname> display lldp neighbor-information agent nearest-bridge verbose
LLDP neighbor-information of port 1[GigabitEthernet1/0/0]:
LLDP agent nearest-bridge:
 LLDP neighbor index : 1
 Update time         : 16 days, 21 hours, 4 minutes, 6 seconds
 Chassis type        : MAC address
 Chassis ID          : 3822-d616-0869
 Port ID type        : Interface name
 Port ID             : GigabitEthernet5/0/26
 Time to live        : 120
 Port description    : GigabitEthernet5/0/26 Interface
 System name         : HeXin_Switch
 System description  :
   NSFOCUS Platform Software, Software Version 5.20 Release 1118
   NSFOCUS NFNX3-HDB680
   Copyright (c) 2004-2013 NSFOCUS. All rights reserved.
 System capabilities supported : Bridge, Router
 System capabilities enabled   : Bridge, Router
 Port VLAN ID(PVID)  : 1
 Port and protocol VLAN ID(PPVID)  : 0
 Port and protocol VLAN supported  : Yes
 Port and protocol VLAN enabled    : No
 VLAN name of VLAN 1        : VLAN 0001
 Link aggregation supported : Yes
 Link aggregation enabled   : No
 Aggregation port ID        : 0
```

```
 Auto-negotiation supported : Yes
 Auto-negotiation enabled   : Yes
 OperMau                    : Speed(1000)/Duplex(Full)
 Power port class           : PD
 PSE power supported        : No
 PSE power enabled          : No
 PSE pairs control ability  : No
 Power pairs                : Signal
 Port power classification  : Class 0
 Maximum frame size         : 9216
```

Display brief LLDP information that all LLDP agents received from all neighboring devices.

```
<Sysname> display lldp neighbor-information
LLDP neighbor-information of port 52 [GigabitEthernet1/0/3]:
LLDP agent nearest-bridge:
 LLDP neighbor index : 3
 ChassisID/subtype   : 0011-2233-4400/MAC address
 PortID/subtype      : 000c-29f5-c71f/MAC address
 Capabilities        : Bridge, Router, Customer Bridge

 LLDP neighbor index : 6
 ChassisID/subtype   : 0011-2233-4400/MAC address
 PortID/subtype      : 000c-29f5-c715/MAC address
 Capabilities        : None

LLDP neighbor-information of port 52 [GigabitEthernet1/0/3]:
LLDP agent nearest-nontpmr:
 LLDP neighbor index : 6
 ChassisID/subtype   : 0011-2233-4400/MAC address
 PortID/subtype      : 000c-29f5-c715/MAC address
 Capabilities        : None
```

Display brief LLDP information that all LLDP agents received from the neighboring devices in a list.

```
<Sysname> display lldp neighbor-information list
Chassis ID : * -- --Nearest nontpmr bridge neighbor
             # -- --Nearest customer bridge neighbor
             Default -- -- Nearest bridge neighbor
Local Interface Chassis ID      Port ID                   System Name
GE1/0/1         000f-e25d-ee91  GigabitEthernet1/0/1      System1
```

Table 2 Command output

Field	Description
LLDP neighbor-information of port 1	LLDP information received through port 1.
Update time	Time when LLDP information about a neighboring device was last updated.
LLDP mac type	Type of the neighbor MAC address: • Nearest bridge. • Nearest customer bridge. • Nearest non-TPMR bridge.

Field	Description
Chassis type	Chassis ID type: • **Chassis component**. • **Interface alias**. • **Port component**. • **MAC address**. • **Network address (ipv4)**. • **Interface name**. • **Locally assigned**—Locally-defined chassis type other than those listed above.
Chassis ID	ID that identifies the LLDP sending device, which can be a MAC address, a network address, an interface, or some other value, depending on the chassis ID type of the neighboring device.
Port ID type	Port ID type: • **Interface alias**. • **Port component**. • **MAC address**. • **Network address (ipv4)**. • **Interface name**. • **Agent circuit ID**. • **Locally assigned**—Locally-defined port ID type other than those listed above.
Port ID	Value of the type of the port ID.
System name	System name of the neighboring device.
System description	System description of the neighboring device.
System capabilities supported	Capabilities supported on the neighboring device: • **Bridge**—Switching is supported. • **Router**—Routing is supported. • . • **Customer Bridge**—The customer bridge feature is enabled. • **Service Bridge**—The service bridge feature is enabled.
System capabilities enabled	Capabilities enabled on the neighboring device: • **Bridge**—Switching is enabled. • **Router**—Routing is enabled. • **Customer Bridge**—The customer bridge feature is enabled. • **Service Bridge**—The service bridge feature is enabled.
Port and protocol VLAN ID(PPVID)	Port and protocol VLAN ID.
Port and protocol VLAN supported	Indicates whether protocol VLAN is supported on the port.
Port and protocol VLAN enabled	Indicates whether protocol VLAN is enabled on the port.
VLAN name of VLAN 12	Name of VLAN 12.
Link aggregation supported	Indicates whether link aggregation is supported.
Link aggregation enabled	Indicates whether link aggregation is enabled.
Aggregation port ID	Member port ID, which is 0 when link aggregation is disabled.
Auto-negotiation supported	Indicates whether autonegotiation is supported on the port.
Auto-negotiation enabled	Indicates whether autonegotiation is enabled on the port.

Field	Description
OperMau	Speed and duplex state on the port.
Power port class	This field is not supported in the current software version. PoE port class: • **PSE**—Power sourcing equipment. • **PD**—Powered device.
PSE power supported	Indicates whether the device can operate as a PSE.
PSE power enabled	Indicates whether the device is operating as a PSE.
PSE pairs control ability	Indicates whether the pair selection ability is available.
Power pairs	This field is not supported in the current software version. Power supply mode: • **Signal**—Uses data pairs to supply power. • **Spare**—Uses spare pairs to supply power.
TLV type	Unknown basic TLV type.
Capabilities	Capabilities enabled on the neighboring device: • **Bridge**—Switching is enabled. • **Router**—Routing is enabled. • **None**—The neighboring device does not advertise this TLV.
Local Interface	Local port that receives the LLDP information.
Chassis ID : * -- -- Nearest nontpmr bridge neighbor #-- -- Nearest customer bridge neighbor	Chassis ID flag: • An asterisk (*) indicates the nearest non-TPMR bridge neighbor. • A pound sign (#) indicates the nearest customer bridge neighbor.

display lldp statistics

Use **display lldp statistics** to display the global LLDP statistics or the LLDP statistics of a port.

Syntax

display lldp statistics [**global** | [**interface** *interface-type interface-number*] [**agent** { **nearest-bridge** | **nearest-customer** | **nearest-nontpmr** }]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

global: Displays the global LLDP statistics.

interface *interface-type interface-number*: Specifies a port by its type and number.

agent: Specifies an LLDP agent type. If you do not specify an agent type, the command displays the statistics for all LLDP agents.

nearest-bridge: Specifies nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

nearest-nontpmr: Specifies nearest non-TPMR bridge agents.

Usage guidelines

If you do not specify any keywords or arguments, the command displays the global LLDP statistics and the LLDP statistics of all ports.

Examples

Display the global LLDP statistics and the LLDP statistics of all ports.

```
<Sysname> display lldp statistics
LLDP statistics global information:
LLDP neighbor information last change time:0 days, 0 hours, 4 minutes, 40 seconds
The number of LLDP neighbor information inserted : 1
The number of LLDP neighbor information deleted  : 1
The number of LLDP neighbor information dropped  : 0
The number of LLDP neighbor information aged out : 1

LLDP statistics information of port 1 [GigabitEthernet1/0/1]:
LLDP agent nearest-bridge:
The number of LLDP frames transmitted           : 0
The number of LLDP frames received              : 0
The number of LLDP frames discarded             : 0
The number of LLDP error frames                 : 0
The number of LLDP TLVs discarded               : 0
The number of LLDP TLVs unrecognized            : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted            : 0
The number of CDP frames received               : 0
The number of CDP frames discarded              : 0
The number of CDP error frames                  : 0

LLDP agent nearest-nontpmr:
The number of LLDP frames transmitted           : 0
The number of LLDP frames received              : 0
The number of LLDP frames discarded             : 0
The number of LLDP error frames                 : 0
The number of LLDP TLVs discarded               : 0
The number of LLDP TLVs unrecognized            : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted            : 0
The number of CDP frames received               : 0
The number of CDP frames discarded              : 0
The number of CDP error frames                  : 0

LLDP agent nearest-customer:
The number of LLDP frames transmitted           : 0
```

```
The number of LLDP frames received              : 0
The number of LLDP frames discarded             : 0
The number of LLDP error frames                 : 0
The number of LLDP TLVs discarded               : 0
The number of LLDP TLVs unrecognized            : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted            : 0
The number of CDP frames received               : 0
The number of CDP frames discarded              : 0
The number of CDP error frames                  : 0
```

Display the LLDP statistics for the nearest customer bridge agents on GigabitEthernet 1/0/1.

```
<Sysname> display lldp statistics interface gigabitethernet 1/0/1 agent nearest-customer
LLDP statistics information of port 1 [GigabitEthernet1/0/1]:
LLDP agent nearest-customer:
The number of LLDP frames transmitted           : 0
The number of LLDP frames received              : 0
The number of LLDP frames discarded             : 0
The number of LLDP error frames                 : 0
The number of LLDP TLVs discarded               : 0
The number of LLDP TLVs unrecognized            : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted            : 0
The number of CDP frames received               : 0
The number of CDP frames discarded              : 0
The number of CDP error frames                  : 0
```

Table 3 Command output

Field	Description
LLDP statistics global information	Global LLDP statistics.
LLDP neighbor information last change time	Time when the neighbor information was last updated.
The number of LLDP neighbor information inserted	Number of times neighbor information was added.
The number of LLDP neighbor information deleted	Number of times neighbor information was removed.
The number of LLDP neighbor information dropped	Number of times neighbor information was dropped due to lack of available memory space.

display lldp status

Use **display lldp status** to display LLDP status.

Syntax

display lldp status [**interface** *interface-type interface-number*] [**agent** { **nearest-bridge** | **nearest-customer** | **nearest-nontpmr** }]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify this option, the command displays the global LLDP status and the LLDP status of all ports.

agent: Specifies an LLDP agent type. If you do not specify an agent type, the command displays the status information for all LLDP agents.

nearest-bridge: Specifies nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

nearest-nontpmr: Specifies nearest non-TPMR bridge agents.

Examples

Display the global LLDP status and the LLDP status of each port.

```
<Sysname> display lldp status
Global status of LLDP: Enable
Bridge mode of LLDP: customer-bridge
The current number of LLDP neighbors: 5
The current number of CDP neighbors: 0
LLDP neighbor information last changed time: 0 days, 0 hours, 4 minutes, 40 seconds
Transmit interval              : 30s
Fast transmit interval         : 1s
Transmit max credit            : 5
Hold multiplier                : 4
Reinit delay                   : 2s
Trap interval                  : 5s
Fast start times               : 3

LLDP status information of port 1 [GigabitEthernet1/0/1]:
LLDP agent nearest-bridge:
Port status of LLDP            : Enable
Admin status                   : TX_RX
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 5
Number of MED neighbors        : 2
Number of CDP neighbors        : 0
Number of sent optional TLV    : 12
Number of received unknown TLV : 5

LLDP agent nearest-nontpmr:
Port status of LLDP            : Enable
Admin status                   : TX_RX
```

```
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 5
Number of MED neighbors        : 2
Number of CDP neighbors        : 0
Number of sent optional TLV    : 12
Number of received unknown TLV : 5

LLDP agent nearest-customer:
Port status of LLDP            : Enable
Admin status                   : TX_RX
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 5
Number of MED neighbors        : 2
Number of CDP neighbors        : 0
Number of sent optional TLV    : 12
Number of received unknown TLV : 5
```

Table 4 Command output

Field	Description
Bridge mode of LLDP	LLDP bridge mode: service-bridge or customer-bridge.
Global status of LLDP	Indicates whether LLDP is globally enabled.
LLDP neighbor information last changed time	Time when the neighbor information was last updated.
Transmit interval	LLDP frame transmission interval.
Hold multiplier	TTL multiplier.
Reinit delay	LLDP reinitialization delay.
Transmit max credit	Token bucket size for sending LLDP frames.
Trap interval	Trap transmission interval.
Fast start times	Number of LLDP frames sent each time fast LLDP frame transmission is triggered.
Port 1	LLDP status of port 1.
Port status of LLDP	Indicates whether LLDP is enabled on the port.
Admin status	LLDP operating mode of the port: • **TX_RX**—The port can send and receive LLDP frames. • **Rx_Only**—The port can only receive LLDP frames. • **Tx_Only**—The port can only send LLDP frames. • **Disable**—The port cannot send or receive LLDP frames.
Trap Flag	Indicates whether trapping is enabled.
Polling interval	LLDP polling interval, which is 0 when LLDP polling is disabled.
Number of neighbors	Number of LLDP neighbors connecting to the port.

Field	Description
Number of MED neighbors	Number of MED neighbors connecting to the port.
Number of CDP neighbors	Number of CDP neighbors connected to the port. This field is not supported in the current software version.
Number of sent optional TLV	Number of optional TLVs contained in an LLDP frame sent through the port.
Number of received unknown TLV	Number of unknown TLVs contained in a received LLDP frame.

display lldp tlv-config

Use **display lldp tlv-config** to display the types of advertisable optional LLDP TLVs of a port.

Syntax

display lldp tlv-config [**interface** *interface-type interface-number*] [**agent** { **nearest-bridge** | **nearest-customer** | **nearest-nontpmr** }]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify this option, the command displays the types of advertisable optional TLVs of all ports.

agent: Specifies an LLDP agent type. If you do not specify an agent type, the command displays the types of advertisable optional LLDP TLVs for all LLDP agents.

nearest-bridge: Specifies nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

nearest-nontpmr: Specifies nearest non-TPMR bridge agents.

Examples

Display the types of advertisable optional LLDP TLVs of GigabitEthernet 1/0/1.

```
<Sysname> display lldp tlv-config interface gigabitethernet 1/0/1
LLDP tlv-config of port 1[GigabitEthernet1/0/1]:
LLDP agent nearest-bridge:
NAME                              STATUS    DEFAULT
Basic optional TLV:
 Port Description TLV             YES       YES
 System Name TLV                  YES       YES
 System Description TLV           YES       YES
 System Capabilities TLV          YES       YES
 Management Address TLV           YES       YES
```

```
IEEE 802.1 extend TLV:
 Port VLAN ID TLV                 NO        NO
 Port And Protocol VLAN ID TLV    NO        NO
 VLAN Name TLV                    NO        NO
 DCBX TLV                         NO        NO
 EVB TLV                          NO        NO
 Link Aggregation TLV             YES       YES
 Management VID TLV               NO        NO
IEEE 802.3 extend TLV:
 MAC-Physic TLV                   YES       YES
 Power via MDI TLV                YES       YES
 Maximum Frame Size TLV           YES       YES
LLDP-MED extend TLV:
 Capabilities TLV                 YES       YES
 Network Policy TLV               NO        NO
 Location Identification TLV      NO        NO
 Extended Power via MDI TLV       YES       YES
 Inventory TLV                    YES       YES

LLDP agent nearest-nontpmr:
NAME                              STATUS    DEFAULT
Basic optional TLV:
 Port Description TLV             NO        NO
 System Name TLV                  NO        NO
 System Description TLV           NO        NO
 System Capabilities TLV          NO        NO
 Management Address TLV           NO        NO
IEEE 802.1 extend TLV:
 Port VLAN ID TLV                 NO        NO
 Port And Protocol VLAN ID TLV    NO        NO
 VLAN Name TLV                    NO        NO
 DCBX TLV                         NO        NO
 EVB TLV                          NO        NO
 Link Aggregation TLV             NO        NO
 Management VID TLV               NO        NO
IEEE 802.3 extend TLV:
 MAC-Physic TLV                   NO        NO
 Power via MDI TLV                NO        NO
 Maximum Frame Size TLV           NO        NO
LLDP-MED extend TLV:
 Capabilities TLV                 NO        NO
 Network Policy TLV               NO        NO
 Location Identification TLV      NO        NO
 Extended Power via MDI TLV       NO        NO
 Inventory TLV                    NO        NO

LLDP agent nearest-customer:
NAME                              STATUS    DEFAULT
```

```
Basic optional TLV:
 Port Description TLV             YES       YES
 System Name TLV                  YES       YES
 System Description TLV           YES       YES
 System Capabilities TLV          YES       YES
 Management Address TLV           YES       YES
IEEE 802.1 extend TLV:
 Port VLAN ID TLV                 NO        NO
 Port And Protocol VLAN ID TLV    NO        NO
 VLAN Name TLV                    NO        NO
 DCBX TLV                         NO        NO
 EVB TLV                          NO        NO
 Link Aggregation TLV             YES       YES
 Management VID TLV               NO        NO
IEEE 802.3 extend TLV:
 MAC-Physic TLV                   NO        NO
 Power via MDI TLV                NO        NO
 Maximum Frame Size TLV           NO        NO
LLDP-MED extend TLV:
 Capabilities TLV                 NO        NO
 Network Policy TLV               NO        NO
 Location Identification TLV      NO        NO
 Extended Power via MDI TLV       NO        NO
 Inventory TLV                    NO        NO
```

Table 5 Command output

Field	Description
LLDP tlv-config of port 1	Advertisable optional TLVs of port 1.
NAME	TLV type.
STATUS	Indicates whether the type of TLV is sent through a port.
DEFAULT	Indicates whether the type of TLV is sent through a port by default.
Basic optional TLV	Basic optional TLVs: • Port Description TLV. • System Name TLV. • System Description TLV. • System Capabilities TLV. • Management Address TLV.
IEEE 802.1 extended TLV	IEEE 802.1 organizationally specific TLVs: • PVID TLV. • Port and protocol VLAN ID TLV. • VLAN name TLV. • DCBX TLV. DCBX TLVs are not supported in the current software version. • EVB TLV. EVB TLVs are not supported in the current software version. • Management VID TLV.
IEEE 802.3 extended TLV	IEEE 802.3 organizationally specific TLVs: • MAC-Physic TLV.

Field	Description
	• Power via MDI TLV. • Link aggregation TLV. • Maximum frame size TLV.
LLDP-MED extend TLV	LLDP-MED TLVs: • Capabilities TLV. • Network Policy TLV. • Extended Power-via-MDI TLV. • Location Identification TLV. • Inventory TLV.
Inventory TLV	Inventory TLVs: • Hardware Revision TLV. • Firmware Revision TLV. • Software Revision TLV. • Serial Number TLV. • Manufacturer Name TLV. • Model name TLV. • Asset ID TLV.

lldp admin-status

Use **lldp admin-status** to set the LLDP operating mode.

Use **undo lldp admin-status** to restore the default.

Syntax

In Layer 2 or Layer 3 Ethernet interface view:

lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **admin-status** { **disable** | **rx** | **tx** | **txrx** }

undo lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **admin-status**

In Layer 2/Layer 3 aggregate interface view:

lldp agent { **nearest-customer** | **nearest-nontpmr** } **admin-status** { **disable** | **rx** | **tx** | **txrx** }

undo lldp agent { **nearest-customer** | **nearest-nontpmr** } **admin-status**

Default

The nearest bridge agent operates in **TxRx** mode, and the nearest customer bridge agent and nearest non-TPMR bridge agent operate in **Disable** mode.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Layer 2 aggregate interface view

Layer 3 aggregate interface view

Predefined user roles

network-admin

context-admin

Parameters

agent: Specifies an LLDP agent type. If you do not specify an agent type in Ethernet interface view, the command sets the operating mode for nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

nearest-nontpmr: Specifies nearest non-TPMR bridge agents.

disable: Specifies the **Disable** mode. A port in this mode cannot send or receive LLDP frames.

rx: Specifies the **Rx** mode. A port in this mode can only receive LLDP frames.

tx: Specifies the **Tx** mode. A port in this mode can only send LLDP frames.

txrx: Specifies the **TxRx** mode. A port in this mode can send and receive LLDP frames.

Examples

Set the LLDP operating mode to **Rx** for the nearest customer bridge agents on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp agent nearest-customer admin-status rx
```

lldp check-change-interval

Use **lldp check-change-interval** to enable LLDP polling and set the polling interval.

Use **undo lldp check-change-interval** to disable LLDP polling.

Syntax

In Layer 2 or Layer 3 Ethernet interface view:

lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **check-change-interval** *interval*

undo lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **check-change-interval**

In Layer 2/Layer 3 aggregate interface view:

lldp agent { **nearest-customer** | **nearest-nontpmr** } **check-change-interval** *interval*

undo lldp agent { **nearest-customer** | **nearest-nontpmr** } **check-change-interval**

Default

LLDP polling is disabled.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Layer 2 aggregate interface view

Layer 3 aggregate interface view

Predefined user roles

network-admin

context-admin

Parameters

agent: Specifies an LLDP agent type. If you do not specify an agent type in Ethernet interface view, the command enables LLDP polling and sets the polling interval for nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

nearest-nontpmr: Specifies nearest non-TPMR bridge agents.

interval: Sets the LLDP polling interval in the range of 1 to 30 seconds.

Examples

Enable LLDP polling and set the polling interval to 30 seconds for the nearest customer bridge agents on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp agent nearest-customer check-change-interval 30
```

lldp compliance admin-status cdp

Use **lldp compliance admin-status cdp** to set the operating mode of CDP-compatible LLDP.

Use **undo lldp compliance admin-status cdp** to restore the default.

Syntax

lldp compliance admin-status cdp { **disable** | **txrx** }

undo lldp compliance admin-status cdp

Default

CDP-compatible LLDP operates in **Disable** mode.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Management Ethernet interface view

Predefined user roles

network-admin

context-admin

Parameters

disable: Specifies the **Disable** mode. CDP-compatible LLDP in this mode cannot receive or transmit CDP packets.

txrx: Specifies the **TxRx** mode. CDP-compatible LLDP in this mode can send and receive CDP packets.

Usage guidelines

For your device to work with Cisco IP phones, you must perform the following tasks:

- Enable CDP-compatible LLDP globally.
- Configure CDP-compatible LLDP to operate in TxRx mode on the specified ports.

Examples

Enable CDP-compatible LLDP globally and configure CDP-compatible LLDP to operate in **TxRx** mode on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] lldp compliance cdp
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp compliance admin-status cdp txrx
```

Related commands

lldp compliance cdp

lldp compliance cdp

Use **lldp compliance cdp** to enable CDP compatibility.

Use **undo lldp compliance cdp** to disable CDP compatibility.

Syntax

lldp compliance cdp

undo lldp compliance cdp

Default

CDP compatibility is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

The maximum TTL that CDP allows is 255 seconds. To make CDP-compatible LLDP work correctly with Cisco IP phones, set the LLDP frame transmission interval to be no more than 1/3 of the TTL value.

Examples

Enable CDP compatibility.

```
<Sysname> system-view
[Sysname] lldp compliance cdp
```

Related commands

lldp hold-multiplier

lldp timer tx-interval

lldp enable

Use **lldp enable** to enable LLDP on a port.

Use **undo lldp enable** to disable LLDP on a port.

Syntax

lldp enable

undo lldp enable

Default

LLDP is enabled on a port.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Layer 2 aggregate interface view

Layer 3 aggregate interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

LLDP takes effect on a port only when LLDP is enabled both globally and on the port.

Examples

Disable LLDP on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo lldp enable
```

Related commands

lldp global enable

lldp encapsulation snap

Use **lldp encapsulation snap** to set the encapsulation format for LLDP frames to SNAP.

Use **undo lldp encapsulation** to restore the default.

Syntax

In Layer 2 or Layer 3 Ethernet interface view:

lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **encapsulation snap**

undo lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **encapsulation**

In Layer 2/Layer 3 aggregate interface view:

lldp agent { **nearest-customer** | **nearest-nontpmr** } **encapsulation snap**

undo lldp agent { **nearest-customer** | **nearest-nontpmr** } **encapsulation**

Default

The encapsulation format for LLDP frames is Ethernet II.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Layer 2 aggregate interface view

Layer 3 aggregate interface view

Predefined user roles

network-admin

context-admin

Parameters

agent: Specifies an LLDP agent type. If you do not specify an agent type in Ethernet interface view, the command sets the LLDP frame encapsulation format for nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

nearest-nontpmr: Specifies nearest non-TPMR bridge agents.

Usage guidelines

LLDP-CDP packets use only SNAP encapsulation.

Examples

Set the encapsulation format for LLDP frames to SNAP on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp encapsulation snap
```

lldp fast-count

Use **lldp fast-count** to set the number of LLDP frames sent each time fast LLDP frame transmission is triggered.

Use **undo lldp fast-count** to restore the default.

Syntax

lldp fast-count *count*

undo lldp fast-count

Default

Four LLDP frames are sent each time fast LLDP frame transmission is triggered.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

count: Sets the number of LLDP frames sent each time fast LLDP frame transmission is triggered. The value range is 1 to 8.

Examples

Configure the device to send five LLDP frames each time fast LLDP frame transmission is triggered.

```
<Sysname> system-view
[Sysname] lldp fast-count 5
```

lldp global enable

Use **lldp global enable** to enable LLDP globally.

Use **undo lldp global enable** to disable LLDP globally.

Syntax

lldp global enable

undo lldp global enable

Default

LLDP is disabled globally.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

LLDP takes effect on a port only when LLDP is enabled both globally and on the port.

Examples

Disable LLDP globally.

```
<Sysname> system-view
[Sysname] undo lldp global enable
```

Related commands

lldp enable

lldp hold-multiplier

Use **lldp hold-multiplier** to set the TTL multiplier.

Use **undo lldp hold-multiplier to** restore the default.

Syntax

lldp hold-multiplier *value*

undo lldp hold-multiplier

Default

The TTL multiplier is 4.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

value: Sets the TTL multiplier in the range of 2 to 10.

Usage guidelines

The TTL TLV carried in an LLDPDU determines how long the device information carried in the LLDPDU can be saved on a recipient device.

By setting the TTL multiplier, you can set the TTL of locally sent LLDP frames. The TTL is expressed by using the following formula:

TTL = Min (65535, (TTL multiplier × LLDP frame transmission interval + 1))

As the expression shows, the TTL can be up to 65535 seconds.

Examples

Set the TTL multiplier to 6.

```
<Sysname> system-view
[Sysname] lldp hold-multiplier 6
```

Related commands

lldp timer tx-interval

lldp ignore-pvid-inconsistency

Use **lldp ignore-pvid-inconsistency** to disable LLDP PVID inconsistency check.

Use **undo lldp ignore-pvid-inconsistency** to enable LLDP PVID inconsistency check.

Syntax

lldp ignore-pvid-inconsistency

undo lldp ignore-pvid-inconsistency

Default

LLDP PVID inconsistency check is enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

By default, when the system receives an LLDP packet, it compares the PVID value contained in packet with the PVID configured on the receiving interface. If the two PVIDs do not match, a log message will be printed to notify the user.

You can disable PVID inconsistency check if different PVIDs are required on a link.

Examples

Disable LLDP PVID inconsistency check.

```
<Sysname> system-view
[Sysname] lldp ignore-pvid-inconsistency
```

lldp management-address

Use **lldp management-address** to enable the device to generate an ARP or ND entry after receiving an LLDP frame that carries a management address TLV.

Use **undo lldp management-address** to restore the default.

Syntax

lldp management-address { **arp-learning** | **nd-learning** } [**vlan** *vlan-id*]

undo lldp management-address { **arp-learning** | **nd-learning** }

Default

The device does not generate an ARP or ND entry after receiving an LLDP frame that carries a management address TLV.

Views

Layer 3 Ethernet interface view

Predefined user roles

network-admin

context-admin

Parameters

arp-learning: Generates an ARP entry if the received management address TLV contains an IPv4 address.

nd-learning: Generates an ND entry if the received management address TLV contains an IPv6 address.

vlan *vlan-id*: Specifies the Layer 3 Ethernet subinterface that terminates the specified VLAN as the output interface. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN ID, the Layer 3 Ethernet interface is recorded as the output interface.

Usage guidelines

This command must be used together with the **lldp source-mac vlan** command for the device to use the MAC address of a Layer 3 Ethernet subinterface as the source MAC address of LLDP frames. This ensures that the LLDP neighbor can learn correct ARP or ND entries.

You can enable the device to generate both ARP entries and ND entries.

If you specify the **vlan** *vlan-id* option, the Layer 3 Ethernet subinterface that terminates the VLAN is recorded as the output interface in the generated ARP or ND entries. If the VLAN is not terminated by any Layer 3 Ethernet subinterface or the **vlan** *vlan-id* option is not specified, the Layer 3 Ethernet interface is recorded as the output interface. For more information about VLAN termination, see VLAN termination configuration in *Layer 2—LAN Switching Configuration Guide*.

Examples

Configure GigabitEthernet 1/0/1 to generate an ARP entry after receiving an LLDP frame carrying an IPv4 management address TLV.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp management-address arp-learning
```

Related commands

lldp source-mac vlan

lldp management-address-format string

Use **lldp management-address-format string** to set the encoding format of the management address to string.

Use **undo lldp management-address-format** to restore the default.

Syntax

In Layer 2 or Layer 3 Ethernet interface view:

lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **management-address-format string**

undo lldp [agent { nearest-customer | nearest-nontpmr }] management-address-format

In Layer 2/Layer 3 aggregate interface view:

lldp agent { nearest-customer | nearest-nontpmr } management-address-format string

undo lldp agent { nearest-customer | nearest-nontpmr } management-address-format

Default

The encoding format of the management address is numeric.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Layer 2 aggregate interface view

Layer 3 aggregate interface view

Predefined user roles

network-admin

context-admin

Parameters

agent: Specifies an LLDP agent type. If you do not specify an agent type in Ethernet interface view, the command sets the encoding format of the management address for nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

nearest-nontpmr: Specifies nearest non-TPMR bridge agents.

Usage guidelines

LLDP neighbors must use the same encoding format for the management address. If a neighbor encodes its management address in string format, set the encoding format of the management address to **string** on the connecting port. This guarantees normal communication with the neighbor.

Examples

Set the encoding format of the management address to string for the nearest customer bridge agents on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp agent nearest-customer management-address-format string
```

lldp max-credit

Use **lldp max-credit** to set the token bucket size for sending LLDP frames.

Use **undo lldp max-credit** to restore the default.

Syntax

lldp max-credit *credit-value*

undo lldp max-credit

Default

The token bucket size for sending LLDP frames is 5.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

credit-value: Specifies the token bucket size for sending LLDP frames, in the range of 1 to 100.

Examples

Set the token bucket size for sending LLDP frames to 10.

```
<Sysname> system-view
[Sysname] lldp max-credit 10
```

lldp mode

Use **lldp mode** to configure LLDP to operate in service bridge mode.

Use **undo lldp mode** to restore the default.

Syntax

lldp mode service-bridge

undo lldp mode

Default

LLDP operates in customer bridge mode.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

service-bridge: Specifies the service bridge mode.

Usage guidelines

The LLDP agent types supported by LLDP depend on the LLDP bridge mode:

- **Service bridge mode**—LLDP supports nearest bridge agents and nearest non-TPMR bridge agents. LLDP processes the LLDP frames with destination MAC addresses for these agents and transparently transmits the LLDP frames with other destination MAC addresses in a VLAN.
- **Customer bridge mode**—LLDP supports nearest bridge agents, nearest non-TPMR bridge agents, and nearest customer bridge agents. LLDP processes the LLDP frames with destination MAC addresses for these agents and transparently transmits the LLDP frames with other destination MAC addresses in a VLAN.

The bridge mode configuration takes effect only when LLDP is enabled globally. If LLDP is disabled globally, LLDP can only operate in customer bridge mode.

Examples

Configure LLDP to operate in service bridge mode.

```
<Sysname> system-view
[Sysname] lldp mode service-bridge
```

Related commands

lldp global enable

lldp notification med-topology-change enable

Use **lldp notification med-topology-change enable** to enable LLDP-MED trapping.

Use **undo lldp notification med-topology-change enable** to disable LLDP-MED trapping.

Syntax

lldp notification med-topology-change enable

undo lldp notification med-topology-change enable

Default

LLDP-MED trapping is disabled.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Predefined user roles

network-admin

context-admin

Examples

Enable LLDP-MED trapping on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp notification med-topology-change enable
```

lldp notification remote-change enable

Use **lldp notification remote-change enable** to enable LLDP trapping.

Use **undo lldp notification remote-change enable** to disable LLDP trapping.

Syntax

In Layer 2 or Layer 3 Ethernet interface view:

lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **notification remote-change enable**

undo lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **notification remote-change enable**

In Layer 2/Layer 3 aggregate interface view:

lldp agent { **nearest-customer** | **nearest-nontpmr** } **notification remote-change enable**

undo lldp agent { **nearest-customer** | **nearest-nontpmr** } **notification remote-change enable**

Default

LLDP trapping is disabled.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Layer 2 aggregate interface view

Layer 3 aggregate interface view

Predefined user roles

network-admin

context-admin

Parameters

agent: Specifies an LLDP agent type. If you do not specify an agent type in Ethernet interface view, the command enables LLDP trapping for nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

nearest-nontpmr: Specifies nearest non-TPMR bridge agents.

Examples

Enable LLDP trapping for the nearest customer bridge agent on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp agent nearest-customer notification remote-change enable
```

lldp source-mac vlan

Use **lldp source-mac vlan** to set the source MAC address of LLDP frames to the MAC address of a Layer 3 Ethernet subinterface.

Use **undo lldp source-mac vlan** to restore the default.

Syntax

lldp source-mac vlan *vlan-id*

undo lldp source-mac vlan

Default

The source MAC address of LLDP frames is the MAC address of the egress interface.

Views

Layer 3 Ethernet interface view

Predefined user roles

network-admin

context-admin

Parameters

vlan *vlan-id*: Specifies the Layer 3 Ethernet subinterface that terminates the specified VLAN to provide the source MAC address for LLDP frames. The VLAN ID is in the range of 1 to 4094.

Usage guidelines

This command must be used together with the **lldp management-address** command for the device to use the MAC address of a Layer 3 Ethernet subinterface as the source MAC address of LLDP frames. This ensures that the LLDP neighbor can learn correct ARP or ND entries.

This command enables the device to use the MAC address of the Layer 3 Ethernet subinterface that terminates the specified VLAN as the source MAC address of outgoing LLDP frames. If the VLAN is not terminated by any Layer 3 Ethernet subinterface, the MAC address of the Layer 3 Ethernet interface is used as the source MAC address of outgoing LLDP frames. For more information about VLAN termination, see VLAN termination configuration in *Layer 2—LAN Switching Configuration Guide*.

Examples

Set the source MAC address of LLDP frames to the MAC address of the Layer 3 Ethernet subinterface that terminates VLAN 4094.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp source-mac vlan 4094
```

Related commands

lldp management-address arp-learning

lldp timer fast-interval

Use **lldp timer fast-interval** to set an interval for fast LLDP frame transmission.

Use **undo lldp timer fast-interval** to restore the default.

Syntax

lldp timer fast-interval *interval*

undo lldp timer fast-interval

Default

The interval for fast LLDP frame transmission is 1 second.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interval: Sets an interval for fast LLDP frame transmission, in the range of 1 to 3600 seconds.

Examples

Set the interval for fast LLDP frame transmission to 2 seconds.

```
<Sysname> system-view
[Sysname] lldp timer fast-interval 2
```

lldp timer notification-interval

Use **lldp timer notification-interval** to set the LLDP trap and LLDP-MED trap transmission interval.

Use **undo lldp timer notification-interval** to restore the default.

Syntax

lldp timer notification-interval *interval*

undo lldp timer notification-interval

Default

The LLDP trap and LLDP-MED trap transmission interval is 30 seconds.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interval: Sets the LLDP trap and LLDP-MED trap transmission interval in the range of 5 to 3600 seconds.

Examples

Set both the LLDP trap and LLDP-MED trap transmission interval to 8 seconds.

```
<Sysname> system-view
[Sysname] lldp timer notification-interval 8
```

lldp timer reinit-delay

Use **lldp timer reinit-delay** to set the LLDP reinitialization delay.

Use **undo lldp timer reinit-delay** to restore the default.

Syntax

lldp timer reinit-delay *delay*

undo lldp timer reinit-delay

Default

The LLDP reinitialization delay is 2 seconds.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

delay: Sets the LLDP reinitialization delay in the range of 1 to 10 seconds.

Examples

Set the LLDP reinitialization delay to 4 seconds.

```
<Sysname> system-view
[Sysname] lldp timer reinit-delay 4
```

lldp timer rx-timeout

Use **lldp timer rx-timeout** to set the timeout for receiving LLDP frames and enable the device to report no LLDP neighbor events.

Use **undo lldp timer rx-timeout** to restore the default.

Syntax

lldp timer rx-timeout *timeout*

undo lldp timer rx-timeout

Default

No timeout is set for receiving LLDP frames, and the device does not report no LLDP neighbor events.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

timeout: Sets the timeout for receiving LLDP frames, in the range of 30 to 32768 seconds.

Usage guidelines

This command can detect only directly connected LLDP neighbors.

When you use this command, make sure the following requirements are met:

- LLDP is enabled.
- Interfaces are physically up.
- Nearest bridge agents operate in **Rx** or **TxRx** mode.

After this command is executed, the device restarts the timeout timer for receiving LLDP frames on an interface in one of the following situations:

- When LLDP is enabled, the interface state changes from down to up.
- When the interface is physically up, LLDP is enabled.
- When LLDP is enabled and the interface is physically up, the mode of nearest bridge agents is changed from disabled to **Rx** or **TxRx**.

If an interface has not received any LLDP frames when the timeout timer expires, the device reports a no LLDP neighbor event to the NETCONF module.

To avoid misdetection, make sure the timeout for receiving LLDP frames is greater than the LLDP frame transmission interval.

Examples

Set the timeout for receiving LLDP frames to 30 seconds.

```
<Sysname> system-view
[Sysname] lldp timer rx-timeout 30
```

Related commands

lldp timer tx-interval

lldp timer tx-interval

Use **lldp timer tx-interval** to set the LLDP frame transmission interval.

Use **undo lldp timer tx-interval** to restore the default.

Syntax

lldp timer tx-interval *interval*

undo lldp timer tx-interval

Default

The LLDP frame transmission interval is 30 seconds.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interval: Sets the LLDP frame transmission interval in the range of 5 to 32768 seconds.

Examples

Set the LLDP frame transmission interval to 20 seconds.

```
<Sysname> system-view
[Sysname] lldp timer tx-interval 20
```

lldp tlv-enable

Use **lldp tlv-enable** to configure the types of advertisable TLVs on a port.

Use **undo lldp tlv-enable** to disable the advertising of the specified types of TLVs on a port.

Syntax

In Layer 2 Ethernet interface view:

- For nearest bridge agents:

lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** | **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] } | **dot3-tlv** { **all** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **network-policy** [*vlan-id*] | **power-over-ethernet** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* }&<1-10> | **elin-address** *tel-number* } } }

undo lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** | **protocol-vlan-id** | **vlan-name** | **management-vid** } | **dot3-tlv** { **all** | **mac-physic** | **max-frame-size** | **power** } |

med-tlv { **all** | **capability** | **inventory** | **network-policy** [*vlan-id*] | **power-over-ethernet** | **location-id** } }

- For nearest non-TPMR bridge agents:

lldp agent nearest-nontpmr tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** } }

lldp tlv-enable dot1-tlv { **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] }

undo lldp agent nearest-nontpmr tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** } }

undo lldp tlv-enable dot1-tlv { **protocol-vlan-id** | **vlan-name** | **management-vid** }

- For nearest customer bridge agents:

lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** } }

lldp tlv-enable dot1-tlv { **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] }

undo lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** } }

undo lldp tlv-enable dot1-tlv { **protocol-vlan-id** | **vlan-name** | **management-vid** }

In Layer 3 Ethernet interface view:

lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address* | **interface loopback** *interface-number*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **power-over-ethernet** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* }&<1-10> | **elin-address** *tel-number* } } }

lldp agent { **nearest-nontpmr** | **nearest-customer** } **tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } }

undo lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address* | **interface loopback** *interface-number*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **power-over-ethernet** | **location-id** } }

undo lldp agent { **nearest-nontpmr** | **nearest-customer** } **tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } }

In Layer 2 aggregate interface view:

lldp agent nearest-nontpmr tlv-enable { **basic-tlv** { **all** | **management-address-tlv** [**ipv6**] [*ip-address*] | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** } }

lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **management-address-tlv** [**ipv6**] [*ip-address*] | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** } }

lldp tlv-enable dot1-tlv { **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] }

undo lldp agent nearest-nontpmr tlv-enable { **basic-tlv** { **all** | **management-address-tlv** [**ipv6**] [*ip-address*] | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** } }

undo lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **management-address-tlv** [**ipv6**] [*ip-address*] | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** } }

undo lldp tlv-enable dot1-tlv { **protocol-vlan-id** | **vlan-name** | **management-vid** }

In Layer 3 aggregate interface view:

lldp agent { **nearest-customer** | **nearest-nontpmr** } **tlv-enable basic-tlv** { **all** | **management-address-tlv** [**ipv6**] [*ip-address*] | **port-description** | **system-capability** | **system-description** | **system-name** }

undo lldp agent { **nearest-customer** | **nearest-nontpmr** } **tlv-enable basic-tlv** { **all** | **management-address-tlv** [**ipv6**] [*ip-address*] | **port-description** | **system-capability** | **system-description** | **system-name** }

Default

On Layer 2 Ethernet interfaces:

- Nearest bridge agents can advertise all types of LLDP TLVs except the following types:
  - Location identification TLVs.
  - Port and protocol VLAN ID TLVs.
  - VLAN name TLVs.
  - Management VLAN ID TLVs.
- Nearest customer bridge agents can advertise basic TLVs and IEEE 802.1 organizationally specific TLVs.

On Layer 3 Ethernet interfaces:

- Nearest bridge agents can advertise all types of LLDP TLVs except network policy TLVs. Among all the 802.1 organizationally specific TLVs, only the link aggregation TLV is supported.
- Nearest non-TPMR bridge agents do not advertise TLVs.
- Nearest customer bridge agents can advertise basic TLVs and IEEE 802.1 organizationally specific TLVs (only link aggregation TLV is supported).

On Layer 2 aggregate interfaces:

- Nearest non-TPMR bridge agents do not advertise any TLVs.

- Nearest customer bridge agents can advertise basic TLVs and IEEE 802.1 organizationally specific TLVs. Among the IEEE 802.1 organizationally specific TLVs, only port and protocol VLAN ID TLVs, VLAN name TLVs, and management VLAN ID TLVs are supported.

On Layer 3 aggregate interfaces:

- Nearest non-TPMR bridge agents do not advertise TLVs.
- Nearest customer bridge agents can advertise only basic TLVs.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Layer 2 aggregate interface view

Layer 3 aggregate interface view

Predefined user roles

network-admin

context-admin

Parameters

agent: Specifies an LLDP agent type. If you do not specify an agent type in Ethernet interface view, the command configures the types of advertisable TLVs for nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

nearest-nontpmr: Specifies nearest non-TPMR bridge agents.

all: Advertises all TLVs of the specified type. This keyword enables the interface to advertise following TLVs:

- All basic LLDP TLVs if the **all** keyword is specified for **basic-tlv**.
- All IEEE 802.1 organizationally specific LLDP TLVs if the **all** keyword is specified for **dot1-tlv**.
- All IEEE 802.3 organizationally specific LLDP TLVs if the **all** keyword is specified for **dot3-tlv**.
- All LLDP-MED TLVs except location identification TLVs if the **all** keyword is specified for **med-tlv**.

basic-tlv: Advertises basic LLDP TLVs.

management-address-tlv [**ipv6**] [*ip-address* | **interface loopback** *interface-number*]: Advertises management address TLVs. The **ipv6** keyword indicates that the management address to be advertised is in IPv6 format. The *ip-address* argument specifies the management address to be advertised. The **interface loopback** *interface-number* option specifies the management address as the IP address of a loopback interface specified by its number. By default, the following rules apply:

- When you execute the **lldp tlv-enable** command:
  - For a Layer 2 Ethernet or aggregate interface, the IPv4 or IPv6 address of the VLAN interface that meets the following requirements will be advertised as the management address:
    - In up state.
    - The corresponding VLAN ID is the lowest among the VLANs permitted on the interface.

    If you specify the **ipv6** keyword, the IPv6 address of the VLAN interface will be advertised. If you do not specify the **ipv6** keyword, the IPv4 address of the VLAN interface will be advertised.

If none of the VLAN interfaces of the permitted VLANs is assigned an IPv4 or IPv6 address or all VLAN interfaces are down, the MAC address of the interface will be advertised.

- For a Layer 3 Ethernet interface, the IPv4 or IPv6 address of the interface will be advertised when the following conditions exist:
  - The *ip-address* argument is not configured.
  - The specified loopback interface does not have an IPv4 or IPv6 address, or the specified loopback interface does not exist.

  If you specify the **ipv6** keyword, the IPv6 address of the interface will be advertised. If you do not specify the **ipv6** keyword, the IPv4 address of the interface will be advertised.

  If the interface does not have an IPv4 or IPv6 address, the MAC address of the interface will be advertised.
- For a Layer 3 aggregate interface, the IPv4 or IPv6 address of the interface will be advertised when the *ip-address* argument is not configured.

  If you specify the **ipv6** keyword, the IPv6 address of the interface will be advertised. If you do not specify the **ipv6** keyword, the IPv4 address of the interface will be advertised.

  If the interface does not have an IPv4 or IPv6 address, the MAC address of the interface will be advertised.

- For a Layer 2/Layer 3 Ethernet interface or Layer 2/Layer 3 aggregate interface, when you execute the **undo lldp tlv-enable** command:
  - If you do not specify *ip-address*, **ipv6**, or **interface loopback** *interface-number*, the interface does not advertise any management address TLVs.
  - If you specify *ip-address*, **ipv6**, or **interface loopback** *interface-number*, the interface advertises the default management address TLVs.

port-description: Advertises port description TLVs.

system-capability: Advertises system capabilities TLVs.

system-description: Advertises system description TLVs.

system-name: Advertises system name TLVs.

dot1-tlv: Advertises IEEE 802.1 organizationally specific LLDP TLVs.

port-vlan-id: Advertises port VLAN ID TLVs.

protocol-vlan-id [*vlan-id*]: Advertises port and protocol VLAN ID TLVs. The *vlan-id* argument specifies a VLAN ID in the TLVs to be advertised. The VLAN ID is in the range of 1 to 4094, and the default is the lowest VLAN ID on the port.

vlan-name [*vlan-id*]: Advertises VLAN name TLVs. The *vlan-id* argument specifies a VLAN ID in the TLVs to be advertised. The VLAN ID is in the range of 1 to 4094, and the default is the lowest VLAN ID on the port. If you do not specify a VLAN ID and the port is not assigned to any VLAN, the PVID of the port is advertised.

management-vid [*mvlan-id*]: Advertises management VLAN ID TLVs. The m*vlan-id* argument specifies a management VLAN ID in the TLVs to be advertised. The management VLAN ID is in the range of 1 to 4094. If you do not specify this option, the value 0 is advertised, which means that the LLDP agent is not configured with a management VLAN ID.

link-aggregation: Advertises link aggregation TLVs.

dot3-tlv: Advertises IEEE 802.3 organizationally specific LLDP TLVs.

mac-physic: Advertises MAC/PHY configuration/status TLVs.

max-frame-size: Advertises maximum frame size TLVs.

power: Advertises power in MDI TLVs and power stateful control TLVs.

med-tlv: Advertises LLDP-MED TLVs.

capability: Advertises LLDP-MED capabilities TLVs.

inventory: Advertises the following TLVs: hardware revision, firmware revision, software revision, serial number, manufacturer name, model name, and asset ID.

location-id: Advertises location identification TLVs.

civic-address: Inserts the typical address information about the network device in location identification TLVs .

device-type: Sets a device type value in the range of 0 to 2:

- Value 0 specifies a DHCP server.
- Value 1 specifies a network device.
- Value 2 specifies an LLDP-MED endpoint.

country-code: Sets a country code defined in ISO 3166.

{ *ca-type ca-value* }&<1-10>: Configures address information. *ca-type* represents the address information type in the range of 0 to 255. *ca-value* represents address information, a string of 1 to 250 characters. &<1-10> indicates that you can specify up to 10 *ca-type ca-value* pairs.

elin-address: Inserts telephone numbers for emergencies in location identification TLVs.

tel-number: Sets the telephone number for emergencies, a string of 10 to 25 characters.

network-policy [*vlan-id*]: Advertises network policy TLVs. The *vlan-id* argument specifies the VLAN ID to be advertised, in the range of 1 to 4094.

power-over-ethernet: Advertises extended power-via-MDI TLVs.

Usage guidelines

Nearest bridge agents are not supported on aggregate interfaces.

You can enable the device to advertise multiple types of TLVs by using this command without the **all** keyword specified.

If the MAC/PHY configuration/status TLV is not advertisable, none of the LLDP-MED TLVs will be advertised whether or not they are advertisable. If the LLDP-MED capabilities TLV is not advertisable, the other LLDP-MED TLVs will not be advertised regardless of whether or not they are advertisable.

The port and protocol VLAN ID, VLAN name, and management VLAN ID TLVs in IEEE 802.1 organizationally specific LLDP TLVs can be configured only for nearest bridge agents. The configuration can be inherited by nearest customer bridge agents and nearest non-TPMR bridge agents.

Examples

Enable the nearest customer bridge agents on GigabitEthernet 1/0/1 to advertise link aggregation TLVs of the IEEE 802.1 organizationally specific TLVs.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp agent nearest-customer tlv-enable dot1-tlv
link-aggregation
```

Contents

Layer 2 forwarding commands

Normal Layer 2 forwarding commands

display mac-forwarding statistics

Use **display mac-forwarding statistics** to display Layer 2 forwarding statistics.

Syntax

display mac-forwarding statistics [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify this option, the command displays Layer 2 forwarding statistics on all interfaces.

Examples

Display Layer 2 forwarding statistics on all interfaces.

```
<Sysname> display mac-forwarding statistics
Input:
   Sum:               888        Unknown Unicast:   0
   Broadcast:         0          Multicast:         0
   Filtered:          0          STP discarded:     0
   Service dropped:   0          Source dropped:    0
   Unknown dropped: 0          Learning dropped:  0
   Blackhole dropped: 0          Suppress dropped:  0
   Source MAC dropped:0
Deliver:
   Sum:               111        L2 protocol:       11
   Local MAC address: 100
Output:
   Sum:               666        Filtered:          0
   Blackhole dropped: 0          STP discarded:     0
   Service dropped:   0          Dest MAC dropped:  0
```

Display Layer 2 forwarding statistics on GigabitEthernet 1/0/1.

```
<Sysname> display mac-forwarding statistics interface gigabitethernet 1/0/1
GigabitEthernet1/0/1:
Input frames: 100    Output frames:100
```

```
Filtered:     0
```

Table 1 Command output

Field	Description
Input	Inbound Ethernet frame statistics. • **Sum**—Total number of received Ethernet frames. • **Filtered**—Number of Ethernet frames filtered out by 802.1Q VLAN inbound filtering rules. • **STP discarded**—Number of inbound Ethernet frames dropped on the ports blocked by STP. • **Service dropped**—Number of Ethernet frames dropped by inbound service features. • **Source dropped**—Number of Ethernet frames dropped because their source MAC addresses are all-zeros, multicast, or broadcast MAC addresses. • **Unknown dropped**—Number of Ethernet frames dropped because the device is disabled from forwarding frames with unknown source MAC addresses. • **Learning dropped**—Number of Ethernet frames dropped because the device is disabled from forwarding unknown frames after the number of learned MAC addresses reaches the upper limit. • **Suppress dropped**—Number of Ethernet frames dropped by storm suppression. • **Broadcast**—Number of received broadcast Ethernet frames. • **Multicast**—Number of received multicast Ethernet frames. • **Unknown unicast**—Number of received unknown unicast Ethernet frames. • **Blackhole dropped**—Number of Ethernet frames dropped because they are sourced from blackhole MAC addresses. • **Source MAC dropped**—Number of Ethernet frames dropped by features based on the source MAC addresses.
Deliver	Statistics of Ethernet frames delivered to the CPU. • **Sum**—Total number of Ethernet frames delivered to the CPU. • **L2 protocol**—Number of Layer 2 protocol Ethernet frames delivered to the CPU. • **Local MAC address**—Number of Ethernet frames that use the MAC addresses of local Layer 3 VLAN interfaces as the destination MAC addresses.
Output	Outbound Ethernet frame statistics. • **Sum**—Total number of sent Ethernet frames. • **Filtered**—Number of Ethernet frames filtered out by 802.1Q VLAN outbound filtering rules. • **Blackhole dropped**—Number of Ethernet frames dropped because they are destined for blackhole MAC addresses. • **STP discarded**—Number of outbound Ethernet frames dropped on the ports blocked by STP. • **Service dropped**—Number of Ethernet frames dropped by outbound service features. • **Dest MAC dropped**—Number of Ethernet frames dropped by features based on the destination MAC addresses.
GigabitEthernet1/0/1	Layer 2 forwarding statistics on GigabitEthernet 1/0/1: • **Input frames**—Number of Ethernet frames received on the interface. • **Output frames**—Number of Ethernet frames sent out of the interface. • **Filtered**—Number of Ethernet frames filtered out because they are from other VLANs.

reset mac-forwarding statistics

Use **reset mac-forwarding statistics** to clear Layer 2 forwarding statistics.

Syntax

reset mac-forwarding statistics

Views

User view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Clear Layer 2 forwarding statistics.

```
<Sysname> reset mac-forwarding statistics
```

Fast Layer 2 forwarding commands

display mac-forwarding cache ip

Use **display mac-forwarding cache ip** to display IPv4 fast forwarding entries.

Syntax

display mac-forwarding cache ip [*ip-address*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ip-address: Specifies an IPv4 address. If you do not specify an IPv4 address, this command displays all IPv4 fast forwarding entries.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv4 fast forwarding entries for all member devices.

Examples

Display all IPv4 fast forwarding entries.

```
<Sysname> display mac-forwarding cache ip
Total number of mac-forwarding entries: 2
SIP            SPort DIP             DPort Pro Input_If    Output_If   VLAN
```

```
1.1.1.2         99    1.1.1.1         2048  1   GE1/0/1     GE1/0/2     2
1.1.1.1         98    1.1.1.2         2012  1   GE1/0/2     GE1/0/1     2
```

Table 2 Command output

Field	Description
Total number of mac-forwarding entries	Total number of IPv4 fast forwarding entries.
SIP	Source IPv4 address.
SPort	Source port number.
DIP	Destination IPv4 address.
DPort	Destination port number.
Pro	Protocol number.
Input_If	Input interface type and number. If no input interface is involved in fast forwarding, this field displays **N/A**. If no input interface is available, this field displays a hyphen (-).
Output_If	Output interface type and number. If no output interface is involved in fast forwarding, this field displays **N/A**. If no output interface is available, this field displays a hyphen (-).
VLAN	VLAN ID.

display mac-forwarding cache ip fragment

Use **display mac-forwarding cache ip fragment** to display IPv4 fast forwarding entries for fragments.

Syntax

display mac-forwarding cache ip fragment [*ip-address*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ip-address: Specifies an IPv4 address. If you do not specify an IPv4 address, this command displays IPv4 fast forwarding entries for all fragments.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv4 fast forwarding entries for fragments on all member devices.

Examples

Display IPv4 fast forwarding entries for all fragments.

```
<Sysname> display mac-forwarding cache ip fragment
Total number of fragment mac-forwarding entries: 2
SIP             SPort DIP             DPort Pro Input_If    ID     VLAN
1.1.1.1         117   1.1.1.2         0     1   GE1/0/1     2828   1
1.1.1.2         110   1.1.1.1         67    17  GE1/0/2     2322   1
```

Table 3 Command output

Field	Description
Total number of fragment mac-forwarding entries	Total number of IPv4 fast forwarding entries for fragments.
SIP	Source IPv4 address.
SPort	Source port number.
DIP	Destination IPv4 address.
DPort	Destination port number.
Pro	Protocol number.
Input_If	Input interface type and number. If no input interface is involved in fast forwarding, this field displays **N/A**. If no input interface is available, this field displays a hyphen (-).
ID	Fragment ID.
VLAN	VLAN ID.

display mac-forwarding cache ipv6

Use **display mac-forwarding cache ipv6** to display IPv6 fast forwarding entries.

Syntax

display mac-forwarding cache ipv6 [*ipv6-address*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ipv6-address: Specifies an IPv6 address. If you do not specify an IPv6 address, this command displays all IPv6 fast forwarding entries.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv6 fast forwarding entries for all member devices.

Examples

Display all IPv6 fast forwarding entries.

```
<Sysname> display mac-forwarding cache ipv6
Total number of IPv6 mac-forwarding items: 1
Src IP: 2002::1                                         Src port: 129
Dst IP: 2001::1                                         Dst port: 65535
VLAN ID: 2
Protocol: 2
Input interface: GE1/0/2
Output interface: GE1/0/1
```

Table 4 Command output

Field	Description
Total number of IPv6 mac-forwarding items	Total number of IPv6 fast forwarding entries.
Src IP	Source IPv6 address.
Src port	Source port number.
Dst IP	Destination IPv6 address.
Dst Port	Destination port number.
Protocol	Protocol number.
Input interface	Input interface type and number. If no input interface is involved in fast forwarding, this field displays **N/A**. If no input interface is available, this field displays a hyphen (-).
Output interface	Output interface type and number. If no output interface is involved in fast forwarding, this field displays **N/A**. If no output interface is available, this field displays a hyphen (-).

mac fast-forwarding check-vlan-id

Use **mac fast-forwarding check-vlan-id** to enable VLAN ID check for fast Layer 2 forwarding.

Use **undo mac fast-forwarding check-vlan-id** to disable VLAN ID check for fast Layer 2 forwarding.

Syntax

mac fast-forwarding check-vlan-id

undo mac fast-forwarding check-vlan-id

Default

VLAN ID check is enabled for fast Layer 2 forwarding.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This feature allows the device to check whether the VLAN ID of a flow matches that of any fast forwarding entry. If no match is found, the flow does not match any fast forwarding entry.

The VLAN ID of a packet helps the device to determine the TCP session to which the packet belongs. On a hot backup system formed by two firewalls, you must disable VLAN ID check if the traffic incoming interfaces on the primary and secondary devices belong to different VLANs. If you enable VLAN ID check, traffic cannot match session entries correctly when asymmetric-path traffic exists.

Examples

Enable VLAN ID check for fast Layer 2 forwarding.

```
<Sysname> system-view
[Sysname] mac fast-forwarding check-vlan-id
```

Bridge forwarding commands

add interface

Use **add interface** to add an interface to a reflect-type, forward-type, or blackhole-type bridge instance.

Use **undo add interface** to remove an interface from a reflect-type, forward-type, or blackhole-type bridge instance.

Syntax

add interface *interface-type interface-number*

undo add interface *interface-type interface-number*

Default

No interfaces exist in a reflect-type, forward-type, or blackhole-type bridge instance.

Views

Reflect-type bridge view

Forward-type bridge view

Blackhole-type bridge view

Predefined user roles

network-admin

context-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

You can add only Layer 2 physical interfaces, Layer 3 physical interfaces, or Layer 2 aggregate interfaces to reflect-type, forward-type, or blackhole-type bridge instances.

Only one interface can be added to a reflect-type or blackhole-type bridge instance.

Only two interfaces can be added to a manually created forward-type bridge instance. The two interfaces must be the same type.

Each interface can be added to only one bridge instance.

This command is not available for a forward-type bridge instance that is automatically created upon insertion of a hardware bypass subcard. An automatically created forward-type bridge instance uses the pair of interfaces on the bypass subcard by default and you cannot edit the interfaces in the instance.

If you execute this command multiple times in reflect-type or blackhole-type bridge view, the most recent configuration takes effect.

If you execute this command multiple times in forward-type bridge view, the most recent two configurations take effect.

Examples

Add GigabitEthernet 1/0/1 to reflect-type bridge instance 1.

```
<Sysname> system-view
[Sysname] bridge 1 reflect
[Sysname-bridge1-reflect] add interface gigabitethernet 1/0/1
```

add vlan

Use **add vlan** to add a list of VLANs to an inter-VLAN bridge instance.

Use **undo add vlan** to remove VLANs from an inter-VLAN bridge instance.

Syntax

add vlan *vlan-id-list*

undo add vlan [*vlan-id-list*]

Default

No VLANs exist in an inter-VLAN bridge instance.

Views

Inter-VLAN bridge view

Predefined user roles

network-admin

context-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 10 VLAN items. Each VLAN item specifies a VLAN ID or a range of VLAN IDs in the form of *start-vlan-id* **to** *end-vlan-id*. The end VLAN ID must be greater than the start VLAN ID. Valid VLAN IDs are from 1 to 4094.

Usage guidelines

You can add VLANs to a bridge instance before or after you create the VLANs.

You can add a VLAN to only one bridge instance.

If you execute the command multiple times, all configurations take effect.

If you do not specify the *vlan-id-list* argument, the **undo add vlan** command removes all VLANs from the inter-VLAN bridge instance.

Examples

Add VLANs 2, 3, 5, and VLANs 50 through 70 to bridge instance 2.

```
<Sysname> system-view
[Sysname] bridge 2 inter-vlan
[Sysname-bridge2-inter-vlan] add vlan 2 3 5 50 to 70
```

bridge

Use **bridge** to create a specific type of bridge instance and enter its view, or enter the view of an existing bridge instance.

Use **undo bridge** to delete bridge instances.

Syntax

bridge *bridge-index* [**blackhole** | **forward** | **inter-vlan** | **reflect**]

undo bridge { *bridge-index* | **all** }

Default

No bridge instances exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

bridge-index: Specifies a bridge instance index. For an automatically created forward-type bridge instance, the system will assign an index in the range of 32768 to 1082400.

The following compatibility matrixes show the value ranges for the *bridge-index* argument for a manually created bridge instance:

Models	Value range
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	1 to 128

blackhole: Specifies a blackhole-type bridge instance.

forward: Specifies a forward-type bridge instance.

inter-vlan: Specifies an inter-VLAN bridge instance.

reflect: Specifies a reflect-type bridge instance.

all: Deletes all bridge instances.

Usage guidelines

Use this command to create a bridge instance. You can create reflect-type, forward-type, and blackhole-type bridge instances for inline forwarding.

When you create a bridge instance, you must specify its type. You can specify only one type for a bridge instance.

The device will automatically create a forward-type bridge instance upon insertion of a hardware bypass subcard. The automatically created forward-type bridge instance uses the pair of interfaces on the bypass subcard by default. You cannot edit the interfaces in the bridge instance or delete the bridge instance.

Examples

Create blackhole-type bridge instance 1 and enter its view.

```
<Sysname> system-view
[Sysname] bridge 1 blackhole
[Sysname-bridge1-blackhole]
```

Create forward-type bridge instance 2 and enter its view.

```
<Sysname> system-view
[Sysname] bridge 2 forward
[Sysname-bridge2-forward]
```

Create inter-VLAN bridge instance 3 and enter its view.

```
<Sysname> system-view
[Sysname] bridge 3 inter-vlan
[Sysname-bridge3-inter-vlan]
```

Create reflect-type bridge instance 4 and enter its view.

```
<Sysname> system-view
[Sysname] bridge 4 reflect
[Sysname-bridge4-reflect]
```

bridge mac-address timer aging

Use **bridge mac-address timer aging** to set the aging timer for dynamic MAC address entries in bridge instances.

Use **undo bridge** to restore the default.

Syntax

bridge mac-address timer aging *seconds*

undo bridge mac-address timer aging

Default

The aging timer for dynamic MAC address entries is 300 seconds.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies a MAC address aging timer, in seconds. The value range is 60 to 1440.

Usage guidelines

Follow these guidelines to set the aging timer appropriately:

- A long aging interval causes the MAC address table to retain outdated entries and fail to accommodate the most recent network changes.

- A short aging interval results in removal of valid entries. Then, unnecessary broadcast packets appear and affect device performance.

After you set an aging time for dynamic MAC address entries, the device automatically deletes the expired dynamic MAC address entries. Then, the device learns new MAC addresses to build new MAC address entries.

Examples

Set the aging timer to 500 seconds for dynamic MAC address entries.

```
<Sysname> system-view
[Sysname] bridge mac-address timer aging 500
```

bridge tunnel-encapsulation skip

Use **bridge tunnel-encapsulation skip** to configure the device to ignore the tunnel encapsulation when forwarding tunneled packets in inline mode.

Use **undo bridge tunnel-encapsulation skip** to restore the default.

Syntax

bridge tunnel-encapsulation skip

undo bridge tunnel-encapsulation skip

Default

In inline forwarding mode, tunneled packets are forwarded based on information in the tunnel encapsulation.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command takes effect only for inline forwarding.

In inline forwarding mode, tunneled packets are forwarded based on information in the tunnel encapsulation by default.

Use this command to enable the device to ignore the tunnel encapsulation and forward tunneled packets based on the original packet header information.

Examples

Configure the device to ignore the tunnel encapsulation when forwarding tunneled packets in inline mode.

```
<Sysname> system-view
[Sysname] bridge tunnel-encapsulation skip
```

bypass enable

Use **bypass enable** to enable internal security service bypass.

Use **undo bypass enable** to disable security service bypass.

Syntax

bypass enable

undo bypass enable

Default

Security service bypass is disabled.

Views

Reflect-type bridge view

Forward-type bridge view

Blockhole-type bridge view

Predefined user roles

network-admin

context-admin

Usage guidelines

This feature enables the device to bypass the security service and to directly process received packets according to the configured bridge forwarding mode.

If you configure the **bypass enable** command multiple times, the most recent configuration takes effect.

Examples

Enable internal security service bypass.

```
<Sysname> system-view
[Sysname] bridge 1 forward
[Sysname-bridge-1-forward] bypass enable
```

display bridge mac-address

Use **display bridge mac-address** to display MAC address entries in bridge instances.

Syntax

display bridge mac-address [*bridge-index* [**vlan** *vlan-id*]] [**count**] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

bridge-index: Specifies a bridge instance by its index.

vlan *vlan-id*: Specifies a VLAN by its ID.

count: Displays only the total number of MAC address entries that match all entry attributes you specify in this command. In this case, the detailed information about MAC address entries is not

displayed. For example, you can use the **display bridge mac-address 2 vlan 20 count** command to display the total number of entries for VLAN 20 in bridge instance 2. If you do not specify this keyword, this command displays detailed information about specified MAC address entries.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays MAC address entries for the master device.

Usage guidelines

If you do not specify any parameters, this command displays MAC address entries for all bridge instances.

This command displays dynamic MAC address entries because the MAC address entries in a bridge instance are all learned MAC addresses.

Examples

Display MAC address entries for bridge instance 100.

```
<Sysname> display bridge mac-address 100
MAC Address      BRIDGE ID  State        VLAN ID  Port            Aging
0033-0033-0033   100        Learned      44       GE1/0/1         Y
0000-0000-0002   100        Learned      66       GE1/0/2         Y
```

Display the number of MAC address entries in bridge instance 100.

```
<Sysname> display bridge mac-address 100 count
1 mac address(es) found.
```

Table 5 Command output

Field	Description
BRIDGE ID	Index of the bridge instance to which the MAC address entry belongs.
State	MAC address entry state: **Learned**.
VLAN ID	VLAN of the outgoing interface.
Port	Outgoing interface.
Aging	Whether the entry can age out: • **Y**—The entry can age out. • **N**—The entry never ages out.
1 mac address(es) found	Number of matching MAC address entries.

mac-address max-mac-count

Use **mac-address max-mac-count** to set the MAC learning limit on an inter-VLAN bridge instance.

Use **undo mac-address max-mac-count** to restore the default.

Syntax

mac-address max-mac-count *count*

undo mac-address max-mac-count

Default

The MAC learning limit is 4096 on an inter-VLAN bridge instance.

Views

Inter-VLAN bridge view

Predefined user roles

network-admin

context-admin

Parameters

count: Sets the maximum number of MAC addresses that can be learned on an inter-VLAN bridge instance. The value range for this argument is 0 to 4096. To prevent an inter-VLAN bridge instance from learning any MAC addresses, set the limit to 0 for the bridge instance.

Usage guidelines

The command sets the size of the inter-VLAN bridge forwarding MAC address table. When the number of MAC address entries learned by an inter-VLAN bridge instance reaches the limit, the bridge instance stops learning MAC address entries.

Examples

Configure inter-VLAN bridge instance 2 to learn a maximum of 10 MAC address entries.

```
<Sysname> system-view
[Sysname] bridge 2 inter-vlan
[Sysname-bridge2-inter-vlan] mac-address max-mac-count 10
```

Fast bridge forwarding commands

bridge fast-forwarding check-vlan-id

Use **bridge fast-forwarding check-vlan-id** to enable VLAN ID check for fast bridge forwarding.

Use **undo bridge fast-forwarding check-vlan-id** to disable VLAN ID check for fast bridge forwarding.

Syntax

bridge fast-forwarding check-vlan-id

undo bridge fast-forwarding check-vlan-id

Default

VLAN ID check is enabled for fast bridge forwarding.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This feature allows the device to check whether the VLAN ID of a flow matches that of any fast forwarding entry. If no match is found, the flow does not match any fast forwarding entry.

The VLAN ID of a packet helps the device to determine the TCP session to which the packet belongs. On a hot backup system formed by two firewalls, you must disable VLAN ID check if the traffic

incoming interfaces on the primary and secondary devices belong to different VLANs. If you enable VLAN ID check, traffic cannot match session entries correctly when asymmetric-path traffic exists.

On a hot backup system formed by two firewalls, inter-VLAN fast bridge forwarding enables a packet to match the same session after being transmitted between the primary and secondary devices. Because the device does not check VLAN IDs for inter-VLAN fast bridge forwarding. That is, this command does not take effect on inter-VLAN fast bridge forwarding.

Examples

Enable VLAN ID check for fast bridge forwarding.

```
<Sysname> system-view
[Sysname] bridge fast-forwarding check-vlan-id
```

display bridge cache ip

Use **display bridge cache ip** to display IPv4 fast bridge forwarding entries.

Syntax

display bridge cache ip { **inline** | **inter-vlan** } [*ip-address*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

inline: Displays IPv4 inline forwarding entries.

inter-vlan: Displays IPv4 inter-VLAN forwarding entries.

ip-address: Specifies an IPv4 address. If you do not specify an IPv4 address, this command displays all IPv4 fast bridge forwarding entries.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv4 fast bridge forwarding entries for all member devices.

Examples

Display IPv4 inline fast bridge forwarding entries.

```
<Sysname> display bridge cache ip inline
Total number of bridge-forwarding entries: 2
SIP             SPort DIP             DPort Pro InVLAN OutVLAN Output_If
1.1.1.3         470   1.1.1.2         0     1   3      2       GE1/0/1
1.1.1.2         470   1.1.1.3         2048  1   2      3       GE1/0/2
```

Table 6 Command output

Field	Description
Total number of bridge-forwarding entries	Total number of IPv4 fast bridge forwarding entries.
SIP	Source IPv4 address.

SPort	Source port number.
DIP	Destination IPv4 address.
DPort	Destination port number.
Pro	Protocol number.
InVLAN	Input VLAN.
OutVLAN	Output VLAN.
Output_If	Output interface.

display bridge cache ip fragment

Use **display bridge cache ip fragment** to display IPv4 fast bridge forwarding entries for fragments.

Syntax

display bridge cache ip fragment { **inline** | **inter-vlan** } [*ip-address*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

inline: Displays IPv4 inline forwarding entries for fragments.

inter-vlan: Displays IPv4 inter-VLAN forwarding entries for fragments.

ip-address: Specifies an IPv4 address. If you do not specify an IPv4 address, this command displays IPv4 fast bridge forwarding entries for all fragments.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv4 fast bridge forwarding entries for fragments on all member devices.

Examples

Display IPv4 inline fast bridge forwarding entries for fragments.

```
<Sysname> display bridge cache ip fragment inline
Total number of fragment bridge-forwarding entries: 2
SIP             SPort DIP             DPort Pro InVLAN ID
2.1.1.2         2320  2.1.1.1         2048  1   2      7298
2.1.1.1         2048  2.1.1.2         2320  1   3      6826
```

Table 7 Command output

Field	Description
Total number of fragment bridge-forwarding entries	Total number of IPv4 fast bridge forwarding entries for fragments.
SIP	Source IPv4 address.
SPort	Source port number.
DIP	Destination IPv4 address.
DPort	Destination port number.
Pro	Protocol number.
InVLAN	Input VLAN.
ID	Fragment ID.

display bridge cache ipv6

Use **display bridge cache ipv6** to display IPv6 fast bridge forwarding entries.

Syntax

display bridge cache ipv6 { **inline** | **inter-vlan** } [*ipv6-address*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

inline: Displays IPv6 inline forwarding entries.

inter-vlan: Displays IPv6 inter-VLAN forwarding entries.

ipv6-address: Specifies an IPv6 address. If you do not specify an IPv6 address, this command displays all IPv6 fast bridge forwarding entries.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv6 fast bridge forwarding entries for all member devices.

Examples

Display IPv6 inline fast bridge forwarding entries.

```
<Sysname> display bridge cache ipv6 inline
Total number of IPv6 bridge-forwarding items: 1
Src IP: 10::12                                  Src Port: 427
Dst IP: 10::11                                  Dst Port: 32768
```

```
InVLAN: 2                                        OutVLAN: 3
Protocol: 58
Context ID: 257
Bridge ID: 10
Output interface: GE1/0/1
```

Table 8 Command output

Field	Description
Total number of IPv6 bridge-forwarding items	Total number of IPv6 fast bridge forwarding entries.
Src IP	Source IPv6 address.
Src port	Source port number.
Dst IP	Destination IPv6 address.
Dst Port	Destination port number.
InVLAN	Input VLAN.
OutVLAN	Output VLAN.
Protocol	Protocol number.
Context ID	Context ID.
Output interface	Output interface type and number. If no output interface is involved in fast forwarding, this field displays **N/A**. If no output interface is available, this field displays a hyphen (-).

NSFOCUS Firewall Series

NF Layer 2—WAN Access Command Reference

NSFOCUS Technologies, Inc.

Document version: 6W600-20230221

Preface

This command reference describes the commands for configuring Layer 2 WAN access features, including PPP and Mobile communication modem.

This preface includes the following topics about the documentation:

- Audience.
- Conventions.

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators.

Conventions

The following information describes the conventions used in the documentation.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select a minimum of one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
CAUTION:	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Contents

PPP commands

PPP commands

bandwidth

Use **bandwidth** to set the expected bandwidth of an interface.

Use **undo bandwidth** to restore the default.

Syntax

bandwidth *bandwidth-value*

undo bandwidth

Default

The expected bandwidth (in kbps) is the interface baud rate divided by 1000.

Views

VT interface view

Predefined user roles

network-admin

context-admin

Parameters

bandwidth-value: Specifies the expected bandwidth in the range of 1 to 400000000 kbps.

Usage guidelines

The expected bandwidth of an interface affects the link costs in OSPF, OSPFv3, and IS-IS. For more information, see *Layer 3—IP Routing Configuration Guide*.

Examples

Set the expected bandwidth of Virtual-Template 10 to 1000 kbps.

```
<Sysname> system-view
[Sysname] interface virtual-template 10
[Sysname-Virtual-Template10] bandwidth 1000
```

default

Use **default** to restore the default settings for an interface.

Syntax

default

Views

VT interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

CAUTION:

The **default** command might interrupt ongoing network services. Make sure you are fully aware of the impact of this command before using it on a live network.

This command might fail to restore the default settings for some commands for reasons such as command dependencies or system restrictions. Use the **display this** command in interface view to identify these commands. Use the **undo** forms of these commands or follow the command reference to individually restore their default settings. If your restoration attempt still fails, follow the error message instructions to resolve the problem.

Examples

Restore the default settings of Virtual-Template 10.

```
<Sysname> system-view
[Sysname] interface virtual-template 10
[Sysname-Virtual-Template10] default
```

description

Use **description** to set the description for an interface.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

The description for an interface is *interface name* **Interface** (for example, **Virtual-Template1 Interface**).

Views

VT interface view

Predefined user roles

network-admin

context-admin

Parameters

text: Specifies the interface description, a case-sensitive string of 1 to 255 characters.

Examples

Set the description for Virtual-Template 10 to **virtual-interface**.

```
<Sysname> system-view
[Sysname] interface virtual-template 10
[Sysname-Virtual-Template10] description virtual-interface
```

display interface virtual-access

Use **display interface virtual-access** to display information about VA interfaces.

Syntax

display interface [**virtual-access** [*interface-number*]] [**brief** [**description** | **down**]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

virtual-access [*interface-number*]: Specifies an existing VA interface by its number. If you do not specify the **virtual-access** keyword, the command displays information about all interfaces except VA interfaces on the device. If you specify the **virtual-access** keyword without the *interface-number* argument, the command displays information about all VA interfaces.

brief: Displays brief interface information. If you do not specify this keyword, the command displays detailed interface information.

description: Displays interface description information. This keyword does not apply to VA interfaces because VA interfaces do not support description configuration.

down: Displays information about interfaces in physically down state and the causes. If you do not specify this keyword, the command displays information about all interfaces.

Examples

Display information about Virtual-Access 1.

```
<Sysname> display interface virtual-access 1
Virtual-Access1
Current state: UP
Line protocol state: UP
Description: Virtual-Access1 Interface
Bandwidth: 1920kbps
Maximum transmission unit: 1500
Hold timer: 10 seconds, retry times: 5
Internet address: 122.1.1.1/24 (primary)
Link layer protocol: PPP
LCP: opened, IPCP: opened
Main interface: Virtual-Template1
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last link flapping: Never
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 2 packets, 24 bytes, 0 drops
Output: 2 packets, 24 bytes, 0 drops
```

Display brief information about Virtual-Access 1.

```
<Sysname> display interface virtual-access 1 brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP         Description
VA1                  DOWN DOWN     --
```

Display brief information about VA interfaces in physically down state and the causes.

```
<Sysname> display interface virtual-access brief down
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Interface            Link Cause
VA1                  DOWN Not connected
```

Table 1 Command output

Field	Description
Current state	Physical and administrative states of the interface: • **DOWN**—The interface is administratively up but physically down. • **UP**—The interface is both administratively and physically up.
Line protocol state	Data link layer state: UP or DOWN.
Description	Interface description.
Bandwidth	Expected bandwidth of the interface.
Hold timer	Interval at which the interface sends keepalive packets.
retry times	Keepalive retry limit. The interface determines that its peer has been down if it does not receive a keepalive response when the keepalive retry limit is reached.
Internet protocol processing: Disabled	The interface cannot process IP packets currently.
Internet address: *ip-address*/*mask-length* (*Type*)	IP address of the interface and type of the address in parentheses. Possible IP address types include: • **Primary**—Manually configured primary IP address. • **Sub**—Manually configured secondary IP address. If the interface has both primary and secondary IP addresses, the primary IP address is displayed. If the interface has only secondary IP addresses, the lowest secondary IP address is displayed. • **DHCP-allocated**—DHCP allocated IP address. For more information, see DHCP client configuration in *Layer 3—IP Services Configuration Guide*. • **BOOTP-allocated**—BOOTP allocated IP address. For more information, see BOOTP client configuration in *Layer 3—IP Services Configuration Guide*. • **PPP-negotiated**—IP address assigned by a PPP server during PPP negotiation. For more information, see PPP configuration in *Layer 2—WAN Access Configuration Guide*. • **Unnumbered**—IP address borrowed from another interface. • **Cellular-allocated**—IP address allocated through the modem-manufacturer's proprietary protocol. For more information, see mobile communication modem management in *Layer 2—WAN Access Configuration Guide*.

Field	Description
	• **MAD**—IP address assigned to an IRF member device for MAD on the interface. For more information, see IRF configuration in *Virtual Technologies Configuration Guide*.
LCP: opened, IPCP: opened	The PPP connection has been successfully established.
Main interface	VT interface associated with the VA interface.
Output queue - Urgent queuing: Size/Length/Discards 0/100/0 Output queue - Protocol queuing: Size/Length/Discards 0/500/0 Output queue - FIFO queuing: Size/Length/Discards 0/75/0	Traffic statistics of the interface output queues.
Last link flapping	The amount of time that has elapsed since the most recent physical state change of the interface. This field displays **Never** if the interface has been physically down since device startup.
Last clearing of counters: Never	Last time when statistics on the interface were cleared. **Never** indicates that statistics on the interface were never cleared.
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec	Average rate of input packets and output packets in the last 300 seconds.
Input: 2 packets, 24 bytes, 0 drops	Total number of inbound packets of the interface (in the number of packets and in bytes), and the number of packets dropped among the inbound packets.
Output: 2 packets, 24 bytes, 0 drops	Total number of outbound packets of the interface (in the number of packets and in bytes), and the number of packets dropped among the outbound packets.
Brief information on interfaces in route mode	Brief information about Layer 3 interfaces.
Link: ADM - administratively down; Stby - standby	Link status: • **ADM**—The interface has been administratively shut down. To recover its physical state, execute the **undo shutdown** command. • **Stby**—The interface is a backup interface. To see the primary interface, use the **display interface-backup state** command in *High Availability Command Reference*.
Protocol: (s) - spoofing	Indicates the line protocol is UP, but the physical link is an on-demand link or is not present.
Interface	Abbreviated interface name.
Link	Physical link state of the interface: • **UP**—The interface is physically up. • **DOWN**—The interface is physically down.
Protocol	Line protocol state: • **UP**—The line protocol is up. • **DOWN**—The line protocol is down. • **UP(s)**—The line protocol is up, but the physical link is an on-demand link or is not present.
Primary IP	Primary IP address of the interface.
Description	Interface description configured by using the **description** command. This field does not apply to VA interfaces because VA

Field	Description
	interfaces do not support description configuration.
Cause	Cause for the physical state of the interface to be Down. **Not connected** indicates no physical link exists (possibly because the network cable is disconnected or faulty).

Related commands

reset counters interface virtual-access

display interface virtual-template

Use **display interface virtual-template** to display information about VT interfaces.

Syntax

display interface [**virtual-template** [*interface-number*]] [**brief** [**description** | **down**]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

virtual-template [*interface-number*]: Specifies an existing VT interface by its number. If you do not specify the **virtual-template** keyword, the command displays information about all interfaces except VA interfaces on the device. If you specify the **virtual-template** keyword without the *interface-number* argument, the command displays information about all existing VT interfaces.

brief: Displays brief interface information. If you do not specify this keyword, the command displays detailed interface information.

description: Displays complete interface description. If you do not specify this keyword, the command displays only the first 27 characters of the interface description if the description contains more than 27 characters.

down: Displays information about interfaces in physically down state and the causes. If you do not specify this keyword, the command displays information about all interfaces.

Examples

Display detailed information about Virtual-Template 1.

```
<Sysname> display interface virtual-template 1
Virtual-Template1
Current state: DOWN
Line protocol state: DOWN
Description: Virtual-Template1 Interface
Bandwidth: 100000kbps
Maximum transmission unit: 1500
Hold timer: 10 seconds, retry times: 5
```

```
Internet address: 192.168.1.200/24 (primary)
Link layer protocol: PPP
LCP: initial
Physical: None, baudrate: 100000000 bps
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
```

Display brief information about Virtual-Template 1.

```
<Sysname> display interface virtual-template 1 brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP       Description
VT1                  DOWN DOWN     --
```

Display brief information about the VT interfaces in physically down state and the causes.

```
<Sysname> display interface Virtual-Template brief down
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Interface            Link Cause
VT0                  DOWN Not connected
VT12                 DOWN Not connected
VT1023               DOWN Not connected
```

Table 2 Command output

Field	Description
Current state	Physical state of the interface. This field for a VT interface can only be **DOWN**.
Line protocol state	Data link layer state. This field for a VT interface can only be **DOWN**.
Description	Interface description.
Bandwidth	Expected bandwidth of the interface.
Hold timer	Interval at which the interface sends keepalive packets.
retry times	Keepalive retry limit. The interface determines that its peer has been down if it does not receive a keepalive response when the keepalive retry limit is reached.
Internet protocol processing: Disabled	The interface cannot process IP packets currently.
Internet address: *ip-address*/*mask-length* (*Type*)	IP address of the interface and type of the address in parentheses. Possible IP address types include: • **Primary**—Manually configured primary IP address. • **Sub**—Manually configured secondary IP address. If the interface has both primary and secondary IP addresses, the primary IP address is displayed. If the interface has only secondary IP addresses, the lowest secondary IP address is displayed. • **DHCP-allocated**—DHCP allocated IP address. For more information, see DHCP client configuration in *Layer 3—IP Services Configuration Guide*. • **BOOTP-allocated**—BOOTP allocated IP address. For more

Field	Description
	information, see BOOTP client configuration in *Layer 3—IP Services Configuration Guide*. • **PPP-negotiated**—IP address assigned by a PPP server during PPP negotiation. For more information, see PPP configuration in *Layer 2—WAN Access Configuration Guide*. • **Unnumbered**—IP address borrowed from another interface. • **Cellular-allocated**—IP address allocated through the modem-manufacturer's proprietary protocol. For more information, see mobile communication modem management in *Layer 2—WAN Access Configuration Guide*. • **MAD**—IP address assigned to an IRF member device for MAD on the interface. For more information, see IRF configuration in *Virtual Technologies Configuration Guide*.
LCP initial	LCP initialization is complete.
Physical	Physical type of the interface.
Output queue - Urgent queuing: Size/Length/Discards 0/100/0) Output queue - Protocol queuing: Size/Length/Discards 0/500/0) Output queue - FIFO queuing: Size/Length/Discards 0/75/0)	Traffic statistics of the interface output queues.
Brief information on interfaces in route mode	Brief information about Layer 3 interfaces.
Link: ADM - administratively down; Stby - standby	Link status: • **ADM**—The interface has been administratively shut down. To recover its physical state, use the **undo shutdown** command. • **Stby**—The interface is operating as a backup interface. To see the primary interface, use the **display interface-backup state** command in *High Availability Command Reference*.
Protocol: (s) - spoofing	Indicates the line protocol is UP, but the physical link is an on-demand link or is not present.
Interface	Abbreviated interface name.
Link	Physical link state of the interface. This field for a VT interface can only be **DOWN**.
Protocol	Line protocol state of the interface. This field for a VT interface can only be **DOWN**.
Primary IP	Primary IP address of the interface.
Description	Interface description configured by using the **description** command. If you do not specify the **description** keyword, the **display interface brief** command displays a maximum of 27 characters of the description. If you specify the **description** keyword, the command displays the complete description.
Cause	Causes for the physical state of the interface to be Down. **Not connected** indicates no physical link exists (possibly because the network cable is disconnected or faulty).

display ip pool

Use **`display ip pool`** to display PPP address pools.

Syntax

display ip pool [*pool-name* | **group** *group-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

pool-name: Specifies a PPP address pool by its name, a case-sensitive string of 1 to 31 characters.

group *group-name*: Displays PPP address pools in a group specified by its name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

If you do not specify any parameters, the command displays brief information about all PPP address pools.

If you specify an address pool, the command displays detailed information about the specified PPP address pool.

Examples

Display brief information about all PPP address pools.

```
<Sysname> display ip pool
Group name: a
  Pool name           Start IP address    End IP address      Free   In use
  aaa1                1.1.1.1             1.1.1.5             5      0
  aaa2                1.1.1.6             1.1.1.10            5      0
Group name: b
  Pool name           Start IP address    End IP address      Free   In use
  bbb                 1.1.2.1             1.1.2.5             4      1
                      2.2.2.1             2.2.2.5             5      0
```

Display brief information about the PPP address pools in group **a**.

```
<Sysname> display ip pool group a
Group name: a
  Pool name           Start IP address    End IP address      Free   In use
  aaa1                1.1.1.1             1.1.1.5             5      0
  aaa2                1.1.1.6             1.1.1.10            5      0
```

Display detailed information about PPP address pool **bbb**.

```
<Sysname> display ip pool bbb
Group name: b
  Pool name           Start IP address    End IP address      Free   In use
  bbb                 1.1.2.1             1.1.2.5             4      1
                      2.2.2.1             2.2.2.5             5      0
In use IP addresses:
  IP address      Interface
```

```
1.1.2.1         Virtual-Template1
```

Table 3 Command output

Field	Description
Free	Number of free IP addresses.
In use	Number of IP addresses that have been assigned.
In use IP addresses	Information about the IP addresses that have been assigned.
Interface	Local interface that requests the IP address for the peer interface.

Related commands

ip pool

display ppp access-user

Use **display ppp access-user** to display PPP user information.

Syntax

display ppp access-user { **domain** *domain-name* | **interface** *interface-type interface-number* [**count**] | **ip-address** *ipv4-address* | **ipv6-address** *ipv6-address* | **username** *user-name* | **user-type** { **lac** | **lns** | **pppoe** } [**count**] }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

domain *domain-name*: Displays information about PPP access users coming online through an ISP domain specified by its name, a case-sensitive string of 1 to 255 characters.

interface *interface-type interface-number*: Displays brief information about PPP users on the specified interface.

ip-address *ipv4-address*: Displays detailed information about the PPP user specified by its IPv4 address.

ipv6-address *ipv6-address*: Displays detailed information about the PPP user specified by its IPv6 address.

username *user-name*: Displays detailed information about the PPP user specified by its username, a case-sensitive string of 1 to 80 characters.

user-type: Displays brief information about online users of the specified type.

lac: Displays brief information about L2TP users for an LAC.

lns: Displays brief information about L2TP users for an LNS.

pppoe: Displays brief information about PPPoE users.

count: Displays the total number of PPP users matching the specified criterion.

Usage guidelines

Brief information about a PPP user includes the following:

- Brief name of the VA interface.
- Username.
- MAC address.
- IPv4 address, IPv6 address, or IPv6 prefix of the PPP user.

Detailed information about a PPP user includes the following:

- Brief name of the VA interface.
- User ID.
- Username.
- Authentication information.
- Uplink and downlink traffic.
- Access start time of the PPP user.

In an L2TP network, this command is supported on an LAC only if a remote system dials in to the LAC through a PPPoE network. For more information about L2TP, see L2TP configuration in *VPN Configuration Guide*.

Examples

Display brief information about PPP users on GigabitEthernet 1/0/1.

```
<Sysname> display ppp access-user interface gigabitethernet 1/0/1
Interface     Username    MAC address     IP address       IPv6 address    IPv6 PDPrefix
VA0           user1@dm1   0001-0101-9101  192.168.100.173  -                 -
VA1           user2@dm2   0001-0101-9101  192.168.80.173   2000::1           -
```

Display the total number of PPP users on GigabitEthernet 1/0/1.

```
<Sysname> display ppp access-user interface gigabitethernet 1/0/1 count
Total users: 2
```

Table 4 Command output

Field	Description
Interface	Name of the VA interface corresponding to the user.
Username	Username of the user. A hyphen (-) means that the user does not need authentication.
MAC address	MAC address of the user. A hyphen (-) means that the user is not a PPPoE user.
IP address	IP address of the user. A hyphen (-) means that no IP address is assigned to the user.
IPv6 address	IPv6 address of the user. A hyphen (-) means that no IPv6 address is assigned to the user.
IPv6 PD prefix	IPv6 prefix of the user. A hyphen (-) means that no IPv6 prefix is assigned to the user.
Total users	Total number of PPP users.

Display detailed information about the PPP user whose IP address is 50.50.50.3.

```
<Sysname> display ppp access-user ip-address 50.50.50.3
Basic:
  Interface: VA0
```

```
  User ID: 0x28000002
  Username: user1@hrss
  Domain: hrss
  Access interface: RAGG2
  Service-VLAN/Customer-VLAN: -/-
  MAC address: 0000-0000-0001
  IP address: 50.50.50.3
  IPv6 address: -
  IPv6 PD prefix: -
  VPN instance: 123
  Access type: PPPoE
  Authentication type: CHAP

AAA:
  Authentication state: Authenticated
  Authorization state: Authorized
  Realtime accounting switch: Open
  Realtime accounting interval: 60s
  Login time: 2013-1-19  2:42:3:358
  Accounting start time: 2013-1-19  2:42:3:382
  Online time(hh:mm:ss): 0:7:34
  Accounting state: Accounting
  Idle cut: 0 sec  0 byte
  Session timeout: 12000 s
  Time remained: 8000 s
  Byte remained: 20971520 bytes
  Redirect WebURL: http://6.6.6.6

ACL&QoS:
  Inbound CAR: CIR 64000bps PIR 640000bps CBS 500bit
  Outbound CAR: CIR 64000bps PIR 640000bps CBS 500bit

NAT:
  Global IP address: 111.8.0.200
  Port block: 28744-28748

Flow Statistic:
  IPv4 uplink   packets/bytes: 7/546
  IPv4 downlink packets/bytes: 0/0
  IPv6 uplink   packets/bytes: 0/0
  IPv6 downlink packets/bytes: 0/0

ITA:
  Level-1 uplink   packets/bytes: 100/128000
          downlink packets/bytes: 200/256000
  Level-2 uplink   packets/bytes: 100/128000
          downlink packets/bytes: 200/256000
```

Table 5 Command output

Field	Description
Basic	Basic information.
Interface	Brief name of the VA interface that corresponds to the user.
Username	Username of the user. A hyphen (-) means that the user does not need authentication.
Domain	ISP domain name for authentication. A hyphen (-) means that no ISP domain is specified for authentication.
Access interface	Name of the access interface of the user.
Service-VLAN/Customer-VLAN	Service provider VLAN and customer VLAN information of the user. A hyphen (-) means that no VLAN information is available.
IP address	IP address of the user. A hyphen (-) means that no IP address is assigned to the user.
IPv6 address	IPv6 address of the user. A hyphen (-) means that no IPv6 address is assigned to the user.
IPv6 PD prefix	Delegated IPv6 prefix of the user. A hyphen (-) means that no delegated IPv6 prefix is assigned to the user.
VPN instance	VPN instance to which the user belongs. A hyphen (-) means that the user is not bound to any VPN instance.
Access type	Access type of the user: • PPPoE. • L2TP.
Authentication type	Authentication type of the user: • PAP. • CHAP. • MS-CHAP. • MS-CHAP-V2.
Authentication state	Authentication state of the user: • **Idle**—The user has not been authenticated. • **Authenticating**—The user is being authenticated. • **Authenticated**—The user has been authenticated.
Authorization state	Authorization state of the user: • **Idle**—The user has not been authorized. • **Authorizing**—The user is being authorized. • **Authorized**—The user has been authorized.
Realtime accounting switch	• **Open**—The switch is on. • **Closed**—The switch is off.
Realtime accounting interval	Realtime accounting interval in seconds. A hyphen (-) means that no real-time accounting interval is authorized.
Login time	Time when the user accessed the device through PPP.
Accounting start time	Time when accounting started. A hyphen (-) means that no accounting is performed on the user.

Field	Description
Online time(hh:mm:ss)	Online duration of the current login.
Accounting state	Accounting state of the user: • **Accounting**—Accounting is on. • **Stop**—Accounting stops.
Idle cut	Traffic threshold for logging off the user in idle state. If the traffic is less than the threshold within the specified period, the user is forcibly logged off.
Session timeout	Authorization time for the user, in seconds. A hyphen (-) means that no authorization time is specified for the user.
Time remained	Remaining time for the user to stay online, in seconds. A hyphen (-) means that no authorization time is specified for the user.
Traffic quota	Authorized traffic quota for the user, in bytes. A hyphen (-) means that no traffic quota is authorized to the user.
Traffic remained	Remaining traffic for the user, in bytes. A hyphen (-) means that no traffic quota is authorized to the user.
Redirect WebURL	Redirect Web URL address for the user. A hyphen (-) means that no redirect Web URL address is specified for the user.
Inbound CAR	Authorized inbound CAR parameters, which contain the CIR (in bps), the PIR (in bps), and the CBS (in bits).
Outbound CAR	Authorized outbound CAR parameters, which contain the CIR (in bps), the PIR (in bps), and the CBS (in bits).
Global IP address	Global IP address of the user. This field is displayed if NAT444 is used. For information about NAT444, see *Layer 3—IP Services Configuration Guide*.
Port block	Port block of the user, from the start port to the end port. This field is displayed if NAT444 is used.
IPv4 uplink packets/bytes	Number of packets and bytes for IPv4 uplink traffic.
IPv4 downlink packets/bytes	Number of packets and bytes for IPv4 downlink traffic.
IPv6 uplink packets/bytes	Number of packets and bytes for IPv6 uplink traffic.
IPv6 downlink packets/bytes	Number of packets and bytes for IPv6 downlink traffic.
ITA	ITA statistics. ITA statistics are displayed after ITA is enabled. If the **`traffic-separate enable`** command is configured, ITA statistics are not included in flow statistics. For information about ITA and the **`traffic-separate enable`** command, see *Security Configuration Guide*.
Level-n uplink packets/bytes downlink packets/bytes	Number of packets and bytes for uplink traffic at accounting level *n*. The value for *n* depends on the **traffic level** command, and its value range is 1 to 8.

Related commands

`reset ppp access-user`

display ppp compression iphc

Use **display ppp compression iphc** to display IP header compression (IPHC) statistics.

Syntax

display ppp compression iphc { **rtp** | **tcp** } [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

rtp: Displays IPHC RTP header compression statistics.

tcp: Displays IPHC TCP header compression statistics.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify this option, the command displays IPHC statistics on all interfaces.

Usage guidelines

When IPHC applies to a normal PPP link, the physical interface performs IPHC. You can view the compression information on the physical interface.

Examples

Display IPHC RTP header compression statistics.

```
<Sysname> display ppp compression iphc rtp
----------------------Slot1----------------------
Interface: Virtual-Access0
  Received:
    Compressed/Error/Total: 0/0/0 packets
  Sent:
    Compressed/Total: 0/0 packets
    Sent/Saved/Total: 0/0/0 bytes
    Packet-based compression ratio: 0%
    Byte-based compression ratio: 0%
  Connections:
    Rx/Tx: 16/16
    Five-Minute-Miss: 0 (Misses/5Mins)
    Max-Miss: 0

----------------------Slot2----------------------
Interface: Virtual-Access0
  Received:
    Compressed/Error/Total: 20/5/40 packets
  Sent:
    Compressed/Total: 34/40 packets
```

```
    Sent/Saved/Total: 1131/1210/2341 bytes
    Packet-based compression ratio: 85%
    Byte-based compression ratio: 51%
  Connections:
    Rx/Tx: 16/16
    Five-Minute-Miss: 0 (Misses/5Mins)
    Max-Miss: 0
```

Display IPHC TCP header compression statistics.

```
<Sysname>display ppp compression iphc tcp
----------------------Slot1----------------------
Interface: Virtual-Access0
  Received:
    Compressed/Error/Total: 0/0/0 packets
  Sent:
    Compressed/Total: 0/0 packets
    Sent/Saved/Total: 0/0/0 bytes
    Packet-based compression ratio: 0%
    Byte-based compression ratio: 0%
  Connections:
    Rx/Tx: 16/16
    Five-Minute-Miss: 0 (Misses/5Mins)
    Max-Miss: 0

----------------------Slot2----------------------
Interface: Virtual-Access0
  Received:
    Compressed/Error/Total: 20/5/40 packets
  Sent:
    Compressed/Total: 34/40 packets
    Sent/Saved/Total: 1131/1210/2341 bytes
    Packet-based compression ratio: 85%
    Byte-based compression ratio: 51%
  Connections:
    Rx/Tx: 16/16
    Five-Minute-Miss: 0 (Misses/5Mins)
    Max-Miss: 0
```

Table 6 Command output

Field	Description
Received: Compressed/Error/Total	Statistics for received packets: • **Compressed**—Number of compressed packets. • **Error**—Number of error packets. • **Total**—Total number of received packets.
Sent: Compressed/Total Sent/Saved/Total Packet-based compression ratio Byte-based compression ratio	Statistics for sent packets: • **Compressed**—Number of compressed packets. • **Total**—Total number of sent packets. • **Sent**—Bytes of sent packets. • **Saved**—Bytes of saved packets.

Field	Description
	• **Total**—Total bytes to be sent if packets are not compressed. • **Packet-based compression ratio**—Ratio of compressed packets to the total sent packets. • **Byte-based compression ratio**—Ratio of saved bytes to the total sent bytes.
Connections: Rx/Tx Five-Minute-Miss Max-Miss	Number of connections. • **Rx**—Number of connections that the receiver can decompress. • **Tx**—Number of connections that the sender can compress. • **Five-Minute-Miss**—Number of search failures within the last 5 minutes. • **Max-Miss**—Maximum number of search failures within 5 minutes.

Related commands

ppp compression iphc enable

reset ppp compression iphc

display ppp packet statistics

Use **display ppp packet statistics** to display PPP negotiation packet statistics.

Syntax

display ppp packet statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays PPP negotiation packet statistics for all IRF member devices.

Examples

Display PPP negotiation packet statistics for slot 1.

```
<Sysname> display ppp packet statistics slot 1
PPP packet statistics in slot 1:
------------------------------LCP-----------------------------------
SEND_LCP_CON_REQ      : 0           RECV_LCP_CON_REQ      : 0
SEND_LCP_CON_NAK      : 0           RECV_LCP_CON_NAK      : 0
SEND_LCP_CON_REJ      : 0           RECV_LCP_CON_REJ      : 0
SEND_LCP_CON_ACK      : 0           RECV_LCP_CON_ACK      : 0
SEND_LCP_CODE_REJ     : 0           RECV_LCP_CODE_REJ     : 0
SEND_LCP_PROT_REJ     : 0           RECV_LCP_PROT_REJ     : 0
```

```
SEND_LCP_TERM_REQ     : 0           RECV_LCP_TERM_REQ     : 0
SEND_LCP_TERM_ACK     : 0           RECV_LCP_TERM_ACK     : 0
SEND_LCP_ECHO_REQ     : 0           RECV_LCP_ECHO_REQ     : 0
SEND_LCP_ECHO_REP     : 0           RECV_LCP_ECHO_REP     : 0
SEND_LCP_FAIL         : 0
-------------------------------IPCP---------------------------------
SEND_IPCP_CON_REQ     : 0           RECV_IPCP_CON_REQ     : 0
SEND_IPCP_CON_NAK     : 0           RECV_IPCP_CON_NAK     : 0
SEND_IPCP_CON_REJ     : 0           RECV_IPCP_CON_REJ     : 0
SEND_IPCP_CON_ACK     : 0           RECV_IPCP_CON_ACK     : 0
SEND_IPCP_CODE_REJ    : 0           RECV_IPCP_CODE_REJ    : 0
SEND_IPCP_PROT_REJ    : 0           RECV_IPCP_PROT_REJ    : 0
SEND_IPCP_TERM_REQ    : 0           RECV_IPCP_TERM_REQ    : 0
SEND_IPCP_TERM_ACK    : 0           RECV_IPCP_TERM_ACK    : 0
SEND_IPCP_FAIL        : 0
-------------------------------IPV6CP-------------------------------
SEND_IPV6CP_CON_REQ   : 0           RECV_IPV6CP_CON_REQ   : 0
SEND_IPV6CP_CON_NAK   : 0           RECV_IPV6CP_CON_NAK   : 0
SEND_IPV6CP_CON_REJ   : 0           RECV_IPV6CP_CON_REJ   : 0
SEND_IPV6CP_CON_ACK   : 0           RECV_IPV6CP_CON_ACK   : 0
SEND_IPV6CP_CODE_REJ  : 0           RECV_IPV6CP_CODE_REJ  : 0
SEND_IPV6CP_PROT_REJ  : 0           RECV_IPV6CP_PROT_REJ  : 0
SEND_IPV6CP_TERM_REQ  : 0           RECV_IPV6CP_TERM_REQ  : 0
SEND_IPV6CP_TERM_ACK  : 0           RECV_IPV6CP_TERM_ACK  : 0
SEND_IPV6CP_FAIL      : 0
-------------------------------OSICP--------------------------------
SEND_OSICP_CON_REQ    : 0           RECV_OSICP_CON_REQ    : 0
SEND_OSICP_CON_NAK    : 0           RECV_OSICP_CON_NAK    : 0
SEND_OSICP_CON_REJ    : 0           RECV_OSICP_CON_REJ    : 0
SEND_OSICP_CON_ACK    : 0           RECV_OSICP_CON_ACK    : 0
SEND_OSICP_CODE_REJ   : 0           RECV_OSICP_CODE_REJ   : 0
SEND_OSICP_PROT_REJ   : 0           RECV_OSICP_PROT_REJ   : 0
SEND_OSICP_TERM_REQ   : 0           RECV_OSICP_TERM_REQ   : 0
SEND_OSICP_TERM_ACK   : 0           RECV_OSICP_TERM_ACK   : 0
SEND_OSICP_FAIL       : 0
-------------------------------MPLSCP-------------------------------
SEND_MPLSCP_CON_REQ   : 0           RECV_MPLSCP_CON_REQ   : 0
SEND_MPLSCP_CON_NAK   : 0           RECV_MPLSCP_CON_NAK   : 0
SEND_MPLSCP_CON_REJ   : 0           RECV_MPLSCP_CON_REJ   : 0
SEND_MPLSCP_CON_ACK   : 0           RECV_MPLSCP_CON_ACK   : 0
SEND_MPLSCP_CODE_REJ  : 0           RECV_MPLSCP_CODE_REJ  : 0
SEND_MPLSCP_PROT_REJ  : 0           RECV_MPLSCP_PROT_REJ  : 0
SEND_MPLSCP_TERM_REQ  : 0           RECV_MPLSCP_TERM_REQ  : 0
SEND_MPLSCP_TERM_ACK  : 0           RECV_MPLSCP_TERM_ACK  : 0
SEND_MPLSCP_FAIL      : 0
-------------------------------AUTH --------------------------------
SEND_PAP_AUTH_REQ       : 0           RECV_PAP_AUTH_REQ       : 0
SEND_PAP_AUTH_ACK       : 0           RECV_PAP_AUTH_ACK       : 0
```

```
SEND_PAP_AUTH_NAK         : 0          RECV_PAP_AUTH_NAK         : 0
SEND_CHAP_AUTH_CHALLENGE  : 0          RECV_CHAP_AUTH_CHALLENGE  : 0
SEND_CHAP_AUTH_RESPONSE   : 0          RECV_CHAP_AUTH_RESPONSE   : 0
SEND_CHAP_AUTH_ACK        : 0          RECV_CHAP_AUTH_ACK        : 0
SEND_CHAP_AUTH_NAK        : 0          RECV_CHAP_AUTH_NAK        : 0
SEND_PAP_AUTH_FAIL        : 0          SEND_CHAP_AUTH_FAIL       : 0
```

Table 7 Command output

Field	Description
LCP	LCP packet statistics. • **SEND_LCP_CON_REQ**—Number of sent link configuration request packets. • **RECV_LCP_CON_REQ**—Number of received link configuration request packets. • **SEND_LCP_CON_NAK**—Number of sent link configuration NAK packets. • **RECV_LCP_CON_NAK**—Number of received link configuration NAK packets. • **SEND_LCP_CON_REJ**—Number of sent link configuration reject packets. • **RECV_LCP_CON_REJ**—Number of received link configuration reject packets. • **SEND_LCP_CON_ACK**—Number of sent link configuration ACK packets. • **RECV_LCP_CON_ACK**—Number of received link configuration ACK packets. • **SEND_LCP_CODE_REJ**—Number of sent link configuration code reject packets. • **RECV_LCP_CODE_REJ**—Number of received link configuration code reject packets. • **SEND_LCP_PROT_REJ**—Number of sent link configuration protocol reject packets. • **RECV_LCP_PROT_REJ**—Number of received link configuration protocol reject packets. • **SEND_LCP_TERM_REQ**—Number of sent link termination request packets. • **RECV_LCP_TERM_REQ**—Number of received link termination request packets. • **SEND_LCP_TERM_ACK**—Number of sent link termination ACK packets. • **RECV_LCP_TERM_ACK**—Number of received link termination ACK packets. • **SEND_LCP_ECHO_REQ**—Number of sent LCP echo request packets. • **RECV_LCP_ECHO_REQ**—Number of received LCP echo request packets. • **SEND_LCP_ECHO_REP**—Number of sent LCP echo reply packets. • **RECV_LCP_ECHO_REP**—Number of received LCP echo reply packets. • **SEND_LCP_FAIL**—Number of sent link failure packets.
IPCP	IPCP packet statistics. • **SEND_IPCP_CON_REQ**—Number of sent IP address negotiation request packets. • **RECV_IPCP_CON_REQ**—Number of received IP address negotiation request packets. • **SEND_IPCP_CON_NAK**—Number of sent IP address negotiation NAK packets. • **RECV_IPCP_CON_NAK**—Number of received IP address negotiation NAK packets. • **SEND_IPCP_CON_REJ**—Number of sent IP address negotiation reject packets. • **RECV_IPCP_CON_REJ**—Number of received IP address negotiation reject packets. • **SEND_IPCP_CON_ACK**—Number of sent IP address negotiation ACK packets. • **RECV_IPCP_CON_ACK**—Number of received IP address negotiation ACK packets. • **SEND_IPCP_CODE_REJ**—Number of sent IP address negotiation code reject packets. • **RECV_IPCP_CODE_REJ**—Number of received IP address negotiation code reject packets. • **SEND_IPCP_PROT_REJ**—Number of sent IP address negotiation protocol reject packets. • **RECV_IPCP_PROT_REJ**—Number of received IP address negotiation protocol reject packets. • **SEND_IPCP_TERM_REQ**—Number of sent IP address negotiation termination request packets. • **RECV_IPCP_TERM_REQ**—Number of received IP address negotiation termination

Field	Description
	request packets. • **SEND_IPCP_TERM_ACK**—Number of sent IP address negotiation termination ACK packets. • **RECV_IPCP_TERM_ACK**—Number of received IP address negotiation termination ACK packets. • **SEND_IPCP_FAIL**—Number of sent IP address negotiation failure packets.
IPV6CP	IPv6CP packet statistics. • **SEND_IPV6CP_CON_REQ**—Number of sent IPv6 address negotiation request packets. • **RECV_IPV6CP_CON_REQ**—Number of received IPv6 address negotiation request packets. • **SEND_IPV6CP_CON_NAK**—Number of sent IPv6 address negotiation NAK packets. • **RECV_IPV6CP_CON_NAK**—Number of received IPv6 address negotiation NAK packets. • **SEND_IPV6CP_CON_REJ**—Number of sent IPv6 address negotiation reject packets. • **RECV_IPV6CP_CON_REJ**—Number of received IPv6 address negotiation reject packets. • **SEND_IPV6CP_CON_ACK**—Number of sent IPv6 address negotiation ACK packets. • **RECV_IPV6CP_CON_ACK**—Number of received IPv6 address negotiation ACK packets. • **SEND_IPV6CP_CODE_REJ**—Number of sent IPv6 address negotiation code reject packets. • **RECV_IPV6CP_CODE_REJ**—Number of received IPv6 address negotiation code reject packets. • **SEND_IPV6CP_PROT_REJ**—Number of sent IPv6 address negotiation protocol reject packets. • **RECV_IPV6CP_PROT_REJ**—Number of received IPv6 address negotiation protocol reject packets. • **SEND_IPV6CP_TERM_REQ**—Number of sent IPv6 address negotiation termination request packets. • **RECV_IPV6CP_TERM_REQ**—Number of received IPv6 address negotiation termination request packets. • **SEND_IPV6CP_TERM_ACK**—Number of sent IPv6 address negotiation termination ACK packets. • **RECV_IPV6CP_TERM_ACK**—Number of received IPv6 address negotiation termination ACK packets. • **SEND_IPV6CP_FAIL**—Number of sent IPv6 address negotiation failure packets.
OSICP	OSICP packet statistics. • **SEND_OSICP_CON_REQ**—Number of sent OSI address negotiation request packets. • **RECV_OSICP_CON_REQ**—Number of received OSI address negotiation request packets. • **SEND_OSICP_CON_NAK**—Number of sent OSI address negotiation NAK packets. • **RECV_OSICP_CON_NAK**—Number of received OSI address negotiation NAK packets. • **SEND_OSICP_CON_REJ**—Number of sent OSI address negotiation reject packets. • **RECV_OSICP_CON_REJ**—Number of received OSI address negotiation reject packets. • **SEND_OSICP_CON_ACK**—Number of sent OSI address negotiation ACK packets. • **RECV_OSICP_CON_ACK**—Number of received OSI address negotiation ACK packets. • **SEND_OSICP_CODE_REJ**—Number of sent OSI address negotiation code reject packets. • **RECV_OSICP_CODE_REJ**—Number of received OSI address negotiation code reject packets.

Field	Description
	• **SEND_OSICP_PROT_REJ**—Number of sent OSI address negotiation protocol packets. • **RECV_OSICP_PROT_REJ**—Number of received OSI address negotiation protocol reject packets. • **SEND_OSICP_TERM_REQ**—Number of sent OSI address negotiation termination request packets. • **RECV_OSICP_TERM_REQ**—Number of received OSI address negotiation termination request packets. • **SEND_OSICP_TERM_ACK**—Number of sent OSI address negotiation termination ACK packets. • **RECV_OSICP_TERM_ACK**—Number of received OSI address negotiation termination ACK packets. • **SEND_OSICP_FAIL**—Number of sent OSI address negotiation failure packets.
MPLSCP	MPLSCP packet statistics. • **SEND_MPLSCP_CON_REQ**—Number of sent MPLS address negotiation request packets. • **RECV_MPLSCP_CON_REQ**—Number of received MPLS address negotiation request packets. • **SEND_MPLSCP_CON_NAK**—Number of sent MPLS address negotiation NAK packets. • **RECV_MPLSCP_CON_NAK**—Number of received MPLS address negotiation NAK packets. • **SEND_MPLSCP_CON_REJ**—Number of sent MPLS address negotiation reject packets. • **RECV_MPLSCP_CON_REJ**—Number of received MPLS address negotiation reject packets. • **SEND_MPLSCP_CON_ACK**—Number of sent MPLS address negotiation ACK packets. • **RECV_MPLSCP_CON_ACK**—Number of received MPLS address negotiation ACK packets. • **SEND_MPLSCP_CODE_REJ**—Number of sent MPLS address negotiation code reject packets. • **RECV_MPLSCP_CODE_REJ**—Number of received MPLS address negotiation code reject packets. • **SEND_MPLSCP_PROT_REJ**—Number of sent MPLS address negotiation protocol packets. • **RECV_MPLSCP_PROT_REJ**—Number of received MPLS address negotiation protocol reject packets. • **SEND_MPLSCP_TERM_REQ**—Number of sent MPLS address negotiation termination request packets. • **RECV_MPLSCP_TERM_REQ**—Number of received MPLS address negotiation termination request packets. • **SEND_MPLSCP_TERM_ACK**—Number of sent MPLS address negotiation termination ACK packets. • **RECV_MPLSCP_TERM_ACK**—Number of received MPLS address negotiation termination ACK packets. • **SEND_MPLSCP_FAIL**—Number of sent MPLS address negotiation failure packets.
AUTH	Authentication packet statistics. • **SEND_PAP_AUTH_REQ**—Number of sent PAP authentication request packets. • **RECV_PAP_AUTH_REQ**—Number of received PAP authentication request packets. • **SEND_PAP_AUTH_ACK**—Number of sent PAP authentication ACK packets. • **RECV_PAP_AUTH_ACK**—Number of received PAP authentication ACK packets. • **SEND_PAP_AUTH_NAK**—Number of sent PAP authentication NAK packets. • **RECV_PAP_AUTH_NAK**—Number of received PAP authentication NAK packets.

Field	Description
	• **SEND_CHAP_AUTH_CHALLENGE**—Number of sent CHAP authentication request packets. • **RECV_CHAP_AUTH_CHALLENGE**—Number of received CHAP authentication request packets. • **SEND_CHAP_AUTH_RESPONSE**—Number of sent CHAP authentication response packets. • **RECV_CHAP_AUTH_RESPONSE**—Number of received CHAP authentication response packets. • **SEND_CHAP_AUTH_ACK**—Number of sent CHAP authentication ACK packets. • **RECV_CHAP_AUTH_ACK**—Number of received CHAP authentication ACK packets. • **SEND_CHAP_AUTH_NAK**—Number of sent CHAP authentication NAK packets. • **RECV_CHAP_AUTH_NAK**—Number of received CHAP authentication NAK packets. • **SEND_PAP_AUTH_FAIL**—Number of sent PAP authentication failure packets. • **SEND_CHAP_AUTH_FAIL**—Number of sent CHAP authentication failure packets.

Related commands

reset ppp packet statistics

interface virtual-template

Use **interface virtual-template** to create a VT interface and enter its view, or enter the view of an existing VT interface.

Use **undo interface virtual-template** to remove a VT interface.

Syntax

interface virtual-template *number*

undo interface virtual-template *number*

Default

No VT interfaces exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

number: Specifies a VT interface by its number. The value range for this argument is 1 to 1024.

Usage guidelines

To remove a VT interface, make sure all the corresponding VA interfaces are removed and the VT interface is not in use.

Examples

Create interface Virtual-Template 10.

```
<Sysname> system-view
[Sysname] interface virtual-template 10
[Sysname-Virtual-Template10]
```

ip address ppp-negotiate

Use **ip address ppp-negotiate** to enable IP address negotiation on an interface, so that the interface can accept the IP address allocated by the server.

Use **undo ip address ppp-negotiate** to restore the default.

Syntax

ip address ppp-negotiate

undo ip address ppp-negotiate

Default

IP address negotiation is disabled on an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

If you execute the **ip address ppp-negotiate** and **ip address** commands multiple times, the most recent configuration takes effect.

Examples

Enable IP address negotiation on Virtual-Template 1.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ip address ppp-negotiate
```

Related commands

ip address (*Layer 3—IP Services Command Reference*)

ip pool

Use **ip pool** to configure a PPP address pool.

Use **undo ip pool** to remove a PPP address pool or an IP address range of the PPP address pool.

Syntax

ip pool *pool-name start-ip-address* [*end-ip-address*] [**group** *group-name*]

undo ip pool *pool-name* [*start-ip-address* [*end-ip-address*]]

Default

No PPP address pool is configured.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

pool-name: Specifies a name for the PPP address pool to be created, a case-sensitive string of 1 to 31 characters.

start-ip-address [*end-ip-address*]: Specifies an IP address range. If you do not specify the *end-ip-address* argument, the PPP address pool has only the start IP address.

group *group-name*: Specifies a group by its name to which the PPP address pool belongs. The group name is a case-sensitive string of 1 to 31 characters. If you do not specify this option, the group name is **default** (the default group).

Usage guidelines

The system supports multiple address spaces that each correspond to a VPN instance. The same IP addresses can exist in different address spaces.

Each address space is represented by a group. One group can contain multiple PPP address pools, but one PPP address pool can belong to only one group.

One PPP address pool can contain multiple IP address ranges. You can execute this command multiple times to specify multiple IP address ranges for a PPP address pool. A PPP address pool can contain a maximum of 65535 IP addresses, and so can an IP address range.

IP address ranges in different groups can be overlapping, but those in the same group cannot.

Changes to a PPP address pool do not affect assigned IP addresses. For example, if you delete a PPP address pool from which an IP address has been assigned, the IP address can still be used.

When assigning IP address to users through a PPP address pool, make sure the PPP address pool excludes the gateway IP address of the PPP address pool.

Examples

Configure PPP address pool **aaa** that contains IP addresses 129.102.0.1 through 129.102.0.10 for group **a**.

```
<Sysname> system-view
[Sysname] ip pool aaa 129.102.0.1 129.102.0.10 group a
```

Related commands

display ip pool

ip pool gateway

Use **ip pool gateway** to configure a gateway address for a PPP address pool.

Use **undo ip pool gateway** to remove the gateway address for the specified PPP address pool.

Syntax

ip pool *pool-name* **gateway** *ip-address* [**vpn-instance** *vpn-instance-name*]

undo ip pool *pool-name* **gateway**

Default

A PPP address pool is not configured with a gateway address.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

pool-name: Specifies an existing PPP address pool by its name, a case-sensitive string of 1 to 31 characters.

ip-address: Specifies a gateway address for the PPP address pool.

vpn-instance *vpn-instance-name*: Specifies an existing MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the specified gateway belongs to the public network.

Usage guidelines

An interface on a BRAS must have an IP address before it can assign an IP address from a PPP or DHCP address pool to a client. This command enables interfaces that have no IP address to use a gateway address for IPCP negotiation and address allocation.

When you configure a gateway address for a PPP address pool, follow these restrictions and guidelines:

- If you also specify an IP address for an interface, the interface uses its own IP address to perform IPCP negotiation.
- You can specify only one gateway address for a PPP address pool. Different PPP address pools must have different gateway addresses (different combinations of *ip-address* and *vpn-instance-name*).
- You can specify any gateway address for a PPP address pool.

Examples

Specify gateway address **1.1.1.1** for PPP address pool **aaa**.

```
<Sysname> system-view
[Sysname] ip pool aaa gateway 1.1.1.1
```

Related commands

ip pool

mtu

Use **mtu** to set the MTU size of an interface.

Use **undo mtu** to restore the default.

Syntax

mtu *size*

undo mtu

Default

The MTU size of a VT interface is 1500 bytes.

Views

VT interface view

Predefined user roles

network-admin

context-admin

Parameters

size: Specifies the MTU size. The value range for this argument is 128 to 1500.

Usage guidelines

The MTU size setting of an interface affects the fragmentation and reassembly of IP packets on that interface.

For the configured MTU size to take effect, you must execute the **shutdown** command and then the **undo shutdown** command on the interface.

Examples

Set the MTU size of Virtual-Template 10 to 1400 bytes.

```
<Sysname> system-view
[Sysname] interface virtual-template 10
[Sysname-Virtual-Template10] mtu 1400
```

nas-port-type

Use **nas-port-type** to configure the NAS-Port-Type attribute on a VT interface.

Use **undo nas-port-type** to restore the default.

Syntax

nas-port-type { **ethernet** | **virtual** }

undo nas-port-type

Default

The NAS-Port-Type attribute is determined by the service type and link type of the PPP user, as shown in Table 8.

Table 8 Default NAS-Port-Type attribute

Service type	Link type	NAS-Port-Type attribute
PPPoE	Any	**ethernet**
L2TP	Any	**virtual**

Views

VT interface view

Predefined user roles

network-admin

context-admin

Parameters

ethernet: Specifies Ethernet. The code value is 15.

virtual: Specifies virtual. The code value is 5.

Usage guidelines

The NAS-Port-Type attribute is used for RADIUS authentication and accounting. For more information about the NAS-Port-Type attribute, see RFC 2865.

This command does not affect existing users.

Examples

Set the NAS-Port-Type attribute to **virtual** for Virtual-Template 1.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
```

```
[Sysname-Virtual-Template1] nas-port-type virtual
```

ppp access-user log enable

Use **ppp access-user log enable** to enable PPP user logging.

Use **undo ppp access-user log enable** to disable PPP user logging.

Syntax

ppp access-user log enable [**abnormal-logout** | **failed-login** | **normal-logout** | **successful-login**] *

undo ppp access-user log enable [**abnormal-logout** | **failed-login** | **normal-logout** | **successful-login**] *

Default

Logging is disabled for PPP users.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

successful-login: Specifies login success logs.

failed-login: Specifies login failure logs.

normal-logout: Specifies normal logout logs.

abnormal-logout: Specifies abnormal logout logs.

Usage guidelines

IMPORTANT:

Typically, disable this feature to prevent excessive PPP log output.

The PPP user logging feature enables the device to generate PPP logs and send them to the information center. Logs are generated after a user comes online, goes offline, or fails to come online. A log entry contains information such as the username, IP address, interface name, inner VLAN, outer VLAN, MAC address, and failure causes. For information about the log destination and output rule configuration in the information center, see *Network Management and Monitoring Configuration Guide*.

When you execute this command without specifying any keyword, this command enables or disables logging for login successes, login failures, normal logouts, and abnormal logouts.

Examples

Enable PPP user logging.

```
<Sysname> system-view
[Sysname] ppp access-user log enable
```

ppp account-statistics enable

Use **ppp account-statistics enable** to enable PPP accounting on an interface.

Use **undo ppp account-statistics enable** to disable PPP accounting on an interface.

Syntax

ppp account-statistics enable [**acl** { *acl-number* | **name** *acl-name* }]

undo ppp account-statistics enable

Default

PPP accounting is disabled on an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

acl: Specifies an ACL to match traffic. If no ACL is specified, the device generates statistics for all PPP traffic.

acl-number: Specifies an ACL by its number in the range of 2000 to 3999, where:

- 2000 to 2999 are numbers for basic IPv4 and IPv6 ACLs.
- 3000 to 3999 are numbers for advanced IPv4 and IPv6 ACLs.

If the specified ACL number corresponds to an IPv4 ACL and an IPv6 ACL, both ACLs take effect.

name *acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters that start with an alphabetical character. To avoid confusion, do not use **all** as an ACL name.

Examples

Enable PPP accounting on Virtual-Template 1.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp account-statistics enable
```

ppp acfc local-request

Use **ppp acfc local-request** to configure an interface to send ACFC requests by including the ACFC option in outbound LCP negotiation requests.

Use **undo ppp acfc local-request** to restore the default.

Syntax

ppp acfc local-request

undo ppp acfc local-request

Default

An interface does not include the ACFC option in outbound LCP negotiation requests.

Views

Interface view

Predefined user roles

network-admin

context-admin

Examples

Configure Virtual-Template 1 to send ACFC requests to the peer in PPP negotiation.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp acfc local-request
```

ppp acfc remote-reject

Use **ppp acfc remote-reject** to configure an interface to reject ACFC requests received from the remote peer.

Use **undo ppp acfc remote-reject** to restore the default.

Syntax

ppp acfc remote-reject

undo ppp acfc remote-reject

Default

An interface accepts ACFC requests received from the remote peer, and it performs ACFC on frames sent to the peer.

Views

Interface view

Predefined user roles

network-admin

context-admin

Examples

Configure Virtual-Template 1 to reject ACFC requests received from the remote peer.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp acfc remote-reject
```

ppp authentication-mode

Use **ppp authentication-mode** to configure PPP authentication on an interface.

Use **undo ppp authentication-mode** to restore the default.

Syntax

ppp authentication-mode { **chap** | **ms-chap** | **ms-chap-v2** | **pap** } * [[**call-in**] **domain** { *isp-name* | **default enable** *isp-name* }]

undo ppp authentication-mode

Default

PPP authentication is disabled on an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

chap: Uses CHAP authentication.

ms-chap: Uses MS-CHAP authentication.

ms-chap-v2: Uses MS-CHAP-V2 authentication.

pap: Uses PAP authentication.

call-in: Authenticates the call-in users only.

domain *isp-name*: Specifies the ISP domain name for authentication, a case-insensitive string of 1 to 255 characters.

default enable *isp-name*: Specifies the default ISP domain name for authentication, a case-insensitive string of 1 to 255 characters.

Usage guidelines

PPP authentication includes the following categories:

- **PAP**—Two-way handshake authentication. The password is in plain text or cipher text.
- **CHAP**—Three-way handshake authentication. The password is in plain text or cipher text.
- **MS-CHAP**—Three-way handshake authentication. The password is in cipher text.
- **MS-CHAP-V2**—Three-way handshake authentication. The password is in cipher text.

You can configure multiple authentication modes.

In any PPP authentication mode, AAA determines whether a user can pass the authentication through a local authentication database or an AAA server. For more information about AAA authentication, see *Security Configuration Guide*.

If multiple ISP domains are available, the ISP domains are used in the following order:

1. ISP domain specified by the **domain** *isp-name* option in this command.
2. ISP domain contained in the username.
3. ISP domain specified by the **domain default enable** *isp-name* option in this command.
4. ISP domain selected by using the AAA module. For more information about AAA, see *Security Configuration Guide*.

For authentication on a dialup interface, configure authentication on both the physical interface and the dialer interface. When a physical interface receives a DDR call request, it first initiates PPP negotiation and authenticates the dial-in user. Then it passes the call to the upper layer protocol.

Examples

Configure Virtual-Template 1 to authenticate the peer by using PAP.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp authentication-mode pap
```

Configure Virtual-Template 1 to authenticate the peer by using PAP and CHAP.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp authentication-mode pap chap
```

Related commands

domain default (*Security Command Reference*)

local-user (*Security Command Reference*)

ppp chap password

ppp chap user

ppp pap local-user

ppp chap password

Use **ppp chap password** to set the password for CHAP authentication on an interface.

Use **undo ppp chap password** to restore the default.

Syntax

ppp chap password { **cipher** | **simple** } *string*

undo ppp chap password

Default

No password is set for CHAP authentication on an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 255 characters. Its encrypted form is a case-sensitive string of 1 to 373 characters.

Examples

Set the password for CHAP authentication to plaintext password **sysname** on Virtual-Template 1.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp chap password simple sysname
```

Related commands

ppp authentication-mode

ppp chap user

Use **ppp chap user** to set the username for CHAP authentication on an interface.

Use **undo ppp chap user** to restore the default.

Syntax

ppp chap user *username*

undo ppp chap user

Default

The username for CHAP authentication is null on an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

username: Specifies the username for CHAP authentication, a case-sensitive string of 1 to 80 characters. The username is sent to the peer for the local device to be authenticated.

Usage guidelines

To pass CHAP authentication, the username/password of one side must be the local username/password on the peer.

Examples

Set the username for CHAP authentication to **Root** on Virtual-Template 1.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp chap user Root
```

Related commands

ppp authentication-mode

ppp compression iphc enable

Use **ppp compression iphc enable** to enable IPHC on an interface.

Use **undo ppp compression iphc enable** to disable IPHC on an interface.

Syntax

ppp compression iphc enable [**nonstandard**]

undo ppp compression iphc enable

Default

IPHC is disabled on an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

nonstandard: Specifies the nonstandard encapsulation format. If you do not specify this keyword, packets are encapsulated in standard format. You must specify this keyword when the device communicates with a non-NSFOCUS device. If you specify this keyword, this command enables RTP header compression.

Usage guidelines

IPHC includes RTP header compression and TCP header compression.

Enabling or disabling IPHC enables or disables both RTP header compression and TCP header compression.

To use IPHC, you must enable it on both sides of a PPP link.

When you enable IPHC on a VT or dialer interface, the setting does not immediately take effect. For the setting to take effect, execute the **shutdown** and then **undo shutdown** commands on the interface or its bound physical interface.

Examples

Enable IPHC on Virtual-Template 1.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp compression iphc enable
```

ppp compression iphc rtp-connections

Use **ppp compression iphc rtp-connections** to set the maximum number of connections for which an interface can perform RTP header compression.

Use **undo ppp compression iphc rtp-connections** to restore the default.

Syntax

ppp compression iphc rtp-connections *number*

undo ppp compression iphc rtp-connections

Default

An interface can perform RTP header compression for a maximum of 16 connections.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

number: Specifies the maximum number of connections for which an interface can perform RTP header compression. The value range for this argument is 3 to 1000:

- When the *number* argument is set to a value less than or equal to 256, packets are compressed in the format of COMPRESSED RTP 8.
- When the *number* argument is set to a value greater than 256, packets are compressed in the format of COMPRESSED RTP 16.

Usage guidelines

RTP is a connection-oriented protocol. An interface can accommodate multiple RTP connections.

RTP header compression occupies memory resources for maintaining connection information. This command can limit memory resources used by compression. For example, if you set the limit to 3, RTP header compression only applies to a maximum of three RTP connections.

After you execute this command, you must shut down and then bring up the interface to make the command take effect.

You can configure this command only when IPHC is enabled. The configuration is removed after IPHC is disabled.

Examples

Set the maximum number of connections for which Virtual-Template 1 can perform RTP header compression to 10.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp compression iphc enable
[Sysname-Virtual-Template1] ppp compression iphc rtp-connections 10
```

Related commands

ppp compression iphc enable

ppp compression iphc tcp-connections

Use **ppp compression iphc tcp-connections** to set the maximum number of connections for which an interface can perform TCP header compression.

Use **undo ppp compression iphc tcp-connections** to restore the default.

Syntax

ppp compression iphc tcp-connections *number*

undo ppp compression iphc tcp-connections

Default

An interface can perform TCP header compression for a maximum of 16 connections.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

number: Specifies the maximum number of connections for which an interface can perform TCP header compression. The value range for this argument is 3 to 256.

Usage guidelines

TCP is a connection-oriented protocol. A link can accommodate multiple TCP connections.

TCP header compression occupies memory resources for maintaining connection information. This command can limit memory resources used by compression. For example, if you set the limit to 3, TCP header compression only applies to a maximum of three TCP connections.

After you execute this command, you must shut down and then bring up the interface to make the command take effect.

You can configure this command only when IPHC is enabled and packets are encapsulated in standard format. The configuration is removed after IPHC is disabled or packets are encapsulated in nonstandard format.

Examples

Set the maximum number of connections for which Virtual-Template 1 can perform TCP header compression to 10.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp compression iphc enable
[Sysname-Virtual-Template1] ppp compression iphc tcp-connections 10
```

Related commands

ppp compression iphc enable

ppp ipcp dns

Use **ppp ipcp dns** to configure the primary and secondary DNS server IP addresses to be allocated in PPP negotiation on an interface.

Use **undo ppp ipcp dns** to delete the primary and secondary DNS server IP addresses to be allocated in PPP negotiation on an interface.

Syntax

ppp ipcp dns *primary-dns-address* [*secondary-dns-address*]

undo ppp ipcp dns *primary-dns-address* [*secondary-dns-address*]

Default

The DNS server IP addresses to be allocated in PPP negotiation are not configured on an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

primary-dns-address: Specifies a primary DNS server IP address.

secondary-dns-address: Specifies a secondary DNS server IP address.

Usage guidelines

A device can assign DNS server IP addresses to its peer during PPP negotiation when the peer initiates requests.

To check the allocated DNS server IP addresses, execute the **winipcfg** or **ipconfig /all** command on the host.

Examples

Set the primary and secondary DNS server IP addresses to 100.1.1.1 and 100.1.1.2 for the peer on Virtual-Template 1.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp ipcp dns 100.1.1.1 100.1.1.2
```

ppp ipcp dns admit-any

Use **ppp ipcp dns admit-any** to configure an interface to accept the DNS server IP addresses assigned by the peer even though it does not request DNS server IP addresses from the peer.

Use **undo ppp ipcp dns admit-any** to restore the default.

Syntax

ppp ipcp dns admit-any

undo ppp ipcp dns admit-any

Default

An interface does not accept the DNS server IP addresses assigned by the peer if it does not request DNS server IP addresses from the peer.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

You can configure an interface to accept the DNS server IP addresses assigned by the peer, through which domain names can be resolved for the device.

Typically, the server assigns a DNS server address to a client in PPP negotiation only when the client is configured with the **ppp ipcp dns request** command. Some servers, however, forcibly assign DNS server addresses to clients. You must configure the **ppp ipcp dns admit-any** command on the client devices to accept the DNS server addresses.

Examples

Configure Virtual-Template 1 to accept DNS server IP addresses allocated by the peer.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp ipcp dns admit-any
```

Related commands

ppp ipcp dns request

ppp ipcp dns request

Use **ppp ipcp dns request** to enable an interface to actively request the DNS server IP address from its peer.

Use **undo ppp ipcp dns request** to restore the default.

Syntax

ppp ipcp dns request

undo ppp ipcp dns request

Default

An interface does not actively request the DNS server IP address from its peer.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

If a device is connected to a provider's access server through a PPP link, you can use this command. Then, the device can obtain the specified DNS server IP address from the access server during IPCP negotiation.

You can check the DNS server IP addresses by displaying information about the interface.

Examples

Enable Virtual-Template 1 to actively request the DNS server IP address from its peer.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp ipcp dns request
```

ppp ipcp remote-address match

Use **ppp ipcp remote-address match** to enable the IP segment match feature for PPP IPCP negotiation on an interface.

Use **undo ppp ipcp remote-address match** to restore the default.

Syntax

ppp ipcp remote-address match

undo ppp ipcp remote-address match

Default

The IP segment match feature is disabled for PPP IPCP negotiation on an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command enables the local interface to check whether its IP address and the IP address of the remote interface are in the same network segment. If they are not, IPCP negotiation fails.

Examples

Enable the IP segment match feature on Virtual-Template 1.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp ipcp remote-address match
```

ppp ip-pool route

Use **ppp ip-pool route** to configure a PPP address pool route.

Use **undo ppp ip-pool route** to remove a PPP address pool route.

Syntax

ppp ip-pool route *ip-address* { *mask-length* | *mask* } [**vpn-instance** *vpn-instance-name*]

undo ppp ip-pool route *ip-address* { *mask-length* | *mask* } [**vpn-instance** *vpn-instance-name*]

Default

No PPP address pool route is configured.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the destination IP address of the PPP address pool route, in dotted decimal notation.

mask-length: Specifies a mask length for the IP address, in the range of 0 to 32.

mask: Specifies a mask for the IP address, in dotted decimal notation.

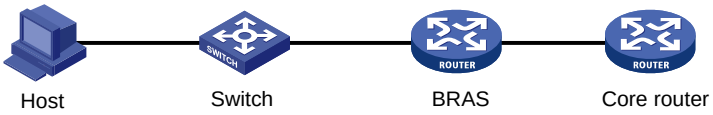
vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the PPP address pool route applies to the public network.

Usage guidelines

The BRAS uses PPP address pool routes to control downlink traffic forwarding.

After you configure a PPP address pool route, the BRAS generates a static blackhole route destined for the specified network. All traffic matching the blackhole route is discarded. When a legal user logs in, the BRAS adds a host route destined for the specified network. In addition, the BRAS uses a dynamic routing protocol to redistribute the PPP address pool route to the upstream device.

Figure 1 Network diagram for the PPP address pool route



Make sure the destination network of the PPP address pool route includes the PPP address pool. You can execute this command multiple times to configure multiple PPP address pool routes.

Examples

Configure the PPP address pool route as 2.2.2.2/24.

```
<Sysname> system-view
[Sysname] ppp ip-pool route 2.2.2.2 24
```

ppp lcp delay

Use **ppp lcp delay** to set the LCP negotiation delay timer.

Use **undo ppp lcp delay** to restore the default.

Syntax

ppp lcp delay *milliseconds*

undo ppp lcp delay

Default

PPP starts LCP negotiation immediately after the physical layer comes up.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

milliseconds: Specifies the LCP negotiation delay timer in the range of 1 to 10000 milliseconds.

Usage guidelines

If two ends of a PPP link vary greatly in the LCP negotiation packet processing rate, configure this command on the end with a higher processing rate. The LCP negotiation delay timer prevents frequent LCP negotiation packet retransmission. After the physical layer comes up, PPP starts LCP negotiation when the delay timer expires. If PPP receives LCP negotiation packets before the delay timer expires, it starts LCP negotiation immediately.

Examples

Set the LCP negotiation delay timer to 130 milliseconds.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp lcp delay 130
```

ppp pap local-user

Use **ppp pap local-user** to set the local username and password for PAP authentication on an interface.

Use **undo ppp pap local-user** to restore the default.

Syntax

ppp pap local-user *username* **password** { **cipher** | **simple** } *string*

undo ppp pap local-user

Default

The local username and password for PAP authentication are blank on an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

username: Specifies the username of the local device for PAP authentication, a case-sensitive string of 1 to 80 characters.

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 255 characters. Its encrypted form is a case-sensitive string of 1 to 373 characters.

Usage guidelines

For the local device to pass PAP authentication on the peer, make sure the username and password configured for the local device are also configured on the peer. You can configure the peer's

username and password by using the **local-user** *username* and **password** { **cipher** | **simple** } *string* commands, respectively.

Examples

Set the local username and password for PAP authentication to **user1** and plaintext **pass1** on Virtual-Template 1.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp pap local-user user1 password simple pass1
```

Related commands

local-user (*Security Command Reference*)

password (*Security Command Reference*)

ppp pfc local-request

Use **ppp pfc local-request** to configure an interface to send PFC requests by including the PFC option in outbound LCP negotiation requests.

Use **undo ppp pfc local** to restore the default.

Syntax

ppp pfc local-request

undo ppp pfc local-request

Default

An interface does not include the PFC option in outbound LCP negotiation requests.

Views

Interface view

Predefined user roles

network-admin

context-admin

Examples

Configure Virtual-Template 1 to send PFC requests during PPP negotiation.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp pfc local-request
```

ppp pfc remote-reject

Use **ppp pfc remote-reject** to configure an interface to reject PFC requests received from the remote peer.

Use **undo ppp pfc remote** to restore the default.

Syntax

ppp pfc remote-reject

undo ppp pfc remote-reject

Default

An interface accepts PFC requests received from the remote peer, and it performs PFC on frames sent to the peer.

Views

Interface view

Predefined user roles

network-admin

context-admin

Examples

Configure Virtual-Template 1 to reject PFC requests received from the remote peer.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp pfc remote-reject
```

ppp timer negotiate

Use **ppp timer negotiate** to set the PPP negotiation timeout time on an interface.

Use **undo ppp timer negotiate** to restore the default.

Syntax

ppp timer negotiate *seconds*

undo ppp timer negotiate

Default

The PPP negotiation timeout time is 3 seconds on an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies the negotiation timeout time in the range of 1 to 10 seconds.

Usage guidelines

In PPP negotiation, if the local device receives no response from the peer during the timeout time after it sends a packet, the local device sends the last packet again.

Examples

Set the PPP negotiation timeout time to 5 seconds on Virtual-Template 1.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp timer negotiate 5
```

remote address

Use **remote address** to configure an interface to assign an IP address to the client.

Use **undo remote address** to restore the default.

Syntax

remote address { *ip-address* | **pool** *pool-name* }

undo remote address

Default

An interface does not assign an IP address to the client.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the IP address to be assigned to the client.

pool *pool-name*: Specifies a PPP or DHCP address pool by its name from which an IP address is assigned to the client. The pool name is a case-sensitive string of 1 to 31 characters.

Usage guidelines

This command can be used when the local interface is configured with an IP address, but the peer has no IP address. To enable the peer to accept the IP address assigned by the local interface (server), you must configure the **ip address ppp-negotiate** command on the peer to make the peer act as a client.

This command enables the local interface to forcibly assign an IP address to the peer. If the peer is not configured with the **ip address ppp-negotiate** command but configured with an IP address, the peer will not accept the assigned IP address. This results in an IPCP negotiation failure.

PPP supports IP address assignment from a PPP or DHCP address pool, but the PPP address pool takes precedence over the DHCP address pool. For example, if you use a pool name that identifies both a PPP address pool and a DHCP address pool, the system uses only the PPP address pool for address assignment.

To make the configuration of the **remote address** command take effect, configure this command before the **ip address** command, which triggers IPCP negotiation. If you configure the **remote address** command after the **ip address** command, the server assigns an IP address to the client during the next IPCP negotiation.

After you use the **remote address** command to assign an IP address to the client, you can configure the **remote address** command again or the **undo remote address** command for the peer. However, the new configuration does not take effect until the next IPCP negotiation.

Examples

Specify the IP address to be assigned to the client as 10.0.0.1 on Virtual-Template 1.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] remote address 10.0.0.1
```

Configure Virtual-Template 1 to assign an IP address from address pool **aaa** to the client.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] remote address pool aaa
```

Related commands

ip address ppp-negotiate

ip pool

remote address dhcp client-identifier

Use **remote address dhcp client-identifier username** to configure the DHCP client IDs for PPP users acting as DHCP clients.

Use **undo remote address dhcp client-identifier** to restore the default.

Syntax

remote address dhcp client-identifier { **callingnum** | **username** }

undo remote address dhcp client-identifier

Default

No DHCP client IDs are configured for PPP users acting as DHCP clients.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

callingnum: Uses the calling numbers as the DHCP client IDs. The calling numbers are carried in the calling number AVPs in L2TP negotiation packets. A calling number is formed by the user MAC address and the VLAN to which the user belongs. For example, if the MAC address of a user is 000f-e235-dc71, and the inner VLAN and outer VLAN of the user are VLAN 1 and VLAN 2, respectively, the calling number of the user is 000f-e235-dc71-00010002.

username: Uses the PPP usernames as the DHCP client IDs.

Usage guidelines

By default, a PPP client randomly selects a DHCP client ID when the PPP client requests an IP address through DHCP. In this case, the DHCP server cannot assign specific IP addresses to specific clients based on client IDs. For the DHCP server to assign specific IP addresses to specific clients based on client IDs, use this command to configure the calling numbers or usernames as the DHCP client IDs.

When PPP usernames are used as the DHCP client IDs, make sure different users use different PPP usernames to come online.

Examples

Use the PPP usernames as the DHCP client IDs for PPP users acting as DHCP clients on Virtual-template 1.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] remote address dhcp client-identifier username
```

reset counters interface virtual-access

Use **reset counters interface virtual-access** to clear statistics on VA interfaces.

Syntax

reset counters interface [**virtual-access** [*interface-number*]]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

virtual-access: Clears statistics on VA interfaces.

interface-number: Specifies an existing VA interface by its number.

Usage guidelines

Before collecting traffic statistics regularly on a VA interface, clear the existing statistics.

If you do not specify the **virtual-access** keyword, the command clears statistics on all interfaces.

If you specify the **virtual-access** keyword without the *interface-number* argument, the command clears statistics on all VA interfaces.

If you specify both **virtual-access** and *interface-number*, the command clears statistics on the specified VA interface.

Examples

Clear statistics on Virtual-Access 10.

```
<Sysname> reset counters interface virtual-access 10
```

Related commands

display interface virtual-access

reset ppp access-user

Use **reset ppp access-user** to log off a PPP user.

Syntax

reset ppp access-user { **ip-address** *ipv4-address* [**vpn-instance** *ipv4-vpn-instance-name*] | **ipv6-address** *ipv6-address* [**vpn-instance** *ipv6-vpn-instance-name*] | **username** *user-name* }

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

ip-address *ipv4-address*: Specifies a PPP user by its IPv4 address.

ipv6-address *ipv6-address*: Specifies a PPP user by its IPv6 address.

vpn-instance *ipv4-vpn-instance-name*: Specifies a PPP user by the VPN to which the user belongs. The *ipv4-vpn-instance-name* argument specifies the name of the IPv4 MPLS

L3VPN instance, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the specified user belongs to the public network.

vpn-instance *ipv6-vpn-instance-name*: Specifies a PPP user by the VPN to which the user belongs. The *ipv6-vpn-instance-name* argument specifies the name of the IPv6 MPLS L3VPN instance, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the specified user belongs to the public network.

username *user-name*: Specifies a PPP user by username, a case-sensitive string of 1 to 80 characters.

Usage guidelines

This command takes effect only on the current login for a PPP user. The user can come online after it is logged off.

Examples

Log off the PPP user at 192.168.100.2.

```
<Sysname> reset ppp access-user ip-address 192.168.100.2
```

Related commands

display ppp access-user

reset ppp compression iphc

Use **reset ppp compression iphc** to clear IPHC statistics.

Syntax

reset ppp compression iphc [**rtp** | **tcp**] [**interface** *interface-type interface-number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

rtp: Clears IPHC RTP header compression statistics.

tcp: Clears IPHC TCP header compression statistics.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify this option, the command clears IPHC statistics on all interfaces.

Usage guidelines

If neither **rtp** nor **tcp** is specified, this command clears both RTP header compression and TCP header compression statistics.

Examples

Clear IPHC statistics on all interfaces.

```
<Sysname> reset ppp compression iphc
```

Related commands

display ppp compression iphc

reset ppp packet statistics

Use **reset ppp packet statistics** to clear PPP negotiation packet statistics.

Syntax

reset ppp packet statistics [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears PPP negotiation packet statistics for all IRF member devices.

Examples

Clear PPP negotiation packet statistics for slot 2.

```
<Sysname> reset ppp packet statistics slot 2
```

Related commands

display ppp packet statistics

timer-hold

Use **timer-hold** to set the keepalive interval on an interface.

Use **undo timer-hold** to restore the default.

Syntax

timer-hold *seconds*

undo timer-hold

Default

The keepalive interval is 10 seconds on an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies the interval for sending keepalive packets, in the range of 0 to 32767 seconds. The value 0 disables an interface from sending keepalive packets. In this case, the interface can respond to keepalive packets from the peer.

Usage guidelines

An interface sends keepalive packets at keepalive intervals to detect the availability of the peer. If the interface receives no response to keepalive packets when the keepalive retry limit is reached, it determines that the link fails and reports a link layer down event.

To set the keepalive retry limit, use the **timer-hold retry** command.

On a slow link, increase the keepalive interval to prevent false shutdown of the interface. This situation might occur when keepalive packets are delayed because a large packet is being transmitted on the link.

Examples

Set the keepalive interval to 20 seconds on Virtual-Template 1.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] timer-hold 20
```

Related commands

timer-hold retry

timer-hold retry

Use **timer-hold retry** to set the keepalive retry limit on an interface.

Use **undo timer-hold retry** to restore the default.

Syntax

timer-hold retry *retries*

undo timer-hold retry

Default

The keepalive retry limit is 5 on an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

retries: Specifies the maximum number of keepalive attempts in the range of 1 to 255.

Usage guidelines

An interface sends keepalive packets at keepalive intervals to detect the availability of the peer. If the interface receives no response to keepalive packets when the keepalive retry limit is reached, it determines that the link fails and reports a link layer down event.

To set the keepalive interval, use the **timer-hold** command.

On a slow link, increase the keepalive retry limit to prevent false shutdown of the interface. This situation might occur when keepalive packets are delayed because a large packet is being transmitted on the link.

Examples

Set the keepalive retry limit to 10 for Virtual-Template 1.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] timer-hold retry 10
```

Related commands

`timer-hold`

PPPoE commands

PPPoE client commands

dialer bundle enable

Use **dialer bundle enable** to enable bundle DDR on a dialer interface.

Use **undo dialer bundle enable** to disable bundle DDR on a dialer interface.

Syntax

dialer bundle enable

undo dialer bundle enable

Default

Bundle DDR is disabled on a dialer interface.

Views

Dialer interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

DDR includes traditional DDR and bundle DDR.

Before using bundle DDR, use this command to enable bundle DDR on a dialer interface. Then assign physical interfaces to the corresponding dialer bundle by using the **dialer bundle-member** command. To enable bundle DDR to receive calls, configure the **dialer peer-name** command on the dialer interface.

After you configure this command on a dialer interface already enabled with traditional DDR, the system clears the original traditional DDR settings.

The **undo dialer bundle enable** command clears all bundle DDR settings on the dialer interface.

Examples

Enable bundle DDR on Dialer 1.

```
<Sysname> system-view
[Sysname] interface dialer 1
[Sysname-Dialer1] dialer bundle enable
```

dialer diagnose

Use **dialer diagnose** to configure DDR to operate in diagnostic mode.

Use **undo dialer diagnose** to restore the default.

Syntax

dialer diagnose [**interval** *interval*]

undo dialer diagnose

Default

DDR operates in non-diagnostic mode.

Views

Dialer interface view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies the diagnostic interval in the range of 5 to 65535 seconds. The default is 120 seconds.

Usage guidelines

This command takes effect only when a dialer interface is used with PPPoE client applications.

In diagnostic mode, the device performs the following operations:

- Dials a PPPoE connection immediately after the device configurations are complete.
- Automatically terminates the connection.
- Starts the auto-dial timer after a configurable diagnostic interval.
- Redials a connection when the auto-dial timer expires.

By establishing and terminating PPPoE sessions periodically, you can monitor the operating status of the PPPoE link.

In diagnostic mode, the link idle-timeout timer is ignored.

Examples

Configure Dialer 1 to operate in diagnostic mode, with a diagnostic interval of 300 seconds.

```
<Sysname> system-view
[Sysname] interface dialer 1
[Sysname-Dialer1] dialer diagnose interval 300
```

Related commands

dialer timer autodial

dialer timer idle

dialer timer autodial

Use **dialer timer autodial** to set the auto-dial timer.

Use **undo dialer timer autodial** to restore the default.

Syntax

dialer timer autodial *autodial-interval*

undo dialer timer autodial

Default

The auto-dial timer is 300 seconds.

Views

Dialer interface view

Predefined user roles

network-admin

context-admin

Parameters

autodial-interval: Specifies the interval between auto-dial attempts, in the range of 1 to 604800 seconds.

Usage guidelines

This command takes effect only when the **autodial** keyword is specified in the **dialer number** or **dialer route** command. DDR automatically dials the dial string at the specified interval until a connection is established. In the auto-dial method, dial attempts are not traffic triggered. Once a connection is established, it will not disconnect based on the idle timer mechanism.

Examples

Set the auto-dial timer to 60 seconds on Dialer 1.

```
<Sysname> system-view
[Sysname] interface dialer 1
[Sysname-Dialer1] dialer timer autodial 60
```

dialer timer idle

Use **dialer timer idle** to set the link idle-timeout timer.

Use **undo dialer timer idle** to restore the default.

Syntax

dialer timer idle *idle* [**in** | **in-out**]

undo dialer timer idle

Default

The link idle-timeout timer is 120 seconds, and only outgoing interesting packets reset this timer.

Views

Dialer interface view

Predefined user roles

network-admin

context-admin

Parameters

idle: Specifies the link idle-timeout timer value in the range of 0 to 65535 seconds.

in: Allows only incoming interesting packets to reset the timer.

in-out: Allows both incoming and outgoing interesting packets to reset the timer.

Usage guidelines

The link idle-timeout timer starts when a link is established. If no interesting packets arrive before the timer expires, DDR disconnects the link.

If you do not specify the **in** or **in-out** keyword, only outgoing interesting packets reset the timer.

If the timer is set to 0, DDR will never disconnect the link. For a PPPoE client application, if the timer is set to 0, a dialup connection is created automatically and remains active permanently.

Examples

Set the link idle-timeout timer to 50 seconds on Dialer 1.

```
<Sysname> system-view
[Sysname] interface dialer 1
[Sysname-Dialer1] dialer timer idle 50
```

dialer-group

Use **dialer-group** to assign a dialer interface to a dialer group.

Use **undo dialer-group** to restore the default.

Syntax

dialer-group *group-number*

undo dialer-group

Default

A dialer interface does not belong to any dialer group.

Views

Dialer interface view

Predefined user roles

network-admin

context-admin

Parameters

group-number: Specifies a dialer group by its number in the range of 1 to 255. Before the assignment, you must create the dialer group by using the **dialer-group rule** command.

Usage guidelines

A dialup interface can belong to only one dialer group. If you configure this command multiple times, the most recent configuration takes effect.

You must configure this command for DDR to send packets.

Examples

Assign Dialer 1 to dialer group 1.

```
<Sysname> system-view
[Sysname] dialer-group 1 rule acl 3101
[Sysname] interface dialer 1
[Sysname-Dialer1] dialer-group 1
```

Related commands

dialer-group rule

dialer-group rule

Use **dialer-group rule** to create a dialer group and configure a dial rule for it.

Use **undo dialer-group rule** to delete a dialer group.

Syntax

dialer-group *group-number* **rule** { **ip** | **ipv6** } { **deny** | **permit** | **acl** { *acl-number* | **name** *acl-name* } }

undo dialer-group *group-number* **rule** [**ip** | **ipv6**]

Default

No dialer group exists.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

group-number: Specifies the number of the dialer group to be created, in the range of 1 to 255.

ip: Specifies the IPv4 protocol.

ipv6: Specifies the IPv6 protocol.

deny: Denies packets of the specified protocol.

permit: Permits packets of the specified protocol.

acl *acl-number*: Specifies an ACL by its number in the range of 2000 to 3999.

name *acl-name*: Specifies an ACL by its name.

Usage guidelines

A dial rule determines when an interface initiates DDR calls. You need to configure dial rules only on the initiator of DDR calls.

You can configure a dial rule to match only IP packets or use an ACL to match packets.

Permitted protocol packets or packets that match a permit statement of an ACL are interesting packets. When receiving an interesting packet, DDR performs one of the following operations:

- Sends it out and resets the idle-timeout timer if a link is present.
- Originates a new call to establish a link if no link is present.

Denied protocol packets or packets that match a deny statement of an ACL are uninteresting packets. When receiving an uninteresting packet, DDR performs one of the following operations:

- Sends it out without resetting the idle-timeout timer if a link is present.
- Drops it if no link is present.

For DDR to forward packets correctly, you must configure a dial rule and associate it with the dialup interface by using the **dialer-group** command.

Examples

Create dialer group 1 and configure DDR to place calls for IPv4 packets. Associate Dialer 1 with dialer group 1.

```
<Sysname> system-view
[Sysname] dialer-group 1 rule ip permit
[Sysname] interface dialer 1
[Sysname-Dialer] dialer-group 1
```

Create dialer group 1 and configure DDR to place calls for IPv6 packets. Associate Dialer 1 with dialer group 1.

```
<Sysname> system-view
[Sysname] dialer-group 1 rule ipv6 permit
[Sysname] interface dialer 1
[Sysname-Dialer1] dialer-group 1
```

Related commands

dialer-group

display pppoe-client session packet

Use **display pppoe-client session packet** to display the protocol packet statistics for a PPPoE session.

Syntax

display pppoe-client session packet [**dial-bundle-number** *number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

dial-bundle-number *number*: Specifies the dialer bundle number corresponding to a PPPoE session. The value range for the number argument is 0 to 1023. If you do not specify this option, the command displays the protocol packet statistics for all PPPoE sessions.

Usage guidelines

To display the data packet statistics for a PPPoE session, use the **display interface virtual-access** command to display information about the specified VA interface.

Examples

Display the protocol packet statistics for all PPPoE sessions.

```
<Sysname> display pppoe-client session packet
Bundle:    1                    Interface:  GE1/0/1
InPackets: 19                   OutPackets: 19
InBytes:   816                  OutBytes:   816
InDrops:   0                    OutDrops:   0

Bundle:    2                    Interface:  GE1/0/1
InPackets: 18                   OutPackets: 18
InBytes:   730                  OutBytes:   730
InDrops:   0                    OutDrops:   0
```

Table 9 Command output

Field	Description
Bundle	Dialer bundle to which a PPPoE session belongs.
Interface	Ethernet interface where the PPPoE session is present.

Field	Description
InPackets	Number of packets received.
OutPackets	Number of packets transmitted.
InBytes	Number of bytes received.
OutBytes	Number of bytes transmitted.
InDrops	Number of discarded incoming packets.
OutDrops	Number of discarded outgoing packets.

Related commands

reset pppoe-client session packet

display pppoe-client session summary

Use **display pppoe-client session summary** to display summary PPPoE session information.

Syntax

display pppoe-client session summary [**dial-bundle-number** *number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

dial-bundle-number *number*: Specifies the dialer bundle number corresponding to a PPPoE session. The value range for the number argument is 0 to 1023. If you do not specify this option, the command displays summary information for all PPPoE sessions.

Examples

Display summary information for all PPPoE sessions.

```
<Sysname> display pppoe-client session summary
Bundle ID    Interface    VA          RemoteMAC      LocalMAC       State
1      1     GE1/0/1      VA0         00e0-1400-4300 00e0-1500-4100 SESSION
2      1     GE1/0/2      VA1         00e0-1500-4300 00e0-1600-4100 SESSION
```

Table 10 Command output

Field	Description
Bundle	Dialer bundle to which the PPPoE session belongs.
Interface	Ethernet interface where the PPPoE session is present.
VA	Virtual access interface created for the PPPoE session.
RemoteMAC	MAC address of the remote end.
LocalMAC	MAC address of the local end.

Field	Description
State	PPPoE session state: • **IDLE**—Initialization state. • **PADI SENT**—A PPPoE Active Discovery Initiation (PADI) packet has been sent, and a PPPoE Active Discovery Offer (PADO) packet is being expected. • **PADR SENT**—A PPPoE Active Discovery Request (PADR) packet has been sent, and a PPPoE Active Discovery Session-confirmation (PADS) packet is being expected. • **SESSION**—The PPPoE session has been successfully established.

mtu

Use **mtu** to set the maximum transmission unit (MTU) of a dialer interface.

Use **undo mtu** to restore the default.

Syntax

mtu *size*

undo mtu

Default

The MTU of dialer interfaces is 1500 bytes.

Views

Dialer interface view

Predefined user roles

network-admin

context-admin

Parameters

size: Specifies the MTU in bytes. The value range for this argument is 128 to 1500.

Usage guidelines

The MTU setting of a dialer interface affects the fragmentation and reassembly of IP packets.

Examples

Set the MTU of Dialer 1 to 1200 bytes.

```
<Sysname> system-view
[Sysname] interface dialer 1
[Sysname-Dialer1] mtu 1200
```

pppoe-client

Use **pppoe-client** to establish a PPPoE session and specify the dialer bundle corresponding to the session.

Use **undo pppoe-client** to remove a PPPoE session.

Syntax

pppoe-client dial-bundle-number *number* [**no-hostuniq**]

undo pppoe-client dial-bundle-number *number*

Default

No PPPoE session is established.

Views

Layer 3 Ethernet interface/subinterface view

VLAN interface view

Layer 3 aggregate interface/subinterface view

Predefined user roles

network-admin

context-admin

Parameters

dial-bundle-number *number*: Specifies the dialer bundle number corresponding to a PPPoE session. A dialer bundle number uniquely identifies a PPPoE session. It can also be used as a PPPoE session ID. The value range for the number argument is 0 to 1023.

no-hostuniq: Configures the client not to carry the Host-Uniq field in discovery packets. If you do not specify this keyword, the client carries the Host-Unique field. The Host-Unique field uniquely identifies a PPPoE client when an interface is configured with multiple PPPoE sessions. When the PPPoE server receives a packet with this field, it must include this field unmodified in the response packet. The device identifies the PPPoE client where the response packet belongs based on the Host-Unique field in the response packet.

Examples

Establish a PPPoE session on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] pppoe-client dial-bundle-number 1
```

Establish a PPPoE session on VLAN-Interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] pppoe-client dial-bundle-number 1
```

reset pppoe-client

Use **reset pppoe-client** to reset a PPPoE session corresponding to a dialer bundle.

Syntax

reset pppoe-client { **all** | **dial-bundle-number** *number* }

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

all: Resets all the PPPoE sessions.

dial-bundle-number *number*: Specifies a dialer bundle by its number. The value range for the number argument is 0 to 1023.

Usage guidelines

A PPPoE session in permanent mode and terminated by this command will be established again when the auto dial timer expires.

A PPPoE session in on-demand mode and terminated by this command will be established again only when there is a need for data transmission.

Examples

Reset all PPPoE sessions.

```
<Sysname> reset pppoe-client all
```

Related commands

dialer timer autodial

reset pppoe-client session packet

Use **reset pppoe-client session packet** to reset the protocol packet statistics for a PPPoE session.

Syntax

reset pppoe-client session packet [**dial-bundle-number** *number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

dial-bundle-number *number*: Specifies the dialer bundle number corresponding to a PPPoE session. The value range for the number argument is 0 to 1023. If you do not specify this option, the command resets the protocol packet statistics for all PPPoE sessions.

Examples

Reset the protocol packet statistics for all PPPoE sessions.

```
<Sysname> reset pppoe-client session packet
```

Related commands

display pppoe-client session packet

Contents

Mobile communication modem management commands

The following compatibility matrixes show the support of hardware platforms for mobile communication modem management:

Models	Mobile communication modem management compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	No
NFNX3-HDB680, NFNX3-HDB1080	Yes

Common management commands

controller cellular

Use **controller cellular** to enter cellular interface view.

Syntax

controller cellular *cellular-number*

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

cellular-number: Specifies a cellular interface by its number.

Examples

Enter Cellular 1/0/1 interface view.

```
<Sysname> system-view
[Sysname] controller cellular 1/0/1
[Sysname-Cellular1/0/1]
```

description

Use **description** to configure the description of an interface.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

The description for a cellular interface is in the *interface name* **Interface** format, for example, Cellular 1/0/1 Interface.

Views

Cellular interface view

Predefined user roles

network-admin

context-admin

Parameters

text: Sets an interface description, a case-sensitive string of 1 to 255 characters.

Examples

Set the description to **Cellular-intf** for Cellular 1/0/1.

```
<Sysname> system-view
[Sysname] controller cellular 1/0/1
[Sysname-Cellular1/0/1] description Cellular-intf
```

display cellular

Use **display cellular** to display call connection information for a mobile communication modem.

Syntax

display cellular [*interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

cellular [*interface-number*]: Specifies a cellular interface by its number. If you do not specify a cellular interface, this command displays call connection information for all cellular interfaces with mobile communication modems installed.

Usage guidelines

The command output might vary by modem manufacturers.

Examples

Display the call connection information for the 4G modem (LTE network).

```
<Sysname> display cellular 1/0/1
Cellular1/0/1:
  Hardware Information:
    Model: MC7750
    Manufacturer: Sierra Wireless, Incorporated
```

```
    Modem Firmware Version: SWI9600M_03.05.10.06
    Hardware Version: 10
    International Mobile Equipment Identity (IMEI): 990000560327506
    Modem Status: Online
  Profile Information:
    Profile index: 1
      PDP Type: IPv4
      Header Compression: Off
      Data Compression: Off
      Access Point Name (APN): vzwinternet
  Network Information:
    Current Service Status: Service available
    Current Roaming Status: Roaming
    Current Data Bearer Technology: Unknown
    Network Selection Mode: Manual
    Mobile Country Code (MCC): 460
    Mobile Network Code (MNC): 00
    Location Area Code (LAC): 4318
    Cell ID: 25381
  Radio Information:
    Technology Preference: LTE only
    Technology Selected: LTE
  LTE related info:
    Current RSSI: -79 dBm
    Current RSRQ: -9 dB
    Current RSRP: -106 dBm
    Current SNR: 5 dB
    Tx Power: -3276 dBm
Modem Security Information:
    PIN Verification: Disabled
    PIN Status: Ready
    SIM Status: OK
      ICCID: 89860113811003195000
```

Table 1 Command output

Field	Description
Model	Modem name.
International Mobile Equipment Identity (IMEI)	IMEI serial number of the modem.
Modem Status	Status of the modem: • **Online**—The modem is powered on. • **Offline**—The modem is powered off or in lower power mode. The cellular interface is unavailable.
Profile Information	Profile settings for the modem.
Profile index	Index of the profile for modem.

Field	Description
PDP Type	PDP type, displayed only when Profile 1 is **Active**: • IPv4. • IPv6. • PPP (transparent transmission).
Header Compression	PDP header compression status • On. • Off.
Data Compression	PDP data compression status: • On. • Off.
Current Service Status	Service status of the modem: • **Limited**—The modem is not in the coverage of the selected network. The cellular interface is not available. • **Service available**—The modem is providing services correctly. • **Emergency**—The modem is providing limited services. The cellular interface is not available. • **No service**—The modem cannot provide services. The cellular interface is not available. • **Low power**—The modem is in low power mode. The cellular interface is not available.
Current Roaming Status	Roaming status: • Roaming. • Home.
Current Data Bearer Technology	Current data carrier technology: • CDMA2000 1X. • CDMA2000 HRPD (1xEV-DO). • GSM. • UMTS. • CDMA2000 HRPD (1xEV-DO RevA). • EDGE. • HSDPA and WCDMA. • WCDMA and HSUPA. • HSDPA and HSUPA. • LTE. • CDMA2000 EHRPD. • HSDPA+ and WCDMA. • HSDPA+ and HSUPA. • DC_HSDPA+ and WCDMA. • DC_HSDPA+ and HSUPA. • HSDPA+ and 64QAM. • HSDPA+, 64QAM and HSUPA. • TDSCDMA. • TDSCDMA and HSDPA. • Unknown.
Network Selection Mode	Network selection mode • Manual. • Automatic.

Field	Description
Mobile Country Code (MCC)	The MCC is displayed if the modem has found the network.
Mobile Network Code (MNC)	The MNC is displayed if the modem is successfully registered with a mobile network.
Location Area Code (LAC)	The LAC is displayed if the modem is successfully registered with a mobile network.
Cell ID	The Cell ID is displayed if the modem is successfully registered with a mobile network.
Radio Information	Radio communication information.
Technology Preference	Network connecting preference: • **AUTO**—Connects to a network automatically. • **GSM only**—Connects to a GSM network only. • **GSM precedence**—Connects to a GSM network with preference. • **WCDMA only**—Connects to a WCDMA network only. • **WCDMA precedence**—Connects to a WCDMA network with preference. • **TD-SCDMA only**—Connects to a TD-SCDMA network only. • **TD-SCDMA precedence**—Connects to a TD-SCDMA network with preference. • **EVDO**—Connects to a CDMA-EVDO network only. • **1x RTT**—Connects to a CDMA-1x RTT network only. • **1xRTT/EVDO HYBRID**—Connects to the CDMA-EVDO and CDMA-1x RTT hybrid networks only. • **LTE only**—Connects to an LTE network only.
Technology Selected	Current network: • **GSM**—Has connected to a GSM network. • **WCDMA**—Has connected to a WCDMA network. • **TD-SCDMA**—Has connected to a TD-SCDMA network. • **EVDO**—Has connected to a CDMA-EVDO network. • **1Xrtt**—Has connected to a CDMA-1x RTT network. • **1xRTT/EVDO HYBRID**—Has connected to the CDMA-EVDO and CDMA-1x RTT networks. • **LTE**—Has connected to an LTE network.
LTE related info	Information about the LTE network.
Current RSSI	Current RSSI: • An RSSI value in the range of –110 dBm and –51 dBm. • **Unknown**—No signal. The cellular interface is unavailable.
Current RSRQ	Reference Signal Received Quality.
Current RSRP	Reference Signal Receiving Power.
Current SNR	Signal to noise ratio.
Tx Power	Transmitting power.
Modem Security Information	Information about modem security.

Field	Description
PIN Verification	PIN authentication status: • Disabled. • Enabled. • Unknown.
PIN Status	PIN status: • **Ready**—The SIM card is ready. • **PIN Requirement**—Requires you to execute the **`pin verify`** command to enter the PIN for PIN verification. • **PUK Requirement**—Requires you to execute the **`pin unlock`** command to unlock the SIM or UIM card.
SIM Status	SIM card status: • **OK**—The SIM card is normal. • **Network Reject**—The SIM card is denied access to the network. The cellular interface is not available. • **Not Insert**—The SIM card is absent. The cellular interface is not available. • **Not Initialized**—The SIM card status cannot be identified.
ICCID	ID of the SIM card, displayed only when the SIM card status is **OK**.

Related commands

`mode`

`pin modify`

`pin unlock`

`pin verification enable`

`pin verify`

`plmn select`

`profile create`

display controller cellular

Use **`display controller cellular`** to display information about cellular interfaces.

Syntax

`display controller` [**`cellular`** [*`interface-number`*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

cellular [*interface-number*]: Specifies cellular interfaces or a cellular interface by its number. If you do not specify the **cellular** keyword, this command displays information about all interfaces. If you specify the **cellular** keyword but not the *interface-number* argument, this command displays information about all cellular interfaces.

Usage guidelines

Hot swapping a USB mobile communication modem clears the cellular interface statistics.

Examples

Display information about Cellular 1/0/1.

```
<Sysname> display controller cellular 1/0/1
Cellular1/0/1
Current state: UP
Description: Cellular1/0/1 Interface
Modem status: Present
DM port status: Disabled
Capability:
  1 Control channel, 1 PPP channel
Control channel 0 traffic statistics:
  TX: 0 packets, 0 errors
  RX: 0 packets, 0 errors
PPP channel 0 traffic statistics:
  TX: 0 packets, 0 errors
  RX: 0 packets, 0 errors
```

Table 2 Command output

Field	Description
Cellular1/0/1 Current state	Status of the interface: • **DOWN(Administratively)**—The interface has been administratively shut down by using the **shutdown** command. • **DOWN**—The interface is administratively up but its physical state is down, possibly because of a connection or link failure. • **UP**—The administrative and physical states of the interface are both up.
Description	Description of the interface.
Modem status	Status of the USB mobile communication modem: • **Present**—The modem is present. • **Absent**—The modem is absent.
DM port status	DM status: • Enabled. • Disabled.
Capability: 1 Control channel, 1 PPP channel	Type and number of channels the cellular interface supports: • **1 Control channel**—Supports one control channel. • **1 PPP channel**—Supports one asynchronous serial subchannel. • **1 ETH channel**—Supports one Ethernet subchannel.

Field	Description
Control channel 0 traffic statistics: TX: 0 packets, 0 errors RX: 0 packets, 0 errors	Control channel statistics: • **TX: 0 packets, 0 errors**—Number of packets and number of error packets sent through the control channel. • **RX: 0 packets, 0 errors**—Number of packets and number of error packets received through the control channel.
PPP channel 0 traffic statistics TX: 0 packets, 0 errors RX: 0 packets, 0 errors	PPP channel statistics: • **TX: 0 packets, 0 errors**—Number of packets and number of error packets sent through the PPP channel. • **RX: 0 packets, 0 errors**—Number of packets and number of error packets received through the PPP channel.
ETH channel 0 traffic statistics TX: 0 packets, 0 errors RX: 0 packets, 0 errors	Ethernet channel statistics: • **TX: 0 packets, 0 errors**—Number of packets and number of error packets sent through the Ethernet channel. • **RX: 0 packets, 0 errors**—Number of packets and number of error packets received through the Ethernet channel.

Related commands

reset counters controller cellular

dm-port open

Use **dm-port open** to enable diagnostic and monitoring (DM) on a mobile communication modem.

Use **undo dm-port open** to disable DM on a mobile communication modem.

Syntax

dm-port open

undo dm-port open

Default

The default setting for this command depends on the modem model.

Views

Cellular interface view

Predefined user roles

network-admin

network-admin

context-admin

Usage guidelines

Enabling DM on a mobile communication modem allows third-party debugging tools to diagnose and monitor the mobile communication modem through cellular interface debugging output.

Examples

Enable DM on a mobile communication modem.

```
<Sysname> system-view
[Sysname] controller cellular 1/0/1
[Sysname-Cellular1/0/1] dm-port open
```

mode

Use **mode** to specify network services for a mobile communication modem.

Syntax

mode { **1xrtt** | **auto** | **evdo** | **gsm** | **gsm-precedence** | **hybrid** | **lte** | **td** | **td-precedence** | **wcdma** | **wcdma-precedence** }

Default

The default setting for this command depends on the modem model.

Views

Cellular interface view

Predefined user roles

network-admin

context-admin

Parameters

1xrtt: Connects to a CDMA-1x RTT network only.

auto: Connects to a network automatically.

evdo: Connects to a CDMA-EVDO network only.

gsm: Connects to a GSM network only.

gsm-preference: Connects to a GSM network with preference.

hybrid: Connects to the CDMA-EVDO and CDMA-1xRTT networks only.

lte: Connects to an LTE network only.

td: Connects to a TD-SCDMA network only.

td-preference: Connects to a TD-SCDMA network with preference.

wcdma: Connects to a WCDMA network only.

wcdma-preference: Connects to a WCDMA network with preference.

Usage guidelines

The available parameters depend on the modem model.

Examples

Specify the LTE service for the 4G modem.

```
<Sysname> system-view
[Sysname] controller cellular 1/0/1
[Sysname-Cellular1/0/1] mode lte
```

modem reboot

Use **modem reboot** to reboot a mobile communication modem.

Syntax

modem reboot

Views

Cellular interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

CAUTION:

Execute this command with caution. This command will disconnect the established 3G/4G modem connections.

A mobile communication modem module can automatically detect running errors and reboot. If the mobile communication modem fails to reboot by itself, you can use this command to reboot it.

Examples

Manually reboot the mobile communication modem.

```
<Sysname> system-view
[Sysname] controller cellular 1/0/1
[Sysname-Cellular1/0/1] modem reboot
```

modem response

Use **modem response** to set a mobile communication modem response timer and a consecutive response failure threshold for auto recovery.

Use **undo modem response** to restore the default.

Syntax

modem response timer *time* **auto-recovery** *threshold*

undo modem response

Default

The response timer is 10 seconds and the consecutive response failure threshold is 3.

Views

Cellular interface view

Predefined user roles

network-admin

context-admin

Parameters

timer *time*: Sets the response timer, in the range of 1 to 300, in seconds.

auto-recovery *threshold*: Specifies the consecutive response failure threshold for auto recovery. The value range for the *threshold* argument is 0 to 10. To disable auto recovery, set the value to 0.

Usage guidelines

A mobile communication modem might malfunction in an unstable mobile communication network or when the application environment changes. During a malfunction, the modem cannot respond to the device's requests or configuration commands. If the device does not receive any responses from the mobile communication modem before the timer times out, a response failure occurs. When the number of consecutive response failures reaches the threshold, the device restarts the mobile communication modem automatically. This releases the user from manually rebooting the modem.

The device does not restart the mobile communication modem when the mobile communication modem has not made a successful dialup since the last restart. This restriction avoids repeated restarts of the mobile communication modem when there are configuration errors.

Examples

Set the response timer to 20 seconds and the consecutive response failure threshold for auto recovery to 4.

```
<Sysname> system-view
[Sysname] controller cellular 1/0/1
[Sysname-Cellular1/0/1] modem response timer 20 auto-recovery 4
```

pin modify

Use **pin modify** to modify the PIN of a SIM/UIM card.

Syntax

pin modify *current-pin new-pin*

Views

Cellular interface view

Predefined user roles

network-admin

context-admin

Parameters

current-pin: Specifies the current PIN of the SIM/UIM card, a string of 4 to 8 digits.

new-pin: Specifies the new PIN, a string of 4 to 8 digits.

Usage guidelines

The new PIN is saved on the SIM/UIM card.

If PIN verification is enabled, execute the **pin verify** command to save the new PIN on the device after the PIN is modified.

Failure to modify the PIN in a maximum number of attempts locks the SIM/UIM card. The maximum number of attempts depend on the mobile communication modem model. To unlock the card, execute the **pin unlock** command.

For some mobile communication modems, you can modify their PINs only when the mobile communication modems pass the PIN authentication.

Examples

Modify the PIN of a SIM/UIM card.

```
<Sysname> system-view
[Sysname] controller cellular 1/0/1
[Sysname-Cellular1/0/1] pin modify 1234 4321
PIN will be changed to “4321”. Continue? [Y/N]:y
PIN has been changed successfully.
```

Related commands

pin unlock

pin verification enable

pin verify

pin unlock

Use **pin unlock** to specify the Personal Unlock Code (PUK) to unlock a SIM/UIM card.

Syntax

pin unlock *puk new-pin*

Views

Cellular interface view

Predefined user roles

network-admin

context-admin

Parameters

puk: Specifies the PUK of the SIM/UIM card, a string of 4 to 8 digits. The PUK code of a SIM/UIM card is provided by the network service provider.

new-pin: Specifies the new PIN, a string of 4 to 8 digits.

Usage guidelines

A SIM/UIM card will be locked in the following circumstances:

- Consecutive PIN modification failures.
- Consecutive failures for enabling or disabling PIN authentication.
- Consecutive PIN authentication failures.

If the SIM/UIM card is locked, the modem cannot be used. To unlock the card, you can use the **pin unlock** command. The new PIN is saved on the SIM/UIM card.

If PIN verification is enabled, use the **pin verify** command to save the new PIN on the device after the SIM/UIM card is unlocked.

If you consecutively fail to unlock a card by using the PUK, the card will be locked permanently. To unlock a permanently locked card, contact the service provider of the card.

Examples

Use the PUK to unlock a SIM/UIM card.

```
<Sysname> system-view
[Sysname] controller cellular 1/0/1
[Sysname-Cellular1/0/1] pin unlock 87654321 1234
PIN will be unlocked and changed to “1234”. Continue? [Y/N]:y
PIN has been unlocked and changed successfully.
```

Related commands

pin modify

pin verification enable

pin verification enable

Use **pin verification enable** to enable PIN verification for a mobile communication modem.

Use **undo pin verification enable** to disable PIN verification for a mobile communication modem.

Syntax

pin verification enable [*pin*]

undo pin verification enable [*pin*]

Default

The default setting for this command depends on the modem model.

Views

Cellular interface view

Predefined user roles

network-admin

context-admin

Parameters

pin: Specifies the PIN of the SIM/UIM card, a string of 4 to 8 digits.

Usage guidelines

If PIN verification is enabled, PIN verification is performed after you perform any of the following tasks:

- Install a mobile communication modem.
- Reboot the device.
- Execute the **modem reboot** command to reboot a mobile communication modem.
- Hot swap a USB mobile communication modem.

To perform PIN verification, you also need to execute the **pin verify** command to save the PIN of the SIM/UIM card on the device. After the PIN is saved on the device, the PIN is used for verification automatically when required.

You might be required to provide the current PIN when you enable or disable PIN verification. Consecutive failures for enabling or disabling PIN verification lock a SIM/UIM card. To unlock the card, execute the **pin unlock** command.

For some mobile communication modems, you can disable PIN verification only when the mobile communication modems pass PIN authentication.

Examples

Enable PIN authentication.

```
<Sysname> system-view
[Sysname] controller cellular 1/0/1
[Sysname-Cellular1/0/1] pin verification enable 1234
```

Related commands

pin unlock

pin verify

pin verify

Use **pin verify** to specify the PIN of a SIM/UIM card on a mobile communication modem.

Use **undo pin verify** to restore the default.

Syntax

pin verify { **cipher** | **simple** } *string*

undo pin verify

Default

No PIN is specified for a SIM/UIM card.

Views

Cellular interface view

Predefined user roles

network-admin

context-admin

Parameters

cipher *ciphered-pin*: Specifies a PIN in encrypted form.

simple *pin*: Specifies a PIN in plaintext form. For security purposes, the PIN specified in plaintext form will be stored in encrypted form.

string: Specifies the PIN. Its plaintext form is 4 to 8 digits long. Its encrypted form is a string of 37 to 41 characters.

Usage guidelines

This command saves the PIN of the SIM/UIM card on the device. The PIN is used for verifying the mobile communication modem when PIN verification is performed. You can execute this command before or after you enable PIN verification.

Consecutive PIN verification failures might lock a SIM/UIM card. To unlock the card, execute the **pin unlock** command.

Examples

Specify the plaintext form PIN **1234** for the SIM/UIM card.

```
<Sysname> system-view
[Sysname] controller cellular 1/0/1
[Sysname-Cellular1/0/1] pin verify simple 1234
```

Related commands

pin unlock

pin verification enable

plmn search

Use **plmn search** to search for available mobile networks.

Syntax

plmn search

Views

Cellular interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

Before you use a mobile communication modem to access a mobile network, use the **plmn search** command to search a PLMN for available mobile networks. The search takes a few minutes. After

the search is complete, the CLI displays the available mobile networks. Some mobile communication modems automatically access an available network. You can also specify a mobile network for the mobile communication modem from the available mobile networks.

Examples

Search for mobile networks on Cellular 1/0/1.

```
<Sysname> system-view
[Sysname] controller cellular 1/0/1
[Sysname-Cellular1/0/1] plmn search
PLMN search done.
Available PLMNs:
PLMN No.     MCC    MNC    Status     Type
01           460    00     Current    GSM
02           460    00     Available  UTRAN
03           460    01     Forbidden  GSM
```

Table 3 Command output

Field	Description
PLMN No	PLMN number.
MCC	Mobile Country Code.
MNC	Mobile Network Code: • **00, 02, and 07**—China Mobile. • **01**—China Unicom. • **03**—China Telecom.
Status	Status of the mobile network: • Current. • Available. • Forbidden.
Type	Type of the mobile network.

Related commands

display cellular

plmn select

plmn select

Use **plmn select** to configure the mobile network selection mode.

Syntax

plmn select { **auto** | **manual** *mcc mnc* }

Default

The default setting for this command depends on the modem model.

Views

Cellular interface view

Predefined user roles

network-admin

context-admin

Parameters

auto: Specifies the auto selection mode. The modem automatically selects a mobile network.

manual: Specifies the manual selection mode.

mcc: Specifies the mobile country code (MCC) in the range of 0 to 65535.

mnc: Specifies the mobile network code (MNC) in the range of 0 to 65535.

Usage guidelines

For manual selection, you can first use the **plmn search** command to obtain the MCC and MNC of a mobile network.

Examples

Manually specify a mobile network.

```
<Sysname> system-view
[Sysname] controller cellular 1/0/1
[Sysname-Cellular1/0/1] plmn select manual 65524 65524
```

Related commands

display cellular

plmn search

reset counters controller cellular

Use **reset counters controller cellular** to clear statistics on cellular interfaces.

Syntax

reset counters controller cellular [*interface-number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

cellular [*interface-number*]: Specifies cellular interfaces or a cellular interface by its number. If you do not specify the *interface-number* argument, this command clears statistics on all cellular interfaces. If you specify the *interface-number* argument, this command clears statistics on the specified cellular interface.

Usage guidelines

To collect traffic statistics on an interface during a period of time, first use the **reset counters controller cellular** command to clear the existing statistics on the interface.

Examples

Clear statistics on Cellular 1/0/1.

```
<Sysname> reset counters controller cellular 1/0/1
```

Related commands

display controller cellular

rssi

Use **rssi** to set the RSSI thresholds for a mobile communication modem.

Use **undo rssi** to restore the default.

Syntax

rssi { **1xrtt** | **evdo** | **gsm** | **lte** } { **low** *lowthreshold* | **medium** *mediumthreshold* } *

undo rssi { **1xrtt** | **evdo** | **gsm** | **lte** } [**low** | **medium**]

Default

The lower and upper RSSI thresholds for a mobile communication modem are –150 dBm and 0 dBm, respectively.

Views

Cellular interface view

Predefined user roles

network-admin

context-admin

Parameters

1xrtt: Specifies the 1xRTT mode.

evdo: Specifies the EVDO mode.

gsm: Specifies the GSM mode.

lte: Specifies the LTE mode.

low *lowthreshold*: Specifies the lower RSSI threshold value in the range of 0 to 150, which represents a lower RSSI threshold in the range of –150 dBm to 0 dBm. The value of *lowthreshold* cannot be smaller than the value of mediumthreshold because the system automatically adds a negative sign to the RSSI thresholds.

medium *mediumthreshold*: Specifies the upper RSSI threshold value in the range of 0 to 150, which represents an upper RSSI threshold in the range of –150 dBm to 0 dBm.

Usage guidelines

The device performs the following operations based on the actual RSSI of the mobile communication modem:

- Sends a trap that indicates high RSSI when the RSSI exceeds the upper threshold.
- Sends a trap that indicates normal RSSI when the RSSI is between the lower threshold and upper threshold (included).
- Sends a trap that indicates low RSSI when the RSSI drops to or below the lower threshold.
- Sends a trap that indicates low RSSI every 10 minutes when the RSSI remains equal to or smaller than the lower threshold.

To view the RSSI change information for a mobile communication modem, use the **display cellular** command.

Examples

Set the lower threshold for a mobile communication modem in GSM mode to –110 dBm.

```
<Sysname> system-view
[Sysname] controller cellular 1/0/1
```

```
[Sysname-Cellular1/0/1] rssi gsm low 110
```

sendat

Use **sendat** to issue a configuration directive to a mobile communication modem.

Syntax

sendat *at-string*

Views

Cellular interface view

Predefined user roles

network-admin

context-admin

Parameters

at-string: Specifies a configuration directive string, a string of 1 to 300 characters. This argument can be an AT directive (containing **+++**, **A/**, or be any string beginning with **AT**) or a CNS directive. For more information about AT directives, see the **sendat** command in *Layer 2—WAN Access Command Reference*. Table 4 describes the CNS directive samples.

Table 4 CNS directive description

Directive	Description
CNS*n*	Controls the CNS heartbeat debugging switch. • **n = 00000500000000000000**—Enables CNS heartbeat debugging. • **n = 00000800000000000000**—Disables CNS heartbeat debugging.

Usage guidelines

The **sendat** command does not verify the configuration directive. Each time it issues one configuration directive to the mobile communication modem, lowercase characters are automatically converted to uppercase characters.

One **sendat** command issues one configuration directive. To issue multiple configuration directives to a modem, you must repeat the **sendat** command.

Configuration directives might cause malfunction of a mobile communication modem. When you issue a configuration directive to the modem, make sure you understand the impact on the mobile communication modem.

Examples

Issue the **ATD169** directive to the mobile communication modem to call number 169.

```
<Sysname> system-view
[Sysname] controller cellular 1/0/1
[Sysname-Cellular1/0/1] sendat ATD169
```

Issue the **cns00000500000000000000** directive to the mobile communication modem to enable CNS heartbeat debugging.

```
<Sysname> system-view
[Sysname] controller cellular 1/0/1
[Sysname-Cellular1/0/1] sendat cns00000500000000000000
```

shutdown

Use **shutdown** to shut down a cellular interface.

Use **undo shutdown** to bring up a cellular interface.

Syntax

shutdown

undo shutdown

Default

The cellular interface is up.

Views

Cellular interface view

Predefined user roles

network-admin

context-admin

Examples

Shut down Cellular 1/0/1.

```
<Sysname> system-view
[Sysname] interface cellular 1/0/1
[Sysname-Cellular1/0/1] shutdown
```

3G modem-specific management commands

gsm band

Use **gsm band** to specify a GSM frequency band.

Use **undo gsm band** to restore the default.

Syntax

gsm band { **egsm900** | **gsm450** | **gsm480** | **gsm750** | **gsm850** | **gsm1800** | **gsm1900** | **pgsm900** | **rsgm900** }

undo gsm band

Default

No GSM band is specified.

Views

Cellular interface view

Predefined user roles

network-admin

context-admin

Parameters

egsm900: Specifies the E-GSM 900 MHz band.

gsm450: Specifies the GSM 450 MHz band.

gsm480: Specifies the GSM 480 MHz band

gsm750: Specifies the GSM 750 MHz band.

gsm850: Specifies the GSM 850 MHz band.

gsm1800: Specifies the GSM 1800 MHz band.

gsm1900: Specifies the GSM 1900 MHz band.

pgsm900: Specifies the P-GSM 900 MHz band.

rgsm900: Specifies the GSM-R 900 MHz band.

Usage guidelines

This command is supported only by Sierra MC7354 (ATT version) and MC7304 4G modules.

Multiple frequency bands are available for accessing the GSM network. When the network environment changes, the 3G/4G modem might change the working band automatically to adapt to the change. To avoid link instability caused by frequency changes, you can specify a GSM band for the 3G/4G modem.

Examples

Specify the GSM 1800 MHz band for the 3G/4G modem.

```
<Sysname> system-view
[Sysname] controller cellular 1/0/1
[Sysname-Cellular1/0/1] gsm band gsm1800
```

Related commands

lte band

wcdma band

profile create

Use **profile create** to create a profile for the 3G modem.

Syntax

profile create *profile-number* { **dynamic** | **static** *apn* } **authentication-mode** { **none** | { **chap** | **pap** } **user** *username* [**password** *password*] }

Default

The default setting for this command depends on the modem model.

Views

Cellular interface view

Predefined user roles

network-admin

context-admin

Parameters

profile-number: Specifies a profile number. The value range varies by the modem model.

dynamic: Uses an access point automatically assigned by the service provider.

static *apn*: Specifies the access point provided by the service provider. It is a string of 1 to 100 characters. Whether the string is case-sensitive varies by service providers.

authentication-mode: Specifies the authentication mode, which can be **none**, **pap**, or **chap**.

none: Performs no authentication.

chap: Specifies CHAP authentication.

pap: Specifies PAP authentication.

user *username*: Specifies the username provided by the service provider. It is a case-sensitive string of 1 to 32 characters.

password *password*: Specifies the authentication password provided by the service provider. It is a case-sensitive string of 1 to 32 characters.

Usage guidelines

If you specify **chap** or **pap,** make sure the authentication settings are identical to those assigned by the service provider.

Examples

Create a profile for Cellular 1/0/1. Specify the profile number as 1 and the access point name as **cmnet**, and specify the PAP authentication mode.

```
<Sysname> system-view
[Sysname] controller cellular 1/0/1
[Sysname-Cellular1/0/1] profile create 1 static cmnet authentication-mode pap user abc password abc
```

Related commands

display cellular

profile delete

profile delete

Use **profile delete** to delete a profile for the 3G modem.

Syntax

profile delete *profile-number*

Views

Cellular interface view

Predefined user roles

network-admin

context-admin

Parameters

profile-number: Specifies a profile by its number. The value range varies by the modem model.

Examples

Delete profile 1 for Cellular 1/0/1.

```
<Sysname> system-view
[Sysname] controller cellular 1/0/1
[Sysname-Cellular1/0/1] profile delete 1
```

Related commands

display cellular

profile create

profile main

Use **profile main** to specify the primary and backup profiles for 3G modem dialup.

Use **undo profile main** to restore the default.

Syntax

profile main *profile-M-number* **backup** *profile-B-number*

undo profile main

Default

Profile 1 is used for 3G modem dialup.

Views

Cellular interface view

Predefined user roles

network-admin

context-admin

Parameters

main *profile-M-number*: Specifies the primary profile by its number. The value range varies by the modem model.

backup *profile-B-number*: Specifies the backup profile by its number. The value range varies by the modem model.

Usage guidelines

The primary profile always has priority over the backup profile. For each dialup connection establishment, the 3G modem uses the backup profile only when it has failed to dial up using the primary profile.

You must configure the same user name and password for the primary and backup profiles.

This command takes effect only on dialup connections initiated after the command is configured. It does not take effect on a dialup connection that has been established.

Examples

Specify the profiles numbered **1** and **2** as the primary and backup profiles, respectively.

```
<sysname>system-view
[sysname]interface cellular 1/0/1
[sysname-Cellular1/0/1]profile main 1 backup 2
```

wcdma band

Use **wcdma band** to specify a WCDMA band.

Use **undo wcdma band** to restore the default.

Syntax

wcdma band { **wcdma800** | **wcdma850** | **wcdma900** | **wcdma1700ip** | **wcdma1700us** | **wcdma1800** | **wcdma1900** | **wcdma2100** | **wcdma2600** }

undo wcdma band

Default

No WCDMA band is specified.

Views

Cellular interface view

Predefined user roles

network-admin

context-admin

Parameters

wcdma800: Specifies the WCDMA 800 MHz band.

wcdma850: Specifies the WCDMA 850 MHz band.

wcdma900: Specifies the WCDMA 900 MHz band.

wcdma1700jp: Specifies the Japan WCDMA 1700 MHz band.

wcdma1700us: Specifies the US WCDMA 1700 MHz band.

wcdma1800: Specifies the WCDMA 1800 MHz band.

wcdma1900: Specifies the WCDMA 1900 MHz band.

wcdma2100: Specifies the WCDMA 2100 MHz band.

wcdma2600: Specifies the WCDMA 2600 MHz band.

Usage guidelines

This command is supported only by Sierra MC7354 (ATT version) and MC7304 4G modules.

Multiple frequency bands are available for accessing the WCDMA network. When the network environment changes, the 3G/4G modem might change the working band automatically to adapt to the change. To avoid link instability caused by frequency changes, you can specify a WCDMA band for the 3G/4G modem.

Examples

Specify the WCDMA 1700 MHz band for the 3G/4G modem.

```
<Sysname> system-view
[Sysname] controller cellular 1/0/1
[Sysname-Cellular1/0/1] wcdma band wcdma1700
```

Related commands

gsm band

lte band

4G modem-specific management commands

apn

Use **apn** to specify an access point name (APN) for a 4G modem.

Use **undo apn** to remove an APN.

Syntax

apn { **dynamic** | **static** *apn* }

undo apn

Default

No APN is specified for a 4G modem.

Views

4G modem profile view

Predefined user roles

network-admin

context-admin

Parameters

dynamic: Uses an APN automatically assigned by the service provider.

static *apn*: Specifies the APN provided by the service provider. The *apn* argument is a string of 1 to 100 characters. Whether the string is case-sensitive depends on the service provider.

Examples

Specify APN **apn1** for 4G modem profile **test**.

```
<Sysname> system-view
[Sysname] apn-profile test
[Sysname-apn-profile-test] apn static apn1
```

Related commands

apn-profile

apn-profile

Use **apn-profile** to create a 4G modem profile.

Use **undo apn-profile** to remove a 4G modem profile.

Syntax

apn-profile *profile-name*

undo apn-profile *profile-name*

Default

No 4G modem profile exists.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

profile-name: Specifies a 4G modem profile name.

Usage guidelines

A 4G modem profile takes effect only after you apply the profile to a 4G interface. To remove a 4G modem profile, you must first remove the association between the profile and the 4G interface.

Examples

Create 4G modem profile **test**.

```
<Sysname> system-view
[Sysname] apn-profile test
```

Related commands

apn-profile apply

apn-profile apply

Use **apn-profile apply** to specify 4G modem profiles for an interface.

Use **undo apn-profile apply** to restore the default.

Syntax

apn-profile apply *profile-name* [**backup** *profile-name*]

undo apn-profile apply

Default

No 4G modem profiles are specified for an interface.

Views

Eth-channel interface view

Predefined user roles

network-admin

context-admin

Parameters

profile-name: Specifies a primary 4G modem profile name.

backup *profile-name*: Specifies a backup 4G modem profile name.

Usage guidelines

After you specify a 4G modem profile, the 4G modem uses the settings in the profile to negotiate with the service provider's device.

A primary profile always takes precedence over a backup profile. For each dialup connection establishment, the 4G modem uses the backup profile only when it has failed to dial up using the primary profile.

This command takes effect only on dialup connections initiated after the command is configured. It does not take effect on a dialup connection that has been established.

Examples

Specify primary 4G modem profile **test** and backup 4G modem profile **bktest** for Eth-channel 1/0/1:0.

```
<Sysname> system-view
[Sysname] interface eth-channel 1/0/1:0
[Sysname-Eth-channel1/0/1:0] apn-profile apply test backup bktest
```

Related commands

apn-profile

attach-format imsi-sn split

Use **attach-format imsi-sn split** to specify a delimiter for the IMSI/SN binding authentication information.

Use **undo attach-format imsi-sn split** to restore the default.

Syntax

attach-format imsi-sn split *splitchart*

undo attach-format imsi-sn split

Default

No delimiter is specified for the IMSI/SN binding authentication information.

Views

4G modem profile view

Predefined user roles

network-admin

context-admin

Parameters

split *splitchart*: Specifies a delimiter. It can be a letter, a digit, or a sign such as a percent sign (%) or a pound sign (#).

Usage guidelines

If IMSI/SN binding authentication is enabled, the IMSI/SN information is included in the authentication information in addition to the username. You need to configure a delimiter to separate different types of information. For example, if you specify the delimiter as #, the authentication information will be sent in the imsiinfo#sninfo#username format.

Examples

Configure the pound sign (#) as the delimiter for the IMSI/SN binding authentication information.

```
<Sysname> system-view
[Sysname] apn-profile test
[Sysname-apn-profile-test] attach-format imsi-sn split #
```

Related commands

apn-profile

authentication-mode

Use **authentication-mode** to specify an authentication mode for accessing a 4G network.

Use **undo authentication-mode** to restore the default.

Syntax

authentication-mode { **pap** | **chap**| **pap-chap** } **user** *user-name* **password** { **cipher** | **simple** } *string*

undo authentication-mode

Default

No authentication mode is specified for accessing a 4G network.

Views

4G modem profile view

Predefined user roles

network-admin

context-admin

Parameters

chap: Specifies CHAP authentication.

pap: Specifies PAP authentication.

pap-chap: Specifies CHAP or PAP authentication.

user *username*: Specifies the username for authentication, a case-sensitive string of 1 to 32 characters.

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 32 characters. Its encrypted form is a case-sensitive string of 1 to 73 characters.

Examples

Specify the CHAP authentication mode for 4G modem profile **test**. Specify the username as **user1** and the password as **123456**.

```
<Sysname> system-view
[Sysname] apn-profile test
[Sysname-apn-profile-test] authentication-mode chap user user1 password simple 123456
```

Related commands

apn-profile

bandwidth

Use **bandwidth** to configure the expected bandwidth for an Eth-channel interface.

Use **undo bandwidth** to restore the default.

Syntax

bandwidth *bandwidth-value*

undo bandwidth

Default

The expected bandwidth (in kbps) is the interface baud rate divided by 1000.

Views

Eth-channel interface view

Predefined user roles

network-admin

context-admin

Parameters

bandwidth-value: Specifies the expected bandwidth in the range of 1 to 400000000 kbps.

Usage guidelines

The expected bandwidth for an interface affects the link costs in OSPF, OSPFv3, and IS-IS. For more information, see *Layer 3—IP Routing Configuration Guide*.

Examples

Set the expected bandwidth for Eth-channel 1/0/1:0 to 1000 kbps.

```
<Sysname> system-view
[Sysname] interface eth-channel 1/0/1:0
[Sysname-Eth-channel1/0/1:0] bandwidth 1000
```

default

Use **default** to restore the default settings for an interface.

Syntax

default

Views

Eth-channel interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

CAUTION:

The **default** command might interrupt ongoing network services. Make sure you are fully aware of the impact of this command before using it on a live network.

This command might fail to restore the default settings for some commands for reasons such as command dependencies and system restrictions. Use the **display this** command in interface view to identify these commands. Then, use their **undo** forms or follow the command reference to individually restore their default settings. If your restoration attempt fails, follow the error message instructions to resolve the problem.

Examples

Restore the default settings for Eth-channel 1/0/1:0.

```
<Sysname> system-view
[Sysname] interface eth-channel 1/0/1:0
[Sysname-Eth-channel1/0/1:0] default
```

description

Use **description** to configure the description of an interface.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

The description for an interface is in the *interface name* Interface format, for example, Echannel1/0/1:0 Interface.

Views

Eth-channel interface view

Predefined user roles

network-admin

context-admin

Parameters

text: Sets an interface description, a case-sensitive string of 1 to 255 characters.

Usage guidelines

Configure the description of an interface for easy identification and management purposes.

You can use the **display interface** command to view the description for an interface.

Examples

Configure the description for Eth-channel 1/0/1:0 as **Echannel-interface**.

```
<Sysname> system-view
[Sysname] interface eth-channel 1/0/1:0
[Sysname-Eth-channel1/0/1:0] description Echannel-interface
```

display interface eth-channel

Use **display interface eth-channel** to display information about the specified or all Eth-channel interfaces.

Syntax

display interface [**eth-channel** [*channel-id*]] [**brief** [**description** | **down**]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

eth-channel [*channel-id*]: Specifies Eth-channel interfaces or an Eth-channel interface by its number. If you do not specify the **eth-channel** keyword, the command displays information about all interfaces. If you specify the **eth-channel** keyword but not the *channel-id* argument, this command displays information about all Eth-channel interfaces.

brief: Displays brief interface information. If you do not specify this keyword, the command displays detailed interface information.

description: Displays complete interface descriptions. If you do not specify this keyword, the command displays only the first 27 characters of interface descriptions.

down: Displays information about interfaces in down state and the causes. If you do not specify this keyword, the command displays information about interfaces in all states.

Examples

Display detailed information about Eth-channel 1/0/1:0, including its operating status.

```
<Sysname> display interface eth-channel 1/0/1:0
Echannel1/0/1:0
Current state: DOWN
Line protocol state: DOWN
Description: Echannel1/0/1:0 Interface
Bandwidth: 100000kbps
Maximum Transmit Unit: 1500
Internet protocol processing: disabled
IP Packet Frame Type:PKTFMT_ETHNT_2, Hardware Address: 000c-2963-b75d
IPv6 Packet Frame Type:PKTFMT_ETHNT_2, Hardware Address: 000c-2963-b75d
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last link flapping: Never
Last clearing of counters: Never
Last 300 seconds input rate 0.00 bytes/sec, 0.00 packets/sec
Last 300 seconds output rate 0.00 bytes/sec, 0.00 packets/sec
Input: 0 packets, 0 bytes, 0 buffers
Output:0 packets, 0 bytes
```

Display brief information about Eth-channel 1/0/1:0.

```
<Sysname> display interface eth-channel 1/0/1:0 brief
Brief information on interface(s) under route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Main IP         Description
Echannel1/0/1:0      UP   UP(s)    192.168.80.239
```

Display information about all Eth-channel interfaces in down state and the causes.

```
<Sysname> display interface eth-channel brief down
Brief information on interface(s) under route mode:
Link: ADM - administratively down; Stby - standby
Interface            Link Cause
Echannel1/0/1:0      ADM  Administratively
```

Table 5 Command output

Field	Description
Current state	Physical link state of the interface: • **Administratively DOWN**—The interface has been shut down by using the **shutdown** command. • **DOWN**—The interface is administratively up, but its physical state is down (possibly because no physical link exists or the link has failed). • **UP**—The interface is both administratively and physically up.

Field	Description
Line protocol state	Data link layer state of the interface. The state is determined through automatic parameter negotiation at the data link layer. • **UP**—The data link layer protocol is up. • **UP (spoofing)**—The data link layer protocol is up, but the link is an on-demand link or does not exist. This attribute is typical of null interfaces and loopback interfaces. • **DOWN**—The data link layer protocol is down.
Description	Description for the interface.
Bandwidth	Expected bandwidth of the interface.
Maximum Transmit Unit	MTU of the interface.
Internet address: *ip-address*/*mask-length* (*Type*)	IP address of the interface and type of the address in parentheses. Possible IP address types include: • **Primary**—Manually configured primary IP address. • **Sub**—Manually configured secondary IP address. If the interface has both primary and secondary IP addresses, the primary IP address is displayed. If the interface has only secondary IP addresses, the lowest secondary IP address is displayed. • **DHCP-allocated**—DHCP allocated IP address. For more information, see DHCP client configuration in *Layer 3—IP Services Configuration Guide*. • **BOOTP-allocated**—BOOTP allocated IP address. For more information, see BOOTP client configuration in *Layer 3—IP Services Configuration Guide*. • **PPP-negotiated**—IP address assigned by a PPP server during PPP negotiation. For more information, see PPP configuration in *Layer 2—WAN Access Configuration Guide*. • **Unnumbered**—IP address borrowed from another interface. • **Cellular-allocated**—IP address allocated through the modem-manufacturer's proprietary protocol. For more information, see mobile communication modem management in *Layer 2—WAN Access Configuration Guide*. • **MAD**—IP address assigned to an IRF member device for MAD on the interface. For more information, see IRF configuration in *Virtual Technologies Configuration Guide*.
Internet protocol processing: disabled	The interface is not assigned an IP address and cannot process IP packets.
Internet Address is 192.168.1.200/24 Primary	IP address of the interface. The **primary** attribute indicates that the address is the primary IP address..
IP Packet Frame Type	IPv4 packet framing format.
Hardware Address	MAC address of the interface.
IPv6 Packet Frame Type	IPv6 packet framing format.
Output queue - Urgent queuing: Size/Length/Discards	Packet statistics for urgent queuing in the output queue of the interface: • **Size**—Current number of packets in the queue. • **Length**—Maximum number of packets that can stay in the queue. • **Discards**—Number of dropped packets.

Field	Description
Output queue - Protocol queuing: Size/Length/Discards	Packet statistics for protocol queuing in the output queue of the interface: • **Size**—Current number of packets in the queue. • **Length**—Maximum number of packets that can stay in the queue. • **Discards**—Number of dropped packets.
Output queue - FIFO queuing: Size/Length/Discards	Packet statistics for FIFO queuing in the output queue of the interface: • **Size**—Current number of packets in the queue. • **Length**—Maximum number of packets that can stay in the queue. • **Discards**—Number of dropped packets.
Last link flapping	The amount of time that has elapsed since the most recent physical state change of the interface. This field displays **Never** if the interface has been physically down since device startup.
Last clearing of counters	Time when statistics on the logical interface were last cleared by using the **reset counters interface** command. If the statistics of the interface have never been cleared by using the **reset counters interface** command since the device started, this field displays **Never**.
Last 300 seconds input rate	Average input rate during the last 300 seconds: • **bytes/sec**—Average number of received bytes per second. • **bits/sec**—Average number of received bits per second. • **packets/sec**—Average number of received packets per second.
Last 300 seconds output rate	Average output rate over the last 300 seconds: • **bytes/sec**—Average number of sent bytes per second. • **bits/sec**—Average number of sent bits per second. • **packets/sec**—Average number of sent packets per second.
Input: 0 packets, 0 bytes, 0 buffers	Incoming packet statistics: • **0 packets**—Packet number. • **0 bytes**—Packet size in bytes. • **0 buffers**—Number of buffered units.
Output: 0 packets, 0 bytes	Outgoing packet statistics: • **0 packets**—Packet number. • **0 bytes**—Packet size in bytes.
Link	Physical link state of the interface: • **UP**—The interface is physically up. • **DOWN**—The interface is physically down. • **ADM**—The interface has been shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command. • **Stby**—The interface is a backup interface in standby state. To see the primary interface, use the **display interface-backup state** command.

Field	Description
Protocol	Data link layer protocol state of the interface: • **UP**—The data link layer protocol of the interface is up. • **DOWN**—The data link layer protocol of the interface is down. • **UP(s)**—The data link layer protocol of the interface is up, but the link is an on-demand link or does not exist. The **(s)** attribute represents the spoofing flag. This value is typical of null interfaces and loopback interfaces.
Main IP	Main IP address of the interface.
Description	Description of the interface.
Cause	Cause for the physical link state of the interface to be **DOWN**. The value of the field varies by device model. **Administratively** represents that the interface has been manually shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command.

eth-channel

Use **eth-channel** to channelize a cellular interface into an Eth-channel interface.

Use **undo eth-channel** to remove the Eth-channel interface channelized from a cellular interface.

Syntax

eth-channel *channel-number*

undo eth-channel *channel-number*

Views

Cellular interface view

Predefined user roles

network-admin

context-admin

Parameters

channel-number: Specifies an Eth-channel interface by its number. The value range for this argument varies by device model.

Usage guidelines

This command names the Eth-channel interface channelized from a cellular interface as **eth-channel** *cellular-number*:*channel-number*.

Examples

Channelize Cellular 1/0/1 into an Eth-channel interface.

```
<Sysname> system-view
[Sysname] controller cellular 1/0/1
[Sysname-Cellular1/0/1] eth-channel 0
```

interface eth-channel

Use **interface eth-channel** to enter Eth-channel interface view.

Syntax

interface eth-channel *interface-number*

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interface-number: Specifies an Eth-channel interface by its number.

Examples

Enter Eth-channel 1/0/1:0 interface view.

```
<Sysname> system-view
[Sysname] interface eth-channel 1/0/1:0
[Sysname-Eth-channel1/0/1:0]
```

ip address cellular-alloc

Use **ip address cellular-alloc** to enable an Eth-channel interface to obtain an IP address by using the modem-manufacturer's proprietary protocol.

Use **undo ip address cellular-alloc** to restore the default.

Syntax

ip address cellular-alloc

undo ip address cellular-alloc

Default

An Eth-channel interface does not obtain an IP address by using the modem-manufacturer's proprietary protocol.

Views

Eth-channel interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

To enable an interface to obtain an IP address from the modem by using the modem-manufacturer's proprietary protocol, use the **ip address cellular-alloc** command.

To enable an interface to obtain an IP address from the modem by using DHCP, use the **ip address dhcp-alloc** command.

The IP address of the modem is automatically allocated by the service provider.

Examples

Channelize Cellular 1/0/1 into an Eth-channel interface. Enable the Eth-channel interface to obtain an IP address by using the modem-manufacturer's proprietary protocol.

```
<Sysname> system-view
[Sysname] controller cellular 1/0/1
[Sysname-Cellular1/0/1] eth-channel 0
[Sysname-Cellular1/0/1] quit
[Sysname] interface eth-channel 1/0/1:0
[Sysname-Eth-channel1/0/1:0] ip address cellular-alloc
```

ipv6 address cellular-alloc

Use **ipv6 address cellular-alloc** to enable an interface to obtain an IPv6 address by using the modem-manufacturer's proprietary protocol.

Use **undo ipv6 address cellular-alloc** to restore the default.

Syntax

ipv6 address cellular-alloc

undo ipv6 address cellular-alloc

Default

An interface does not obtain an IPv6 address by using the modem-manufacturer's proprietary protocol.

Views

Eth-channel interface view

Predefined user roles

network-admin

Usage guidelines

To enable an interface to obtain an IPv6 address by using the modem-manufacturer's proprietary protocol, use the **ipv6 address cellular-alloc** command.

To enable an interface to obtain an IP address by using DHCP, use the **ipv6 address dhcp-alloc** command.

The IPv6 address of the modem is automatically allocated by the service provider.

Examples

Channelize Cellular 1/0/1 into an Eth-channel interface. Enable the Eth-channel interface to obtain an IPv6 address by using the modem-manufacturer's proprietary protocol.

```
<Sysname> system-view
[Sysname] controller cellular 1/0/1
[Sysname-Cellular1/0/1] eth-channel 0
[Sysname-Cellular1/0/1] quit
[Sysname] interface eth-channel 1/0/1:0
[Sysname-Eth-channel1/0/1:0] ipv6 address cellular-alloc
```

Related commands

ip address cellular-alloc

lte band

Use **lte band** to specify a band for a 4G module.

Use **undo lte band** to restore the default.

Syntax

lte band *band-number*

undo lte band

Default

The default setting for this command varies by 4G modem model.

Views

Cellular interface view

Predefined user roles

network-admin

context-admin

Parameters

band-number: Specifies an LTE band for a 4G module. The available bands vary by module model.

Usage guidelines

This command is supported by the following 4G modules:

- Sierra MC7354 and MC7304.
- Long Sung U8300C, U8300W, and U8300.
- WNC DM11-2.

Examples

Specify band 3 for Cellular 1/0/1.

```
<Sysname> system-view
[Sysname] controller cellular 1/0/1
[Sysname-Controller-Cellular1/0/1] lte band 3
```

mtu

Use **mtu** to set the maximum transmission unit (MTU) for an interface.

Use **undo mtu** to restore the default.

Syntax

mtu *size*

undo mtu

Default

The MTU of an interface is 1500 bytes.

Views

Eth-channel interface view

Predefined user roles

network-admin

context-admin

Parameters

size: Sets the MTU in bytes. The value range for this argument varies by device model.

Examples

Set the MTU for Eth-channel 1/0/1:0 to 1430 bytes.

```
<Sysname> system-view
[Sysname] interface eth-channel 1/0/1:0
[Sysname-Eth-channel1/0/1:0] mtu 1430
```

pdp-type

Use **pdp-type** to specify the PDP data carrying protocol.

Use **undo pdp-type** to restore the default.

Syntax

pdp-type { **ipv4** | **ipv6** | **ipv4v6** }

undo pdp-type

Default

The PDP data carrying protocol is IPv4 and IPv6.

Views

Apn-profile view

Predefined user roles

network-admin

Parameters

ipv4: Specifies the IPv4 protocol.

ipv6: Specifies the IPv6 protocol.

ipv4v6: Specifies the IPv4 and IPv6 protocols.

Examples

Specify the PDP data carrying protocol as IPv4.

```
<Sysname> system-view
[Sysname] apn-profile 1
[Sysname-apn-profile-1] pdp-type ipv4
```

reset counters interface

Use **reset counters interface** to clear the statistics on the specified or all Eth-channel interfaces.

Syntax

reset counters interface [**eth-channel** [*channel-id*]]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

eth-channel [*channel-id*]: Specifies Eth-channel interfaces or an Eth-channel interface by its number. If you do not the **eth-channel** keyword, the command clears statistics on all interfaces. If you specify the **eth-channel** keyword but not the *channel-id* argument, this command clears statistics on all Eth-channel interfaces. If you specify both the **eth-channel** keyword and the *channel-id* argument, this command clears statistics on the specified Eth-channel interface.

Usage guidelines

Use this command to clear history statistics if you want to collect traffic statistics for a specific period.

Examples

Clear the statistics on Eth-channel 1/0/1:0.

```
<Sysname> reset counters interface eth-channel 1/0/1:0
```

shutdown

Use **shutdown** to shut down an Eth-channel interface.

Use **undo shutdown** to bring up an Eth-channel interface.

Syntax

shutdown

undo shutdown

Default

The default setting for this command depends on the device model.

Views

Eth-channel interface view

Predefined user roles

network-admin

context-admin

Examples

Shut down Eth-channel 1/0/1:0.

```
<Sysname> system-view
[Sysname] interface eth-channel 1/0/1:0
[Sysname-Eth-channel1/0/1:0] shutdown
```

NSFOCUS Firewall Series

NF Layer 3—IP Services Command Reference

NSFOCUS Technologies, Inc.

Document version: 6W600-20230221

Preface

This command reference describes the commands for configuring IP services features, including ARP, IP addressing, DHCP, DNS, IP forwarding basics, fast forwarding, adjacency table, IP performance optimization, IPv6 basics, DHCPv6, IPv6 fast forwarding, and multi-CPU packet distribution.

This preface includes the following topics about the documentation:

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators.

Conventions

The following information describes the conventions used in the documentation.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select a minimum of one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
CAUTION:	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Contents

IP addressing commands

display ip interface

Use **display ip interface** to display IP configuration and statistics for Layer 3 interfaces.

Syntax

display ip interface [*interface-type* [*interface-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface-type: Specifies an interface by its type.

interface-number: Specifies an interface by its number.

Usage guidelines

Use the **display ip interface** command to display IP configuration and statistics for the specified Layer 3 interface. The statistics include the following information:

- The number of unicast packets, bytes, and multicast packets the interface has sent and received.
- The number of TTL-invalid packets and ICMP packets the interface has received.

The packet statistics helps you locate a possible attack on the network.

If you specify only the interface type, this command displays IP configuration and statistics for all interfaces of this interface type. If you do not specify any optional parameters, this command displays IP configuration and statistics for all Layer 3 interfaces except VA interfaces. For more information about VA interfaces, see PPP configuration in *PPP and PPPoE Configuration Guide*.

Examples

Display IP configuration and statistics for GigabitEthernet 1/0/1.

```
<Sysname> display ip interface gigabitethernet 1/0/1
GigabitEthernet1/0/1 current state : DOWN
Line protocol current state : DOWN
Internet address is 1.1.1.1/8 Primary
Broadcast address : 1.255.255.255
The Maximum Transmit Unit : 1500 bytes
input packets : 0, bytes : 0, multicasts : 0
output packets : 0, bytes : 0, multicasts : 0
TTL invalid packet number:         0
ICMP packet input number:          0
  Echo reply:                      0
  Unreachable:                     0
```

```
Source quench:                  0
Routing redirect:               0
Echo request:                   0
Router advert:                  0
Router solicit:                 0
Time exceed:                    0
IP header bad:                  0
Timestamp request:              0
Timestamp reply:                0
Information request:            0
Information reply:              0
Netmask request:                0
Netmask reply:                  0
Unknown type:                   0
```

Table 1 Command output

Field	Description
current state	Physical link state of the interface: • **Administrative DOWN**—The interface has been shut down by using the **shutdown** command. • **DOWN**—The interface is administratively up, but its physical state is down (possibly because no physical link exists or the link has failed). • **UP**—The interface is both administratively and physically up.
Line protocol current state	Data link layer state of the interface. • **DOWN**—The data link layer protocol is down. • **UP**—The data link layer protocol is up. • **UP (spoofing)**—The data link layer protocol is up, but the link is an on-demand link or does not exist.
Internet address is *ip-address*/*mask-length* (*Type*)	IP address of the interface and type of the address in parentheses. Possible IP address types include: • **Primary**—Manually configured primary IP address. • **Sub**—Manually configured secondary IP address. • **SSLVPN**—An SSL VPN AC interface IP address. For more information, see SSL VPN configuration in V*PN Configuration Guide.* • **PPP-negotiated**—IP address assigned by a PPP server during PPP negotiation. For more information, see PPP configuration in *Layer 2—WAN Access Configuration Guide*. • **Unnumbered**—IP address borrowed from another interface. • **DHCP-allocated**—DHCP allocated IP address. For more information, see DHCP client configuration in *Layer 3—IP Services Configuration Guide*. • **BOOTP-allocated**—BOOTP allocated IP address. For more information, see BOOTP client configuration in *Layer 3—IP Services Configuration Guide*. • **Cellular-allocated**—IP address allocated through the modem-manufacturer's proprietary protocol. For more information, see mobile communication modem management in *Layer 2—WAN Access Configuration Guide*.
Broadcast address	Broadcast address of the subnet attached to an interface.
The Maximum Transmit Unit	MTU of the interface, in bytes.

Field	Description
input packets, bytes, multicasts output packets, bytes, multicasts	All received and sent packets and bytes, and received and sent multicast packets on an interface (statistics start at the device startup).
TTL invalid packet number	Number of TTL-invalid packets received on the interface (statistics start at the device startup).
ICMP packet input number: Echo reply: Unreachable: Source quench: Routing redirect: Echo request: Router advert: Router solicit: Time exceed: IP header bad: Timestamp request: Timestamp reply: Information request: Information reply: Netmask request: Netmask reply: Unknown type:	Total number of ICMP packets received on the interface (statistics start at the device startup): • Echo reply packets. • Unreachable packets. • Source quench packets. • Routing redirect packets. • Echo request packets. • Router advertisement packets. • Router solicitation packets. • Time exceeded packets. • IP header bad packets. • Timestamp request packets. • Timestamp reply packets. • Information request packets. • Information reply packets. • Netmask request packets. • Netmask reply packets. • Unknown type packets.

Related commands

`display ip interface brief`

`ip address`

display ip interface brief

Use **`display ip interface brief`** to display brief IP configuration for Layer 3 interfaces.

Syntax

`display ip interface` [*`interface-type`* [*`interface-number`*]] **`brief`** [**`description`**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface-type: Specifies an interface type. If you do not specify an interface type, this command displays brief IP configuration for all Layer 3 interfaces.

interface-number: Specifies an interface number. If you do not specify an interface number, this command displays brief IP configuration for all Layer 3 interfaces of the specified type.

description: Displays complete interface descriptions. If you do not specify this keyword, the command displays a maximum of 16 characters for each interface description. If the description is longer than 16 characters, the first 14 characters are displayed, followed by an ellipsis (...).

Usage guidelines

Information displayed by the command includes the state of the physical and link layer protocols, IP address, and interface descriptions.

Examples

Display brief IP configuration for GigabitEthernet interfaces.

```
<Sysname> display ip interface gigabitethernet brief
*down: administratively down
(s): spoofing  (l): loopback
Interface           Physical Protocol IP address/Mask    VPN instance Description
GE1/0/1             up       up       5.5.5.1/24         --           Link to Co...
<Sysname> display ip interface gigabitethernet brief description
*down: administratively down
(s): spoofing  (l): loopback
Interface           Physical Protocol IP address/Mask    VPN instance Description
GE1/0/1             up       up       5.5.5.1/24         --           Link to CoreR
                                                                      outer
```

Table 2 Command output

Field	Description
*down: administratively down	The interface is administratively shut down by using the **shutdown** command.
(s) : spoofing	Spoofing attribute of the interface. The link protocol state of the interface is up, but the link is temporarily established on demand or does not exist.
Interface	Interface name.
Physical	Physical state of the interface: • ***down**—The interface is administratively shut down by using the **shutdown** command. • **down**—The interface is administratively up but its physical state is down, possibly because of a connection or link failure. • **up**—Both the administrative and physical states of the interface are up.
Protocol	Link layer protocol state of the interface: • **down**—The protocol state of the interface is down. • **down(l)**—The protocol state of the interface is down (loopback). • **up**—The protocol state of the interface is up. • **up(l)**—The protocol state of the interface is up (loopback). • **up(s)**—The protocol state of the interface is up (spoofing).
IP address/Mask	IP address and mask length of the interface. If no IP address is configured, this field displays hyphens (**--**).

Field	Description
VPN instance	Name of the VPN instance to which the interface belongs. This field displays a maximum of 12 characters. If the VPN instance name is longer than 12 characters, the first 9 characters are displayed, followed by an ellipsis (...). If the interface does not belong to any VPN instance, this field displays hyphens (**--**).
Description	Description of the interface. This field displays a maximum of 13 characters. If the description is longer than 13 characters, the first 10 characters are displayed, followed by an ellipsis (...). If no description is configured, this field displays hyphens (**--**).

Related commands

`display ip interface`

`ip address`

ip address

Use **`ip address`** to assign an IP address to the interface.

Use **`undo ip address`** to remove the IP address from the interface.

Syntax

Default

No IP address is assigned to an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

`ip-address`: Specifies the IP address of the interface, in dotted decimal notation.

`mask-length`: Specifies the subnet mask length in the range of 1 to 31. For a loopback interface, the value range is 1 to 32.

`mask`: Specifies the subnet mask in dotted decimal notation.

`sub`: Assigns a secondary IP address to the interface.

Usage guidelines

Use the command to assign a primary or secondary IP address to an interface.

An interface can have only one primary IP address. If you execute this command multiple times to specify different primary IP addresses, the most recent configuration takes effect. If the interface connects to multiple subnets, configure primary and secondary IP addresses on the interface so the subnets can communicate with each other through the interface.

You cannot assign secondary IP addresses to an interface that obtains an IP address through BOOTP, DHCP, PPP address negotiation, or IP unnumbered.

If you do not specify any parameters, the **undo ip address** command removes all IP addresses from the interface. The **undo ip address** *ip-address* { *mask* | *mask-length* } command removes the primary IP address. The **undo ip address** *ip-address* { *mask* | *mask-length* } **sub** command removes a secondary IP address.

The primary and secondary IP addresses assigned to the interface can be located on the same network segment. Different interfaces on your device must reside on different network segments.

Examples

Assign GigabitEthernet 1/0/1 a primary IP address 129.102.0.1 and a secondary IP address 202.38.160.1, with the subnet masks both 255.255.255.0.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip address 129.102.0.1 255.255.255.0
[Sysname-GigabitEthernet1/0/1] ip address 202.38.160.1 255.255.255.0 sub
```

Related commands

display ip interface

display ip interface brief

ip address unnumbered

Use **ip address unnumbered** to configure the current interface as IP unnumbered to borrow an IP address from the specified interface.

Use **undo ip address unnumbered** to restore the default.

Syntax

ip address unnumbered interface *interface-type interface-number*

undo ip address unnumbered

Default

The interface does not borrow IP addresses from other interfaces.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

interface *interface-type interface-number*: Specifies an interface from which the current interface can borrow an IP address.

Usage guidelines

Typically, you assign an IP address to an interface either manually or through DHCP. If the IP addresses are not enough, or the interface is used only occasionally, you can configure an interface to borrow an IP address from other interfaces. This is called IP unnumbered, and the interface borrowing the IP address is called IP unnumbered interface.

Loopback interfaces cannot borrow IP addresses of other interfaces, but other interfaces can borrow IP addresses of loopback interfaces.

Multiple interfaces can use the same unnumbered IP address. If an interface has multiple manually configured IP addresses, only the primary IP address manually configured can be borrowed.

You cannot enable a dynamic routing protocol on the interface that has no IP address configured. To enable the interface to communicate with other devices, you must configure a static route to the peer device on the interface.

Examples

Configure GigabitEthernet 1/0/2 to borrow the IP address of GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet1/0/2
[Sysname-GigabitEthernet1/0/2] ip address unnumbered interface gigabitethernet 1/0/1
```

Contents

Basic IP forwarding commands

display fib

Use **display fib** to display FIB entries.

Syntax

display fib [**vpn-instance** *vpn-instance-name*] [*ip-address* [*mask* | *mask-length*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. To display the FIB entries for the public network, do not specify any VPN instance.

ip-address: Displays the FIB entry that matches the specified destination IP address.

mask: Specifies the mask for the IP address.

mask-length: Specifies the mask length for the IP address. The value range is 0 to 32.

Usage guidelines

If you specify an IP address without a mask or mask length, this command displays the longest matching FIB entry.

If you specify an IP address and a mask or mask length, this command displays the exactly matching FIB entry.

Examples

Display all FIB entries of the public network.

```
<Sysname> display fib

Destination count: 5 FIB entry count: 5

Flag:
  U:Useable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
  R:Relay     F:FRR

Destination/Mask   Nexthop         Flag     OutInterface/Token       Label
0.0.0.0/32         127.0.0.1       UH       InLoop0                  Null
192.168.100.0/24   192.168.100.96  U        GE1/0/0                  Null
127.0.0.0/8        127.0.0.1       U        InLoop0                  Null
127.0.0.0/32       127.0.0.1       UH       InLoop0                  Null
```

```
127.0.0.1/32       127.0.0.1       UH       InLoop0                 Null
```

Display the FIB entries for VPN **vpn1**.

```
<Sysname> display fib vpn-instance vpn1
Destination count: 6 FIB entry count: 6

Flag:
  U:Useable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
  R:Relay     F:FRR

Destination/Mask   Nexthop         Flag     OutInterface/Token      Label
0.0.0.0/32         127.0.0.1       UH       InLoop0                  Null
20.20.20.0/24      20.20.20.25     U        GE1/0/0                 Null
20.20.20.0/32      20.20.20.25     UBH      GE1/0/0                 Null
20.20.20.25/32     127.0.0.1       UH       InLoop0                  Null
20.20.20.25/32     20.20.20.25     H        GE1/0/0                 Null
20.20.20.255/32    20.20.20.25     UBH      GE1/0/0                 Null
```

Display the FIB entries matching the destination IP address 10.2.1.1.

```
<Sysname> display fib 10.2.1.1

Destination count: 1 FIB entry count: 1

Flag:
  U:Useable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
  R:Relay     F:FRR

Destination/Mask   Nexthop         Flag     OutInterface/Token       Label
10.2.1.1/32        127.0.0.1       UH       InLoop0                  Null
```

Table 1 Command output

Field	Description
Destination count	Total number of destination addresses.
FIB entry count	Total number of FIB entries.
Destination/Mask	Destination address and the mask length.
Nexthop	Next hop address.
Flag	Flags of routes: • **U**—Usable route. • **G**—Gateway route. • **H**—Host route. • **B**—Blackhole route. • **D**—Dynamic route. • **S**—Static route. • **R**—Relay route. • **F**—Fast reroute.
OutInterface/Token	Output interface/LSP index number.
Label	Inner label.

inner-interface learn arp-nd

Use **inner-interface learn arp-nd** to enable ARP and ND entry learning on inner interfaces

Use **undo inner-interface learn arp-nd** to disable ARP and ND entry learning on inner interfaces.

Syntax

inner-interface learn arp-nd vlan *vlan-id*

undo inner-interface learn arp-nd

Default

ARP and ND entry learning is disabled on inner interfaces.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

vlan *vlan-id*: Specifies a VLAN by its ID in the range of 2 to 4094. The specified VLAN must be a VLAN terminated on an inner subinterface and cannot be the default VLAN ID of the peer inner interface.

Usage guidelines

You must enable this feature if NetStream statistics are sent out by inner interfaces. Otherwise, inner interfaces cannot learn ARP or ND entries and fail to transmit NetStream statistics.

This command is supported only on the default context.

Examples

Enable inner interfaces to learn ARP and ND entries in VLAN 200.

```
<Sysname> system-view
[Sysname] inner-interface learn arp-nd vlan 200
```

last-hop backup enable

Use **last-hop backup enable** to enable last hop backup.

Use **undo last-hop backup enable** to disable last hop backup.

Syntax

last-hop backup enable

undo last-hop backup enable

Default

Last hop backup is enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This feature enables the system to transmit the forward flow and reverse flow between the local node and a peer node over the same path.

In an IRF fabric enabled with this feature, the IRF master device performs the following operations when receiving the first IP packet of a forward flow on an interface enabled with last hop holding:

1. Saves the last hop information of the packet.
2. Synchronizes the last hop information to subordinate devices in the IRF fabric.

The last hop information can be used for guiding the backward flow when the flow arrives at the master device or is forwarded through a subordinate device.

For this feature to take effect in an IRF fabric, you must also enable session synchronization by using the **session synchronization enable** command. For more information about the **session synchronization enable** command, see *Security Command Reference*.

This feature is also applicable to multi-module devices enabled with service backup. If this feature is enabled on such a device, a device module performs the following operations when receiving the first IP packet of a forward flow on an interface enabled with last hop holding:

1. Saves the last hop information of the packet.
2. Synchronizes the last hop information to other modules in the device.

The last hop information can be used for guiding the backward flow when the flow arrives at one of these modules.

For this feature to take effect on a multi-module device, you must also enable session flow redirection by using the **session flow-redirect enable** command. For more information about the **session flow-redirect enable** command, see *Security Command Reference*.

Examples

Disable last hop backup.

```
<Sysname> system-view
[Sysname] undo last-hop backup enable
```

Related commands

ip last-hop hold

session flow-redirect enable (*Security Command Reference*)

session synchronization enable (*Security Command Reference*)

ip last-hop hold

Use **ip last-hop hold** to enable last hop holding.

Use **undo ip last-hop hold** to disable last hop holding.

Syntax

ip last-hop hold

undo ip last-hop hold

Default

Last hop holding is disabled.

Views

Layer 3 Ethernet interface view

Layer 3 Ethernet subinterface view

Predefined user roles

network-admin

context-admin

Usage guidelines

Last hop holding implements symmetric routing.

When the interface enabled with this feature receives the first IP packet of a forward flow, this feature implements the following operations:

- Obtains the forward flow information and last hop information of the packet.
- Based on the obtained information, creates a fast forwarding entry for the return flow.

When packets of the return flow arrive at the device, the device forwards those packets according to the fast forwarding entry.

Last hop holding relies on fast forwarding entries. If the MAC address of a last hop changes on an Ethernet link, this feature can function correctly only after the fast forwarding entry is updated for the MAC address.

Examples

Enable the last hop holding feature.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip last-hop hold
```

Load sharing commands

ip load-sharing local-first enable

Use **ip load-sharing local-first enable** to enable local-first load sharing.

Use **undo ip load-sharing local-first enable** to disable local-first load sharing.

Syntax

ip load-sharing local-first enable

undo ip load-sharing local-first enable

Default

Local-first load sharing is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

Local-first load sharing takes effect only on an IRF fabric.

Examples

Enable local-first load sharing.

```
<Sysname> system-view
[Sysname] ip load-sharing local-first enable
```

ip load-sharing mode

Use **ip load-sharing mode** to configure the load sharing mode.

Use **undo ip load-sharing mode** to restore the default.

Syntax

ip load-sharing mode { **per-flow** [**dest-ip** | **dest-port** | **ip-pro** | **src-ip** | **src-port**] * | **per-packet** } { **global** | **slot** *slot-number* }

undo ip load-sharing mode { **global** | **slot** *slot-number* }

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB1180, NFNX3-HDB1480	No

Default

The device performs per-flow load sharing.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

`per-flow`: Implements per-flow load sharing.

`dest-ip`: Identifies flows by destination IP address.

`dest-port`: Identifies flows by destination port.

`ip-pro`: Identifies flows by protocol number.

`src-ip`: Identifies flows by source IP address.

`src-port`: Identifies flows by source port.

`global`: Configures the load sharing mode globally.

`per-packet`: Implements per-packet load sharing.

`slot` *`slot-number`*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command configures the load sharing mode for all member devices.

Usage guidelines

The per-packet load sharing mode does not take effect in fast forwarding.

Examples

Configure per-flow load sharing for slot 1.

```
<Sysname> system-view
[Sysname] ip load-sharing mode per-flow slot 1
```

Contents

Fast forwarding commands

display ip fast-forwarding aging-time

Use **display ip fast-forwarding aging-time** to display the aging time of fast forwarding entries.

Syntax

display ip fast-forwarding aging-time

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display the aging time of fast forwarding entries.

```
<Sysname> display ip fast-forwarding aging-time
 Aging time: 30s
```

Related commands

ip fast-forwarding aging-time

display ip fast-forwarding cache

Use **display ip fast-forwarding cache** to display fast forwarding entries.

Syntax

display ip fast-forwarding cache [*ip-address*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ip-address: Specifies an IP address. If you do not specify an IP address, this command displays all fast forwarding entries.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays fast forwarding entries for all member devices.

Examples

Display all fast forwarding entries.

```
<Sysname> display ip fast-forwarding cache
Total number of fast-forwarding entries: 1
SIP            SPort DIP            DPort Pro Input_If   Output_If   Flg
7.0.0.13       68    8.0.0.1        67    17  GE1/0/3    GE1/0/1     5
```

Table 1 Command output

Field	Description
SIP	Source IP address.
SPort	Source port number.
DIP	Destination IP address.
DPort	Destination port number.
Pro	Protocol number.
Input_If	Input interface type and number. If no interface is involved in fast forwarding, this field displays **N/A**. If the input interface does not exist, this field displays a hyphen (-).
Output_If	Output interface type and number. If no interface is involved in fast forwarding, this field displays **N/A**. If the output interface does not exist, this field displays a hyphen (-).
Flg	Internal tag, marking internal operation information, such as fragmentation.

Related commands

reset ip fast-forwarding cache

display ip fast-forwarding fragcache

Use **display ip fast-forwarding fragcache** to display fast forwarding entries for fragmented packets.

Syntax

display ip fast-forwarding fragcache [*ip-address*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ip-address: Specifies an IP address. If you do not specify an IP address, this command displays fast forwarding entries for all fragmented packets.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays fast forwarding entries for fragmented packets on all member devices.

Examples

Display fast forwarding entries about all fragmented packets.

```
<Sysname> display ip fast-forwarding fragcache
Total number of fragment fast-forwarding entries: 1
SIP             SPort DIP             DPort Pro Input_If    ID     Relay_flag
7.0.0.13        68    8.0.0.1         67    17  GE1/0/3     2      1
```

Table 2 Command output

Field	Description
SIP	Source IP address.
SPort	Source port number.
DIP	Destination IP address.
DPort	Destination port number.
Pro	Protocol number.
Input_If	Input interface type and number. If no interface is involved in fast forwarding, this field displays **N/A**. If the input interface does not exist, this field displays a hyphen (-).
ID	Fragment ID.
Relay_flag	Fragment pass-through flag: • **0**—Not pass through. • **1**—Pass through.

Related commands

reset ip fast-forwarding cache

ip fast-forwarding aging-time

Use **ip fast-forwarding aging-time** to configure the aging time for fast forwarding entries.

Use **undo ip fast-forwarding aging-time** to restore the default.

Syntax

ip fast-forwarding aging-time *aging-time*

undo ip fast-forwarding aging-time

Default

The aging time is 30 seconds.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

aging-time: Specifies the aging time in the range of 10 to 300 seconds.

Examples

Set the aging time to 20 seconds for fast forwarding entries.

```
<Sysname> system-view
[Sysname] ip fast-forwarding aging-time 20
```

Related commands

display ip fast-forwarding aging-time

ip fast-forwarding dscp

Use **ip fast-forwarding dscp** to enable DSCP-based fast forwarding for GRE packets.

Use **undo ip fast-forwarding dscp** to restore the default.

Syntax

ip fast-forwarding dscp

undo ip fast-forwarding dscp

Default

DSCP-based fast forwarding for GRE packets is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command is applicable to GRE packets (with IP as the passenger protocol) that are processed by software.

This feature uses the DSCP value in the outer header instead of the source port number among the identification criteria to identify GRE traffic flows.

This command is mutually exclusive with NAT and load balancing.

Examples

Enable DSCP-based GRE packet fast forwarding.

```
<Sysname> system-view
[Sysname] ip fast-forwarding dscp
```

ip fast-forwarding load-sharing

Use **ip fast-forwarding load-sharing** to enable fast forwarding load sharing.

Use **undo ip fast-forwarding load-sharing** to disable fast forwarding load sharing.

Syntax

ip fast-forwarding load-sharing

undo ip fast-forwarding load-sharing

Default

Fast forwarding load sharing is enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

Fast forwarding load sharing enables the device to load share packets of the same flow. This feature identifies a data flow by using the packet information.

If fast forwarding load sharing is disabled, the device identifies a data flow by the packet information and the input interface. No load sharing is implemented.

Examples

Enable fast forwarding load sharing.

```
<Sysname> system-Views
[Sysname] ip fast-forwarding load-sharing
```

ip fast-forwarding vxlan-port

Use **ip fast-forwarding vxlan-port** to specify the destination UDP port number for identifying VXLAN packets.

Use **undo ip fast-forwarding vxlan-port** to restore the default.

Syntax

ip fast-forwarding vxlan-port *port-number*

undo ip fast-forwarding vxlan-port

Default

The destination UDP port number is 4789.

Views

System view

Predefined use roles

network-admin

context-admin

Parameters

port-number: Specifies a UDP port number in the range of 1 to 65535.

Usage guidelines

This feature is applicable to only the UDP packets that are processed by software.

In a VXLAN network, configure this command on intermediate devices to identify VXLAN packets.

Examples

Specify the destination UDP port number to 4900 for identifying VXLAN packets.

```
<Sysname> system-view
```

```
[Sysname] ip fast-forwarding vxlan-port 4900
```

reset ip fast-forwarding cache

Use **reset ip fast-forwarding cache** to clear the fast forwarding table.

Syntax

reset ip fast-forwarding cache [**slot** *slot-number*]

Views

User view

Predefined use roles

network-admin

context-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears the fast forwarding table for all member devices.

Examples

Clear the fast forwarding table.

```
<Sysname> reset ip fast-forwarding cache
```

Related commands

display ip fast-forwarding cache

display ip fast-forwarding fragcache

Contents

ARP commands

arp check enable

Use **arp check enable** to enable dynamic ARP entry check.

Use **undo arp check enable** to disable dynamic ARP entry check.

Syntax

arp check enable

undo arp check enable

Default

Dynamic ARP entry check is enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

Dynamic ARP entry check disables a device from supporting dynamic ARP entries with multicast MAC addresses. The device cannot learn dynamic ARP entries containing multicast MAC addresses. You cannot manually add static ARP entries that contain multicast MAC addresses.

When dynamic ARP entry check is disabled, ARP entries containing multicast MAC addresses are supported. The device can learn dynamic ARP entries containing multicast MAC addresses obtained from the ARP packets sourced from a unicast MAC address. You can also manually add static ARP entries containing multicast MAC addresses.

Examples

Enable dynamic ARP entry check.

```
<Sysname> system-view
[Sysname] arp check enable
```

arp check log enable

Use **arp check log enable** to enable the ARP logging feature.

Use **undo arp check log enable** to disable the ARP logging feature.

Syntax

arp check log enable

undo arp check log enable

Default

ARP logging is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This feature enables a device to log ARP events when ARP cannot resolve IP addresses correctly. The log information helps administrators locate and solve problems. The device can log the following ARP events:

- On a proxy ARP-disabled interface, the target IP address of a received ARP packet is not one of the following IP addresses:
  - The IP address of the receiving interface.
  - The virtual IP address of the VRRP group.
  - The public IP address after NAT.
- The sender IP address of a received ARP reply conflicts with one of the following IP addresses:
  - The IP address of the receiving interface.
  - The virtual IP address of the VRRP group.
  - The public IP address after NAT.

The device sends ARP log messages to the information center. You can use the **info-center source** command to specify the log output rules for the information center. For more information about information center, see *Network Management and Monitoring Configuration Guide*.

The device can generate a large number of ARP logs. To conserve system resources, enable ARP logging only when you are auditing or troubleshooting ARP events.

Examples

Enable ARP logging.

```
<Sysname> system-view
[Sysname] arp check log enable
```

arp ip-unnumbered learning enable

Use **arp ip-unnumbered learning enable** to enable an IP unnumbered interface to learn ARP entries for different subnets.

Use **undo arp ip-unnumbered learning enable** to disable an IP unnumbered interface from learning ARP entries for different subnets.

Syntax

arp ip-unnumbered learning enable

undo arp ip-unnumbered learning enable

Default

An IP unnumbered interface cannot learn ARP entries for different subnets.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

An IP unnumbered interface cannot learn the ARP entry of the peer device if the unnumbered interface and the peer device are on different subnets. To ensure communication between them, you can enable this feature on the IP unnumbered interface.

This feature takes effect only on an interface configured with the **ip address unnumbered** command. This interface is an unnumbered interface and borrows the IP address from another interface.

If an IP unnumbered interface is disabled from learning ARP entries for different subnets, existing ARP entries learned for different subnets are deleted after they age out.

Examples

Configure GigabitEthernet 1/0/1 to borrow the IP address of GigabitEthernet 1/0/2, and enable GigabitEthernet 1/0/1 to learn ARP entries for different subnets.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip address unnumbered interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/1] arp ip-unnumbered learning enable
```

Related commands

ip address unnumbered

arp max-learning-num

Use **arp max-learning-num** to set the dynamic ARP learning limit for an interface.

Use **undo arp max-learning-num** to restore the default.

Syntax

arp max-learning-num *max-number*

undo arp max-learning-num

Default

An interface can learn a maximum of 16384 dynamic ARP entries.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Layer 3 Ethernet interface view

Layer 3 Ethernet subinterface view

Layer 3 aggregate interface view

Layer 3 aggregate subinterface view

Reth interface view

Reth subinterface view

VLAN interface view

Predefined user roles

network-admin

context-admin

Parameters

max-number: Specifies the maximum number of dynamic ARP entries for an interface. The value range for this argument is 0 to 16384.

Usage guidelines

An interface can dynamically learn ARP entries. To prevent an interface from holding too many ARP entries, you can set the maximum number of dynamic ARP entries that the interface can learn. When the maximum number is reached, the interface stops learning ARP entries.

When the *number* argument is set to 0, the interface is disabled from learning dynamic ARP entries.

Examples

Specify VLAN-interface 40 to learn a maximum of 10 dynamic ARP entries.

```
<Sysname> system-view
[Sysname] interface vlan-interface 40
[Sysname-Vlan-interface40] arp max-learning-num 10
```

Specify GigabitEthernet 1/0/1 to learn a maximum of 10 dynamic ARP entries.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp max-learning-num 10
```

Specify Layer 2 aggregate interface Bridge-Aggregation 1 to learn a maximum of 10 dynamic ARP entries.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] arp max-learning-num 10
```

Specify Layer 3 aggregate interface Route-Aggregation 1 to learn a maximum of 10 dynamic ARP entries.

```
<Sysname> system-view
[Sysname] interface route-aggregation 1
[Sysname-Route-Aggregation1] arp max-learning-num 10
```

arp max-learning-number

Use **arp max-learning-number** to set the dynamic ARP learning limit for a device.

Use **undo arp max-learning-number** to restore the default.

Syntax

arp max-learning-number *max-number* **slot** *slot-number*

undo arp max-learning-number slot *slot-number*

Default

The device can learn a maximum of 16384 dynamic ARP entries.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

max-number: Specifies the maximum number of dynamic ARP entries for a device. The value range for this argument is 0 to 16384.

slot *slot-number*: Specifies an IRF member device by its member ID.

Usage guidelines

A device can dynamically learn ARP entries. To prevent a device from holding too many ARP entries, you can set the maximum number of dynamic ARP entries that the device can learn. When the maximum number is reached, the device stops learning ARP entries.

When the *number* argument is set to 0, the device is disabled from learning dynamic ARP entries.

Examples

Set the ARP learning limit to 64 for slot 1.

```
<Sysname> system-view
[Sysname] arp max-learning-number 64 slot 1
```

arp static

Use **arp static** to configure a static ARP entry.

Use **undo arp** to delete an ARP entry.

Syntax

arp static *ip-address mac-address* [*vlan-id interface-type interface-number*] [**vpn-instance** *vpn-instance-name*] [**description** *text*]

undo arp *ip-address* [*vpn-instance-name*]

Default

No static ARP entries exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies an IP address for the static ARP entry.

mac-address: Specifies a MAC address for the static ARP entry, in the format of H-H-H.

vlan-id: Specifies the ID of a VLAN to which the static ARP entry belongs. The value range is 1 to 4094.

interface-type interface-number: Specifies an interface by its type and number.

tunnel *number*: Specifies a tunnel interface by its number. The value range for the *number* argument is 0 to 1023.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance to which the static ARP entry belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. The VPN instance must already exist. To specify a static ARP entry on the public network, do not specify this option.

description *text*: Specifies the description for the static ARP entry, a case-sensitive string of 1 to 255 characters.

Usage guidelines

A static ARP entry is manually configured and maintained. It does not age out and cannot be overwritten by any dynamic ARP entry.

Static ARP entries can be short or long.

A resolved short static ARP entry becomes unresolved upon certain events, for example, when the resolved output interface goes down, or the corresponding VLAN or VLAN interface is deleted.

Long static ARP entries are effective or ineffective. Ineffective long static ARP entries cannot be used for packet forwarding. A long static ARP entry is ineffective when any of the following conditions exists:

- The IP address in the entry conflicts with a local IP address.
- No local interface has an IP address in the same subnet as the IP address in the ARP entry.

If you specify the *vlan-id interface-type interface-number* argument, follow these restrictions and guidelines:

- The interface can be an Ethernet interface or an aggregate interface.
- The VLAN and VLAN interface must already exist. The specified Ethernet interface must belong to the specified VLAN.
- The IP address of the VLAN interface and the IP address specified by the *ip-address* argument must be on the same network.
- If a VLAN or VLAN interface is deleted, a long static ARP entry for the VLAN is deleted and a resolved short static ARP entry for the VLAN becomes unresolved.

You can configure a description for each static ARP entry for easy identification.

Examples

Configure a long static ARP entry that contains IP address 202.38.10.2, MAC address 00e0-fc01-0000, and output interface GigabitEthernet 1/0/1 in VLAN 10.

```
<Sysname> system-view
[Sysname] arp static 202.38.10.2 00e0-fc01-0000 10 gigabitethernet 1/0/1
```

Configure a long static ARP entry that contains IP address 1.1.1.1, MAC address 00e0-fc01-0000, input interface VSI-interface 1, output interface Tunnel 1, and the VSI **a**.

```
<Sysname> system-view
[Sysname] arp static 1.1.1.1 00e0-fc01-0000 vsi-interface 1 tunnel 1 vsi a
```

Related commands

display arp

reset arp

arp timer aging

Use **arp timer aging** to set the aging timer for dynamic ARP entries.

Use **undo arp timer aging** to restore the default.

Syntax

arp timer aging *aging-time*

undo arp timer aging

Default

The aging timer for dynamic ARP entries is 20 minutes.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

aging-time: Specifies the aging timer in minutes. The value range for this argument is 1 to 1440.

Usage guidelines

Each dynamic ARP entry in the ARP table has a limited lifetime, called an aging timer. The aging timer of a dynamic ARP entry is reset each time the dynamic ARP entry is updated. Dynamic ARP entries that are not updated before their aging timers expire are deleted from the ARP table.

Set the aging timer for dynamic ARP entries as needed. For example, when you configure proxy ARP, set a short aging time so that invalid dynamic ARP entries can be deleted in a timely manner.

Examples

Set the aging timer for dynamic ARP entries to 10 minutes.

```
<Sysname> system-view
[Sysname] arp timer aging 10
```

Related commands

display arp timer aging

display arp

Use **display arp** to display ARP entries.

Syntax

display arp [[**all** | **dynamic** | **static**] [**slot** *slot-number*] | **vlan** *vlan-id* | **interface** *interface-type interface-number*] [**count** | **verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

all: Displays all ARP entries.

dynamic: Displays dynamic ARP entries.

static: Displays static ARP entries.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays ARP entries for the master device.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID. The VLAN ID is in the range of 1 to 4094.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays ARP entries for all interfaces.

count: Displays the number of ARP entries.

verbose: Displays detailed information about ARP entries.

Usage guidelines

This command displays information about static and dynamic ARP entries, including the IP address, MAC address, VLAN ID, output interface, entry type, and aging timer.

Examples

Display all ARP entries.

```
<Sysname> display arp all
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule  I-Invalid
IP address      MAC address    VLAN/VSI name Interface/Link ID        Aging Type
1.1.1.1         02e0-f102-0023 1             GE1/0/1                 --    S
1.1.1.2         00e0-fc00-0001 12            GE1/0/2                 16    D
```

Display detailed information about all ARP entries.

```
<Sysname> display arp all verbose
IP address          : 1.1.1.1             MAC address    : 02e0-f102-0023
Type                : Static              Aging          : --
Interface           : GE1/0/1             SVLAN/CVLAN    : 1/--
VPN instance        : --
Link ID             : --
VXLAN ID            : --
VSI name            : --
VSI interface       : --
MPLS PW ID          : --
MPLS peer PE address: --
Nickname            : 0x0000
Description         : User1

IP address          : 1.1.1.2             MAC address    : 00e0-fc00-0001
Type                : Dynamic             Aging          : 16 min
Interface           : GE1/0/2             SVLAN/CVLAN    : 12/--
VPN instance        : --
Link ID             : --
VXLAN ID            : --
VSI name            : --
VSI interface       : --
MPLS PW ID          : --
MPLS peer PE address: --
Nickname            : 0x0000
Description         : --

IP address          : 1.1.1.3             MAC address    : 00e0-fe50-6503
Type                : Dynamic             Aging          : 16 min
Interface           : Tunnel1             SVLAN/CVLAN    : --/--
```

```
VPN instance        : --
Link ID             : --
VXLAN ID            : --
VSI name            : vsi1
VSI interface       : --
MPLS PW ID          : --
MPLS peer PE address: --
Nickname            : 0x0000
Description         : --
```

Display the number of all ARP entries.

```
<Sysname> display arp all count
 Total number of entries : 3
```

Table 1 Command output

Field	Description
IP address	IP address in an ARP entry.
MAC address	MAC address in an ARP entry.
VLAN/VSI name	ID of the VLAN to which the ARP entry belongs. This field displays hyphens (**--**) in either of the following situations: • The ARP entry is an unresolved short static ARP entry. • The output interface of the ARP entry does not belong to the VLAN.
Interface	Output interface in the ARP entry. This field displays hyphens (**--**) in either of the following situations: The ARP entry is an unresolved short static ARP entry.
Link ID	Link ID in the ARP entry. This field displays hyphens (**--**) if the ARP entry does not belong to any VSI.
Aging	Aging time for an ARP entry in minutes. For a static ARP entry, this field always displays hyphens (**--**). The static ARP entry never ages out unless you delete it manually. For a dynamic ARP entry, this field displays hyphens (**--**) if the aging time is unknown.
Type	ARP entry type: • **D**—Dynamic. • **S**—Static. • **R**—Rule. • **I**—Invalid.
SVLAN/CVLAN	Outer VLAN ID and inner VLAN ID in the ARP entry. This field displays hyphens (**--**) in either of the following situations: • The ARP entry is an unresolved short static ARP entry. • The interface in the ARP entry does not belong to the VLAN.
VPN instance	Name of VPN instance. If no VPN instance is configured for the ARP entry, this field displays hyphens (**--**).
VXLAN ID	This field is not supported in the current software version. ID of the VXLAN to which the ARP entry belongs. VXLAN ID is also called VNI. If the ARP entry does not belong to any VXLAN, this field displays hyphens (**--**).
VSI name	Name of the VSI to which the ARP entry belongs. If the ARP entry does not belong to any VSI, this field displays hyphens (**--**).

Field	Description
VSI interface	This field is not supported in the current software version. Name of the gateway interface of the VSI. If no gateway interface is specified for the VSI, this field displays hyphens (**--**).
MPLS PW ID	This field is not supported in the current software version. ID of the PW to which the ARP entry belongs. This field displays two hyphens (**--**) if the ARP entry does not belong to a PW.
MPLS peer PE address	This field is not supported in the current software version. IP address of the remote PE on the PW. This field displays two hyphens (**--**) if the ARP entry does not belong to a PW.
Nickname	This field is not supported in the current software version. Nickname of the ARP entry. The nickname is a string of four hexadecimal numbers, for example, 0x012a.
Description	Description of the ARP entry. If no description is configured for the ARP entry, this field displays hyphens (**--**).
Total number of entries	Number of ARP entries.

Related commands

arp static

reset arp

display arp *ip-address*

Use **display arp** *ip-address* to display the ARP entry for an IP address.

Syntax

display arp *ip-address* [**slot** *slot-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ip-address: Displays the ARP entry for the specified IP address.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for the master device.

verbose: Displays the detailed information about the specified ARP entry.

Usage guidelines

The ARP entry information includes the IP address, MAC address, VLAN ID, output interface, entry type, and aging timer.

Examples

Display the ARP entry for the IP address 20.1.1.1.

```
<Sysname> display arp 20.1.1.1
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule  I-Invalid
IP address      MAC address    VLAN/VSI name Interface/Link ID        Aging Type
20.1.1.1        00e0-fc00-0001 --            --                      --    S
```

Related commands

arp static

reset arp

display arp timer aging

Use **display arp timer aging** to display the aging timer of dynamic ARP entries.

Syntax

display arp timer aging

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display the aging timer of dynamic ARP entries.

```
<Sysname> display arp timer aging
Current ARP aging time is 20 minute(s)(default)
```

Related commands

arp timer aging

display arp vpn-instance

Use **display arp vpn-instance** to display the ARP entries for a VPN instance.

Syntax

display arp vpn-instance *vpn-instance-name* [**count** | **verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance-name: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. The VPN instance name cannot contain any spaces.

count: Displays the number of ARP entries.

verbose: Displays detailed information about ARP entries.

Usage guidelines

This command displays information about ARP entries for a VPN instance, including the IP address, MAC address, VLAN ID, output interface, entry type, and aging timer.

Examples

Display ARP entries for VPN instance **test**.

```
<Sysname> display arp vpn-instance test
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule  I-Invalid
IP address      MAC address    VLAN/VSI name Interface/Link ID        Aging Type
20.1.1.1        00e0-fc00-0001 --            --                      --    S
```

Related commands

arp static

reset arp

reset arp

Use **reset arp** to clear ARP entries from the ARP table.

Syntax

reset arp { **all** | **dynamic** | **interface** *interface-type interface-number* | **slot** *slot-number* | **static** }

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

all: Clears all ARP entries.

dynamic: Clears all dynamic ARP entries.

static: Clears all static ARP entries.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears ARP entries for the master device.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command clears ARP entries for all interfaces.

Examples

Clear all static ARP entries.

```
<Sysname> reset arp static
```

Related commands

arp static

display arp

Gratuitous ARP commands

arp ip-conflict log prompt

Use **arp ip-conflict log prompt** to enable IP conflict notification.

Use **undo arp ip-conflict log prompt** to restore the default.

Syntax

arp ip-conflict log prompt

undo arp ip-conflict log prompt

Default

If the system starts up with the factory defaults, IP conflict notification is enabled.

If the system starts up with the initial configuration, IP conflict notification is disabled.

For more information about factory defaults and initial configuration, see configuration file management in *Fundamentals Configuration Guide*.

Views

System view

Predefined user roles

network-admin

context-admin

Examples

Enable IP conflict notification on the device.

```
<Sysname> system-view
[Sysname] arp ip-conflict log prompt
```

arp send-gratuitous-arp

Use **arp send-gratuitous-arp** to enable periodic sending of gratuitous ARP packets on an interface.

Use **undo arp send-gratuitous-arp** to disable the interface from periodically sending gratuitous ARP packets.

Syntax

arp send-gratuitous-arp [**interval** *interval*]

undo arp send-gratuitous-arp

Default

Periodic sending of gratuitous ARP packets is disabled.

Views

Layer 3 Ethernet interface view

Layer 3 Ethernet subinterface view

Layer 3 aggregate interface view

Layer 3 aggregate subinterface view

VLAN interface view

Reth interface view

Reth subinterface view

Predefined user roles

network-admin

context-admin

Parameters

interval *interval*: Specifies the sending interval in the range of 200 to 200000 milliseconds. The default value is 2000 milliseconds.

Usage guidelines

This feature takes effect on an interface only when the interface has an IP address and the data link layer state of the interface is up.

This feature can send gratuitous ARP requests only for a VRRP virtual IP address, or the sending interface's primary IP address or manually configured secondary IP address. The primary IP address can be configured manually or automatically, whereas the secondary IP address must be configured manually.

If you change the sending interval for gratuitous ARP packets, the configuration takes effect at the next sending interval.

The sending interval for gratuitous ARP packets might be much longer than the set interval when any of the following conditions exist:

- This feature is enabled on multiple interfaces.
- Each interface is configured with multiple secondary IP addresses.
- A small sending interval is configured in the preceding cases.

Examples

Enable GigabitEthernet 1/0/1 to send gratuitous ARP packets every 300 milliseconds.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp send-gratuitous-arp interval 300
```

gratuitous-arp mac-change retransmit

Use **gratuitous-arp mac-change retransmit** to set the times and the interval for retransmitting a gratuitous ARP packet for the device MAC address change.

Use **undo gratuitous-arp mac-change retransmit** to restore the default.

Syntax

gratuitous-arp mac-change retransmit *times* **interval** *seconds*

undo gratuitous-arp mac-change retransmit

Default

The device sends a gratuitous packet for its MAC address change once only.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

times: Specifies the times of retransmitting a gratuitous packet, in the range of 1 to 10.

interval *seconds*: Specifies the interval for retransmitting a gratuitous packet, in the range of 1 to 10 seconds.

Usage guidelines

The device sends a gratuitous ARP packet to inform other devices of its MAC address change. However, the other devices might fail to receive the packet because the device sends the gratuitous ARP packet once only by default. Use this command to configure gratuitous ARP retransmission parameters to ensure that the other devices can receive the packet.

After you execute this command, the device will retransmit a gratuitous ARP packet for its MAC address change at the specified interval for the specified times.

Examples

Set the times to 3 and the interval to 5 for retransmitting a gratuitous ARP packet for the device MAC address change.

```
<Sysname> system-view
[Sysname] gratuitous-arp mac-change retransmit 3 interval 5
```

gratuitous-arp-learning enable

Use **gratuitous-arp-learning enable** to enable learning of gratuitous ARP packets.

Use **undo gratuitous-arp-learning enable** to disable learning of gratuitous ARP packets.

Syntax

```
gratuitous-arp-learning enable
undo gratuitous-arp-learning enable
```

Default

Learning of gratuitous ARP packets is enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

The learning of gratuitous ARP packets feature allows a device to maintain its ARP table by creating or updating ARP entries based on received gratuitous ARP packets.

When this feature is disabled, the device uses received gratuitous ARP packets to update existing ARP entries only. ARP entries are not created based on the received gratuitous ARP packets, which saves ARP table space.

Examples

Enable learning of gratuitous ARP packets.

```
<Sysname> system-view
[Sysname] gratuitous-arp-learning enable
```

gratuitous-arp-sending enable

Use **gratuitous-arp-sending enable** to enable sending gratuitous ARP packets upon receiving ARP requests whose sender IP address is on a different subnet.

Use **undo gratuitous-arp-sending enable** to disable sending gratuitous ARP packets upon receiving ARP requests whose sender IP address is on a different subnet.

Syntax

gratuitous-arp-sending enable

undo gratuitous-arp-sending enable

Default

A device does not send gratuitous ARP packets when it receives ARP requests whose sender IP address is on a different subnet.

Views

System view

Predefined user roles

network-admin

context-admin

Examples

Disable a device from sending gratuitous ARP packets upon receiving ARP requests whose sender IP address is on a different subnet.

```
<Sysname> system-view
[Sysname] undo gratuitous-arp-sending enable
```

Proxy ARP commands

display local-proxy-arp

Use **display local-proxy-arp** to display the local proxy ARP status.

Syntax

display local-proxy-arp [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays the local proxy ARP status for all interfaces.

Usage guidelines

You can use this command to check whether local proxy ARP is enabled or disabled.

Examples

Display the local proxy ARP status for GigabitEthernet 1/0/1.

```
<Sysname> display local-proxy-arp interface gigabitethernet 1/0/1
Interface GigabitEthernet1/0/1
 Local Proxy ARP status: enabled
```

Related commands

local-proxy-arp enable

display proxy-arp

Use **display proxy-arp** to display the proxy ARP status.

Syntax

display proxy-arp [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays the proxy ARP status for all interfaces.

Usage guidelines

You can use this command to check whether proxy ARP is enabled or disabled.

Examples

Display the proxy ARP status on GigabitEthernet 1/0/1.

```
<Sysname> display proxy-arp interface gigabitethernet 1/0/1
Interface GigabitEthernet1/0/1
 Proxy ARP status: disabled
```

Related commands

proxy-arp enable

local-proxy-arp enable

Use **local-proxy-arp enable** to enable local proxy ARP.

Use **undo local-proxy-arp enable** to disable local proxy ARP.

Syntax

local-proxy-arp enable [**ip-range** *start-ip-address* **to** *end-ip-address*]

undo local-proxy-arp enable

Default

Local proxy ARP is disabled.

Views

Layer 3 Ethernet interface view

Layer 3 Ethernet subinterface view

Layer 3 aggregate interface view

Layer 3 aggregate subinterface view

VLAN interface view

Reth interface view

Reth subinterface view

Predefined user roles

network-admin

context-admin

Parameters

ip-range *start-ip-address* **to** *end-ip-address*: Specifies the IP address range for which local proxy ARP is enabled. The start IP address must be lower than or equal to the end IP address.

Usage guidelines

Proxy ARP enables a device on a network to answer ARP requests for an IP address not on that network. With proxy ARP, hosts in different broadcast domains can communicate with each other as they do on the same network.

Proxy ARP includes common proxy ARP and local proxy ARP.

Common proxy ARP allows communication between hosts that connect to different Layer 3 interfaces and reside in different broadcast domains.

Local proxy ARP allows communication between hosts that connect to the same Layer 3 interface and reside in different broadcast domains.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Enable local proxy ARP on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] local-proxy-arp enable
```

Enable local proxy ARP on GigabitEthernet 1/0/1 for an IP address range.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] local-proxy-arp enable ip-range 1.1.1.1 to 1.1.1.20
```

Related commands

display local-proxy-arp

proxy-arp enable

Use **proxy-arp enable** to enable proxy ARP.

Use **undo proxy-arp enable** to disable proxy ARP.

Syntax

proxy-arp enable

undo proxy-arp enable

Default

Proxy ARP is disabled.

Views

Layer 3 Ethernet interface view

Layer 3 Ethernet subinterface view

Layer 3 aggregate interface view

Layer 3 aggregate subinterface view

VLAN interface view

Reth interface view

Reth subinterface view

Predefined user roles

network-admin

context-admin

Usage guidelines

Proxy ARP enables a device on a network to answer ARP requests for an IP address not on that network. With proxy ARP, hosts in different broadcast domains can communicate with each other as they do on the same network.

Proxy ARP includes common proxy ARP and local proxy ARP.

Common proxy ARP allows communication between hosts that connect to different Layer 3 interfaces and reside in different broadcast domains.

Local proxy ARP allows communication between hosts that connect to the same Layer 3 interface and reside in different broadcast domains.

Examples

Enable proxy ARP on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] proxy-arp enable
```

Related commands

display proxy-arp

ARP snooping commands

arp snooping enable

Use **arp snooping enable** to enable ARP snooping.

Use **undo arp snooping enable** to disable ARP snooping.

Syntax

arp snooping enable

undo arp snooping enable

Default

ARP snooping is disabled.

Views

VLAN view

Predefined user roles

network-admin

context-admin

Examples

Enable ARP snooping for VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] arp snooping enable
```

display arp snooping

Use **display arp snooping** to display ARP snooping entries.

Syntax

display arp snooping [**vlan** *vlan-id*] [**slot** *slot-number*] [**count**]

display arp snooping ip *ip-address* [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vlan *vlan-id*: Displays ARP snooping entries for a VLAN. The *vlan-id* argument is in the range of 1 to 4094.

count: Displays the number of the ARP snooping entries.

ip *ip-address*: Displays the ARP snooping entry for the specified IP address.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays ARP snooping entries for the master device.

Examples

Display ARP snooping entries for VLAN 2.

```
<Sysname> display arp snooping vlan 2
IP Address   MAC Address    VLAN ID Interface  Aging       Status
3.3.3.3      0003-0003-0003 2       GE1/0/1    20          Valid
3.3.3.4      0004-0004-0004 2       GE1/0/2    5           Invalid
```

Display the number of the ARP snooping entries.

```
<Sysname> display arp snooping count
Total entries: 2
```

Table 2 Command output

Field	Description
IP Address	IP address in an ARP snooping entry.
MAC Address	MAC address in an ARP snooping entry.
VLAN ID	ID of the VLAN to which the ARP snooping entry belongs.
Interface	Input interface in an ARP snooping entry.
Aging	Aging time for an ARP snooping entry in minutes.
Status	Status of an ARP snooping entry: **Valid**, **Invalid**, **Collision**.
Total entries	Number of ARP snooping entries.

Related commands

reset arp snooping

reset arp snooping

Use **reset arp snooping** to delete ARP snooping entries.

Syntax

reset arp snooping [**ip** *ip-address* | **vlan** *vlan-id*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

ip *ip-address*: Deletes the ARP snooping entry for the specified IP address.

vlan *vlan-id*: Deletes ARP snooping entries for the specified VLAN. The value range for the *vlan-id* argument is 1 to 4094.

Usage guidelines

If you do not specify any option, the command deletes all ARP snooping entries.

Examples

Delete ARP snooping entries for VLAN 2.

```
<Sysname> reset arp snooping vlan 2
```

Related commands

display arp snooping

ARP fast-reply commands

arp fast-reply enable

Use **arp fast-reply enable** to enable ARP fast-reply for a VLAN.

Use **undo arp fast-reply enable** to disable ARP fast-reply for a VLAN.

Syntax

arp fast-reply enable

undo arp fast-reply enable

Default

ARP fast-reply is disabled on a VLAN.

Views

VLAN view

Predefined user roles

network-admin

context-admin

Examples

Enable ARP fast-reply for VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] arp fast-reply enable
```

ARP direct route advertisement commands

arp route-direct advertise

Use **arp route-direct advertise** to enable ARP direct route advertisement.

Use **undo arp route-direct advertise** to disable ARP direct route advertisement.

Syntax

arp route-direct advertise

undo arp route-direct advertise

Default

ARP direct route advertisement is disabled.

Views

Interface view

Predefined user roles

network-admin

context-admin

Examples

Enable ARP direct route advertisement on Layer 3 Ethernet interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp route-direct advertise
```

Contents

IPv6 basics commands

display ipv6 fib

Use **display ipv6 fib** to display IPv6 FIB entries.

Syntax

display ipv6 fib [**vpn-instance** *vpn-instance-name*] [*ipv6-address* [*prefix-length*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays IPv6 FIB entries for the public network.

ipv6-address: Displays IPv6 FIB entries for a destination IPv6 address. If you do not specify an IPv6 address, this command displays all IPv6 FIB entries.

prefix-length: Specifies a prefix length for the IPv6 address, in the range of 0 to 128. If you do not specify the prefix length, this command displays the IPv6 FIB entry longest matching the IPv6 address.

Examples

Display all IPv6 FIB entries for the public network.

```
<Sysname> display ipv6 fib

Destination count: 1 FIB entry count: 1

Flag:
  U:Useable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
  R:Relay     F:FRR

Destination: ::1                                    Prefix length: 128
Nexthop    : ::1                                    Flags: UH
Time stamp : 0x1                                    Label: Null
Interface  : InLoop0                                Token: Invalid
```

Table 1 Command output

Field	Description
Destination count	Total number of destination addresses.
FIB entry count	Total number of IPv6 FIB entries.

Field	Description
Destination	Destination address.
Prefix length	Prefix length of the destination address.
Nexthop	Next hop address.
Flags	Route flag: • **U**—Usable route. • **G**—Gateway route. • **H**—Host route. • **B**—Black hole route. • **D**—Dynamic route. • **S**—Static route. • **R**—Recursive route. • **F**—Fast re-route.
Time stamp	Time when the IPv6 FIB entry was generated.
Label	This field is not supported in the current software version. Inner MPLS label. For IPv6 FIB entries for the public network, this field displays **Null**.
Interface	Outgoing interface.
Token	Label switched path index number.

display ipv6 icmp statistics

Use **display ipv6 icmp statistics** to display ICMPv6 packet statistics.

Syntax

display ipv6 icmp statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays ICMPv6 packet statistics for all member devices.

Examples

Display ICMPv6 packet statistics.

```
<Sysname> display ipv6 icmp statistics
  Input: bad code              0         too short               0
         checksum error        0         bad length              0
         path MTU changed      0         destination unreachable 0
         too big               0         parameter problem       0
```

```
        echo request           0         echo reply              0
        neighbor solicit       0         neighbor advertisement  0
        router solicit         0         router advertisement    0
        redirect               0         router renumbering      0
output: parameter problem      0         echo request            0
        echo reply             0         unreachable no route    0
        unreachable admin      0         unreachable beyond scope 0
        unreachable address    0         unreachable no port     0
        too big                0         time exceed transit     0
        time exceed reassembly 0         redirect                0
        ratelimited            0         other errors            0
```

Table 2 Command output

Field	Description
bad code	Number of received packets with error codes.
too short	Number of received packets with the length too short.
checksum error	Number of received packets with checksum errors.
bad length	Number of received packets with incorrect packet size.
path MTU changed	Number of received packets with path MTU changed.
destination unreachable	Number of destination unreachable packets that have been received.
too big	Number of received or sent oversized packets.
parameter problem	Number of received or sent packets with incorrect parameters.
echo request	Number of received or sent echo request packets.
echo reply	Number of received or sent echo reply packets.
neighbor solicit	Number of received NS packets.
neighbor advertisement	Number of received NA packets.
router solicit	Number of received RS packets.
router advertisement	Number of received RA packets.
redirect	Number of received or sent redirect packets.
router renumbering	Number of received packets with router renumbering.
unreachable no route	Number of sent packets to report the error that no route is available to the destination.
unreachable admin	Number of sent packets to report the error that the communication with the destination is administratively prohibited.
unreachable beyondscope	Number of sent packets to report the error that the source addresses is beyond the scope.
unreachable address	Number of address unreachable packets that have been sent.

unreachable no port	Number of port unreachable packets that have been sent.
time exceed transit	Number of sent packets to report the time exceeded in transmit error.
time exceed reassembly	Number of sent packets to report the fragment reassembly time exceeded error.
ratelimited	Number of packets that were not sent out because of the rate limit.
other errors	Number of sent packets with other errors.

display ipv6 interface

Use **`display ipv6 interface`** to display IPv6 interface information.

Syntax

`display ipv6 interface` [*`interface-type`* [*`interface-number`*]] [**`brief`**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

`interface-type`: Specifies an interface by its type.

`interface-number`: Specifies an interface by its number.

`brief`: Displays brief IPv6 interface information, including physical status, link-layer protocols, and IPv6 address. If you do not specify the keyword, this command displays detailed IPv6 interface information, including IPv6 configuration and operating information, and IPv6 packet statistics.

Usage guidelines

If you do not specify an interface, this command displays IPv6 information about all interfaces except VA interfaces.

If you specify only the *`interface-type`* argument, this command displays IPv6 information about the interfaces of the specified type.

If you specify both the *`interface-type`* and the *`interface-number`* arguments, this command displays IPv6 information about the specified interface.

Examples

Display IPv6 information about GigabitEthernet 1/0/1.

```
<Sysname> display ipv6 interface gigabitethernet 1/0/1
GigabitEthernet1/0/1 current state: UP
Line protocol current state: UP
IPv6 is enabled, link-local address is FE80::200:1FF:FE04:5D00 [TENTATIVE]
  Global unicast address(es):
    10::1234:56FF:FE65:4322, subnet is 10::/64 [TENTATIVE] [AUTOCFG]
```

```
    [valid lifetime 4641s/preferred lifetime 4637s]
   20::1234:56ff:fe65:4322, subnet is 20::/64 [TENTATIVE] [EUI-64]
   30::1, subnet is 30::/64 [TENTATIVE] [ANYCAST]
   40::2, subnet is 40::/64 [TENTATIVE] [DHCP]
   50::3, subnet is 50::/64 [TENTATIVE]
  Joined group address(es):
   FF02::1
   FF02::2
   FF02::1:FF00:1
   FF02::1:FF04:5D00
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
IPv6 Packet statistics:
  InReceives:                0
  InTooShorts:               0
  InTruncatedPkts:           0
  InHopLimitExceeds:         0
  InBadHeaders:              0
  InBadOptions:              0
  ReasmReqds:                0
  ReasmOKs:                  0
  InFragDrops:               0
  InFragTimeouts:            0
  OutFragFails:              0
  InUnknownProtos:           0
  InDelivers:                0
  OutRequests:               0
  OutForwDatagrams:          0
  InNoRoutes:                0
  InTooBigErrors:            0
  OutFragOKs:                0
  OutFragCreates:            0
  InMcastPkts:               0
  InMcastNotMembers:         0
  OutMcastPkts:              0
  InAddrErrors:              0
  InDiscards:                0
  OutDiscards:               0
```

Table 3 Command output

Field	Description
GigabitEthernet1/0/1 current state	Physical state of the interface: • **Administratively DOWN**—The interface has been administratively shut down by using the **shutdown** command. • **DOWN**—The interface is administratively up but its physical state is down, possibly because of a connection or link failure.

Field	Description
	• **UP**—The administrative and physical states of the interface are both up.
Line protocol current state	Link layer state of the interface: • **DOWN**—The link layer protocol state of the interface is down. • **UP**—The link layer protocol state of the interface is up.
IPv6 is enabled	IPv6 is enabled on the interface. This feature is automatically enabled after an IPv6 address is configured for an interface.
link-local address	Link-local address of the interface.
Global unicast address(es)	Global unicast addresses of the interface. IPv6 address states: • **TENTATIVE**—Initial state. DAD is being performed or is to be performed on the address. • **DUPLICATE**—The address is not unique on the link. • **PREFERRED**—The address is preferred and can be used as the source or destination address of a packet. If an address is in this state, the command does not display the address state. • **DEPRECATED**—The address is beyond the preferred lifetime but in the valid lifetime. It is valid, but it cannot be used as the source address for a new connection. Packets destined for the address are processed correctly. If a global unicast address is not manually configured, the following notations indicate how the address is obtained: • **AUTOCFG**—Stateless autoconfigured. • **DHCP**—Assigned by a DHCPv6 server. • **EUI-64**—Manually configured EUI-64 IPv6 address. • **RANDOM**—Random address automatically generated. If the address is a manually configured anycast address, it is noted with **ANYCAST**.
valid lifetime	Specifies how long autoconfigured global unicast addresses using a prefix are valid.
preferred lifetime	Specifies how long autoconfigured global unicast addresses using a prefix are preferred.
Joined group address(es)	Addresses of the multicast groups that the interface has joined.
MTU	MTU of the interface.
ND DAD is enabled, number of DAD attempts	DAD is enabled. • If DAD is enabled, this field displays the number of attempts to send an NS message for DAD (set by using the **ipv6 nd dad attempts** command). • If DAD is disabled, this field displays **ND DAD is disabled**. To disable DAD, set the number of attempts to 0.
ND reachable time	Time during which a neighboring device is reachable.
ND retransmit interval	Interval for retransmitting an NS message.
Hosts use stateless autoconfig for addresses	Hosts obtained IPv6 addresses through stateless autoconfiguration.
InReceives	Received IPv6 packets, including error messages.
InTooShorts	Received IPv6 packets that are too short. For example, the received IPv6 packet is less than 40 bytes.
InTruncatedPkts	Received IPv6 packets with a length less than the payload length field

Field	Description
	specified in the packet header.
InHopLimitExceeds	Received IPv6 packets with a hop count exceeding the hop limit field specified in the packet header.
InBadHeaders	Received IPv6 packets with incorrect basic headers.
InBadOptions	Received IPv6 packets with incorrect extension headers.
ReasmReqds	Received IPv6 fragments.
ReasmOKs	Number of reassembled IPv6 packets.
InFragDrops	Received IPv6 fragments that are discarded because of certain errors.
InFragTimeouts	Received IPv6 fragments that are discarded because the amount of time they stay in the system buffer exceeds the specified interval.
OutFragFails	IPv6 packets that fail to be fragmented on the output interface.
InUnknownProtos	Received IPv6 packets with unknown or unsupported protocol type.
InDelivers	Received IPv6 packets that are delivered to user protocols (such as ICMPv6, TCP, and UDP).
OutRequests	Local IPv6 packets sent by IPv6 user protocols.
OutForwDatagrams	IPv6 packets forwarded by the interface.
InNoRoutes	Received IPv6 packets that are discarded because no matching route can be found.
InTooBigErrors	Received IPv6 packets that fail to be forwarded because they exceeded the Path MTU.
OutFragOKs	Fragmented IPv6 packets on the output interface.
OutFragCreates	Number of IPv6 fragments on the output interface.
InMcastPkts	Received IPv6 multicast packets.
InMcastNotMembers	Received IPv6 multicast packets that are discarded because the interface is not in the multicast group.
OutMcastPkts	IPv6 multicast packets sent by the interface.
InAddrErrors	Received IPv6 packets that are discarded due to invalid destination addresses.
InDiscards	Received IPv6 packets that are discarded due to resource problems rather than packet errors.
OutDiscards	IPv6 packets that fail to be sent due to resource problems rather than packet errors.

Display brief IPv6 information about all interfaces.

```
<Sysname> display ipv6 interface brief
*down: administratively down
(s): spoofing
Interface                         Physical Protocol IPv6 Address
GigabitEthernet1/0/1              up       up       2001::1
GigabitEthernet1/0/2              up       up       Unassigned
GigabitEthernet1/0/3              down     down     Unassigned
```

Table 4 Command output

Field	Description
*down: administratively down	The interface has been administratively shut down by using the **shutdown** command.
(s): spoofing	Spoofing attribute of the interface. The link protocol state of the interface is up, but the link is temporarily established on demand or does not exist.
Interface	Name of the interface.
Physical	Physical state of the interface: • ***down**—The interface has been administratively shut down by using the **shutdown** command. • **down**—The interface is administratively up but its physical state is down, possibly because of a connection or link failure. • **up**—The administrative and physical states of the interface are both up.
Protocol	Link layer protocol state of the interface: • **down**—The network layer protocol state of the interface is down. • **up**—The network layer protocol state of the interface is up.
IPv6 Address	IPv6 address of the interface. • If multiple global unicast addresses are configured, this field displays the lowest address. • If no global unicast address is configured, this field displays the link-local address. • If no address is configured, this field displays **Unassigned**.

display ipv6 interface prefix

Use **display ipv6 interface prefix** to display IPv6 prefix information for an interface.

Syntax

display ipv6 interface *interface-type interface-number* **prefix**

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Examples

Display IPv6 prefix information for GigabitEthernet 1/0/1.

```
<Sysname> display ipv6 interface gigabitethernet 1/0/1prefix
Prefix: 1001::/65                                  Origin: ADDRESS
Age:    -                                           Flag:   AL
Lifetime(Valid/Preferred): 2592000/604800
```

```
Prefix: 2001::/64                                   Origin: STATIC
Age:    -                                            Flag:   L
Lifetime(Valid/Preferred): 3000/2000

Prefix: 3001::/64                                   Origin: RA
Age:    600                                          Flag:   A
Lifetime(Valid/Preferred): -
```

Table 5 Command output

Filed	Description
Prefix	IPv6 address prefix.
Origin	How the prefix is generated: • **STATIC**—Manually configured by using the **ipv6 nd ra prefix** command. • **RA**—Advertised in RA messages after stateless autoconfiguration is enabled. • **ADDRESS**—Generated by a manually configured address.
Age	Aging time in seconds. If the prefix does not age out, this field displays a hyphen (-).
Flag	Flags carried in RA messages. If no flags are available, this field displays a hyphen (-). • **L**—The address with the prefix is directly reachable on the link. • **A**—The prefix is used for stateless autoconfiguration.
Lifetime	Lifetime in seconds advertised in RA messages. If the prefix does not need to be advertised, this field displays a hyphen (-). • **Valid**—Valid lifetime of the prefix. • **Preferred**—Preferred lifetime of the prefix.

Related commands

ipv6 nd ra prefix

display ipv6 neighbors

Use **display ipv6 neighbors** to display IPv6 neighbor information.

Syntax

display ipv6 neighbors { { *ipv6-address* | **all** | **dynamic** | **static** } [**slot** *slot-number*] | **interface** *interface-type interface-number* | **vlan** *vlan-id* } [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ipv6-address: Specifies the IPv6 address of a neighbor whose information is displayed.

all: Displays information about all neighbors, including neighbors acquired dynamically and configured statically on the public network and all private networks.

dynamic: Displays information about all neighbors acquired dynamically.

static: Displays information about all neighbors configured statically.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv6 neighbor information for all member devices.

interface *interface-type interface-number*: Specifies an interface by its type and number.

vlan *vlan-id*: Displays information about neighbors in the specified VLAN. The value range for VLAN ID is 1 to 4094.

verbose: Displays detailed neighbor information.

Examples

Display all neighbor information.

```
<Sysname> display ipv6 neighbors all
Type: S-Static   D-Dynamic   O-Openflow    R-Rule   IS-Invalid static
IPv6 address            MAC address   VID  Interface         State T  Age
FE80::200:5EFF:FE32:B800  0000-5e32-b800 --   GE1/0/1           REACH S  --
```

Display detailed information about all neighbors.

```
<Sysname> display ipv6 neighbors all verbose
IPv6 address : FE80::200:5EFF:FE32:B800
MAC address  : 0000-5e32-b800          Type  : Static
State       : REACH                 Age   : --
Interface    : GE1/0/1               VID   : --
VPN instance : vpn1
Nickname     : 0x0
```

Table 6 Command output

Field	Description
IPv6 address	IPv6 address of the neighbor.
MAC address	MAC address of the neighbor.
VID	VLAN or virtual switch instance (VSI) to which the interface connected to a neighbor belongs.
Interface	Interface connected to the neighbor.
State	State of the neighbor: • **INCMP**—The address is being resolved. The link layer address of the neighbor is unknown. • **REACH**—The neighbor is reachable. • **STALE**—Whether the neighbor is reachable is unknown. The device does not verify the reachability any longer unless data is sent to the neighbor. • **DELAY**—Whether the neighbor is reachable is unknown. The device sends an NS message after a delay. • **PROBE**—Whether the neighbor is reachable is unknown. The device sends an NS message to verify the reachability of the neighbor.
Type	Neighbor information type: • **Static**—Statically configured. • **Dynamic**—Dynamically obtained. • **Openflow**—Learned from the OpenFlow module. This field is not supported in the

Field	Description
	current software version. • **Rule**—Learned from IPoE or Portal module. • **Invalid static**—Invalid static entries.
Age	A hyphen (-) indicates a static entry. For a dynamic entry, this field displays the elapsed time in seconds. If the neighbor is never reachable, this field displays a pound sign (#).
VPN instance	Name of a VPN instance. If no VPN instance is configured, this field displays a hyphen (-).
Nickname	This field is not supported in the current software version. Nickname of a neighbor entry. The name is a string of four hexadecimal numbers, such as 012a.

Related commands

ipv6 neighbor

reset ipv6 neighbors

display ipv6 neighbors count

Use **display ipv6 neighbors count** to display the number of neighbor entries.

Syntax

display ipv6 neighbors { { **all** | **dynamic** | **static** } [**slot** *slot-number*] | **interface** *interface-type interface-number* | **vlan** *vlan-id* } **count**

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

all: Displays the total number of all neighbor entries, including neighbor entries created dynamically and configured statically.

dynamic: Displays the total number of neighbor entries created dynamically.

static: Displays the total number of neighbor entries configured statically.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the number of neighbor entries for all member devices.

interface *interface-type interface-number*: Specifies an interface by its type and number.

vlan *vlan-id*: Displays the total number of neighbor entries in the specified VLAN. The value range for VLAN ID is 1 to 4094.

Examples

Display the total number of neighbor entries created dynamically.

```
<Sysname> display ipv6 neighbors dynamic count
 Total number of dynamic entries: 2
```

display ipv6 neighbors vpn-instance

Use **display ipv6 neighbors vpn-instance** to display neighbor information about a VPN instance.

Syntax

display ipv6 neighbors vpn-instance *vpn-instance-name* [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance-name: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. The VPN instance must already exist.

count: Displays the total number of neighbor entries in the specified VPN instance.

Examples

Display neighbor information about the VPN instance **vpn1**.

```
<Sysname> display ipv6 neighbors vpn-instance vpn1
Type: S-Static   D-Dynamic   O-Openflow    R-Rule   IS-Invalid static
IPv6 address            MAC address   VID  Interface         State T  Age
FE80::200:5EFF:FE32:B800  0000-5e32-b800 --   GE1/0/1           REACH IS --
```

Table 7 Command output

Field	Description
IPv6 address	IPv6 address of a neighbor.
MAC address	MAC address of a neighbor.
VID	VLAN to which the interface connected to a neighbor belongs.
Interface	Interface connected to a neighbor.
State	Neighbor state: • **INCMP**—The address is being resolved. The link layer address of the neighbor is unknown. • **REACH**—The neighbor is reachable. • **STALE**—Whether the neighbor is reachable is unknown. The device does not verify the reachability any longer unless data is sent to the neighbor. • **DELAY**—Whether the neighbor is reachable is unknown. The device sends an NS message after a delay. • **PROBE**—Whether the neighbor is reachable is unknown. The device sends an NS message to verify the reachability of the neighbor.
T	Neighbor information type: • **Static**—Statically configured.

Field	Description
	• **Dynamic**—Dynamically obtained. • **Openflow**—Learned from the OpenFlow module. This type is not supported in the current software version. • **Rule**—Learned from the IPoE or portal module. • **Invalid static**—Invalid static entry.
Age	A hyphen (-) indicates a static entry. For a dynamic entry, this field displays the elapsed time in seconds. If the neighbor is never reachable, this field displays a pound sign (#).

display ipv6 pathmtu

Use the **display ipv6 pathmtu** command to display IPv6 Path MTU information.

Syntax

display ipv6 pathmtu [**vpn-instance** *vpn-instance-name*] { *ipv6-address* | { **all** | **dynamic** | **static** } [**count**] }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays IPv6 Path MTU information about the public network.

ipv6-address: Specifies the destination IPv6 address for which the Path MTU information is to be displayed.

all: Displays all Path MTU information for the public network.

dynamic: Displays all dynamic Path MTU information.

static: Displays all static Path MTU information.

count: Displays the total number of Path MTU entries.

Examples

Display all Path MTU information.

```
<Sysname> display ipv6 pathmtu all
IPv6 destination address             PathMTU   Age   Type
1:2::3:2                             1800      -     Static
1:2::4:2                             1400      10    Dynamic
1:2::5:2                             1280      10    Dynamic
```

Displays the total number of Path MTU entries.

```
<Sysname> display ipv6 pathmtu all count
Total number of entries: 3
```

Table 8 Command output

Field	Description
PathMTU	Path MTU value on the network path to an IPv6 address.
Age	Time for a Path MTU to live. For a static Path MTU, this field displays a hyphen (-).
Type	Path MTU type: • **Dynamic**—Dynamically negotiated. • **Static**—Statically configured.
Total number of entries	Total number of Path MTU entries.

Related commands

ipv6 pathmtu

reset ipv6 pathmtu

display ipv6 prefix

Use **display ipv6 prefix** to display information about IPv6 prefixes, including dynamic and static prefixes.

Syntax

display ipv6 prefix [*prefix-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

prefix-number: Specifies the ID of an IPv6 prefix, in the range of 1 to 1024. If you do not specify an IPv6 prefix ID, this command displays information about all IPv6 prefixes.

Usage guidelines

A static IPv6 prefix is configured by using the **ipv6 prefix** command.

A dynamic IPv6 prefix is obtained from the DHCPv6 server, and its prefix ID is configured by using the **ipv6 dhcp client pd** command. For more information about prefix generation, see DHCPv6 client configuration in *Layer 3—IP Services Configuration Guide*.

Examples

Display information about all IPv6 prefixes.

```
<Sysname> display ipv6 prefix
Number  Prefix                                  Type
1       1::/16                                  Static
2       11:77::/32                              Dynamic
```

Display information about the IPv6 prefix with prefix ID 1.

```
<Sysname> display ipv6 prefix 1
Number: 1
Type  : Dynamic
Prefix: ABCD:77D8::/32
Preferred lifetime 90 sec, valid lifetime 120 sec
```

Table 9 Command output

Field	Description
Number	Prefix ID.
Type	Prefix type: • **Static**—Static IPv6 prefix. • **Dynamic**—Dynamic IPv6 prefix.
Prefix	Prefix and its length. If no prefix is obtained, this field displays **Not-available**.
Preferred lifetime 90 sec	Preferred lifetime in seconds. For a static IPv6 prefix, this field is not displayed.
valid lifetime 120 sec	Valid lifetime in seconds. For a static IPv6 prefix, this field is not displayed.

Related commands

ipv6 dhcp client pd

ipv6 prefix

display ipv6 rawip

Use **display ipv6 rawip** to display brief information about IPv6 RawIP connections.

Syntax

display ipv6 rawip [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays brief information about IPv6 RawIP connections for all member devices.

Examples

Display brief information about IPv6 RawIP connections.

```
<Sysname> display ipv6 rawip
Local Addr          Foreign Addr       Protocol Slot  PCB
2001:2002:2003:2    3001:3002:3003:3   58       1     0x0000000000000009
004:2005:2006:20    004:3005:3006:30
07:2008             07:3008
```

```
2002::100           2002::138          58       1      0x0000000000000008
::                  ::                 58       1      0x0000000000000002
```

Table 10 Command output

Field	Description
Local Addr	Local IPv6 address.
Foreign Addr	Peer IPv6 address.
Protocol	Protocol number.
PCB	PCB index.

display ipv6 rawip verbose

Use **display ipv6 rawip verbose** to display detailed information about IPv6 RawIP connections.

Syntax

display ipv6 rawip verbose [**slot** *slot-number* [**pcb** *pcb-index*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays detailed information about IPv6 RawIP connections for all member devices.

pcb *pcb-index*: Displays detailed information about IPv6 RawIP connections of the specified PCB. The value range for the *pcb-index* argument is 1 to 16.

Examples

Display detailed information about an IPv6 RawIP connection.

```
<Sysname> display ipv6 rawip verbose
Total RawIP socket number: 1

 Connection info: src = ::, dst = ::
 Location: slot: 1
 Creator: vrrpd[894]
 State: N/A
 Options: N/A
 Error: 0
 Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 9216 / 1 / 0 / N/A
 Sending buffer(cc/hiwat/lowat/state): 0 / 9216 / 512 / N/A
 Type: 3
```

```
Protocol: 58
Inpcb flags: N/A
Inpcb extflag: N/A
Inpcb vflag: INP_IPV6
Hop limit: 255 (minimum hop limit: 0)
Send VRF: 0xffff
Receive VRF: 0xffff
```

Table 11 Command output

Field	Description
Total RawIP socket number	Total number of IPv6 RawIP sockets.
Connection info	Connection information, including the source and destination IPv6 addresses.
Location	Socket location.
Creator	Task name of the socket. The process number is in the square brackets.
State	Socket state: • **NOFDREF**—The user has closed the connection. • **ISCONNECTED**—The connection has been established. • **ISCONNECTING**—The connection is being established. • **ISDISCONNECTING**—The connection is being interrupted. • **ASYNC**—Asynchronous mode. • **ISDISCONNECTED**—The connection has been terminated. • **ISSMOOTHING**—Cross-card data smoothing is in progress. • **CANBIND**—The socket supports the bind operation. • **PROTOREF**—Indicates strong protocol reference. • **ISPCBSYNCING**—Cross-card PCB synchronization is in progress • **N/A**—None of above state.
Options	Socket options: • **SO_DEBUG**—Records socket debugging information. • **SO_ACCEPTCONN**—Enables the server to listen connection requests. • **SO_REUSEADDR**—Allows the local address reuse. • **SO_KEEPALIVE**—Requires the protocol to test whether the connection is still alive. • **SO_DONTROUTE**—Bypasses the routing table query for outgoing packets because the destination is in a directly connected network. • **SO_BROADCAST**—Supports broadcast packets. • **SO_LINGER**—Closes the socket. The system can still send remaining data in the socket send buffer. • **SO_OOBINLINE**—Stores the out-of-band data in the input queue. • **SO_REUSEPORT**—Allows the local port reuse. • **SO_TIMESTAMP**—Records the timestamps of the input packets, accurate to milliseconds. This option is applicable to protocols that are not connection orientated. • **SO_NOSIGPIPE**—Disables the socket from sending data. As a result, a sigpipe cannot be established when a return failure occurs. • **SO_TIMESTAMPNS**—Has a similar function with the timestamp, accurate to nanoseconds. • **SO_KEEPALIVETIME**—Sets a keepalive time. This option is supported in TCP. • **SO_FILTER**—Supports setting the packet filter criterion. This option

Field	Description
	is available for OSI Socket and RawIP. • **SO_SEQPACKET**—Preserves the boundaries of packets sent to the socket buffer. • **SO_FILLTWAMPTIME**—Sets the timestamp for TWAMP. • **SO_LOCAL**—Local socket option. • **SO_NBMAADDR**—Obtains the remote NBMA address of the ADVPN tunnel. • **SO_DONTDELIVER**—Do not deliver the data to the application. • **N/A**—No options are set.
Error	Error code.

Receiving buffer(cc/hiwat/lowat/drop/state)	Displays receive buffer information in the following order:
	• **cc**—Used space.
	• **hiwat**—Maximum space.
	• **lowat**—Minimum space.
	• **drop**—Number of dropped packets.
	• **state**—Buffer state:
	  ○ **CANTSENDMORE**—Unable to send data to the peer.
	  ○ **CANTRCVMORE**—Unable to receive data from the peer.
	  ○ **RCVATMARK**—Receiving tag.
	  ○ **N/A**—None of the above states.

Sending buffer(cc/hiwat/lowat/state)	Displays send buffer information in the following order:
	• **cc**—Used space.
	• **hiwat**—Maximum space.
	• **lowat**—Minimum space.
	• **state**—Buffer state:
	  ○ **CANTSENDMORE**—Unable to send data to the peer.
	  ○ **CANTRCVMORE**—Unable to receive data from the peer.
	  ○ **RCVATMARK**—Receiving tag.
	  ○ **N/A**—None of the above states.

Type	Socket type: • **1**—**SOCK_STREAM**. This socket uses TCP to provide reliable transmission of byte streams. • **2**—**SOCK_DGRAM**. This socket uses UDP to provide datagram transmission. • **3**—**SOCK_RAW**. This socket allows an application to change the next upper-layer protocol header. • **N/A**—None of the above types.
Protocol	Number of protocol using the socket. 58 represents ICMP.
Inpcb flags	Flags in the Internet PCB: • **INP_RECVOPTS**—Receives IPv6 options. • **INP_RECVRETOPTS**—Receives replied IPv6 options. • **INP_RECVDSTADDR**—Receives destination IPv6 address. • **INP_HDRINCL**—Provides the entire IPv6 header. • **INP_REUSEADDR**—Reuses the IPv6 address. • **INP_REUSEPORT**—Reuses the port number. • **INP_ANONPORT**—Port number not specified. • **INP_PROTOCOL_PACKET**—Identifies a protocol packet. • **INP_RCVVLANID**—Receives the VLAN ID of the packet. Only UDP and RawIP support this flag. • **IN6P_IPV6_V6ONLY**—Only supports IPv6 protocol stack.

Field	Description
	• **IN6P_PKTINFO**—Receives the source IPv6 address and input interface of the packet. • **IN6P_HOPLIMIT**—Receives the hop limit. • **IN6P_HOPOPTS**—Receives the hop-by-hop options extension header. • **IN6P_DSTOPTS**—Receives the destination options extension header. • **IN6P_RTHDR**—Receives the routing extension header. • **IN6P_RTHDRDSTOPTS**—Receives the destination options extension header preceding the routing extension header. • **IN6P_TCLASS**—Receives the traffic class of the packet. • **IN6P_AUTOFLOWLABEL**—Attaches a flow label automatically. • **IN6P_RFC2292**—Uses the API specified in RFC 2292. • **IN6P_MTU**—Discovers differences in the MTU size of every link along a given data path. TCP does not support this flag. • **INP_RCVMACADDR**—Receives the MAC address of the frame. • **INP_USEICMPSRC**—Uses the specified IPv6 address as the source IPv6 address for outgoing ICMP packets. • **INP_SYNCPCB**—Waits until Internet PCB is synchronized. • **INP_LOCAL**—Preferentially matches the INPCB with this flag on the same card. • **N/A**—None of the above flags.
Inpcb extflag	Extension flags in the Internet PCB: • **INP_EXTRCVPVCIDX**—Records the PVC index of the received packet. • **INP_RCVPWID**—Records the PW ID of the received packet. • **INP_EXTRCVICMPERR**—Receives an ICMP error packet. • **INP_EXTFILTER**—Filters the contents in the received packets. • **INP_EXTDONTDROP**—Does not drop the received packet. • **INP_EXLISTEN**—Adds the INPCB carrying this flag to the listen hash table. • **INP_SELECTMATCHSRCBYFIB**—Uses the FIB table to select a matching source. • **INP_EXTPRIVATESOCKET**—Associates the INPCB with the NSR private socket. • **INP_EXLISTENNET**—Sets this flag when the connection information is added to the network segment linked list. • **N/A**—None of the above flags.
Inpcb vflag	IP version flag in the Internet PCB: • **INP_IPV4**—IPv4 protocol. • **INP_IPV6**—IPv6 protocol. • **INP_IPV6PROTO**—Creates an Internet PCB based on IPv6 protocol. • **INP_TIMEWAIT**—In **TIMEWAIT** state. • **INP_ONESBCAST**—Sends broadcast packets. • **INP_DROPPED**—Protocol dropped flag. • **INP_SOCKREF**—Strong socket reference. • **INP_DONTBLOCK**—Do not block synchronization of the Internet PCB. • **N/A**—None of the above flags.
Hop limit	Hop limit in the Internet PCB.
Send VRF	VRF from which packets are sent.

Field	Description
Receive VRF	VRF from which packets are received.

display ipv6 statistics

Use **display ipv6 statistics** to display IPv6 and ICMPv6 packet statistics.

Syntax

display ipv6 statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv6 and ICMPv6 packet statistics for all member devices.

Examples

Display IPv6 and ICMPv6 packet statistics.

```
<Sysname> display ipv6 statistics
  IPv6 statistics:

    Sent packets:
      Total:     0
        Sent locally:        0          Forwarded:            0
        Raw packets:         0          Discarded:            0
        Fragments:           0          Fragments failed:     0
        Routing failed:      0

    Received packets:
      Total:     0
        Received locally:    0          Hop limit exceeded:  0
        Fragments:           0          Reassembled:         0
        Reassembly failures:  0          Reassembly timeout:  0
        Format errors:       0          Option errors:       0
        Protocol errors:     0

  ICMPv6 statistics:

    Sent packets:
      Total:     0
        Unreachable:         0           Too big:             0
        Hop limit exceeded:  0           Reassembly timeouts: 0
```

```
    Parameter problems:   0
    Echo requests:        0          Echo replies:         0
    Neighbor solicits:    0          Neighbor adverts:     0
    Router solicits:      0          Router adverts:       0
    Redirects:            0          Router renumbering:   0
  Send failed:
    Rate limitation:      0          Other errors:         0

Received packets:
  Total:     0
    Checksum errors:      0          Too short:            0
    Bad codes:            0
    Unreachable:          0          Too big:              0
    Hop limit exceeded:   0          Reassembly timeouts:  0
    Parameter problems:   0          Unknown error types:  0
    Echo requests:        0          Echo replies:         0
    Neighbor solicits:    0          Neighbor adverts:     0
    Router solicits:      0          Router adverts:       0
    Redirects:            0          Router renumbering:   0
    Unknown info types:   0
  Deliver failed:
    Bad length:           0
```

Table 12 Command output

Field	Description
IPv6 statistics:	IPv6 packet statistics.
Sent packets: Total: Sent locally: Forwarded: Raw packets: Discarded: Fragments: Fragments failed: Routing failed:	Statistics for sent IPv6 packets: • **Total**—Total number of packets that have been locally sent and forwarded. • **Sent locally**—Number of locally sent packets. • **Forwarded**—Number of forwarded packets. • **Raw packets**—Number of packets sent by using a raw socket. • **Discarded**—Number of discarded packets. • **Fragments**—Number of sent fragments. • **Fragments failed**—Number of fragments that were failed to send. • **Routing failed**—Number of packets with routing failures.
Received packets: Total: Received locally: Hop limit exceeded: Fragments: Reassembled: Reassembly failures: Reassembly timeout: Format errors:	Statistics for received IPv6 packets: • **Total**—Total number of received packets. • **Received locally**—Number of received packets that are destined for the device. • **Hop limit exceeded**—Number of packets with hop limit exceeded. • **Fragments**—Number of received fragments. • **Reassembled**—Number of reassembled packets. • **Reassembly failures**—Number of packets with reassembly failures.

Option errors: Protocol errors:	• **Reassembly timeout**—Number of packets with reassembly timed out. • **Format errors**—Number of packets with format errors. • **Option errors**—Number of packets with option errors. • **Protocol errors**—Number of packets with protocol errors.
ICMPv6 statistics:	ICMPv6 message statistics.
Sent packets: Total: Unreached: Too big: Hop limit exceeded: Reassembly timeouts: Parameter problems: Echo requests: Echo replies: Neighbor solicits: Neighbor adverts: Router solicits: Router adverts: Redirects: Router renumbering Sent failed: Rate limitation: Other errors:	Statistics for sent ICMPv6 messages: • **Total**—Total number of sent messages. • **Unreached**—Number of Destination Unreachable messages. • **Too big**—Number of Packet Too Big messages. • **Hop limit exceeded**—Number of Hop Limit Exceeded messages. • **Reassembly timeouts**—Number of Fragment Reassembly Time Exceeded messages. • **Parameter problems**—Number of Parameter Problem messages. • **Echo requests**—Number of Echo Requests. • **Echo replies**—Number of Echo Replies. • **Neighbor solicits**—Number of Neighbor Solicitation messages. • **Neighbor adverts**—Number of Neighbor Advertisement messages. • **Router solicits**—Number of Router Solicitation messages. • **Router adverts**—Number of Router Advertisement messages. • **Redirects**—Number of Redirect messages. • **Router renumbering**—Number of Router Renumbering messages. This value is not supported in the current software version. • **Sent failed**—Number of messages that were failed to send locally. • **Rate limitation**—Number of unsent messages because of rate limiting. • **Other errors**—Number of messages with other errors.
Received packets: Total: Checksum errors: Too short: Bad codes: Unreachable: Too big: Hop limit exceeded: Reassembly timeouts: Parameter problems: Unknown error types: Echo requests:	Statistics for received ICMPv6 messages: • **Total**—Total number of received messages. • **Checksum errors**—Number of messages with checksum errors. • **Too short**—Number of messages with a too short length. • **Bad codes**—Number of messages with error codes. • **Unreached**—Number of Destination Unreachable messages. • **Too big**—Number of Packet Too Big messages. • **Hop limit exceeded**—Number of Hop Limit Exceeded messages.

Echo replies: Neighbor solicits: Neighbor adverts: Router solicits: Router adverts: Redirects: Router renumbering: Unknown info types: Deliver failed: Bad length:	• **Reassembly timeouts**—Number of Fragment Reassembly Time Exceeded messages. • **Parameter problems**—Number of Parameter Problem messages. • **Unknown error types**—Number of messages with unknown error types. • **Echo requests**—Number of Echo Requests. • **Echo replies**—Number of Echo Replies. • **Neighbor solicits**—Number of Neighbor Solicitation messages. • **Neighbor adverts**—Number of Neighbor Advertisement messages. • **Router solicits**—Number of Router Solicitation messages. • **Router adverts**—Number of Router Advertisement messages. • **Redirects**—Number of Redirect messages. **Router renumbering**—Number of Router Renumbering messages. This field is not supported in the current software version. • **Unknown info types**—Number of messages with unknown information types. • **Deliver failed**—Number of messages with local delivery failures. • **Bad length**—Number of messages with error length.

Related commands

`reset ipv6 statistics`

display ipv6 tcp

Use **`display ipv6 tcp`** to display brief information about IPv6 TCP connections.

Syntax

`display ipv6 tcp` [**`slot`** *`slot-number`*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

`slot` *`slot-number`*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays brief information about IPv6 TCP connections for all member devices.

Examples

Display brief information about IPv6 TCP connections.

```
<Sysname> display ipv6 tcp
*: TCP MD5 Connection
 LAddr->port        FAddr->port      State       Slot  PCB
*2001:2002:2003:2   3001:3002:3003:3 ESTABLISHED 1    0x000000000000c387
004:2005:2006:20    004:3005:3006:30
07:2008->1200       07:3008->1200
2001::1->23         2001::5->1284    ESTABLISHED 1    0x0000000000000008
2003::1->25         2001::2->1283    LISTEN      1    0x0000000000000009
```

Table 13 Command output

Field	Description
*	Indicates that the TCP connection uses MD5 authentication.
LAddr->port	Local IPv6 address and port number.
FAddr->port	Peer IPv6 address and port number.
State	IPv6 TCP connection state: • **CLOSED**—The server receives a disconnection request's reply from the client. • **LISTEN**—The server is waiting for connection requests. • **SYN_SENT**—The client is waiting for the server to reply to the connection request. • **SYN_RCVD**—The server receives a connection request. • **ESTABLISHED**—The server and client have established connections and can transmit data bidirectionally. • **CLOSE_WAIT**—The server receives a disconnection request from the client. • **FIN_WAIT_1**—The client is waiting for the server to reply to a disconnection request. • **CLOSING**—The server and client are waiting for peer's disconnection reply when receiving disconnection requests from each other. • **LAST_ACK**—The server is waiting for the client to reply to a disconnection request. • **FIN_WAIT_2**—The client receives a disconnection reply from the server. • **TIME_WAIT**—The client receives a disconnection request from the server.
PCB	PCB index.

display ipv6 tcp verbose

Use **display ipv6 tcp verbose** to display detailed information about IPv6 TCP connections.

Syntax

display ipv6 tcp verbose [**slot** *slot-number* [**pcb** *pcb-index*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays detailed information about IPv6 TCP connections for all member devices.

pcb *pcb-index*: Displays detailed information about IPv6 TCP connections of the specified PCB. The value range for the *pcb-index* argument is 1 to 16.

Examples

Display detailed information about an IPv6 TCP connection.

```
<Sysname> display ipv6 tcp verbose
TCP inpcb number: 1(tcpcb number: 1)

 Connection info: src = 2001::1->179 ,  dst = 2001::2->4181
 Location: Slot:2
 NSR standby: N/A
 Creator: bgpd[199]
 State: ISCONNECTED
 Options: N/A
 Error: 0
 Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 65536 / 1 / 0 / N/A
 Sending buffer(cc/hiwat/lowat/state): 0 / 65536 / 512 / N/A
 Type: 1
 Protocol: 6
 Inpcb flags: N/A
 Inpcb extflag: N/A
 Inpcb vflag: INP_IPV6
 Hop limit: 255 (minimum hop limit: 0)
 Connection state: ESTABLISHED
 TCP options: TF_REQ_SCALE TF_REQ_TSTMP TF_SACK_PERMIT TF_NSR
 NSR state: READY(M)
 Send VRF: 0x0
 Receive VRF: 0x0
```

Table 14 Command output

Field	Description
TCP inpcb number	Number of IPv6 TCP Internet PCBs.
Connection info	Connection information, including source IPv6 address, source port number, destination IPv6 address, and destination port number.
Location	Socket location.
tcpcb number	Number of IPv6 TCP PCBs (excluding PCBs of TCP in TIME_WAIT state).
NSR standby	ID of the IRF member device and number of the slot where the NSR standby card resides. This field displays **N/A** if no NSR standby card is present.
Creator	Task name of the socket. The process number is in the square brackets.
State	Socket state:

Field	Description
	• **NOFDREF**—The user has closed the connection. • **ISCONNECTED**—The connection has been established. • **ISCONNECTING**—The connection is being established. • **ISDISCONNECTING**—The connection is being interrupted. • **ASYNC**—Asynchronous mode. • **ISDISCONNECTED**—The connection has been terminated. • **ISSMOOTHING**—Cross-card data smoothing is in progress. • **CANBIND**—The socket supports the bind operation. • **PROTOREF**—Indicates strong protocol reference. • **ISPCBSYNCING**—Cross-card PCB synchronization is in progress • **N/A**—None of above state.
Options	Socket options: • **SO_DEBUG**—Records socket debugging information. • **SO_ACCEPTCONN**—Enables the server to listen connection requests. • **SO_REUSEADDR**—Allows the local address reuse. • **SO_KEEPALIVE**—Requires the protocol to test whether the connection is still alive. • **SO_DONTROUTE**—Bypasses the routing table query for outgoing packets because the destination is in a directly connected network. • **SO_BROADCAST**—Supports broadcast packets. • **SO_LINGER**—Closes the socket. The system can still send remaining data in the socket send buffer. • **SO_OOBINLINE**—Stores the out-of-band data in the input queue. • **SO_REUSEPORT**—Allows the local port reuse. • **SO_TIMESTAMP**—Records the timestamps of the input packets, accurate to milliseconds. This option is applicable to protocols that are not connection orientated. • **SO_NOSIGPIPE**—Disables the socket from sending data. As a result, a sigpipe cannot be established when a return failure occurs. • **SO_TIMESTAMPNS**—Has a similar function with the timestamp, accurate to nanoseconds. • **SO_KEEPALIVETIME**—Sets a keepalive time. This option is supported in TCP. • **SO_FILTER**—Supports setting the packet filter criterion. This option is available for OSI Socket and RawIP. • **SO_SEQPACKET**—Preserves the boundaries of packets sent to the socket buffer. • **SO_FILLTWAMPTIME**—Sets the timestamp for TWAMP. • **SO_LOCAL**—Local socket option. • **SO_NBMAADDR**—Obtains the remote NBMA address of the ADVPN tunnel. • **SO_DONTDELIVER**—Do not deliver the data to the application. • **N/A**—No options are set.
Error	Error code.
Receiving buffer(cc/hiwat/lowat/drop/state)	Displays receive buffer information in the following order: • **cc**—Used space. • **hiwat**—Maximum space. • **lowat**—Minimum space. • **drop**—Number of dropped packets. • **state**—Buffer state. Buffer states include the following:

Field	Description
	• **CANTSENDMORE**—Unable to send data to the peer. • **CANTRCVMORE**—Unable to receive data from the peer. • **RCVATMARK**—Receiving tag. • **N/A**—None of the above states.

Sending buffer(cc/hiwat/lowat/state)	Displays send buffer information in the following order:
	• **cc**—Used space.
	• **hiwat**—Maximum space.
	• **lowat**—Minimum space.
	• **state**—Buffer state:
	  ○ **CANTSENDMORE**—Unable to send data to the peer.
	  ○ **CANTRCVMORE**—Unable to receive data from the peer.
	  ○ **RCVATMARK**—Receiving tag.
	  ○ **N/A**—None of the above states.

Type	Socket type: • **1**—**SOCK_STREAM**. This socket uses TCP to provide reliable transmission of byte streams. • **2**—**SOCK_DGRAM**. This socket uses UDP to provide datagram transmission. • **3**—**SOCK_RAW**. This socket allows an application to change the next upper-layer protocol header. • **N/A**—None of the above types.
Protocol	Number of the protocol using the socket. 6 represents TCP.
Inpcb flags	Flags in the Internet PCB: • **INP_RECVOPTS**—Receives IPv6 options. • **INP_RECVRETOPTS**—Receives replied IPv6 options. • **INP_RECVDSTADDR**—Receives destination IPv6 address. • **INP_HDRINCL**—Provides the entire IPv6 header. • **INP_REUSEADDR**—Reuses the IPv6 address. • **INP_REUSEPORT**—Reuses the port number. • **INP_ANONPORT**—Port number not specified. • **INP_PROTOCOL_PACKET**—Identifies a protocol packet. • **INP_RCVVLANID**—Receives the VLAN ID of the packet. Only UDP and RawIP support this flag. • **IN6P_IPV6_V6ONLY**—Only supports IPv6 protocol stack. • **IN6P_PKTINFO**—Receives the source IPv6 address and input interface of the packet. • **IN6P_HOPLIMIT**—Receives the hop limit. • **IN6P_HOPOPTS**—Receives the hop-by-hop options extension header. • **IN6P_DSTOPTS**—Receives the destination options extension header. • **IN6P_RTHDR**—Receives the routing extension header. • **IN6P_RTHDRDSTOPTS**—Receives the destination options extension header preceding the routing extension header. • **IN6P_TCLASS**—Receives the traffic class of the packet. • **IN6P_AUTOFLOWLABEL**—Attaches a flow label automatically. • **IN6P_RFC2292**—Uses the API specified in RFC 2292. • **IN6P_MTU**—Discovers differences in the MTU size of every link along a given data path. TCP does not support this flag. • **INP_RCVMACADDR**—Receives the MAC address of the frame. • **INP_SYNCPCB**—Waits until Internet PCB is synchronized.

Field	Description
	• **INP_LOCAL**—Preferentially matches the INPCB with this flag on the same card. • **N/A**—None of the above flags.
Inpcb extflag	Extension flags in the Internet PCB: • **INP_EXTRCVPVCIDX**—Records the PVC index of the received packet. • **INP_RCVPWID**—Records the PW ID of the received packet. • **INP_EXTDONTDROP**—Does not drop the received packet. • **INP_EXLISTEN**—Listening socket. • **INP_EXTFILTER**—Filters the contents in the received packets. • **INP_SELECTMATCHSRCBYFIB**—Uses the FIB table to select a matching source. • **INP_EXTRCVICMPERR**—Receives an ICMP error packet. • **INP_EXTPRIVATESOCKET**—Associates the INPCB with the NSR private socket. • **INP_EXLISTENNET**—Sets this flag when the connection information is added to the network segment linked list. • **N/A**—None of the above flags.
Inpcb vflag	IP version flags in the Internet PCB: • **INP_IPV4**—IPv4 protocol. • **INP_IPV6**—IPv6 protocol. • **INP_IPV6PROTO**—Creates an Internet PCB based on IPv6 protocol. • **INP_TIMEWAIT**—In **TIMEWAIT** state. • **INP_ONESBCAST**—Sends broadcast packets. • **INP_DROPPED**—Protocol dropped flag. • **INP_SOCKREF**—Strong socket reference. • **INP_DONTBLOCK**—Do not block synchronization of the Internet PCB. • **N/A**—None of the above flags.
Hop limit	Hop limit in the Internet PCB.
Connection state	TCP connection state: • **CLOSED**—The server receives a disconnection request's reply from the client. • **LISTEN**—The server is waiting for connection requests. • **SYN_SENT**—The client is waiting for the server to reply to the connection request. • **SYN_RCVD**—The server receives a connection request. • **ESTABLISHED**—The server and client have established connections and can transmit data bidirectionally. • **CLOSE_WAIT**—The server receives a disconnection request from the client. • **FIN_WAIT_1**—The client is waiting for the server to reply to a disconnection request. • **CLOSING**—The server and client are waiting for peer's disconnection reply when receiving disconnection requests from each other. • **LAST_ACK**—The server is waiting for the client to reply to a disconnection request. • **FIN_WAIT_2**—The client receives a disconnection reply from the server. • **TIME_WAIT**—The client receives a disconnection request from the

Field	Description
	server.
TCP options	TCP options: • **TF_ACKNOW**—Immediately replies an ACK packet to the peer. • **TF_DELACK**—Delays sending ACK packets. • **TF_SENTFIN**—A FIN packet has been sent. • **TF_RCVD_SCALE**—Requests the receive window size scale factor. • **TF_RCVD_TSTMP**—A timestamp was received in the SYN packet. • **TF_NEEDSYN**—Sends a SYN packet. • **TF_NEEDFIN**—Sends a FIN packet. • **TF_MORETOCOME**—More data is to be added to the socket. • **TF_LQ_OVERFLOW**—The listening queue overflows. • **TF_LASTIDLE**—Idle connection. • **TF_RXWIN0SENT**—A reply with receive window size 0 was sent. • **TF_FASTRECOVERY**—Enters NewReno fast recovery mode. • **TF_WASFRECOVERY**—In NewReno fast recovery mode. • **TF_SIGNATURE**—MD5 signature. • **TF_FORCEDATA**—Forces to send one byte. • **TF_TSO**—TSO is enabled. • **TF_PMTU**—Supports RFC 1191. • **TF_PMTUD**—Starts Path MTU discovery. • **TF_PASSIVE_CONN**—Passive connection. • **TF_APP_SEND**—The application sends data. • **TF_NODELAY**—Disables the Nagle algorithm that buffers the sent data inside the TCP. • **TF_NOOPT**—No TCP options. • **TF_NOPUSH**—Forces TCP to delay sending any TCP data until a full sized segment is buffered in the TCP buffers. • **TF_NSR**—Enables TCP NSR. • **TF_REQ_SCALE**—Enables the TCP window scale option. • **TF_REQ_TSTMP**—Enables the time stamp option. • **TF_SACK_PERMIT**—Enables the TCP selective acknowledgement option. • **TF_ENHANCED_AUTH**—Enables the enhanced authentication option.
NSR state	NSR state of the TCP connection: • **CLOSED**—Closed (initial) state. • **CLOSING**—The connection is to be closed. • **ENABLED**—The connection backup is enabled. • **OPEN**—The connection synchronization has started. • **PENDING**—The connection backup is not ready. • **READY**—The connection backup is ready. • **SMOOTH**—The connection data is being smoothed. Between the parentheses is the role of the connection: • **M**—Main connection. • **S**—Standby connection.
Send VRF	VRF from which packets are sent.
Receive VRF	VRF from which packets are received.

display ipv6 tcp-proxy

Use **display ipv6 tcp-proxy** to display brief information about IPv6 TCP proxy.

Syntax

display ipv6 tcp-proxy slot *slot-number*

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID.

Examples

Display brief information about IPv6 TCP proxy.

```
<Sysname> display ipv6 tcp-proxy slot 1
LAddr->port          FAddr->port           State       Service type
2001::1->45          11:22:33:44->54602     ESTABLISHED LB
11:22:33:44->54602    2001::1->45           ESTABLISHED LB
```

Table 15 Command output

Field	Description
LAddr->port	Local IPv6 address and port number.
Faddr->port	Peer IPv6 address and port number.
State	IPv6 TCP connection state: • **CLOSED**—The server receives a disconnection request's reply from the client. • **LISTEN**—The server is waiting for connection requests. • **SYN_SENT**—The client is waiting for the server to reply to the connection request. • **SYN_RECEIVED**—The server receives a connection request. • **ESTABLISHED**—The server and client have established connections and can transmit data bidirectionally. • **CLOSE_WAIT**—The server receives a disconnection request from the client. • **FIN_WAIT_1**—The client is waiting for the server to reply to a disconnection request. • **CLOSING**—The server and client are waiting for peer's disconnection reply when receiving disconnection requests from each other. • **LAST_ACK**—The server is waiting for the client to reply to a disconnection request. • **FIN_WAIT_2**—The client receives a disconnection reply from the server. • **TIME_WAIT**—The client receives a disconnection request from the server.
Service type	Type of services that the IPv6 TCP proxy is used for: • **NONE**—No service type is specified. • **LB**—Load balancing services.

Field	Description
	• **SSL VPN**—SSL VPN services. • **APPPROXY**—Application proxy services.

display ipv6 tcp-proxy port-info

Use **display ipv6 tcp-proxy port-info** to display the usage of non-well known ports for IPv6 TCP proxy.

Syntax

display ipv6 tcp-proxy port-info slot *slot-number*

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays non-well known port usage for all member devices.

Usage guidelines

The TCP ports are divided into well-known ports (port numbers from 0 through 1023) and non-well known ports (port numbers from 1024 through 65535).

- Well known ports are for certain services, for example, port 23 for Telnet service, ports 20 and 21 for FTP service, and port 80 for HTTP service.
- Non-well known ports are available for various services. You can use the **display ipv6 tcp-proxy port-info** command to display the usage of these ports.

Examples

Display the usage of non-well known ports for IPv6 TCP proxy.

```
<Sysname> display ipv6 tcp-proxy port-info slot 1
Index  Range          State
16     [1024, 1087]    USABLE
17     [1088, 1151]    USABLE
18     [1152, 1215]    USABLE
19     [1216, 1279]    USABLE
20     [1280, 1343]    USABLE
...
1020   [65280, 65343]   USABLE
1021   [65344, 65407]   USABLE
1022   [65408, 65471]   USABLE
1023   [65472, 65535]   USABLE
```

Table 16 Command output

Field	Description
Index	Index of the port range.
Range	Start port number and end port number.
State	State of the port range: • **USABLE**—The ports are assignable. • **ASSIGNED**—Some ports are dynamically assigned and some ports are not. • **ALLASSIGNED**—All ports are dynamically assigned. The assigned ports can be reclaimed. • **TO RECLAIM**—Some ports are statically assigned. The assigned ports can be reclaimed. • **RESERVED**—The ports are reserved. The reserved ports cannot be dynamically assigned.

display ipv6 udp

Use **display ipv6 udp** to display brief information about IPv6 UDP connections.

Syntax

display ipv6 udp [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays brief information about IPv6 UDP connections for all member devices.

Examples

Displays brief information about IPv6 UDP connections.

```
<Sysname> display ipv6 udp
 LAddr->port        FAddr->port        Slot  PCB
 2001:2002:2003:2   3001:3002:3003:3   1     0x000000000000c387
 004:2005:2006:20   004:3005:3006:30
 07:2008->1200      07:3008->1200
 2001::1->23        2001::5->1284      1     0x0000000000000008
 2003::1->25        2001::2->1283      1     0x0000000000000009
```

Table 17 Command output

Field	Description
LAddr->port	Local IPv6 address and port number.

Field	Description
FAddr->port	Peer IPv6 address and port number.
PCB	PCB index.

display ipv6 udp verbose

Use **display ipv6 udp verbose** to display detailed information about IPv6 UDP connections.

Syntax

display ipv6 udp verbose [**slot** *slot-number* [**pcb** *pcb-index*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays detailed information about IPv6 UDP connections for all member devices.

pcb *pcb-index*: Displays detailed information about IPv6 UDP connections of the specified PCB. The value range for the *pcb-index* argument is 1 to 16.

Examples

Display detailed information about an IPv6 UDP connection.

```
<Sysname> display ipv6 udp verbose
Total UDP socket number: 1

 Connection info: src = ::->69, dst = ::->0
 Location: slot: 1
 Creator: sock_test_mips[250]
 State: N/A
 Options: N/A
 Error: 0
 Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 41600 / 1 / 0 / N/A
 Sending buffer(cc/hiwat/lowat/state): 0 / 9216 / 512 / N/A
 Type: 2
 Protocol: 17
 Inpcb flags: N/A
 Inpcb extflag: N/A
 Inpcb vflag: INP_IPV6
 Hop limit: 255 (minimum hop limit: 0)
 Send VRF: 0xffff
 Receive VRF: 0xffff
```

Table 18 Command output

Field	Description
Total UDP socket number	Total number of IPv6 UDP sockets.
Connection info	Connection information, including source IPv6 address, source port number, destination IPv6 address, and destination port number.
Location	Socket location.
Creator	Task name of the socket. The progress number is in the square brackets.
State	Socket state: • **NOFDREF**—The user has closed the connection. • **ISCONNECTED**—The connection has been established. • **ISCONNECTING**—The connection is being established. • **ISDISCONNECTING**—The connection is being interrupted. • **ASYNC**—Asynchronous mode. • **ISDISCONNECTED**—The connection has been terminated. • **ISSMOOTHING**—Cross-card data smoothing is in progress. • **CANBIND**—The socket supports the bind operation. • **PROTOREF**—Indicates strong protocol reference. • **ISPCBSYNCING**—Cross-card PCB synchronization is in progress. • **N/A**—None of above state.
Options	Socket options: • **SO_DEBUG**—Records socket debugging information. • **SO_ACCEPTCONN**—Enables the server to listen connection requests. • **SO_REUSEADDR**—Allows the local address reuse. • **SO_KEEPALIVE**—Requires the protocol to test whether the connection is still alive. • **SO_DONTROUTE**—Bypasses the routing table query for outgoing packets because the destination is in a directly connected network. • **SO_BROADCAST**—Supports broadcast packets. • **SO_LINGER**—Closes the socket. The system can still send remaining data in the socket send buffer. • **SO_OOBINLINE**—Stores the out-of-band data in the input queue. • **SO_REUSEPORT**—Allows the local port reuse. • **SO_TIMESTAMP**—Records the timestamps of the input packets, accurate to milliseconds. This option is applicable to protocols that are not connection orientated. • **SO_NOSIGPIPE**—Disables the socket from sending data. As a result, a sigpipe cannot be established when a return failure occurs. • **SO_TIMESTAMPNS**—Has a similar function with the timestamp, accurate to nanoseconds. • **SO_KEEPALIVETIME**—Sets a keepalive time. This option is supported in TCP. • **SO_FILTER**—Supports setting the packet filter criterion. This option is available for OSI Socket and RawIP. • **SO_SEQPACKET**—Preserves the boundaries of packets sent to the socket buffer. • **SO_FILLTWAMPTIME**—Sets the timestamp for TWAMP. • **SO_LOCAL**—Local socket option. • **SO_NBMAADDR**—Obtains the remote NBMA address of the ADVPN tunnel. • **SO_DONTDELIVER**—Do not deliver the data to the application.

Field	Description
	• **N/A**—No options are set.
Error	Error code.

Receiving buffer(cc/hiwat/lowat/drop/state)	Displays receive buffer information in the following order:
	• **cc**—Used space.
	• **hiwat**—Maximum space.
	• **lowat**—Minimum space.
	• **drop**—Number of dropped packets.
	• **state**—Buffer state:
	  ○ **CANTSENDMORE**—Unable to send data to the peer.
	  ○ **CANTRCVMORE**—Unable to receive data from the peer.
	  ○ **RCVATMARK**—Receiving tag.
	  ○ **N/A**—None of the above states.

Sending buffer(cc/hiwat/lowat/state)	Displays send buffer information in the following order:
	• **cc**—Used space.
	• **hiwat**—Maximum space.
	• **lowat**—Minimum space.
	• **state**—Buffer state:
	  ○ **CANTSENDMORE**—Unable to send data to the peer.
	  ○ **CANTRCVMORE**—Unable to receive data from the peer.
	  ○ **RCVATMARK**—Receiving tag.
	  ○ **N/A**—None of the above states.

Type	Socket type: • **1**—**SOCK_STREAM**. This socket uses TCP to provide reliable transmission of byte streams. • **2**—**SOCK_DGRAM**. This socket uses UDP to provide datagram transmission. • **3**—**SOCK_RAW**. This socket allows an application to change the next upper-layer protocol header. • **N/A**—None of the above types.
Protocol	Number of the protocol using the socket. 17 represents UDP.
Inpcb flags	Flags in the Internet PCB: • **INP_RECVOPTS**—Receives IPv6 options. • **INP_RECVRETOPTS**—Receives replied IPv6 options. • **INP_RECVDSTADDR**—Receives destination IPv6 address. • **INP_HDRINCL**—Provides the entire IPv6 header. • **INP_REUSEADDR**—Reuses the IPv6 address. • **INP_REUSEPORT**—Reuses the port number. • **INP_ANONPORT**—Port number not specified. • **INP_PROTOCOL_PACKET**—Identifies a protocol packet. • **INP_RCVVLANID**—Receives the VLAN ID of the packet. Only UDP and RawIP support this flag. • **IN6P_IPV6_V6ONLY**—Only supports IPv6 protocol stack. • **IN6P_PKTINFO**—Receives the source IPv6 address and input interface of the packet. • **IN6P_HOPLIMIT**—Receives the hop limit. • **IN6P_HOPOPTS**—Receives the hop-by-hop options extension header. • **IN6P_DSTOPTS**—Receives the destination options extension header. • **IN6P_RTHDR**—Receives the routing extension header.

Field	Description
	• **IN6P_RTHDRDSTOPTS**—Receives the destination options extension header preceding the routing extension header. • **IN6P_TCLASS**—Receives the traffic class of the packet. • **IN6P_AUTOFLOWLABEL**—Attaches a flow label automatically. • **IN6P_RFC2292**—Uses the API specified in RFC 2292. • **IN6P_MTU**—Discovers differences in the MTU size of every link along a given data path. TCP does not support this flag. • **INP_RCVMACADDR**—Receives the MAC address of the frame. • **INP_SYNCPCB**—Waits until Internet PCB is synchronized. • **INP_LOCAL**—Preferentially matches the INPCB with this flag on the same card. • **N/A**—None of the above flags.
Inpcb extflag	Extension flags in the Internet PCB: • **INP_EXTRCVPVCIDX**—Records the PVC index of the received packet. • **INP_RCVPWID**—Records the PW ID of the received packet. • **INP_EXTDONTDROP**—Do not drop the received packet. • **INP_EXLISTEN**—Adds the INPCB carrying this flag to the listen hash table. • **INP_EXTFILTER**—Filters the contents in the received packets. • **INP_SELECTMATCHSRCBYFIB**—Uses the FIB table to select a matching source. • **INP_EXTRCVICMPERR**—Receives an ICMP error packet. • **INP_EXTPRIVATESOCKET**—Associates the INPCB with the NSR private socket. • **INP_EXLISTENNET**—Sets this flag when the connection information is added to the network segment linked list. • **N/A**—None of the above flags.
Inpcb vflag	IP version flags in the Internet PCB: • **INP_IPV4**—IPv4 protocol. • **INP_IPV6**—IPv6 protocol. • **INP_IPV6PROTO**—Creates an Internet PCB based on IPv6 protocol. • **INP_TIMEWAIT**—In **TIMEWAIT** state. • **INP_ONESBCAST**—Sends broadcast packets. • **INP_DROPPED**—Protocol dropped flag. • **INP_SOCKREF**—Strong socket reference. • **INP_DONTBLOCK**—Do not block synchronization of the Internet PCB. • **N/A**—None of the above flags.
Hop limit	Hop limit in the Internet PCB.
Send VRF	VRF from which packets are sent.
Receive VRF	VRF from which packets are received.

ipv6 address

Use **ipv6 address** to configure an IPv6 global unicast address for an interface.

Use **undo ipv6 address** to delete an IPv6 global unicast address of the interface.

Syntax

ipv6 address { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* }

undo ipv6 address [*ipv6-address prefix-length* | *ipv6-address*/*prefix-length*]

Default

No IPv6 global unicast address is configured for an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address: Specifies an IPv6 address.

prefix-length: Specifies a prefix length in the range of 1 to 128.

Usage guidelines

Like public IPv4 addresses, IPv6 global unicast addresses are assigned to ISPs. This type of address allows for prefix aggregation to reduce the number of global routing entries.

If you do not specify any parameters, the **undo ipv6 address** command deletes all IPv6 addresses of an interface.

Examples

Set the IPv6 global unicast address of GigabitEthernet 1/0/1 to 2001::1 with prefix length 64.

Method 1:

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 address 2001::1/64
```

Method 2:

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 address 2001::1 64
```

ipv6 address anycast

Use **ipv6 address anycast** to configure an IPv6 anycast address for an interface.

Use **undo ipv6 address anycast** to delete the IPv6 anycast address of the interface.

Syntax

ipv6 address { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* } **anycast**

undo ipv6 address { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* } **anycast**

Default

No IPv6 anycast address is configured for an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address: Specifies an IPv6 anycast address.

prefix-length: Specifies a prefix length in the range of 1 to 128.

Examples

Set the IPv6 anycast address of interface GigabitEthernet 1/0/1 to 2001::1 with prefix length 64.

Method 1:

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 address 2001::1/64 anycast
```

Method 2:

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 address 2001::1 64 anycast
```

ipv6 address auto

Use **ipv6 address auto** to enable the stateless address autoconfiguration feature on an interface, so that the interface can automatically generate a global unicast address.

Use **undo ipv6 address auto** to disable this feature.

Syntax

ipv6 address auto

undo ipv6 address auto

Default

The stateless address autoconfiguration feature is disabled.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

After a global unicast address is generated through stateless autoconfiguration, a link-local address is generated automatically.

To delete the global unicast address and the link-local address that are automatically generated, use either of the following commands:

- **undo ipv6 address auto**
- **undo ipv6 address**

Examples

Enable stateless address autoconfiguration on interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 address auto
```

ipv6 address auto link-local

Use **ipv6 address auto link-local** to automatically generate a link-local address for an interface.

Use **undo ipv6 address auto link-local** to restore the default.

Syntax

ipv6 address auto link-local

undo ipv6 address auto link-local

Default

No link-local address is configured on an interface. A link-local address is automatically generated after an IPv6 global unicast address is configured for the interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

Link-local addresses are used for neighbor discovery and stateless autoconfiguration on the local link. Packets using link-local addresses as the source or destination addresses cannot be forwarded to other links.

After an IPv6 global unicast address is configured for an interface, a link-local address is automatically generated. This link-local address is the same as the one generated by using the **ipv6 address auto link-local** command.

The **undo ipv6 address auto link-local** command deletes only the link-local addresses generated through the **ipv6 address auto link-local** command. If the **undo** command is executed on an interface with an IPv6 global unicast address configured, the interface still has a link-local address.

You can also manually assign an IPv6 link-local address for an interface by using the **ipv6 address link-local** command. Manual assignment takes precedence over automatic generation for IPv6 link-local addresses.

- If you first use automatic generation and then manual assignment, the manually assigned link-local address overwrites the automatically generated address.
- If you first use manual assignment and then automatic generation, both of the following occur:
  - The automatically generated link-local address does not take effect.
  - The link-local address of an interface is still the manually assigned address.

  If you delete the manually assigned address, the automatically generated link-local address takes effect.

Examples

Configure GigabitEthernet 1/0/1 to automatically generate a link-local address.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 address auto link-local
```

Related commands

ipv6 address link-local

ipv6 address eui-64

Use **ipv6 address eui-64** to configure an EUI-64 IPv6 address for an interface.

Use **undo ipv6 address eui-64** to delete an EUI-64 IPv6 address from an interface.

Syntax

ipv6 address { *ipv6-address prefix-length* | *ipv6-address/prefix-length* } **eui-64**

undo ipv6 address { *ipv6-address prefix-length* | *ipv6-address/prefix-length* } **eui-64**

Default

No EUI-64 IPv6 address is configured for an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address prefix-length: Specifies an IPv6 address and IPv6 prefix length. The *ipv6-address* and *prefix-length* arguments specify the prefix of an EUI-64 IPv6 address. The value range for the *prefix-length* argument is 1 to 64. The IPv6 address and IPv6 prefix length support the following formats:

- *ipv6-address/prefix-length*. For example: 2001::1/64.
- *ipv6-address prefix-length*. For example: 2001::1 64.

Usage guidelines

An EUI-64 IPv6 address is generated based on the specified prefix and the automatically generated interface ID. To display the EUI-64 IPv6 address, use the **display ipv6 interface** command.

The prefix length of an EUI-64 IPv6 address cannot be greater than 64.

Examples

Configure an EUI-64 IPv6 address for interface GigabitEthernet 1/0/1. The prefix of the address is the same as that of 2001::1/64, and the interface ID is generated based on the MAC address of the device.

Method 1:

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 address 2001::1/64 eui-64
```

Method 2:

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 address 2001::1 64 eui-64
```

Related commands

display ipv6 interface

ipv6 address link-local

Use **ipv6 address link-local** to configure a link-local address for the interface.

Use **undo ipv6 address link-local** to restore the default.

Syntax

ipv6 address *ipv6-address* **link-local**

undo ipv6 address *ipv6-address* **link-local**

Default

No link-local address is configured for the interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address: Specifies an IPv6 link-local address. The first 10 bits of an address must be 1111111010 (binary). The first group of hexadecimals in the address must be FE80 to FEBF.

Usage guidelines

Manual assignment takes precedence over automatic generation.

If you use automatic generation, and then use manual assignment, the manually assigned link-local address overwrites the one that is automatically generated.

If you use manual assignment and then use automatic generation, both of the following occur:

- The automatically generated link-local address does not take effect.
- The manually assigned link-local address of an interface remains.

After you delete the manually assigned address, the automatically generated link-local address takes effect. For automatic generation of an IPv6 link-local address, see the **ipv6 address auto link-local** command.

Examples

Configure a link-local address for GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 address fe80::1 link-local
```

Related commands

ipv6 address auto link-local

ipv6 address *prefix-number*

Use **ipv6 address** *prefix-number* to specify an IPv6 prefix for an interface to automatically generate an IPv6 global unicast address and advertise the prefix.

Use **undo ipv6 address** *prefix-number* to restore the default.

Syntax

ipv6 address *prefix-number sub-prefix/prefix-length*

undo ipv6 address *prefix-number*

Default

No IPv6 prefix is specified for IPv6 address autoconfiguration.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

prefix-number: Specifies an IPv6 prefix by its ID in the range of 1 to 1024. The specified IPv6 prefix can be manually configured or obtained through DHCPv6.

sub-prefix: Specifies the sub-prefix bit and host bit for the IPv6 global unicast address.

prefix-length: Specifies the sub-prefix length in the range of 1 to 128.

Usage guidelines

This command enables an interface to automatically generate an IPv6 global unicast address based on the specified IPv6 prefix, sub-prefix bit, and host bit.

An interface can generate only one IPv6 global unicast address based on the prefix specified by using the **ipv6 address** command. To configure the interface to generate a new IPv6 address, execute the **undo ipv6 address** command to delete the configuration, and then execute the **ipv6 address** command.

Examples

Configure a static IPv6 prefix AAAA::/16 and assign ID 1 to the prefix. Configure GigabitEthernet 1/0/1 to use this prefix to generate the IPv6 address AAAA:CCCC:DDDD::10/32 and advertise this prefix.

```
<Sysname> system-view
[Sysname] ipv6 prefix 1 AAAA::/16
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 address 1 BBBB:CCCC:DDDD::10/32
```

Configure GigabitEthernet 1/0/2 to obtain an IPv6 prefix through DHCPv6 and assign ID 2 to the obtained prefix. Configure GigabitEthernet 1/0/1 to use the obtained prefix to generate the IPv6 address AAAA:CCCC:DDDD::10/32 and advertise the prefix.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] ipv6 dhcp client pd 2 rapid-commit option-group 1
[Sysname-GigabitEthernet1/0/2] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 address 2 BBBB:CCCC:DDDD::10/32
```

Related commands

ipv6 prefix

ipv6 dhcp client pd

ipv6 extension-header drop enable

Use **ipv6 extension-header drop enable** to enable a device to discard IPv6 packets that contain extension headers.

Use **undo ipv6 extension-header drop enable** to disable a device from discarding IPv6 packets that contain extension headers.

Syntax

ipv6 extension-header drop enable

undo ipv6 extension-header drop enable

Default

A device does not discard IPv6 packets that contain extension headers.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This feature enables a device to discard a received IPv6 packet in which the extension headers cannot be processed by the device.

Examples

Enable the device to discard IPv6 packets that contain extension headers.

```
<Sysname> system-view
[Sysname] ipv6 extension-header drop enable
```

ipv6 hop-limit

Use **ipv6 hop-limit** to set the Hop Limit field in the IPv6 header.

Use **undo ipv6 hop-limit** to restore the default.

Syntax

ipv6 hop-limit *value*

undo ipv6 hop-limit

Default

The hop limit is 64.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

value: Specifies the number of hops, in the range of 1 to 255.

Usage guidelines

The hop limit determines the number of hops that an IPv6 packet generated by the device can travel.

The device advertises the hop limit in RA messages. All RA message receivers use the advertised value to fill in the Hop Limit field for IPv6 packets to be sent. To disable the device from advertising the hop limit, use the **ipv6 nd ra hop-limit unspecified** command.

Examples

Set the maximum number of hops to 100.

```
<Sysname> system-view
[Sysname] ipv6 hop-limit 100
```

Related commands

ipv6 nd ra hop-limit unspecified

ipv6 hoplimit-expires enable

Use **ipv6 hoplimit-expires enable** to enable sending ICMPv6 time exceeded messages.

Use **undo ipv6 hoplimit-expires** to disable sending ICMPv6 time exceeded messages.

Syntax

ipv6 hoplimit-expires enable

undo ipv6 hoplimit-expires enable

Default

Sending ICMPv6 time exceeded messages is enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

ICMPv6 time exceeded messages are sent to the source of IPv6 packets after the device discards IPv6 packets because hop or reassembly times out.

To prevent too many ICMPv6 error messages from affecting device performance, disable this feature. Even with the feature disabled, the device still sends fragment reassembly time exceeded messages.

Examples

Disable sending ICMPv6 time exceeded messages.

```
<Sysname> system-view
[Sysname] undo ipv6 hoplimit-expires enable
```

ipv6 icmpv6 error-interval

Use **ipv6 icmpv6 error-interval** to set the bucket size and the interval for tokens to arrive in the bucket for ICMPv6 error messages.

Use **undo ipv6 icmpv6 error-interval** to restore the default.

Syntax

ipv6 icmpv6 error-interval *interval* [*bucketsize*]

undo ipv6 icmpv6 error-interval

Default

The bucket allows a maximum of 10 tokens, and a token is placed in the bucket every 100 milliseconds.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies the interval for tokens to arrive in the bucket. The value range is 0 to 2147483647 milliseconds. To disable the ICMPv6 rate limit, set the value to 0.

bucketsize: Specifies the maximum number of tokens allowed in the bucket. The value range is 1 to 200.

Usage guidelines

This command limits the rate at which ICMPv6 error messages are sent. Use this command to prevent network congestion caused by excessive ICMPv6 error messages generated within a short period. A token bucket algorithm is used with one token representing one ICMPv6 error message.

A token is placed in the bucket at intervals until the maximum number of tokens that the bucket can hold is reached.

A token is removed from the bucket when an ICMPv6 error message is sent. When the bucket is empty, ICMPv6 error messages are not sent until a new token is placed in the bucket.

Examples

Set the bucket size to 40 tokens and the interval for tokens to arrive in the bucket to 200 milliseconds for ICMPv6 error messages.

```
<Sysname> system-view
[Sysname] ipv6 icmpv6 error-interval 200 40
```

ipv6 icmpv6 multicast-echo-reply enable

Use **ipv6 icmpv6 multicast-echo-reply enable** to enable replying to multicast echo requests.

Use **undo ipv6 icmpv6 multicast-echo-reply** to restore the default.

Syntax

ipv6 icmpv6 multicast-echo-reply enable

undo ipv6 icmpv6 multicast-echo-reply enable

Default

The device is disabled from replying to multicast echo requests.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

If a host is configured to reply to multicast echo requests, an attacker can use this mechanism to attack the host. For example, the attacker can send an echo request to a multicast address with Host A as the source. All hosts in the multicast group will send echo replies to Host A.

To prevent attacks, do not enable the device to reply to multicast echo requests unless necessary.

Examples

Enable replying to multicast echo requests.

```
<Sysname> system-view
[Sysname] ipv6 icmpv6 multicast-echo-reply enable
```

ipv6 icmpv6 source

Use **ipv6 icmpv6 source** to specify an IPv6 address as the source address for outgoing ICMPv6 packets.

Use **undo ipv6 icmpv6 source** to remove the specified IPv6 source address for outgoing ICMPv6 packets.

Syntax

ipv6 icmpv6 source [**vpn-instance** *vpn-instance-name*] *ipv6-address*

undo ipv6 icmpv6 source [**vpn-instance** *vpn-instance-name*]

Default

No IPv6 source address for outgoing ICMPv6 packets is specified. The device uses the IPv6 address of the sending interface as the source IPv6 address for outgoing ICMPv6 packets.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance to which the specified address belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the *ipv6-address* argument specifies an IPv6 address on the public network. The specified VPN instance must already exist.

ipv6-address: Specifies an IPv6 address.

Usage guidelines

It is a good practice to specify the IPv6 address of the loopback interface as the source IPv6 address for outgoing ping echo request and ICMPv6 error messages. This feature helps users to easily locate the sending device.

Examples

Specify IPv6 address 1::1 as the source address for outgoing ICMPv6 packets.

```
<Sysname> system-view
[Sysname] ipv6 icmpv6 source 1::1
```

ipv6 last-hop hold

Use **ipv6 last-hop hold** to enable IPv6 last hop holding.

Use **undo ipv6 last-hop hold** to disable IPv6 last hop holding.

Syntax

ipv6 last-hop hold

undo ipv6 last-hop hold

Default

IPv6 last hop holding is disabled.

Views

Layer 3 Ethernet interface view

Layer 3 Ethernet subinterface view

Dialer interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

Last hop holding implements symmetric routing.

When the interface enabled with this feature receives the first IPv6 packet of a forward flow, this feature implements the following operations:

- Obtains the forward flow information and last hop information of the packet.
- Based on the information, creates an IPv6 fast forwarding entry for the reverse flow.

When packets of the reverse flow arrive at the device, the device forwards those packets based on the entry.

Last hop holding is based on IPv6 fast forwarding entries. If the MAC address of a last hop changes on an Ethernet link, this feature can function correctly only after the fast forwarding entry is updated for the MAC address.

Examples

Enable the IPv6 last hop holding feature on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 last-hop hold
```

Enable the IPv6 last hop holding feature on Dialer 0.

```
<Sysname> system-view
```

```
[Sysname] interface dialer 0
[Sysname-Dialer0] ipv6 last-hop hold
```

ipv6 mtu

Use **ipv6 mtu** to configure the interface MTU for IPv6 packets.

Use **undo ipv6 mtu** to restore the default MTU.

Syntax

ipv6 mtu *size*

undo ipv6 mtu

Default

The interface MTU is not configured.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

size: Specifies the MTU size in bytes. The value range is 1280 to 1500 for VLAN interfaces and 1280 to 1560 for other interfaces.

Usage guidelines

IPv6 routers do not support packet fragmentation. After an IPv6 router receives an IPv6 packet, if the packet size is larger than the MTU of the forwarding interface, the router discards the packet. Meanwhile, the router sends the MTU to the source host through an ICMPv6 packet — Packet Too Big message. The source host fragments the packet according to the MTU and resends it. To reduce the extra flow overhead resulting from packet drops, set an appropriate interface MTU for your network.

Examples

Set the interface MTU for IPv6 packets to 1280 bytes on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 mtu 1280
```

ipv6 nd autoconfig managed-address-flag

Use **ipv6 nd autoconfig managed-address-flag** to set the managed address configuration flag (M) to 1 in RA advertisements to be sent.

Use **undo ipv6 nd autoconfig managed-address-flag** to restore the default.

Syntax

ipv6 nd autoconfig managed-address-flag

undo ipv6 nd autoconfig managed-address-flag

Default

The M flag is set to **0** in RA advertisements. Hosts receiving the advertisements will obtain IPv6 addresses through stateless autoconfiguration.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

The M flag in RA advertisements determines whether receiving hosts use stateful autoconfiguration to obtain IPv6 addresses.

- If the M flag is set to 1 in RA advertisements, receiving hosts use stateful autoconfiguration (for example, from an DHCPv6 server) to obtain IPv6 addresses.
- If the M flag is set to 0 in RA advertisements, receiving hosts use stateless autoconfiguration. Stateless autoconfiguration generates IPv6 addresses according to link-layer addresses and the prefix information in the RA advertisements.

Examples

Set the M flag to 1 in RA advertisements to be sent.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 nd autoconfig managed-address-flag
```

ipv6 nd autoconfig other-flag

Use **ipv6 nd autoconfig other-flag** to set the other stateful configuration flag (O) to 1 in RA advertisements to be sent.

Use **undo ipv6 nd autoconfig other-flag** to restore the default.

Syntax

ipv6 nd autoconfig other-flag

undo ipv6 nd autoconfig other-flag

Default

The O flag is set to **0** in RA advertisements. Hosts receiving the advertisements will acquire other information through stateless autoconfiguration.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

The O flag in RA advertisements determines whether receiving hosts use stateful autoconfiguration to obtain configuration information other than IPv6 addresses.

- If the O flag is set to 1 in RA advertisements, receiving hosts use stateful autoconfiguration (for example, from a DHCPv6 server) to obtain configuration information other than IPv6 addresses.
- If the O flag is set to 0 in RA advertisements, receiving hosts use stateless autoconfiguration to obtain configuration information other than IPv6 addresses.

Examples

Set the O flag to 0 in RA advertisements to be sent.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo ipv6 nd autoconfig other-flag
```

ipv6 nd dad attempts

Use **ipv6 nd dad attempts** to set the number of attempts to send an NS message for DAD.

Use **undo ipv6 nd dad attempts** to restore the default.

Syntax

ipv6 nd dad attempts *times*

undo ipv6 nd dad attempts

Default

The number of attempts to send an NS message for DAD is 1.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

times: Specifies the number of attempts to send an NS message for DAD, in the range of 0 to 600. If it is set to 0, DAD is disabled.

Usage guidelines

An interface sends an NS message for DAD after obtaining an IPv6 address.

If the interface does not receive a response within the time specified by using **ipv6 nd ns retrans-timer**, it resends an NS message.

If the interface receives no response after making the maximum sending attempts, the interface uses the obtained address.

Examples

Set the number of attempts to send an NS message for DAD to 20.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 nd dad attempts 20
```

Related commands

display ipv6 interface

ipv6 nd ns retrans-timer

ipv6 nd ns retrans-timer

Use **ipv6 nd ns retrans-timer** to set the interval for retransmitting an NS message.

Use **undo ipv6 nd ns retrans-timer** to restore the default.

Syntax

ipv6 nd ns retrans-timer *value*

undo ipv6 nd ns retrans-timer

Default

The local interface sends NS messages at every an interval of 1000 milliseconds, and the Retrans Timer field in the RA messages sent is 0. The interval for retransmitting an NS message is determined by the receiving device.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

value: Specifies the interval value in the range of 1000 to 4294967295 milliseconds.

Usage guidelines

If a device does not receive a response from the peer within the specified interval, the device resends an NS message. The device retransmits an NS message at the specified interval and uses the interval value to fill the Retrans Timer field in RA messages to be sent.

Examples

Specify GigabitEthernet 1/0/1 to retransmit NS messages every 10000 milliseconds.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 nd ns retrans-timer 10000
```

Related commands

display ipv6 interface

ipv6 nd nud reachable-time

Use **ipv6 nd nud reachable-time** to set the neighbor reachable time on an interface.

Use **undo ipv6 nd nud reachable-time** to restore the default.

Syntax

ipv6 nd nud reachable-time *time*

undo ipv6 nd nud reachable-time

Default

The neighbor reachable time on the local interface is 30000 milliseconds, and the value of the Reachable Time field in RA messages is 0. The reachable time is determined by the receiving device.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

time: Specifies the neighbor reachable time in the range of 1 to 3600000 milliseconds.

Usage guidelines

If the neighbor reachability detection shows that a neighbor is reachable, the device considers the neighbor reachable within the specified reachable time. If the device must send a packet to the neighbor after the specified reachable time expires, the device reconfirms whether the neighbor is reachable. The device sets the specified value as the neighbor reachable time on the local interface and uses the value to fill the Reachable Time field in RA messages to be sent.

Examples

Set the neighbor reachable time on GigabitEthernet 1/0/1 to 10000 milliseconds.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 nd nud reachable-time 10000
```

Related commands

display ipv6 interface

ipv6 nd ra dns search-list

Use **ipv6 nd ra dns search-list** to specify DNS suffix information to be advertised in RA messages.

Use **undo ipv6 nd ra dns search-list** to remove a DNS suffix from RA message advertisement.

Syntax

ipv6 nd ra dns search-list *domain-name* [*seconds* | **infinite**] **sequence** *seqno*

undo ipv6 nd ra dns search-list *domain-name*

Default

DNS suffix information is not specified and RA messages do not contain DNS suffix options.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

domain-name: Specifies a DNS suffix. It is a dot-separated, case-insensitive string that can include letters, digits, hyphens (-), underscores (_), and dots (.), for example, aabbcc.com. The DNS suffix can include a maximum of 253 characters, and each separated string includes no more than 63 characters.

seconds: Specifies the lifetime of the DNS suffix, in seconds. The value range is 4 to 4294967295. Value 4294967295 indicates that the lifetime of the DNS suffix is infinite.

infinite: Sets the lifetime of the DNS suffix to infinite.

seqno: Specifies the sequence number of the DNS suffix, in the range of 0 to 4294967295. The sequence number for a DNS suffix must be unique. A smaller sequence number represents a higher priority.

Usage guidelines

The DNS search list (DNSSL) option in RA messages provides DNS suffix information for hosts. The RA messages allow hosts to obtain their IPv6 addresses and the DNS suffix through stateless autoconfiguration. This method is useful in a network where DHCPv6 infrastructure is not provided.

The default lifetime of the DNS suffix is three times the maximum interval for advertising RA messages. To set the maximum interval, use the **ipv6 nd ra interval** command.

You can configure a maximum of eight DNS suffixes on an interface. One DNSSL option contains one DNS suffix. All DNSSL options are sorted in ascending order of the sequence number of the DNS suffix.

The sequence number uniquely identifies a DNS suffix. To modify a DNS suffix or its sequence number, you must first use the **undo ipv6 nd ra dns search-list** command to remove the DNS suffix from RA message advertisement.

After you execute the **ipv6 nd ra dns search-list** command, the device immediately sends an RA message with the existing and newly specified DNS suffix information.

After you execute the **undo ipv6 nd ra dns search-list** command, the device immediately sends two RA messages.

- The first RA message contains information about all DNS suffixes, including DNS suffixes specified in the **undo** command with their lifetime set to 0 seconds.
- The second RA message contains information about remaining DNS suffixes.

Each time the device sends an RA message from an interface, it immediately refreshes the RA message advertisement interval for that interface.

Examples

Specify the DNS suffix as **com**, the suffix lifetime as **3600** seconds, and the sequence number as **1** for RA messages on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 nd ra dns search-list com 3600 sequence 1
```

Related commands

ipv6 nd ra dns search-list suppress

ipv6 nd ra interval

ipv6 nd ra dns search-list suppress

Use **ipv6 nd ra dns search-list suppress** to enable DNS suffix suppression in RA messages.

Use **undo ipv6 nd ra dns search-list suppress** to disable DNS suffix suppression in RA messages.

Syntax

ipv6 nd ra dns search-list suppress

undo ipv6 nd ra dns search-list suppress

Default

DNS suffix suppression in RA messages is disabled.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command suppresses advertising DNS suffixes in RA messages on an interface. If you specify a new DNS suffix or remove a DNS suffix on the interface, the device immediately sends an RA message without any DNSSL options.

RA messages are suppressed by default. To disable RA message suppression, use the **undo ipv6 nd ra halt** command.

Whether enabling this feature on an interface will trigger sending RA message immediately depends on the interface configuration:

- If the interface has DNS suffix information configured, the device immediately sends two RA messages. In the first message, the lifetime for DNS suffixes is 0 seconds. The second RA message does not contain any DNSSL options.
- If the interface has no DNS suffix information specified, no RA messages are triggered.

Whether disabling this feature on an interface will trigger sending RA message immediately depends on the interface configuration:

- If the interface has DNS suffix information configured, the device immediately sends an RA message containing the DNS suffix information.
- If the interface has no DNS suffix information specified, no RA messages are triggered.

Each time the device sends an RA message from an interface, it immediately refreshes the RA message advertisement interval for that interface.

Examples

Enable DNS suffix suppression in RA messages on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 nd ra dns search-list suppress
```

Related commands

ipv6 nd ra dns search-list

ipv6 nd ra dns server

Use **ipv6 nd ra dns server** to specify DNS server information to be advertised in RA messages.

Use **undo ipv6 nd ra dns server** to remove a DNS server from RA message advertisement.

Syntax

ipv6 nd ra dns server *ipv6-address* [*seconds* | **infinite**] **sequence** *seqno*

undo ipv6 nd ra dns server *ipv6-address*

Default

DNS server information is not specified and RA messages do not contain DNS server options.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address: Specifies the IPv6 address of the DNS server, which must be a global unicast address or a link-local address.

seconds: Specifies the lifetime of the DNS server, in seconds. The value range is 4 to 4294967295. Value 4294967295 indicates that the lifetime of the DNS server is infinite.

infinite: Sets the lifetime of the DNS server to infinite.

sequence *seqno*: Specifies the sequence number of the DNS server, in the range of 0 to 4294967295. The sequence number for a DNS server must be unique. A smaller sequence number represents a higher priority.

Usage guidelines

The DNS server option in RA messages provides DNS server information for hosts. The RA messages allow hosts to obtain their IPv6 addresses and the DNS server through stateless autoconfiguration. This method is useful in a network where DHCPv6 infrastructure is not provided.

The default lifetime of the DNS server is three times the maximum interval for advertising RA messages. To set the maximum interval, use the **ipv6 nd ra interval** command.

You can configure a maximum of eight DNS servers on an interface. One DNS server option contains one DNS server. All DNS server options are sorted in ascending order of the DNS server sequence number.

The sequence number uniquely identifies a DNS server. To modify the IPv6 address or sequence number of a DNS server, you must first use the **undo ipv6 nd ra dns server** command to remove the DNS server from RA message advertisement.

After you execute the **ipv6 nd ra dns server** command, the device immediately sends an RA message with the existing and newly specified DNS server options.

After you execute the **undo ipv6 nd ra dns server** command, the device immediately sends two RA messages.

- The first RA message contains information about all DNS servers, including the DNS servers specified in the **undo** command with their lifetime set to 0 seconds.
- The second RA message contains information about remaining DNS servers.

Each time the device sends an RA message from an interface, it immediately refreshes the RA message advertisement interval for that interface.

In an IPv6 environment, PPP users and IPoE IPv6-ND-RS users can obtain the IPv6 DNS server address through AAA authorization. This AAA-authorized IPv6 DNS server address is also carried in RA messages. If an interface obtains the AAA-authorized and manually specified IPv6 DNS server addresses, the RA messages contain both, with the AAA-authorized address in the front. When the two addresses conflict, the AAA-authorized DNS-related attributes are used.

For more information about the PPP support for IPv6, see PPP configuration in *Layer 2—WAN Access Configuration Guide*.

For more information about IPoE IPv6-ND-RS users, see IPoE configuration in *Security Configuration Guide*.

Examples

Specify the DNS server address as **2001:10::100**, the server lifetime as **3600** seconds, and the sequence number as **1** for RA messages on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 nd ra dns server 2001:10::100 3600 sequence 1
```

Related commands

ipv6 nd ra dns server suppress

ipv6 nd ra interval

ipv6 nd ra dns server suppress

Use **ipv6 nd ra dns server suppress** to enable DNS server suppression in RA messages.

Use **undo ipv6 nd ra dns server suppress** to disable DNS server suppression in RA messages.

Syntax

ipv6 nd ra dns server suppress

undo ipv6 nd ra dns server suppress

Default

DNS server suppression in RA messages is disabled.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command suppresses advertising DNS server addresses in RA messages on an interface. If you specify a new DNS server or remove a DNS server on the interface, the device immediately sends an RA message without any DNS server options.

RA messages are suppressed by default. To disable RA message suppression, use the **undo ipv6 nd ra halt** command.

Whether enabling this feature on an interface will trigger sending RA message immediately depends on the interface configuration:

- If the interface has DNS server information configured or has obtained an AAA-authorized DNS server address, the device immediately sends two RA messages. In the first message, the lifetime for DNS server addresses is 0 seconds. The second RA message does not contain any DNS server options.
- If the interface has no DNS server information specified or no AAA-authorized DNS server address assigned, no RA messages are triggered.

Whether disabling this feature on an interface will trigger sending RA message immediately depends on the interface configuration:

- If the interface has DNS server information configured or has obtained an AAA-authorized DNS server address, the device immediately sends an RA message containing the DNS server information.

- If the interface has no DNS server information specified or no AAA-authorized DNS server address assigned, no RA messages are triggered.

Each time the device sends an RA message from an interface, it immediately refreshes the RA message advertisement interval for that interface.

Examples

Enable DNS server suppression in RA messages on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 nd ra dns server suppress
```

Related commands

ipv6 nd ra dns server

ipv6 nd ra halt

Use **ipv6 nd ra halt** to suppress an interface from advertising RA messages.

Use **undo ipv6 nd ra halt** to disable this feature.

Syntax

ipv6 nd ra halt

undo ipv6 nd ra halt

Default

An interface is suppressed from sending RA messages.

Views

Interface view

Predefined user roles

network-admin

context-admin

Examples

Disable RA message suppression on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo ipv6 nd ra halt
```

ipv6 nd ra hop-limit unspecified

Use **ipv6 nd ra hop-limit unspecified** to specify unlimited hops in RA messages.

Use **undo ipv6 nd ra hop-limit unspecified** to restore the default.

Syntax

ipv6 nd ra hop-limit unspecified

undo ipv6 nd ra hop-limit unspecified

Default

The maximum number of hops in the RA messages is limited to 64.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

To set the maximum number of hops to a value rather than the default setting, use the **ipv6 hop-limit** command.

Examples

Specify unlimited hops in the RA messages on interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 nd ra hop-limit unspecified
```

Related commands

ipv6 hop-limit

ipv6 nd ra interval

Use **ipv6 nd ra interval** to set the maximum and minimum intervals for advertising RA messages.

Use **undo ipv6 nd ra interval** to restore the default.

Syntax

ipv6 nd ra interval *max-interval min-interval*

undo ipv6 nd ra interval

Default

The maximum interval between RA messages is 600 seconds, and the minimum interval is 200 seconds.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

max-interval: Specifies the maximum interval value in seconds, in the range of 4 to 1800.

min-interval: Specifies the minimum interval value in the range of 3 seconds to three-fourths of the maximum interval.

Usage guidelines

The device advertises RA messages randomly between the maximum interval and the minimum interval.

The maximum interval for sending RA messages should be less than or equal to the router lifetime in RA messages.

Examples

Set the maximum interval for advertising RA messages to 1000 seconds and the minimum interval to 700 seconds.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 nd ra interval 1000 700
```

Related commands

ipv6 nd ra router-lifetime

ipv6 nd ra no-advlinkmtu

Use **ipv6 nd ra no-advlinkmtu** to turn off the MTU option in RA messages.

Use **undo ipv6 nd ra no-advlinkmtu** to restore the default.

Syntax

ipv6 nd ra no-advlinkmtu

undo ipv6 nd ra no-advlinkmtu

Default

RA messages contain the MTU option.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

The MTU option in the RA messages specifies the link MTU to ensure that all nodes on the link use the same MTU.

Examples

Turn off the MTU option in RA messages on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 nd ra no-advlinkmtu
```

ipv6 nd ra prefix

Use **ipv6 nd ra prefix** to configure the prefix information in RA messages.

Use **undo ipv6 nd ra prefix** to restore the default.

Syntax

ipv6 nd ra prefix { *ipv6-prefix prefix-length* | *ipv6-prefix*/*prefix-length* } [*valid-lifetime preferred-lifetime* [**no-autoconfig** | **off-link**] * | **no-advertise**]

undo ipv6 nd ra prefix { *ipv6-prefix* | *ipv6-prefix/prefix-length* }

Default

No prefix information is configured for RA messages. Instead, the IPv6 address of the interface sending RA messages is used as the prefix information.

If the IPv6 address is manually configured, the prefix uses the fixed valid lifetime 2592000 seconds (30 days) and preferred lifetime 604800 seconds (7 days).

If the IPv6 address is automatically obtained (through DHCP, for example), the prefix uses the valid and preferred lifetime of the IPv6 address.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-prefix: Specifies the IPv6 prefix.

prefix-length: Specifies the prefix length of the IPv6 address.

valid-lifetime: Specifies the valid lifetime of a prefix, in the range of 0 to 4294967295 seconds. The default value is 2592000 seconds (30 days).

preferred-lifetime: Specifies the preferred lifetime of a prefix used for stateless autoconfiguration, in the range of 0 to 4294967295 seconds. The preferred lifetime cannot be longer than the valid lifetime. The default value is 604800 seconds (7 days).

no-autoconfig: Specifies a prefix not to be used for stateless autoconfiguration. If you do not specify this keyword, the prefix is used for stateless autoconfiguration.

off-link: Indicates that the address with the prefix is not directly reachable on the link. If you do not specify this keyword, the address with the prefix is directly reachable on the link.

no-advertise: Disables the device from advertising the prefix specified in this command. If you do not specify this keyword, the device advertises the prefix specified in this command.

Usage guidelines

After hosts on the same link receive RA messages, they can use the prefix information in the RA messages for stateless autoconfiguration.

A prefix specified without a parameter in this command preferentially uses the default settings configured by using the **ipv6 nd ra prefix default** command. If the default settings are unavailable, the prefix uses the following settings:

- Valid lifetime of 2592000 seconds (30 days).
- Preferred lifetime of 604800 seconds (7 days).
- The prefix is used for stateless autoconfiguration.
- The address with the prefix is directly reachable on the link.
- The prefix is advertised in RA messages.

Examples

Configure the prefix information in RA messages on GigabitEthernet 1/0/1.

Method 1:

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 nd ra prefix 2001:10::100/64 100 10
```

Method 2:

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 nd ra prefix 2001:10::100 64 100 10
```

ipv6 nd ra prefix default

Use **ipv6 nd ra prefix default** to configure the default settings for prefixes advertised in RA messages.

Use **undo ipv6 nd ra prefix default** to restore the default.

Syntax

ipv6 nd ra prefix default [*valid-lifetime preferred-lifetime* [**no-autoconfig** | **off-link**] * | **no-advertise**]

undo ipv6 nd ra prefix default

Default

No default settings are configured for prefixes advertised in RA messages.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

valid-lifetime: Specifies the valid lifetime of a prefix, in the range of 0 to 4294967295 seconds. The default value is 2592000 seconds (30 days).

preferred-lifetime: Specifies the preferred lifetime of a prefix used for stateless autoconfiguration, in the range of 0 to 4294967295 seconds. The preferred lifetime cannot be longer than the valid lifetime. The default value is 604800 seconds (7 days).

no-autoconfig: Specifies a prefix not to be used for stateless autoconfiguration. If you do not specify this keyword, the prefix is used for stateless autoconfiguration.

off-link: Indicates that the address with the prefix is not directly reachable on the link. If you do not specify this keyword, the address with the prefix is directly reachable on the link.

no-advertise: Disables the device from advertising the prefix specified in this command. If you do not specify this keyword, the device advertises the prefix specified in this command.

Usage guidelines

This command specifies the default settings for the prefix specified by using the **ipv6 nd ra prefix** command. If none of the parameters (*valid-lifetime*, *preferred-lifetime*, **no-autoconfig**, **off-link**, and **no-advertise**) is configured in the **ipv6 nd ra prefix** command, the prefix uses the default settings.

Examples

Configure the default settings for prefixes advertised in RA messages on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 nd ra prefix default 100 10
```

ipv6 nd ra router-lifetime

Use **ipv6 nd ra router-lifetime** to set the router lifetime in RA messages.

Use **undo ipv6 nd ra router-lifetime** to restore the default.

Syntax

ipv6 nd ra router-lifetime *time*

undo ipv6 nd ra router-lifetime

Default

The router lifetime in RA messages is three times as long as the maximum interval for advertising RA messages.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

time: Specifies the router lifetime in the range of 0 to 9000 seconds. If the value is set to 0, the router does not act as the default router.

Usage guidelines

The router lifetime in RA messages specifies how long the router sending the RA messages acts as the default router. Hosts receiving the RA messages check this value to determine whether to use the sending router as the default router. If the router lifetime is 0, the router cannot be used as the default router.

The router lifetime in RA messages must be greater than or equal to the advertising interval.

Examples

Set the router lifetime in RA messages on GigabitEthernet 1/0/1 to 1000 seconds.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 nd ra router-lifetime 1000
```

Related commands

ipv6 nd ra interval

ipv6 nd router-preference

Use **ipv6 nd router-preference** to set a router preference in RA messages.

Use **undo ipv6 nd router-preference** to restore the default.

Syntax

ipv6 nd router-preference { **high** | **low** | **medium** }

undo ipv6 nd router-preference

Default

The router preference is **medium**.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

high: Sets the router preference to the highest setting.

low: Sets the router preference to the lowest setting.

medium: Sets the router preference to the medium setting.

Usage guidelines

A hosts selects a router with the highest preference as the default router.

When router preferences are the same in RA messages, a host selects the router corresponding to the first received RA message as the default gateway.

Examples

Set the router preference in RA messages to the lowest on interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 nd router-preference low
```

ipv6 nd unsolicited-na-learning enable

Use **ipv6 nd unsolicited-na-learning enable** to enable unsolicited NA learning.

Use **undo ipv6 nd unsolicited-na-learning enable** to disable unsolicited NA learning.

Syntax

ipv6 nd unsolicited-na-learning enable

undo ipv6 nd unsolicited-na-learning enable

Default

Unsolicited NA learning is disabled.

Views

Layer 3 interface view

Predefined user roles

network-admin

context-admin

context-operator

Usage guidelines

With this feature enabled, the device can learns ND entries from unsolicited NA messages. The ND entries generated by using this method are in stale state. To ensure that the device learns ND entries from trusted NA messages, enable this feature only on a secure network.

This feature might cause the device to learn excessive ND entries that consume too many system resources. As a best practice, execute the **ipv6 neighbor stale-aging** command to set a smaller aging timer before you enable this feature. The smaller aging timer accelerates the aging of ND entries in stale state.

Examples

Enable unsolicited NA learning on Layer 3 Ethernet interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 nd unsolicited-na-learning enable
```

Related commands

ipv6 neighbor stale-aging

ipv6 neighbor

Use **ipv6 neighbor** to configure a static neighbor entry.

Use **undo ipv6 neighbor** to delete a neighbor entry.

Syntax

ipv6 neighbor *ipv6-address mac-address* { *vlan-id port-type port-number* | **interface** *interface-type interface-number* } [**vpn-instance** *vpn-instance-name*]

undo ipv6 neighbor *ipv6-address interface-type interface-number*

Default

No static neighbor entries exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address: Specifies the IPv6 address of the static neighbor entry.

mac-address: Specifies the MAC address (48 bits) of the static neighbor entry, in the format of H-H-H.

vlan-id: Specifies the VLAN ID of the static neighbor entry, in the range of 1 to 4094.

port-type port-number: Specifies a Layer 2 port of the static neighbor entry by its type and number.

interface *interface-type interface-number*: Specifies a Layer 3 interface of the static neighbor entry by its type and number.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance to which the static neighbor entry belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command configures a static neighbor entry for the public network.

Usage guidelines

A neighbor entry stores information about a link-local node. The entry can be created dynamically through NS and NA messages, or configured statically.

The device uniquely identifies a static neighbor entry by using the neighbor's IPv6 address and the number of the Layer 3 interface that connects to the neighbor. You can configure a static neighbor entry by using either of the following methods:

- **Method 1**—Associate a neighbor IPv6 address and link-layer address with the Layer 3 interface of the local node.
- **Method 2**—Associate a neighbor IPv6 address and link-layer address with a Layer 2 port in a VLAN containing the local node.

You can use either of the previous configuration methods to configure a static neighbor entry for a VLAN interface.

- If Method 1 is used, the neighbor entry is in INCMP state. After the device obtains the corresponding Layer 2 port information, the neighbor entry goes into REACH state.
- If Method 2 is used, the port specified by *port-type port-number* must belong to the VLAN specified by *vlan-id* and the corresponding VLAN interface must already exist. After the static neighbor entry is configured, the device associates the VLAN interface with the IPv6 address to uniquely identify the static neighbor entry. The entry will be in REACH state.

You can use the **undo ipv6 neighbor** command to delete both static and dynamic neighbor entries.

To delete a neighbor entry for a VLAN interface, specify only the corresponding VLAN interface.

Do not specify a Reth interface as the outgoing interface in IPv6 static neighbor entries if its member interfaces contain subinterfaces. For more information about Reth interfaces, see *Virtual Technologies Configuration Guide*.

Examples

Configure a static neighbor entry for Layer 3 interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] ipv6 neighbor 2000::1 fe-e0-89 interface gigabitethernet 1/0/1
```

Related commands

display ipv6 neighbors

reset ipv6 neighbors

ipv6 neighbor link-local minimize

Use **ipv6 neighbor link-local minimize** to minimize link-local ND entries.

Use **undo ipv6 neighbor link-local minimize** to restore the default.

Syntax

ipv6 neighbor link-local minimize

undo ipv6 neighbor link-local minimize

Default

All ND entries are assigned to the driver.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

Perform this command to minimize link-local ND entries assigned to the driver. Link-local ND entries refer to ND entries that contain link-local addresses.

With this feature enabled, the device does not add newly learned link-local ND entries whose link local addresses are not the next hop of any route to the driver. This saves driver resources.

This feature affects only newly learned link-local ND entries rather than existing ND entries.

Examples

Minimize link-local ND entries.

```
<Sysname> system-view
[Sysname] ipv6 neighbor link-local minimize
```

ipv6 neighbor stale-aging

Use **ipv6 neighbor stale-aging** to set the aging timer for ND entries in stale state.

Use **undo ipv6 neighbor stale-aging** to restore the default.

Syntax

ipv6 neighbor stale-aging *aging-time*

undo ipv6 neighbor stale-aging

Default

The aging timer for ND entries in stale state is 240 minutes.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

aging-time: Specifies the aging timer for ND entries in stale state, in the range of 1 to 1440 minutes.

Usage guidelines

This aging time applies to all ND entries in stale state. If an ND entry in stale state is not updated before the timer expires, it moves to the delay state. If it is still not updated in 5 seconds, the ND entry moves to the probe state. The device sends an NS message for detection a maximum of three times. If no response is received, the device deletes the ND entry.

Examples

Set the aging timer for ND entries in stale state to 120 minutes.

```
<Sysname> system-view
[Sysname] ipv6 neighbor stale-aging 120
```

ipv6 neighbors max-learning-num

Use **ipv6 neighbors max-learning-num** to set the maximum number of dynamic neighbor entries that an interface can learn. This prevents the interface from occupying too many neighbor table resources.

Use **undo ipv6 neighbors max-learning-num** to restore the default.

Syntax

ipv6 neighbors max-learning-num *max-number*

undo ipv6 neighbors max-learning-num

Default

An interface can learn a maximum of 65536 dynamic neighbor entries.

Views

Layer 2/Layer 3 interface view

Layer 2 aggregate interface view

Layer 3 aggregate interface view

Predefined user roles

network-admin

context-admin

Parameters

max-number: Specifies the maximum number of dynamic neighbor entries that an interface can learn. The value range for this argument is 0 to 65536.

Usage guidelines

The device can dynamically acquire the link-layer address of a neighboring node through NS and NA messages and add it into the neighbor table.

When the number of dynamic neighbor entries reaches the threshold, the interface stops learning neighbor information.

To disable the device from learning neighbor entries, set the learning limit to 0.

Examples

Set the maximum number of dynamic neighbor entries that GigabitEthernet 1/0/1 can learn to 10.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 neighbors max-learning-num 10
```

ipv6 pathmtu

Use **ipv6 pathmtu** to set a static Path MTU for an IPv6 address.

Use **undo ipv6 pathmtu** to delete the Path MTU configuration for an IPv6 address.

Syntax

ipv6 pathmtu [**vpn-instance** *vpn-instance-name*] *ipv6-address value*

undo ipv6 pathmtu [**vpn-instance** *vpn-instance-name*] *ipv6-address*

Default

No static Path MTU is set.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance to which the Path MTU belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command sets the Path MTU for the public network.

ipv6-address: Specifies an IPv6 address.

value: Specifies the Path MTU of the specified IPv6 address, in the range of 1280 to 10240 bytes.

Usage guidelines

You can set a static Path MTU for a destination IPv6 address. When a source host sends a packet through an interface, it compares the interface MTU with the static Path MTU of the specified destination IPv6 address. If the packet size is larger than the smaller one of the two values, the host fragments the packet according to the smaller value.

Examples

Set a static Path MTU for an IPv6 address.

```
<Sysname> system-view
[Sysname] ipv6 pathmtu fe80::12 1300
```

Related commands

display ipv6 pathmtu

reset ipv6 pathmtu

ipv6 pathmtu age

Use **ipv6 pathmtu age** to set the aging time for a dynamic Path MTU.

Use **undo ipv6 pathmtu age** to restore the default.

Syntax

ipv6 pathmtu age *age-time*

undo ipv6 pathmtu age

Default

The aging time for dynamic Path MTU is 10 minutes.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

age-time: Specifies the aging time for Path MTU in minutes, in the range of 10 to 100.

Usage guidelines

After the path MTU from a source host to a destination host is dynamically determined, the source host sends subsequent packets to the destination host based on this MTU. After the aging time expires, the following events occur:

- The dynamic Path MTU is removed.
- The source host determines a dynamic path MTU through the Path MTU mechanism again.

The aging time is invalid for a static Path MTU.

Examples

Set the aging time for a dynamic Path MTU to 40 minutes.

```
<Sysname> system-view
[Sysname] ipv6 pathmtu age 40
```

Related commands

display ipv6 pathmtu

ipv6 prefer temporary-address

Use **ipv6 prefer temporary-address** to enable the system to preferentially use the temporary IPv6 address of the sending interface as the source address of a packet.

Use **undo ipv6 prefer temporary-address** to disable the system to preferentially use the temporary IPv6 address of the sending interface as the source address of a packet.

Syntax

ipv6 prefer temporary-address

undo ipv6 prefer temporary-address

Default

The system is disabled to preferentially use the temporary IPv6 address of the sending interface as the source address of a packet.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

The temporary address feature enables the system to generate and preferentially use the temporary IPv6 address of the sending interface as the source address of a packet. If the temporary IPv6 address cannot be used because of a DAD conflict, the system uses the public IPv6 address.

Examples

Enable the system to preferentially use the temporary IPv6 address of the sending interface as the source address of the packet.

```
<Sysname> system-view
[Sysname] ipv6 prefer temporary-address
```

Related commands

ipv6 address auto

ipv6 nd ra prefix

ipv6 temporary-address

ipv6 prefix

Use **ipv6 prefix** to configure a static IPv6 prefix.

Use **undo ipv6 prefix** to delete a static IPv6 prefix.

Syntax

ipv6 prefix *prefix-number ipv6-prefix/prefix-length*

undo ipv6 prefix *prefix-number*

Default

No static IPv6 prefix is configured.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

prefix-number: Specifies a prefix ID in the range of 1 to 1024.

ipv6-prefix/prefix-length: Specifies a prefix and its length. The value range for the *prefix-length* argument is 1 to 128.

Usage guidelines

To modify an existing static prefix, execute the **undo ipv6 prefix** command to delete the existing static prefix, and then execute the **ipv6 prefix** command.

Dynamic IPv6 prefixes obtained from DHCPv6 servers cannot be manually removed or modified.

A static IPv6 prefix can have the same prefix ID with a dynamic IPv6 prefix, but the static one takes precedence over the dynamic one.

Examples

Create static IPv6 prefix 2001:0410::/32 with prefix ID 1.

```
<Sysname> system-view
[Sysname] ipv6 prefix 1 2001:0410::/32
```

Related commands

display ipv6 prefix

ipv6 reassemble local enable

Use **ipv6 reassemble local enable** to enable IPv6 local fragment reassembly.

Use **undo ipv6 reassemble local enable** to disable IPv6 local fragment reassembly.

Syntax

ipv6 reassemble local enable

undo ipv6 reassemble local enable

Default

IPv6 local fragment reassembly is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

Configure this command on a multichassis IRF fabric to improve fragment reassembly efficiency. The command enables the subordinate to reassemble the IPv6 fragments of a packet if all the fragments arrive at it. If this feature is disabled, all IPv6 fragments are delivered to the master for reassembly. The command applies only to fragments destined for the same subordinate.

Examples

Enable IPv6 local fragment reassembly.

```
<Sysname> system-view
[Sysname] ipv6 reassemble local enable
```

ipv6 redirects enable

Use **ipv6 redirects enable** to enable sending ICMPv6 redirect messages.

Use **undo ipv6 redirects enable** to disable sending ICMPv6 redirect messages.

Syntax

ipv6 redirects enable

undo ipv6 redirects enable

Default

Sending ICMPv6 redirect messages is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

The default gateway sends an ICMPv6 redirect message to the source of an IPv6 packet to inform the source of a better first hop.

Sending ICMPv6 redirect messages enables hosts that hold few routes to establish routing tables and find the best route. Because this feature adds host routes into the routing tables, host performance degrades when there are too many host routes. As a result, sending ICMPv6 redirect messages is disabled by default.

Examples

Enable sending ICMPv6 redirect messages.

```
<Sysname> system-view
[Sysname] ipv6 redirects enable
```

ipv6 temporary-address

Use **ipv6 temporary-address** to enable the temporary IPv6 address feature.

Use **undo ipv6 temporary-address** to restore the default.

Syntax

ipv6 temporary-address [*valid-lifetime preferred-lifetime*]

undo ipv6 temporary-address

Default

The system does not generate any temporary IPv6 address.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

valid-lifetime: Specifies the valid lifetime for temporary IPv6 addresses, in the range of 600 to 4294967295 seconds. The default valid lifetime is 604800 seconds (7 days).

preferred-lifetime: Specifies the preferred lifetime for temporary IPv6 addresses, in the range of 600 to 4294967295 seconds. The default preferred lifetime is 86400 seconds (1 day).

Usage guidelines

You must enable stateless autoconfiguration before enabling the temporary address feature.

The valid lifetime for temporary IPv6 addresses must be greater than or equal to the preferred lifetime for temporary IPv6 addresses.

In stateless address autoconfiguration, an interface automatically generates an IPv6 global unicast address by using the address prefix in the received RA message and the interface ID. On an IEEE 802 interface (such as an Ethernet interface or a VLAN interface), the interface ID is generated based on the interface's MAC address and is globally unique. An attacker can exploit this rule to easily identify the sending device.

To fix the vulnerability, you can enable the temporary address feature. An IEEE 802 interface generates the following addresses:

- **Public IPv6 address**—Includes an address prefix in the RA message and a fixed interface ID generated based on the interface's MAC address.
- **Temporary IPv6 address**—Includes an address prefix in the RA message and a random interface ID generated through MD5.

When the valid lifetime of a temporary IPv6 address expires, the system deletes the address and generates a new one. This enables the system to send packets with different source addresses through the same interface. The preferred lifetime and valid lifetime for a temporary IPv6 address are determined as follows:

- The preferred lifetime of a temporary IPv6 address takes the smaller of the following values:
  - The preferred lifetime of the address prefix in the RA message.
  - The preferred lifetime configured for temporary IPv6 addresses minus DESYNC_FACTOR (a random number in the range of 0 to 600 seconds).
- The valid lifetime of a temporary IPv6 address takes the smaller of the following values:
  - The valid lifetime of the address prefix.
  - The valid lifetime configured for temporary IPv6 addresses.

Examples

Enable the system to generate a temporary IPv6 address.

```
<Sysname> system-view
[Sysname] ipv6 temporary-address
```

Related commands

ipv6 address auto

ipv6 nd ra prefix

ipv6 prefer temporary-address

ipv6 unreachables enable

Use **ipv6 unreachables enable** to enable sending ICMPv6 destination unreachable messages.

Use **undo ipv6 unreachables** to disable sending ICMPv6 destination unreachable messages.

Syntax

ipv6 unreachables enable

undo ipv6 unreachables enable

Default

Sending ICMPv6 destination unreachable messages is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

If the device fails to forward a received IPv6 packet because of a destination unreachable error, it performs the following operations:

- Drops the packet.
- Sends an ICMPv6 destination unreachable message to the source.

If the device is generating ICMPv6 destination unreachable messages incorrectly, disable sending ICMPv6 destination unreachable messages to prevent attack risks.

Examples

Enable sending ICMPv6 destination unreachable messages.

```
<Sysname> system-view
[Sysname] ipv6 unreachables enable
```

local-proxy-nd enable

Use **local-proxy-nd enable** to enable local ND proxy.

Use **undo local-proxy-nd enable** to disable local ND proxy.

Syntax

local-proxy-nd enable

undo local-proxy-nd enable

Default

Local ND proxy is disabled.

Views

VLAN interface view

Layer 3 Ethernet interface view

Layer 3 Ethernet subinterface view

Layer 3 aggregate interface view

Layer 3 aggregate subinterface view

Predefined user roles

network-admin

context-admin

Examples

Enable local ND proxy on interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] local-proxy-nd enable
```

Related commands

proxy-nd enable

proxy-nd enable

Use **proxy-nd enable** to enable common ND proxy.

Use **undo proxy-nd enable** to disable common ND proxy.

Syntax

proxy-nd enable

undo proxy-nd enable

Default

Common ND proxy is disabled.

Views

VLAN interface view

Layer 3 Ethernet interface view

Layer 3 Ethernet subinterface view

Layer 3 aggregate interface view

Layer 3 aggregate subinterface view

Predefined user roles

network-admin

context-admin

Examples

Enable common ND proxy on interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] proxy-nd enable
```

Related commands

local-proxy-nd enable

reset ipv6 neighbors

Use **reset ipv6 neighbors** to clear IPv6 neighbor information.

Syntax

reset ipv6 neighbors { **all** | **dynamic** | **interface** *interface-type interface-number* | **slot** *slot-number* | **static** }

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

all: Clears static and dynamic neighbor information for all interfaces.

dynamic: Clears dynamic neighbor information for all interfaces.

interface *interface-type interface-number*: Clears dynamic neighbor information for the interface specified by its type and number.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears dynamic neighbor information for all member devices.

static: Clears static neighbor information for all interfaces.

Examples

Clear neighbor information for all interfaces.

```
<Sysname> reset ipv6 neighbors all
This will delete all the entries. Continue? [Y/N]:Y
```

Clear dynamic neighbor information for all interfaces.

```
<Sysname> reset ipv6 neighbors dynamic
This will delete all the dynamic entries. Continue? [Y/N]:Y
```

Clear all neighbor information for GigabitEthernet 1/0/1.

```
<Sysname> reset ipv6 neighbors interface gigabitethernet 1/0/1
This will delete all the dynamic entries by the interface you specified. Continue? [Y/N]:Y
```

Related commands

display ipv6 neighbors

ipv6 neighbor

reset ipv6 pathmtu

Use **reset ipv6 pathmtu** to clear the Path MTU information.

Syntax

reset ipv6 pathmtu { **all** | **dynamic** | **static** }

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

all: Clears all Path MTUs.

dynamic: Clears all dynamic Path MTUs.

static: Clears all static Path MTUs.

Examples

Clear all Path MTUs.

```
<Sysname> reset ipv6 pathmtu all
```

Related commands

display ipv6 pathmtu

reset ipv6 statistics

Use **reset ipv6 statistics** to clear IPv6 and ICMPv6 packet statistics.

Syntax

reset ipv6 statistics [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears IPv6 and ICMPv6 packet statistics for all member devices.

Examples

Clear IPv6 and ICMPv6 packet statistics.

```
<Sysname> reset ipv6 statistics
```

Related commands

display ipv6 statistics

Contents

IPv6 fast forwarding commands

display ipv6 fast-forwarding aging-time

Use **display ipv6 fast-forwarding aging-time** to display the aging time of IPv6 fast forwarding entries.

Syntax

display ipv6 fast-forwarding aging-time

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display the aging time of IPv6 fast forwarding entries.

```
<Sysname> display ipv6 fast-forwarding aging-time
Aging time: 30s
```

Table 1 Command output

Field	Description
Aging time	Aging time of IPv6 fast forwarding entries, in seconds.

Related commands

ipv6 fast-forwarding aging-time

display ipv6 fast-forwarding cache

Use **display ipv6 fast-forwarding cache** to display IPv6 fast forwarding entries.

Syntax

display ipv6 fast-forwarding cache [*ipv6-address*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ipv6-address: Specifies an IPv6 address. If you do not specify an IPv6 address, this command displays all IPv6 fast forwarding entries.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv6 fast forwarding entries for all member devices.

Examples

Display all IPv6 fast forwarding entries.

```
<Sysname> display ipv6 fast-forwarding cache
Total number of IPv6 fast-forwarding items: 2
Src IP: 2002::1                                         Src port: 129
Dst IP: 2001::1                                         Dst port: 65535
Protocol: 58
VPN instance: N/A
Input interface: GE1/0/2
Output interface: GE1/0/1

Src IP: 2001::1                                         Src port: 128
Dst IP: 2002::1                                         Dst port: 0
Protocol: 58
VPN instance: N/A
Input interface: GE1/0/1
Output interface: GE1/0/2
```

Table 2 Command output

Field	Description
Total number of IPv6 fast-forwarding items	Number of IPv6 fast forwarding entries.
Src IP	Source IPv6 address.
Src port	Source port number.
Dst IP	Destination IPv6 address.
Dst Port	Destination port number.
Protocol	Protocol number.
VPN instance	VPN instance. If the entry does not belong to any VPN instance, this field displays **N/A**.
Input interface	Input interface type and number. If no interface is involved in fast forwarding, this field displays **N/A**. If the input interface does not exist, this field displays a hyphen (-).
Output interface	Output interface type and number. If no interface is involved in fast forwarding, this field displays **N/A**. If the output interface does not exist, this field displays a hyphen (-).

Related commands

reset ipv6 fast-forwarding cache

display ipv6 fast-forwarding fragcache

Use **display ipv6 fast-forwarding fragcache** to display IPv6 fast forwarding entries for fragmented datagrams.

Syntax

display ipv6 fast-forwarding fragcache [*ipv6-address*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ipv6-address: Specifies an IPv6 address. If you do not specify this argument, this command displays IPv6 fast forwarding entries for all fragmented datagrams.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv6 fast forwarding entries for fragmented datagrams on all member devices.

Examples

Display IPv6 fast forwarding entries for all fragmented datagrams.

```
<Sysname> display ipv6 fast-forwarding fragcache
Total number of fragment fast-forwarding entries: 2
Src IP: 18::18                  Src Port: 0
Dst IP: 14::38                  Dst Port: 0
Protocol: 58
Input interface: N/A
ID: 736
Relay flag: 0

Src IP: 14::38                  Src Port: 51389
Dst IP: 18::18                  Dst Port: 32768
Protocol: 58
Input interface: GE1/0/3
ID: 774
Relay flag: 0
```

Table 3 Command output

Field	Description
Total number of fragment fast-forwarding entries	Number of IPv6 fast forwarding entries for fragmented datagrams.
Src IP	Source IPv6 address.

Field	Description
Src port	Source port number.
Dst IP	Destination IPv6 address.
Dst Port	Destination port number.
Protocol	Protocol number.
Input interface	Input interface type and number. If no interface is involved in fast forwarding, this field displays **N/A**. If the input interface does not exist, this field displays a hyphen (-).
ID	Fragment ID.
Relay_flag	Fragment pass-through flag: • **0**—Not pass through. • **1**—Pass through.

ipv6 fast-forwarding enable

Use **ipv6 fast-forwarding enable** to enable IPv6 fast forwarding.

Use **undo ipv6 fast-forwarding enable** to disable IPv6 fast forwarding.

Syntax

ipv6 fast-forwarding enable

undo ipv6 fast-forwarding enable

Default

IPv6 fast forwarding is enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

The IPv6 fast forwarding feature will create fast forwarding entries for the device to speed up packet forwarding. When the traffic volume is high, the device will generate a large number of fast forwarding entries. These entries will cause high memory usage, which eventually leads to memory allocation failure for other services. In this case, you can disable this feature temporarily to free up device memory.

Do not disable IPv6 fast forwarding if the device runs session-based services. Disabling fast forwarding will make these services become ineffective:

- NAT.
- ASPF.
- Attack detection and prevention.

Examples

Disable IPv6 fast forwarding.

```
<Sysname> system-view
[Sysname] undo ipv6 fast-forwarding enable
```

Related commands

display ipv6 fast-forwarding cache

reset ipv6 fast-forwarding cache

ipv6 fast-forwarding load-sharing

Use **ipv6 fast-forwarding load-sharing** to enable IPv6 fast forwarding load sharing.

Use **undo ipv6 fast-forwarding load-sharing** to disable IPv6 fast forwarding load sharing.

Syntax

ipv6 fast-forwarding load-sharing

undo ipv6 fast-forwarding load-sharing

Default

IPv6 fast forwarding load sharing is enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

IPv6 fast forwarding load sharing enables the device to load share packets of the same flow. This feature identifies a data flow by using the packet information.

If IPv6 fast forwarding load sharing is disabled, the device identifies a data flow by the packet information and the input interface. No load sharing is implemented.

Examples

Enable IPv6 fast forwarding load sharing.

```
<Sysname> system-Views
[Sysname] ipv6 fast-forwarding load-sharing
```

reset ipv6 fast-forwarding cache

Use **reset ipv6 fast-forwarding cache** to clear the IPv6 fast forwarding table.

Syntax

reset ipv6 fast-forwarding cache [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears the IPv6 fast forwarding table for all member devices.

Examples

Clear the IPv6 fast forwarding table.

```
<Sysname> reset ipv6 fast-forwarding cache
```

Related commands

display ipv6 fast-forwarding cache

Contents

DHCP commands

Common DHCP commands

dhcp client-detect

Use **dhcp client-detect** to enable client offline detection on the DHCP server or DHCP relay agent.

Use **undo dhcp client-detect** to disable client offline detection on the DHCP server or DHCP relay agent.

Syntax

dhcp client-detect

undo dhcp client-detect

Default

Client offline detection is disabled on the DHCP server or DHCP relay agent.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

The client offline detection feature on the DHCP server reclaims an assigned IP address and deletes the binding entry when the ARP entry ages out for the IP address.

This feature on the DHCP relay agent deletes the related relay entry and sends a RELEASE message to the DHCP server when an ARP entry ages out.

Examples

Enable client offline detection.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp client-detect
```

dhcp dscp

Use **dhcp dscp** to set the DSCP value for DHCP packets sent by the DHCP server or the DHCP relay agent.

Use **undo dhcp dscp** to restore the default.

Syntax

dhcp dscp *dscp-value*

undo dhcp dscp

Default

The DSCP value is 56 in DHCP packets sent by the DHCP server or the DHCP relay agent.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

dscp-value: Specifies the DSCP value for DHCP packets, in the range of 0 to 63.

Usage guidelines

The DSCP value of a packet specifies the priority level of the packet and affects the transmission priority of the packet. A bigger DSCP value represents a higher priority.

Examples

Set the DSCP value to 30 for DHCP packets sent by the DHCP server or the DHCP relay agent.

```
<Sysname> system-view
[Sysname] dhcp dscp 30
```

dhcp enable

Use **dhcp enable** to enable DHCP.

Use **undo dhcp enable** to disable DHCP.

Syntax

dhcp enable

undo dhcp enable

Default

DHCP is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

DHCP related configuration takes effect only after you enable DHCP.

Enable DHCP before you configure the DHCP server or relay agent.

Examples

Enable DHCP.

```
<Sysname> system-view
[Sysname] dhcp enable
```

dhcp log enable

Use **dhcp log enable** to enable DHCP server logging.

Use **undo dhcp log enable** to disable DHCP server logging.

Syntax

dhcp log enable

undo dhcp log enable

Default

DHCP server logging is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command enables the DHCP server to generate DHCP logs and send them to the information center. The information helps administrators to locate and solve problems. For information about the log destination and output rule configuration in the information center, see *Network Management and Monitoring Configuration Guide*.

As a best practice, disable this feature if the log generation affects the device performance or reduces the address allocation efficiency. For example, this situation might occur when a large number of clients frequently come online or go offline.

Examples

Enable DHCP server logging.

```
<Sysname> system-view
[Sysname] dhcp log enable
```

dhcp select

Use **dhcp select** to enable the DHCP server or DHCP relay agent on an interface.

Use **undo dhcp select** to disable the DHCP server or DHCP relay agent on an interface. The interface will discard incoming DHCP packets.

Syntax

dhcp select { **relay** | **server** }

undo dhcp select { **relay** | **server** }

Default

The interface operates in the DHCP server mode and responds to DHCP requests with configuration parameters.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

relay: Enables the DHCP relay agent on the interface.

server: Enables the DHCP server on the interface.

Usage guidelines

Before enabling a DHCP server to operate as a DHCP relay agent, use the **reset dhcp server ip-in-use** command to clear address bindings and authorized ARP entries. These authorized ARP entries might conflict with ARP entries that are created after the DHCP relay agent is enabled.

Examples

Enable the DHCP relay agent on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp select relay
```

Related commands

dhcp smart-relay enable

reset dhcp server ip-in-use

DHCP server commands

address range

Use **address range** to configure an IP address range in a DHCP address pool for dynamic allocation.

Use **undo address range** to restore the default.

Syntax

address range *start-ip-address end-ip-address*

undo address range

Default

No IP address range exists.

Views

DHCP address pool view

Predefined user roles

network-admin

context-admin

Parameters

start-ip-address: Specifies the start IP address.

end-ip-address: Specifies the end IP address.

Usage guidelines

If no IP address range is specified, all IP addresses in the subnet specified by the **network** command in address pool view are assignable. If an IP address range is specified, only the IP addresses in the IP address range are assignable.

After you use the **address range** command, you cannot use the **network secondary** command to specify a secondary subnet in the address pool.

If you execute this command multiple times, the most recent configuration takes effect.

The address range specified by the **address range** command must be within the subnet specified by the **network** command. The addresses outside of the subnet cannot be assigned.

Examples

Specify an address range of 192.168.8.1 through 192.168.8.150 in address pool 1.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 1
[Sysname-dhcp-pool-1] network 192.168.8.1 mask 255.255.255.0
[Sysname-dhcp-pool-1] address range 192.168.8.1 192.168.8.150
```

Related commands

class

dhcp class

display dhcp server pool

network

bims-server

Use **bims-server** to specify the IP address, port number, and shared key of the BIMS server in a DHCP address pool.

Use **undo bims-server** to restore the default.

Syntax

bims-server ip *ip-address* [**port** *port-number*] **sharekey** { **cipher** | **simple** } *string*

undo bims-server

Default

No BIMS server information is specified.

Views

DHCP address pool view

Predefined user roles

network-admin

context-admin

Parameters

ip *ip-address*: Specifies the IP address of the BIMS server.

port *port-number*: Specifies the port number of the BIMS server, in the range of 1 to 65534.

cipher: Specifies a key in encrypted form.

simple: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key string. Its plaintext form is a case-sensitive string of 1 to 16 characters. Its encrypted form is a case-sensitive string of 1 to 53 characters. The DHCP client uses the shared key to encrypt packets sent to the BIMS server.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify BIMS server IP address 1.1.1.1, port number 80, and shared key **aabbcc** in address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] bims-server ip 1.1.1.1 port 80 sharekey simple aabbcc
```

Related commands

display dhcp server pool

bootfile-name

Use **bootfile-name** to specify a configuration file name or URL.

Use **undo bootfile-name** to restore the default.

Syntax

bootfile-name { *bootfile-name* | *url* }

undo bootfile-name

Default

No configuration file name or URL is specified.

Views

DHCP address pool view

Predefined user roles

network-admin

context-admin

Parameters

bootfile-name: Specifies the configuration file name, a case-sensitive string of 1 to 63 characters.

url: Specifies the HTTP URL of the configuration file. It is a case-sensitive string of 1 to 63 characters.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

To specify a configuration file on a TFTP server, use the *bootfile-name* argument.

To specify a configuration file on an HTTP server, use the *url* argument.

Examples

Specify configuration file name **boot.cfg** in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] bootfile-name boot.cfg
```

Specify configuration file URL **http://10.1.1.1/boot.cfg** in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] bootfile-name http://10.1.1.1/boot.cfg
```

Related commands

display dhcp server pool

next-server

tftp-server domain-name

tftp-server ip-address

class ip-pool

Use **class ip-pool** to specify a DHCP address pool for a DHCP user class.

Use **undo class ip-pool** to remove the DHCP address pool specified for a DHCP user class.

Syntax

class *class-name* **ip-pool** *pool-name*

undo class *class-name* **ip-pool**

Default

No DHCP address pool is specified for a DHCP user class.

Views

DHCP policy view

Predefined user roles

network-admin

context-admin

Parameters

class-name: Specifies a DHCP user class by its name, a case-insensitive string of 1 to 63 characters.

pool-name: Specifies a DHCP address pool by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

You can specify only one DHCP address pool for a DHCP user class in a DHCP policy. If you execute this command multiple times for a user class, the most recent configuration takes effect.

Examples

Specify DHCP address pool **pool1** for DHCP user class **test** in DHCP policy 1.

```
<Sysname> system-view
[Sysname] dhcp policy 1
[Sysname-dhcp-policy-1] class test ip-pool pool1
```

Related commands

default ip-pool

dhcp policy

dhcp server ip-pool

class option-group

Use **class option-group** to specify a DHCP option group for a DHCP user class.

Use **undo class option-group** to remove the configuration.

Syntax

class *class-name* **option-group** *option-group-number*

undo class *class-name* **option-group**

Default

No DHCP option group is specified for a DHCP user class.

Views

DHCP address pool view

Predefined user roles

network-admin

context-admin

Parameters

class-name: Specifies a DHCP user class by its name, a case-insensitive string of 1 to 63 characters.

option-group-number: Specifies a DHCP option group by its number in the range of 1 to 32768.

Usage guidelines

When receiving a DHCP-DISCOVER message, the server compares the client against the user classes in the order that they are specified by this command. If a match is found, the server assigns the client the DHCP options in the option group. If multiple matches are found, the server selects option groups by using the following methods:

- If the option groups have options in common, the server selects the option group specified for the first matching user class.
- If the option groups have different options, the server selects all the matching option groups.

You can specify only one option group for a DHCP user class in a DHCP address pool. If you execute this command multiple times for a user class, the most recent configuration takes effect.

Examples

Specify DHCP option group 1 for user class **user** in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] class user option-group 1
```

Related commands

dhcp option-group

class range

Use **class range** to specify an IP address range for a DHCP user class.

Use **undo class range** to remove the IP address range for the DHCP user class.

Syntax

class *class-name* **range** *start-ip-address end-ip-address*

undo class *class-name* **range**

Default

No IP address range is specified for a DHCP user class.

Views

DHCP address pool view

Predefined user roles

network-admin

context-admin

Parameters

class-name: Specifies a DHCP user class name, a case-insensitive string of 1 to 63 characters. If the specified user class does not exist, the DHCP server will not assign the addresses in the address range specified for the user class to any clients.

start-ip-address: Specifies the start IP address.

end-ip-address: Specifies the end IP address.

Usage guidelines

The **class range** command allows you to divide an address range into multiple address ranges for different DHCP user classes. The address range for a user class must be within the primary subnet specified by the **network** command. If the DHCP client does not match any DHCP user class, the DHCP server selects an address in the IP address range specified by the **address range** command. If the address range has no assignable IP addresses or no address range is configured, the address allocation fails.

After you specify an address range for a user class, you cannot use the **network secondary** command to specify a secondary subnet in the address pool.

You can specify only one address range for a DHCP user class in an address pool. If you execute this command multiple times for a DHCP user class, the most recent configuration takes effect.

Examples

Specify an IP address range of 192.168.8.1 through 192.168.8.150 for DHCP user class **user** in DHCP address pool 1.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 1
[Sysname-dhcp-pool-1] class user range 192.168.8.1 192.168.8.150
```

Related commands

address range

dhcp class

display dhcp server pool

default ip-pool

Use **default ip-pool** to specify the default DHCP address pool.

Use **undo default ip-pool** to restore the default.

Syntax

default ip-pool *pool-name*

undo default ip-pool

Default

No default DHCP address pool is specified.

Views

DHCP policy view

Predefined user roles

network-admin

context-admin

Parameters

pool-name: Specifies a DHCP address pool by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

In a DHCP policy, the DHCP server uses the default DHCP address pool to assign IP addresses and other parameters to clients that do not match any user classes. If no default address pool is specified or the default address pool does not have assignable IP addresses, the address assignment fails.

You can specify only one default address pool in a DHCP policy. If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify DHCP address pool **pool1** as the default DHCP address pool in DHCP policy 1.

```
<Sysname> system-view
[Sysname] dhcp policy 1
[Sysname-dhcp-policy-1] default ip-pool pool1
```

Related commands

class ip-pool

dhcp policy

dhcp apply-policy

Use **dhcp apply-policy** to apply a DHCP policy to an interface.

Use **undo dhcp apply-policy** to restore the default.

Syntax

dhcp apply-policy *policy-name*

undo dhcp apply-policy

Default

No DHCP policy is applied to an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies a DHCP policy by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

You can apply only one DHCP policy to an interface. If you execute this command multiple times, the most recent configuration takes effect.

Examples

Apply DHCP policy **test** to GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp apply-policy test
```

Related commands

dhcp policy

dhcp class

Use **dhcp class** to create a DHCP user class and enter its view, or enter the view of an existing DHCP user class.

Use **undo dhcp class** to delete the specified DHCP user class.

Syntax

dhcp class *class-name*

undo dhcp class *class-name*

Default

No DHCP user classes exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

class-name: Specifies the name of a DHCP user class, a case-insensitive string of 1 to 63 characters.

Usage guidelines

In the DHCP user class view, you can use the **if-match** command to configure match rules to group clients to the user class.

Examples

Create DHCP user class **test** and enter DHCP user class view.

```
<Sysname> system-view
[Sysname] dhcp class test
[Sysname-dhcp-class-test]
```

Related commands

address range

class ip-pool

class option-group

class range

dhcp policy

if-match

dhcp option-group

Use **dhcp option-group** to create a DHCP option group and enter its view, or enter the view of an existing DHCP option group.

Use **undo dhcp option-group** to delete a DHCP option group.

Syntax

dhcp option-group *option-group-number*

undo dhcp option-group *option-group-number*

Default

No DHCP option groups exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

option-group-number: Assigns a number to the DHCP option group, in the range of 1 to 32768.

Examples

Create DHCP option group 1 and enter DHCP option group view.

```
<Sysname> system-view
[Sysname] dhcp option-group 1
[Sysname-dhcp-option-group-1]
```

Related commands

class option-group

option

dhcp policy

Use **dhcp policy** to create a DHCP policy and enter its view, or enter the view of an existing DHCP policy.

Use **undo dhcp policy** to delete a DHCP policy.

Syntax

dhcp policy *policy-name*

undo dhcp policy *policy-name*

Default

No DHCP policies exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Assigns a name to the DHCP policy. The policy name is a case-insensitive string of 1 to 63 characters.

Usage guidelines

In DHCP policy view, you can specify address pools for different user classes. Clients matching a user class will obtain IP addresses and other parameters from the specified address pool.

For a DHCP policy to take effect, you must apply it to an interface.

Examples

Create DHCP policy **test** and enter its view.

```
<Sysname> system-view
[Sysname] dhcp policy test
[Sysname-dhcp-policy-test]
```

Related commands

class ip-pool

default ip-pool

dhcp apply-policy

dhcp class

dhcp server always-broadcast

Use **dhcp server always-broadcast** to enable the DHCP server to broadcast all responses.

Use **undo dhcp server always-broadcast** to restore the default.

Syntax

dhcp server always-broadcast

undo dhcp server always-broadcast

Default

The DHCP server reads the broadcast flag in a DHCP request to decide whether to broadcast or unicast the response.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command enables the DHCP server to ignore the broadcast flag in DHCP requests and broadcast all responses.

The DHCP server always unicasts a response in the following situations, regardless of whether this command is executed:

- The DHCP request is from a DHCP client that has an IP address (the **ciaddr** field is not 0).
- The DHCP request is forwarded by a DHCP relay agent from a DHCP client (the **giaddr** field is not 0).

Examples

Enable the DHCP server to broadcast all responses.

```
<Sysname> system-view
[Sysname] dhcp server always-broadcast
```

dhcp server apply ip-pool

Use **dhcp server apply ip-pool** to apply an address pool to an interface.

Use **undo dhcp server apply ip-pool** to restore the default.

Syntax

dhcp server apply ip-pool *pool-name*

undo dhcp server apply ip-pool

Default

No address pool is applied to an interface

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

pool-name: Specifies the name of a DHCP address pool, a case-insensitive string of 1 to 63 characters.

Usage guidelines

Upon receiving a DHCP request from the interface, the DHCP server searches for a static binding for the client from all address pools. If no static binding is found, the server assigns configuration parameters from the address pool applied on the interface to the client. If the address pool has no assignable IP address or does not exist, the DHCP client cannot obtain an IP address.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Apply DHCP address pool 0 to GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp server apply ip-pool 0
```

Related commands

dhcp server ip-pool

dhcp server bootp ignore

Use **dhcp server bootp ignore** to configure the DHCP server to ignore BOOTP requests.

Use **undo dhcp server bootp ignore** to restore the default.

Syntax

dhcp server bootp ignore

undo dhcp server bootp ignore

Default

The DHCP server does not ignore BOOTP requests.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

The lease duration of IP addresses obtained by BOOTP clients is unlimited. For scenarios that do not allow unlimited leases, you can configure the DHCP server to ignore BOOTP requests.

Examples

Configure the DHCP server to ignore BOOTP requests.

```
<Sysname> system-view
[Sysname] dhcp server bootp ignore
```

dhcp server bootp reply-rfc-1048

Use **dhcp server bootp reply-rfc-1048** to enable the sending of BOOTP responses in RFC 1048 format.

Use **undo dhcp server bootp reply-rfc-1048** to disable this feature.

Syntax

dhcp server bootp reply-rfc-1048

undo dhcp server bootp reply-rfc-1048

Default

This feature is disabled. The DHCP server does not process the Vend field of RFC 1048-incompliant requests but copies the Vend field into responses.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

Not all BOOTP clients can send requests compliant with RFC 1048. This command enables the DHCP server to fill the Vend field in RFC 1048-compliant format in DHCP responses to RFC 1048-incompliant requests sent by BOOTP clients.

Examples

Enable the sending of BOOTP responses in RFC 1048 format on the DHCP server.

```
<Sysname> system-view
[Sysname] dhcp server bootp reply-rfc-1048
```

dhcp server database filename

Use **dhcp server database filename** to configure the DHCP server to back up the DHCP bindings to a file.

Use **undo dhcp server database filename** to restore the default.

Syntax

dhcp server database filename { *filename* | **url** *url* [**username** *username* [**password** { **cipher** | **simple** } *string*]] }

undo dhcp server database filename

Default

The DHCP server does not back up the DHCP bindings.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

filename: Specifies the name of a local backup file. For information about the *filename* argument, see *Fundamentals Configuration Guide*.

url *url*: Specifies the URL of a remote backup file, a case-sensitive string of 1 to 255 characters. Do not include a username or password in the URL.

username *username*: Specifies the username for accessing the URL of the remote backup file, a case-sensitive string of 1 to 32 characters. Do not specify this option if a username is not required for accessing the URL of the remote backup file.

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 32 characters. Its encrypted form is a case-sensitive string of 1 to 73 characters. Do not specify this argument if a password is not required for accessing the URL of the remote backup file.

Usage guidelines

The command automatically creates the file if you specify a nonexistent file.

With this command executed, the DHCP server backs up its bindings immediately and runs auto backup. The server, by default, waits 300 seconds after a binding change to update the backup file. You can use the **dhcp server database update interval** command to change the waiting time. If no DHCP binding changes, the backup file is not updated.

As a best practice, back up the bindings to a remote file. If you use the local storage medium, the frequent erasing and writing might damage the medium and then cause the DHCP server to malfunction.

When the backup file is on a remote device, follow these restrictions and guidelines to specify the URL, username, and password:

If the file is on an FTP server, enter URL in the following format: ftp://*server address:port/file path*, where the port number is optional.

If the file is on a TFTP server, enter URL in the following format: tftp://*server address:port/file path*, where the port number is optional.

- The username and password must be the same as those configured on the FTP server. If the server authenticates only the username, the password can be omitted.
- If the IP address of the server is an IPv6 address, enclose the address in a pair of brackets, for example, **ftp://[1::1]/database.dhcp**.
- You can also specify the DNS domain name for the server address field, for example, **ftp://company/database.dhcp**.

Examples

Configure the DHCP server to back up its bindings to file **database.dhcp**.

```
<Sysname> system-view
[Sysname] dhcp server database filename database.dhcp
```

Configure the DHCP server to back up its bindings to file **database.dhcp** in the working directory of the FTP server at 10.1.1.1.

```
<Sysname> system-view
[Sysname] dhcp server database filename url ftp://10.1.1.1/database.dhcp username 1
password simple 1
```

Related commands

dhcp server database update interval

dhcp server database update now

dhcp server database update stop

dhcp server database update interval

Use **dhcp server database update interval** to set the waiting time for the DHCP server to update the backup file after a DHCP binding change.

Use **undo dhcp server database update interval** to restore the default.

Syntax

dhcp server database update interval *interval*

undo dhcp server database update interval

Default

The DHCP server waits 300 seconds to update the backup file after a DHCP binding change. If no DHCP binding changes, the backup file is not updated.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies the waiting time in the range of 60 to 864000 seconds.

Usage guidelines

When a DHCP binding is created, updated, or removed, the waiting period starts. The DHCP server updates the backup file when the waiting period is reached. All bindings changed during the period will be saved to the backup file.

The waiting time takes effect only after you configure the DHCP binding auto backup by using the **dhcp server database filename** command.

Examples

Set the waiting time to 10 minutes for the DHCP server to update the backup file.

```
<Sysname> system-view
[Sysname] dhcp server database update interval 600
```

Related commands

dhcp server database filename

dhcp server database update now

dhcp server database update stop

dhcp server database update now

Use **dhcp server database update now** to manually save the DHCP bindings to the backup file.

Syntax

dhcp server database update now

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

Each time this command is executed, the DHCP bindings are saved to the backup file.

For this command to take effect, you must configure the DHCP auto backup by using the **dhcp server database filename** command.

Examples

Manually save the DHCP bindings to the backup file.

```
<Sysname> system-view
[Sysname] dhcp server database update now
```

Related commands

dhcp server database filename

dhcp server database update interval

dhcp server database update stop

dhcp server database update stop

Use **dhcp server database update stop** to terminate the download of DHCP bindings from the backup file.

Syntax

dhcp server database update stop

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

The DHCP server does not provide services during the binding download process. If the connection disconnects during the process, the waiting timeout timer is 60 minutes. When the timer expires, the DHCP server stops waiting and starts providing address allocation services.

To enable the DHCP server to provide services without waiting for the connection to be repaired, use this command to terminate the download immediately. The IP addresses associated with the undownloaded bindings will be assigned to clients. Address conflicts might occur.

Examples

Terminate the download of the backup DHCP bindings.

```
<Sysname> system-view
[Sysname] dhcp server database update stop
```

Related commands

dhcp server database filename

dhcp server database update interval

dhcp server database update now

dhcp server forbidden-ip

Use **dhcp server forbidden-ip** to exclude IP addresses from dynamic allocation globally.

Use **undo dhcp server forbidden-ip** to remove the configuration.

Syntax

dhcp server forbidden-ip *start-ip-address* [*end-ip-address*] [**vpn-instance** *vpn-instance-name*]

undo dhcp server forbidden-ip *start-ip-address* [*end-ip-address*] [**vpn-instance** *vpn-instance-name*]

Default

No IP addresses are excluded from dynamic allocation globally.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

start-ip-address: Specifies the start IP address.

end-ip-address: Specifies the end IP address, which cannot be lower than the *start-ip-address*. If you do not specify this argument, only the *start-ip-address* is excluded from dynamic allocation.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If the excluded IP addresses belong to the public network, do not specify this option.

Usage guidelines

The IP addresses of some devices such as the gateway and FTP server cannot be assigned to clients. Use this command to exclude such addresses from dynamic allocation.

If the excluded IP address is in a static DHCP binding, the address can still be assigned to the client.

The address or address range specified in the **undo dhcp server forbidden-ip** command must be the same as that specified in the **dhcp server forbidden-ip** command. To remove an IP address from the specified address range, you must remove the entire address range.

You can execute this command multiple times to exclude multiple IP address ranges from dynamic allocation.

Examples

Exclude the IP addresses of 10.110.1.1 through 10.110.1.63 from dynamic allocation globally.

```
<Sysname> system-view
[Sysname] dhcp server forbidden-ip 10.110.1.1 10.110.1.63
```

Related commands

forbidden-ip

static-bind

dhcp server ip-pool

Use **dhcp server ip-pool** to create a DHCP address pool and enter its view, or enter the view of an existing DHCP address pool.

Use **undo dhcp server ip-pool** to delete the specified DHCP address pool.

Syntax

dhcp server ip-pool *pool-name*

undo dhcp server ip-pool *pool-name*

Default

No DHCP address pools exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

pool-name: Specifies a DHCP address pool name, a case-insensitive string of 1 to 63 characters. The pool name uniquely identifies an address pool.

Usage guidelines

A DHCP address pool is used to store the configuration parameters to be assigned to DHCP clients.

Examples

Create a DHCP address pool named **pool1**.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool pool1
[Sysname-dhcp-pool-pool1]
```

Related commands

class ip-pool

dhcp server apply ip-pool

display dhcp server pool

dhcp server ping packets

Use **dhcp server ping packets** to set the maximum number of ping packets.

Use **undo dhcp server ping packets** to restore the default.

Syntax

dhcp server ping packets *number*

undo dhcp server ping packets

Default

The maximum number of ping packets is 1.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

number: Sets the maximum number of ping packets, in the range of 0 to 10. To disable the address conflict detection, set the value to 0.

Usage guidelines

To avoid IP address conflicts, the DHCP server pings an IP address before assigning it to a DHCP client.

If a ping attempt succeeds, the server determines that the IP address is in use and picks a new IP address. If all the ping attempts fail, the server assigns the IP address to the requesting DHCP client.

Examples

Set the maximum number of ping packets to 10.

```
<Sysname> system-view
[Sysname] dhcp server ping packets 10
```

Related commands

dhcp server ping timeout

display dhcp server conflict

reset dhcp server conflict

dhcp server ping timeout

Use **dhcp server ping timeout** to set the ping response timeout time on the DHCP server.

Use **undo dhcp server ping timeout** to restore the default.

Syntax

dhcp server ping timeout *milliseconds*

undo dhcp server ping timeout

Default

The ping response timeout time is 500 milliseconds.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

milliseconds: Specifies the timeout time in the range of 0 to 10000 milliseconds. To disable the ping operation for address conflict detection, set the value to 0 milliseconds.

Usage guidelines

To avoid IP address conflicts, the DHCP server pings an IP address before assigning it to a DHCP client.

If a ping attempt succeeds, the server determines that the IP address is in use and picks a new IP address. If all the ping attempts fail, the server assigns the IP address to the requesting DHCP client.

Examples

Set the response timeout time to 1000 milliseconds.

```
<Sysname> system-view
[Sysname] dhcp server ping timeout 1000
```

Related commands

dhcp server ping packets

display dhcp server conflict

reset dhcp server conflict

dhcp server relay information enable

Use **dhcp server relay information enable** to enable the DHCP server to handle Option 82.

Use **undo dhcp server relay information enable** to configure the DHCP server to ignore Option 82.

Syntax

dhcp server relay information enable

undo dhcp server relay information enable

Default

The DHCP server handles Option 82.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

Upon receiving a DHCP request that contains Option 82, the server copies the original Option 82 into the response. If the server is configured to ignore Option 82, the response will not contain Option 82.

Examples

Configure the DHCP server to ignore Option 82.

```
<Sysname> system-view
[Sysname] undo dhcp server relay information enable
```

dhcp server reply-exclude-option60

Use **dhcp server reply-exclude-option60** to disable the DHCP server from encapsulating Option 60 in DHCP replies.

Use **undo dhcp server reply-exclude-option60** to restore the default.

Syntax

dhcp server reply-exclude-option60

undo dhcp server reply-exclude-option60

Default

The DHCP server can encapsulate Option 60 in DHCP replies.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

If you do not disable the capability, the DHCP server encapsulates Option 60 in a DHCP reply in the following situations:

- The received DHCP packet contains Option 60.
- Option 60 is configured for the address pool.

If you disable the capability, the DHCP server does not encapsulate Option 60 in DHCP replies.

Examples

Disable the DHCP server from encapsulating Option 60 in DHCP replies.

```
<Sysname> system-view
[Sysname] dhcp server reply-exclude-option60
```

display dhcp server conflict

Use **display dhcp server conflict** to display information about IP address conflicts.

Syntax

display dhcp server conflict [**ip** *ip-address*] [**vpn-instance** *vpn-instance-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ip *ip-address*: Displays conflict information about the specified IP address. If you do not specify this option, this command displays information about all IP address conflicts.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays IP address conflict information for the public network.

Usage guidelines

The DHCP server generates IP address conflict information in the following situations:

- Before assigning an IP address to a DHCP client, the DHCP server pings the IP address and discovers that another host is using the address.
- The DHCP client sends a DECLINE packet to the DHCP server to inform the server of an IP address conflict.
- The DHCP server discovers that the only assignable address in the address pool is its own IP address.

Examples

Display information about all IP address conflicts.

```
<Sysname> display dhcp server conflict
IP address          Detect time
4.4.4.1             Apr 25 16:57:20 2019
4.4.4.2             Apr 25 17:00:10 2019
```

Table 1 Command output

Field	Description
IP address	Conflicted IP address.
Detect time	Time when the conflict was discovered.

Related commands

reset dhcp server conflict

display dhcp server database

Use **display dhcp server database** to display information about DHCP binding auto backup.

Syntax

display dhcp server database

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display information about DHCP binding auto backup.

```
<Sysname> display dhcp server database
 File name               :   database.dhcp
 Username                :
 Password                :
 Update interval         :   600 seconds
 Latest write time       :   Feb  8 16:09:53 2014
 Status                  :   Last write succeeded.
```

Table 2 Command output

Field	Description
File name	Name of the DHCP binding backup file.
Username	Username for accessing the URL of the remote backup file.
Password	Password for accessing the URL of the remote backup file. This field displays ********** if a password is configured.
Update interval	Waiting time in seconds after a DHCP binding change for the DHCP server to update the backup file.
Latest write time	Time of the latest update.
Status	Status of the update: • **Writing**—The backup file is being updated. • **Last write succeeded**—The backup file was successfully updated. • **Last write failed**—The backup file failed to be updated.

display dhcp server expired

Use **display dhcp server expired** to display the lease expiration information.

Syntax

display dhcp server expired [[**ip** *ip-address*] [**vpn-instance** *vpn-instance-name*] | **pool** *pool-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ip *ip-address*: Displays lease expiration information about the specified IP address. If you do not specify an IP address, this command displays lease expiration information about all IP addresses.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays lease expiration information about IP addresses for the public network.

pool *pool-name*: Displays lease expiration information about the specified address pool. The pool name is a case-insensitive string of 1 to 63 characters. If you do not specify an address pool, this command displays lease expiration information about all address pools.

Usage guidelines

DHCP assigns these expired IP addresses to DHCP clients when all available addresses have been assigned.

Examples

Display all lease expiration information.

```
<Sysname> display dhcp server expired
IP address       Client-identifier/Hardware address    Lease expiration
4.4.4.6          3030-3066-2e65-3230-302e-3130-3234    Apr 25 17:10:47 2019
                 -2d45-7468-6572-6e65-7430-2f31
```

Table 3 Command output

Field	Description
IP address	Expired IP address.
Client-identifier/Hardware address	Client ID or MAC address. For the client ID: • If an ASCII string is used as the client ID value, the type value is 00. • If the MAC address of an interface is used as the client ID value, the type value is 01. • If a hexadecimal string is used as the client ID value, the type value is the first two digits of the string.
Lease expiration	Time when the lease expired.

Related commands

reset dhcp server expired

display dhcp server free-ip

Use **display dhcp server free-ip** to display information about assignable IP addresses.

Syntax

display dhcp server free-ip [**pool** *pool-name* | **vpn-instance** *vpn-instance-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

pool *pool-name*: Displays assignable IP addresses in the specified address pool. The pool name is a case-insensitive string of 1 to 63 characters. If you do not specify an address pool, this command displays all assignable IP addresses for all address pools.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays assignable IP addresses in address pools for the public network.

Examples

Display assignable IP addresses in all address pools.

```
<Sysname> display dhcp server free-ip
Pool name: 1
  Network: 10.0.0.0 mask 255.0.0.0
    IP ranges from 10.0.0.10 to 10.0.0.100
    IP ranges from 10.0.0.105 to 10.0.0.255
  Secondary networks:
    10.1.0.0 mask 255.255.0.0
      IP ranges from 10.1.0.0 to 10.1.0.255
    10.2.0.0 mask 255.255.0.0
      IP Ranges from 10.2.0.0 to 10.2.0.255

Pool name: 2
  Network: 20.1.1.0 mask 255.255.255.0
    IP ranges from 20.1.1.0 to 20.1.1.255
```

Table 4 Command output

Field	Description
Pool name	Name of the address pool.
Network	Assignable network.
IP ranges	Assignable IP address range.
Secondary networks	Assignable secondary networks.

Related commands

address range

dhcp server ip-pool

network

display dhcp server ip-in-use

Use **display dhcp server ip-in-use** to display binding information about assigned IP addresses.

Syntax

display dhcp server ip-in-use [[**ip** *ip-address*] [**vpn-instance** *vpn-instance-name*] | **pool** *pool-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ip *ip-address*: Displays binding information about the specified assigned IP address. If you do not specify an IP address, this command displays binding information about all assigned IP addresses.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays binding information about assigned IP addresses for the public network.

pool *pool-name*: Displays binding information about assigned IP addresses in the specified address pool. The pool name is a case-insensitive string of 1 to 63 characters. If you do not specify an address pool, this command displays binding information about assigned IP addresses in all address pools.

Usage guidelines

The binding information can be used by other security modules only when the DHCP server is configured on the gateway of DHCP clients.

If the lease deadline exceeds the year 2100, the lease expiration time is displayed as **After 2100**.

Examples

Display binding information about all assigned DHCP addresses.

```
<Sysname> display dhcp server ip-in-use
IP address       Client identifier/    Lease expiration      Type
                 Hardware address
10.1.1.1         4444-4444-4444        Not used              Static(F)
10.1.1.2         0030-3030-302e-3030-  May 1 14:02:49 2015   Auto(C)
                 3066-2e30-3030-332d-
                 4574-6865-726e-6574
10.1.1.3         1111-1111-1111        After 2100            Static(C)
```

Table 5 Command output

Field	Description
IP address	IP address assigned.
Client identifier/Hardware address	Client ID or hardware address. Client ID is specified as a string of hexadecimal numbers, in which the first two characters represents the hardware type value. • If an ASCII string is used, the hardware type value is 00, which means no type. • If the hardware type is Ethernet, the type value is 01. • If the hardware type is token ring, the type value is 06.

Field	Description
Lease expiration	Lease expiration time: • **Exact time (May 1 14:02:49 2015 in this example)**—Time when the lease will expire. • **Not used**—The IP address of the static binding has not been assigned to the specific client. • **Unlimited**—Infinite lease expiration time. • **After 2100**—The lease will expire after 2100.
Type	Binding types: • **Static(F)**—A free static binding whose IP address has not been assigned. • **Static(O)**—An offered static binding whose IP address has been selected and sent by the DHCP server in a DHCP-OFFER packet to the client. **Static(C)**—A committed static binding whose IP address has been assigned to the DHCP client. • **Auto(O)**—An offered dynamic binding whose IP address has been dynamically selected by the DHCP server and sent in a DHCP-OFFER packet to the DHCP client. • **Auto(C)**—A committed dynamic binding whose IP address has been dynamically assigned to the DHCP client.

Related commands

`reset dhcp server ip-in-use`

display dhcp server pool

Use **`display dhcp server pool`** to display information about a DHCP address pool.

Syntax

`display dhcp server pool` [*`pool-name`* | **`vpn-instance`** *`vpn-instance-name`*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

`pool-name`: Displays information about the specified address pool. The pool name is a case-insensitive string of 1 to 63 characters. If you do not specify the *`pool-name`* argument, this command displays information about all address pools.

`vpn-instance` *`vpn-instance-name`*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays information about address pools for the public network.

Examples

Display information about all DHCP address pools.

```
<Sysname> display dhcp server pool
Pool name: 0
```

```
  Network 20.1.1.0 mask 255.255.255.0
  class a range 20.1.1.50 20.1.1.60
  bootfile-name abc.cfg
  dns-list 20.1.1.66 20.1.1.67 20.1.1.68
  domain-name www.aabbcc.com
  bims-server ip 192.168.0.51 sharekey cipher $c$3$K13OmQPi791YvQoF2Gs1E+65LOU=
  option 2 ip-address 1.1.1.1
  expired day 1 hour 2 mimute 3 second 0

Pool name: 1
  Network 20.1.2.0 mask 255.255.255.0
  secondary networks:
    20.1.3.0 mask 255.255.255.0
    20.1.4.0 mask 255.255.255.0
  bims-server ip 192.168.0.51 port 50 sharekey cipher $c$3$K13OmQPi791YvQoF2Gs1E+65LOU=
  forbidden-ip 20.1.2.35 20.1.2.36 20.1.2.37
  forbidden-ip 20.1.2.22 20.1.2.23 20.1.2.24
  forbidden-ip-range 20.1.2.50 20.1.2.55
  gateway-list 20.1.2.1 20.1.2.2 20.1.2.4
  nbns-list 20.1.2.5 20.1.2.6 20.1.2.7
  netbios-type m-node
  option 2 ip-address 1.1.1.1
  expired day 1 hour 0 minute 0 second 0

Pool name: 2
  Network 20.1.3.0 mask 255.255.255.0
  address range 20.1.3.1 to 20.1.3.15
  class departmentA range 20.1.3.20 to 20.1.3.29
  class departmentB range 20.1.3.30 to 20.1.3.40
  next-server 20.1.3.33
  tftp-server domain-name www.dian.org.cn
  tftp-server ip-address 192.168.0.120
  voice-config ncp-ip 20.1.3.2
  voice-config as-ip 20.1.3.5
  voice-config voice-vlan 3 enable
  voice-config fail-over 20.1.3.6 123*
  option 2 ip-address 20.1.3.10
expired day 1 hour 0 minute 0 second 0

Pool name: 3
  static bindings:
    ip-address 10.10.1.2 mask 255.0.0.0
      hardware-address 00e0-00fc-0001 ethernet
      description ClientA
    ip-address 10.10.1.3 mask 255.0.0.0
      client-identifier aaaa-bbbb
      description ClientB
  expired unlimited
```

Table 6 Command output

Field	Description
Pool name	Name of an address pool.
Network	Assignable network.
secondary networks	Assignable secondary networks.
address range	Assignable address range.
class *class-name* range	DHCP user class and its address range.
static bindings	Static IP-to-MAC/client ID bindings.
ip-address mask	IP address and mask in the static binding.
hardware-address	Hardware address in the static binding.
client-identifier	Client ID in the static binding.
description	Description of the static binding.
option	Customized DHCP option.
expired	Lease duration.
bootfile-name	Boot file name
dns-list	DNS server IP address.
domain-name	Domain name suffix.
bims-server	BIMS server information.
forbidden-ip	IP addresses excluded from dynamic allocation.
forbidden-ip-range	IP address range excluded from dynamic allocation.
gateway-list	Gateway addresses.
nbns-list	WINS server addresses.
netbios-type	NetBIOS node type.
next-server	Next server IP address.
tftp-server domain-name	TFTP server name.
tftp-server ip-address	TFTP server address.
voice-config ncp-ip	Primary network calling processor address.
voice-config as-ip	Backup network calling processor address.
voice-config voice-vlan	Voice VLAN.
voice-config fail-over	Failover route.

display dhcp server statistics

Use **display dhcp server statistics** to display the DHCP server statistics.

Syntax

display dhcp server statistics [**pool** *pool-name* | **vpn-instance** *vpn-instance-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

pool *pool-name*: Specifies an address pool by its name, a case-insensitive string of 1 to 63 characters. If you do not specify this option, this command displays information about all address pools.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays DHCP server statistics for the public network.

Examples

Display the DHCP server statistics.

```
<Sysname> display dhcp server statistics
    Pool number:                    1
    Pool utilization:               0.39%
    Bindings:
      Automatic:                    1
      Manual:                       0
      Expired:                      0
    Conflict:                       1
    Messages received:              10
      DHCPDISCOVER:                 5
      DHCPREQUEST:                  3
      DHCPDECLINE:                  0
      DHCPRELEASE:                  2
      DHCPINFORM:                   0
      BOOTPREQUEST:                 0
    Messages sent:                  6
      DHCPOFFER:                    3
      DHCPACK:                      3
      DHCPNAK:                      0
      BOOTPREPLY:                   0
    Bad Messages:                   0
```

Table 7 Command output

Field	Description
Pool number	Total number of address pools. This field is not displayed when you display statistics for a specific address pool.

Field	Description
Pool utilization	Pool usage rate: • If you display statistics for all address pools, this field displays the usage rate of all address pools. • If you display statistics for an address pool, this field displays the pool usage rate of the specified address pool.
Bindings	Bindings include the following types: • **Automatic**—Number of dynamic bindings. • **Manual**—Number of static bindings. • **Expired**—Number of expired bindings.
Conflict	Total number of conflict addresses. This field is not displayed if you display statistics for a specific address pool.
Messages received	DHCP packets received from clients: • DHCPDISCOVER. • DHCPREQUEST. • DHCPDECLINE. • DHCPRELEASE. • DHCPINFORM. • BOOTPREQUEST. This field is not displayed if you display statistics for a specific address pool.
Messages sent	DHCP packets sent to clients: • DHCPOFFER. • DHCPACK. • DHCPNAK. • BOOTPREPLY. This field is not displayed if statistics about a specific address pool are displayed.
Bad Messages	Number of bad messages. This field is not displayed if you display statistics for a specific address pool.

Related commands

reset dhcp server statistics

dns-list

Use **dns-list** to specify DNS server addresses in a DHCP address pool.

Use **undo dns-list** to remove DNS server addresses from a DHCP address pool.

Syntax

dns-list *ip-address*&<1-8>

undo dns-list [*ip-address*&<1-8>]

Default

No DNS server address is specified.

Views

DHCP address pool view

Predefined user roles

network-admin

context-admin

Parameters

ip-address&<1-8>: Specifies a space-separated list of up to eight DNS servers.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

If you do not specify any parameters, the **undo dns-list** command deletes all DNS server addresses in the DHCP address pool.

Examples

Specify DNS server address 10.1.1.254 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] dns-list 10.1.1.254
```

Related commands

display dhcp server pool

domain-name

Use **domain-name** to specify a domain name in a DHCP address pool.

Use **undo domain-name** to restore the default.

Syntax

domain-name *domain-name*

undo domain-name

Default

No domain name is specified.

Views

DHCP address pool view

Predefined user roles

network-admin

context-admin

Parameters

domain-name: Specifies the domain name, a case-sensitive string of 1 to 50 characters.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify domain name **company.com** in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] domain-name company.com
```

Related commands

display dhcp server pool

expired

Use **expired** to set the lease duration in a DHCP address pool.

Use **undo expired** to restore the default lease duration for a DHCP address pool.

Syntax

expired { **day** *day* [**hour** *hour* [**minute** *minute* [**second** *second*]]] | **unlimited** }

undo expired

Default

The lease duration of a dynamic DHCP address pool is one day.

Views

DHCP address pool view

Predefined user roles

network-admin

context-admin

Parameters

day *day*: Specifies the number of days, in the range of 0 to 365.

hour *hour*: Specifies the number of hours, in the range of 0 to 23. The default is 0.

minute *minute*: Specifies the number of minutes, in the range of 0 to 59. The default is 0.

second *second*: Specifies the number of seconds, in the range of 0 to 59. The default is 0.

unlimited: Specifies the unlimited lease duration, which is actually 136 years.

Usage guidelines

The DHCP server assigns an IP address together with the lease duration to the DHCP client. Before the lease expires, the DHCP client must extend the lease duration.

- If the lease extension operation succeeds, the DHCP client can continue to use the IP address.
- If the lease extension operation does not succeed, both of the following events occur:
  - The DHCP client cannot use the IP address after the lease duration expires.
  - The DHCP server will label the IP address as an expired address.

Examples

Set the lease duration to 1 day, 2 hours, 3 minutes, and 4 seconds in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] expired day 1 hour 2 minute 3 second 4
```

Related commands

display dhcp server expired

display dhcp server pool

reset dhcp server expired

forbidden-ip

Use **forbidden-ip** to exclude IP addresses from dynamic allocation in an address pool.

Use **undo forbidden-ip** to remove the configuration.

Syntax

forbidden-ip *ip-address*&<1-8>

undo forbidden-ip [*ip-address*&<1-8>]

Default

No IP addresses are excluded from dynamic allocation in an address pool.

Views

DHCP address pool view

Predefined user roles

network-admin

context-admin

Parameters

ip-address&<1-8>: Specifies a space-separated list of up to eight excluded IP addresses.

Usage guidelines

The excluded IP addresses in an address pool are still assignable in other address pools.

You can exclude a maximum of 4096 IP addresses in an address pool by executing this command multiple times.

If you do not specify any parameters, the **undo forbidden-ip** command removes all excluded IP addresses.

Examples

Exclude IP addresses 192.168.1.3 and 192.168.1.10 from dynamic allocation in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] forbidden-ip 192.168.1.3 192.168.1.10
```

Related commands

dhcp server forbidden-ip

display dhcp server pool

forbidden-ip-range

Use **forbidden-ip-range** to exclude an IP address range from dynamic allocation in an address pool.

Use **undo forbidden-ip-range** to remove the configuration.

Syntax

forbidden-ip-range *start-ip-address* [*end-ip-address*]

undo forbidden-ip-range [*start-ip-address* [*end-ip-address*]]

Default

No IP address ranges are excluded from dynamic allocation in an address pool.

Views

DHCP address pool view

Predefined user roles

network-admin

contextmdc-admin

Parameters

start-ip-address: Specifies a start IP address.

end-ip-address: Specifies an end IP address. The end IP address cannot be lower than the start IP address. If you do not specify this argument, the excluded IP range includes only the start IP address.

Usage guidelines

The excluded IP address range in an address pool is still assignable in other address pools.

To specify multiple excluded IP address ranges, execute the **forbidden-ip-range** command multiple times. IP addresses in excluded IP address ranges can overlap.

If you do not specify any parameters, the **undo forbidden-ip-range** command removes all excluded IP address ranges.

If the **undo** command specifies an address range smaller than the existing excluded address range, the **undo** command removes only the specified address range. If the **undo** command specifies an address range broader than the existing excluded address range, the existing excluded range is removed.

Examples

Exclude IP address range 192.168.1.3 to 192.168.1.10 from dynamic allocation in DHCP address pool **0**.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] forbidden-ip-range 192.168.1.3 192.168.1.10
```

Related commands

display dhcp server pool

gateway-list

Use **gateway-list** to specify gateway addresses in a DHCP address pool or a DHCP secondary subnet.

Use **undo gateway-list** to remove the specified gateway addresses from a DHCP address pool or a DHCP secondary subnet.

Syntax

gateway-list *ip-address*&<1-64> [**export-route**]

undo gateway-list [*ip-address*&<1-64>] [**export-route**]

Default

No gateway address is configured in a DHCP address pool or a DHCP secondary subnet.

Views

DHCP address pool view

DHCP secondary subnet view

Predefined user roles

network-admin

context-admin

Parameters

ip-address&<1-64>: Specifies a space-separated list of up to 64 gateway addresses. Gateway addresses must reside on the same subnet as the assignable IP addresses.

export-route: Binds the gateways to the device's MAC address in the address management module. The ARP module will use the entries to reply to ARP requests from the DHCP clients. If you do not specify this keyword, the gateways will not be bound to the device's MAC address.

Usage guidelines

The DHCP server assigns gateway addresses to clients on a secondary subnet in the following ways:

- If gateways are specified in both address pool view and secondary subnet view, DHCP assigns those specified in the secondary subnet view.
- If gateways are specified in address pool view but not in secondary subnet view, DHCP assigns those specified in address pool view.

If you do not specify any parameters, the **undo gateway-list** command deletes all gateway addresses.

Examples

Specify gateway address 10.1.1.1 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] gateway-list 10.1.1.1
```

Related commands

display dhcp server pool

if-match

Use **if-match** to configure a match rule for a DHCP user class.

Use **undo if-match** to delete a match rule for a DHCP user class.

Syntax

if-match rule *rule-number* { **hardware-address** *hardware-address* **mask** *hardware-address-mask* | **option** *option-code* [**ascii** *ascii-string* [**offset** *offset* | **partial**] | **hex** *hex-string* [**mask** *mask* | **offset** *offset* **length** *length* | **partial**]] | **relay-agent** *gateway-address* }

undo if-match rule *rule-number*

Default

No match rules are configured for the DHCP user class.

Views

DHCP user class view

Predefined user roles

network-admin

context-admin

Parameters

rule *rule-number*: Assigns the match rule an ID in the range of 1 to 128. A smaller ID represents a higher match priority.

hardware-address *hardware-address*: Specifies a hardware address, a string of 4 to 39 characters. The string contains hyphen-separated hexadecimal numbers. The last hexadecimal number can be a two-digit or four-digit number, and the other hexadecimal numbers must be four-digit numbers. For example, **aabb-ccdd-ee** is valid, and **aabb-c-dddd** or **aabb-cc-dddd** is invalid.

mask *hardware-address-mask*: Specifies the mask to be ANDed with the specified hardware address for the match operation. The length of the mask must be the same as that of the hardware address.

option *option-code*: Specifies a DHCP option by its number in the range of 1 to 254.

ascii *ascii-string*: Specifies an ASCII string of 1 to 128 characters.

offset *offset*: Specifies the offset in bytes after which the match operation starts. The value range is 0 to 254. If you do not specify an offset value, the match starts from the first byte of the option content. If you specify an ASCII string, a packet matches the rule if the option content after the offset is the same as the ASCII string. If you specify a hexadecimal number, a packet matches the rule if the option content of the specified length after the offset is the same as the hexadecimal number.

partial: Enables partial match. A packet matches a rule if the specified option in the packet contains the ASCII string or hexadecimal number specified in the rule. For example, if you specify **abc** in the rule, option content **xabc**, **xyzabca**, **xabcyz**, and **abcxyz** all match the rule.

hex *hex-string*: Specifies a hexadecimal number. The length of the hexadecimal number must be an even number in the range of 2 to 256.

mask *mask*: Specifies a hexadecimal mask for the match operation. The mask length must be an even number in the range of 2 to 256 and be the same as the *hex-string* length. The DHCP server selects option content of the mask length from the start and ANDs the selected option content and the specified hexadecimal number with the mask. The packet matches the rule if the two AND operation results are the same.

length *length*: Specifies the length of the option content to be matched, in the range of 1 to 128 bytes. The length must be the same as the *hex-string* length.

relay-agent *gateway-address*: Specifies a **giaddr** field value. The value is an IPv4 address in the dotted decimal notation. A packet matches the rule if its **giaddr** field value is the same as that in the rule.

Usage guidelines

If a DHCP request sent by a DHCP client matches a rule in a DHCP user class, the DHCP client matches the user class.

You can configure multiple match rules for a DHCP user class. Each match rule is uniquely identified by a rule ID within its type (hardware address, option, or relay agent address).

- If the rule that you are configuring has the same ID and type as an existing rule, the new rule overwrites the existing rule.
- If the rule that you are configuring has the same ID as an existing rule but a different type, the new rule takes effect and coexists with the existing rule. As a best practice, do not assign the same ID to rules of different types.
- Rules of different IDs cannot have the same rule content.

When you configure an **if-match hardware-address** rule, follow these guidelines:

- The hardware address type supports only the MAC address. A rule does not match clients with hardware addresses of other types.
- The specified hardware address must be of the same length as the client hardware addresses to be matched. To match MAC addresses, the specified hardware address must be six bytes long.
- The fs and 0s in the mask for the hardware match operation can be noncontiguous. For example, the rule **if-match rule** 1 **hardware-address** 0094-0000-1100 **mask** ffff-0000-ff00 matches hardware addresses in which the first two bytes are 0094 and the fifth byte is 11.

When you configure an **if-match option** rule, follow these guidelines:

- To match packets that contain an option, specify only the *option-code* argument.
- To match a hexadecimal number by AND operations, specify the **option** *option-code* **hex** *hex-string* **mask** *mask* options.
- To match a hexadecimal number directly, specify the **option** *option-code* **hex** *hex-string* [**offset** *offset* **length** *length* | **partial**] options. If you do not specify the **offset**, **length**, or **partial** parameter, a packet matches a rule if the option content starts with the hexadecimal number.
- To match an ASCII string, specify the **option** *option-code* **ascii** *ascii-string* [**offset** *offset* | **partial**] options. If you do not specify the **offset** or **partial** parameter, a packet matches a rule if the option content starts with the ASCII string.

Examples

Configure match rule **1** for DHCP user class **exam** to match DHCP requests in which the hardware address is six bytes long and begins with **0094**.

```
<Sysname> system-view
[Sysname] dhcp class exam
[Sysname-dhcp-class-exam] if-match rule 1 hardware-address 0094-0000-0101 mask
ffff-0000-0000
```

Configure match rule **2** for DHCP user class **exam** to match DHCP requests that contain Option 82.

```
<Sysname> system-view
[Sysname] dhcp class exam
[Sysname-dhcp-class-exam] if-match rule 2 option 82
```

Configure match rule **3** for DHCP user class **exam**. The rule matches DHCP requests in which the highest bit of the fourth byte in Option 82 is the hexadecimal number **1**.

```
<Sysname> system-view
[Sysname] dhcp class exam
[Sysname-dhcp-class-exam] if-match rule 3 option 82 hex 00000080 mask 00000080
```

Configure match rule **4** for DHCP user class **exam**. The rule matches DHCP requests in which the first three bytes of Option 82 are the hexadecimal number **13ae92**.

```
<Sysname> system-view
[Sysname] dhcp class exam
[Sysname-dhcp-class-exam] if-match rule 4 option 82 hex 13ae92 offset 0 length 3
```

Configure match rule **5** for DHCP user class **exam**. The rule matches DHCP requests in which the Option 82 contains the hexadecimal number **13ae**.

```
<Sysname> system-view
[Sysname] dhcp class exam
[Sysname-dhcp-class-exam] if-match rule 5 option 82 hex 13ae partial
```

Configure match rule **6** for DHCP user class **exam** to match DHCP requests in which the **giaddr** field is 10.1.1.1.

```
<Sysname> system-view
[Sysname] dhcp class exam
[Sysname-dhcp-class-exam] if-match rule 6 relay-agent 10.1.1.1
```

Related commands

dhcp class

ip-in-use threshold

Use **ip-in-use threshold** to set a threshold for the address pool usage alarming.

Use **undo ip-in-use threshold** to restore the default.

Syntax

ip-in-use threshold *threshold-value*

undo ip-in-use threshold

Default

The address pool usage threshold is 100%.

Views

DHCP address pool view

Predefined user roles

network-admin

context-admin

Parameters

threshold-value: Specifies the threshold for the address pool usage percentage. The value range is 1 to 100.

Usage guidelines

If you execute this command in the same address pool view multiple times, the most recent configuration takes effect.

When the address pool usage exceeds the threshold, the system sends notifications to the SNMP module. For DHCP notifications to be sent correctly, you must also configure SNMP on the device. For more information about SNMP configuration, see *Network Management and Monitoring Configuration Guide*.

Examples

Set the address pool usage threshold to 85%.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool p1
[Sysname-dhcp-pool-p1] ip-in-use threshold 85
```

nbns-list

Use **nbns-list** to specify WINS server addresses in a DHCP address pool.

Use **undo nbns-list** to remove the specified WINS server addresses.

Syntax

nbns-list *ip-address*&<1-8>

undo nbns-list [*ip-address*&<1-8>]

Default

No WINS server address is specified.

Views

DHCP address pool view

Predefined user roles

network-admin

context-admin

Parameters

ip-address&<1-8>: Specifies a space-separated list of up to eight WINS server IP addresses.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

If you do not specify any parameters, the **undo nbns-list** command deletes all WINS server addresses.

Examples

Specify WINS server address 10.1.1.1 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] nbns-list 10.1.1.1
```

Related commands

display dhcp server pool

netbios-type

netbios-type

Use **netbios-type** to specify the NetBIOS node type in a DHCP address pool.

Use **undo netbios-type** to restore the default.

Syntax

netbios-type { **b-node** | **h-node** | **m-node** | **p-node** }

undo netbios-type

Default

No NetBIOS node type is specified.

Views

DHCP address pool view

Predefined user roles

network-admin

context-admin

Parameters

b-node: Specifies the broadcast node. A b-node client sends the destination name in a broadcast message to get the name-to-IP mapping from a server.

h-node: Specifies the hybrid node. An h-node client unicasts the destination name to a WINS server. If it does not receive a response, the h-node client broadcasts the destination name to get the mapping from a server.

m-node: Specifies the mixed node. An m-node client broadcasts the destination name. If it does not receive a response, the m-node client unicasts the destination name to the WINS server to get the mapping.

p-node: Specifies the peer-to-peer node. A p-node client sends the destination name in a unicast message to get the mapping from the WINS server.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the NetBIOS node type as p-node in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] netbios-type p-node
```

Related commands

display dhcp server pool

nbns-list

network

Use **network** to specify the subnet for dynamic allocation in a DHCP address pool.

Use **undo network** to remove the specified subnet.

Syntax

network *network-address* [*mask-length* | **mask** *mask*] [**secondary**] [**export-route**]

undo network *network-address* [*mask-length* | **mask** *mask*] [**secondary**]

Default

No subnet is specified in a DHCP address pool.

Views

DHCP address pool view

Predefined user roles

network-admin

context-admin

Parameters

network-address: Specifies the subnet for dynamic allocation. If no mask length or mask is specified, the natural mask will be used.

mask-length: Specifies the mask length in the range of 1 to 30.

mask *mask*: Specifies the mask in dotted decimal format.

secondary: Specifies the subnet as a secondary subnet. If you do not specify this keyword, this command specifies the primary subnet. If the addresses in the primary subnet are used up, the DHCP server can select addresses from a secondary subnet for clients.

export-route: Advertises the subnet assigned to DHCP clients. If you do not specify this keyword, the subnet will not be advertised.

Usage guidelines

You can use the **secondary** keyword to specify a secondary subnet and enter its view. In secondary subnet view, you can specify gateways by using the **gateway-list** command for DHCP clients in the secondary subnet.

You can specify only one primary subnet for a DHCP address pool. If you execute the **network** command multiple times, the most recent configuration takes effect.

You can specify up to 32 secondary subnets for a DHCP address pool.

The primary subnet and secondary subnets in a DHCP address pool must not have the same network address and mask.

If you have used the **address range** or **class** command in an address pool, you cannot specify a secondary subnet in the same address pool.

Modifying or removing the **network** configuration deletes the assigned addresses from the current address pool.

If you execute the **network export-route** command multiple times, the most recent configuration takes effect.

Examples

Specify primary subnet 192.168.8.0/24 and secondary subnet 192.168.10.0/24 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] network 192.168.8.0 mask 255.255.255.0
[Sysname-dhcp-pool-0] network 192.168.10.0 mask 255.255.255.0 secondary
[Sysname-dhcp-pool-0-secondary]
```

Related commands

display dhcp server pool

gateway-list

next-server

Use **next-server** to specify the IP address of a server in a DHCP address pool.

Use **undo next-server** to restore the default.

Syntax

next-server *ip-address*

undo next-server

Default

No server's IP address is specified in a DHCP address pool.

Views

DHCP address pool view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the IP address of a server.

Usage guidelines

Upon startup, the DHCP client obtains an IP address and the specified server IP address. Then it contacts the specified server, such as a TFTP server, to get other boot information.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify a server's IP address 10.1.1.254 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] next-server 10.1.1.254
```

Related commands

display dhcp server pool

option

Use **option** to customize a DHCP option.

Use **undo option** to remove a customized DHCP option.

Syntax

option *code* { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address*&<1-8> }

undo option *code*

Default

No DHCP option is customized.

Views

DHCP address pool view

DHCP option group view

Predefined user roles

network-admin

context-admin

Parameters

code: Specifies the number of the customized option, in the range of 2 to 254, excluding 50 through 54, 56, 58, 59, 61, and 82.

ascii *ascii-string*: Specifies a case-sensitive ASCII string of 1 to 255 characters as the option content.

hex *hex-string*: Specifies a hexadecimal number as the option content. The length of the hexadecimal number must be an even number in the range of 2 to 256.

ip-address *ip-address*&<1-8>: Specifies a space-separated list of up to eight IP addresses as the option content.

Usage guidelines

The DHCP server fills the customized option with the specified ASCII string, hexadecimal number, or IP addresses, and sends it in a response to the client.

You can customize options for the following purposes:

- Add newly released options.
- Add options for which the vendor defines the contents, for example, Option 43.
- Add options for which the CLI does not provide a dedicated configuration command. For example, you can use the **`option 4 ip-address 1.1.1.1`** command to define the time server address 1.1.1.1 for DHCP clients.
- Add all option values if the actual requirement exceeds the limit for a dedicated option configuration command. For example, the **`dns-list`** command can specify up to eight DNS servers. To specify more than eight DNS server, you must use the **`option 6`** command to define all DNS servers.

DHCP options specified by dedicated commands take precedence over those specified by the **`option`** commands. For example, if a DNS server address is specified by both the **`dns-list`** command and the **`option 6`** command, the server uses the address specified by the **`dns-list`** command.

DHCP options specified in DHCP option groups take precedence over those specified in DHCP address pools.

If you execute this command multiple times with the same *`code`* specified, the most recent configuration takes effect.

Examples

Configure Option 7 to specify log server address 2.2.2.2 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] option 7 ip-address 2.2.2.2
```

Related commands

`display dhcp server pool`

reset dhcp server conflict

Use **`reset dhcp server conflict`** to clear IP address conflict information.

Syntax

`reset dhcp server conflict` [**`ip`** *`ip-address`*] [**`vpn-instance`** *`vpn-instance-name`*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

`ip` *`ip-address`*: Clears conflict information about the specified IP address. If you do not specify this option, this command clears all address conflict information.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears conflict information about IP addresses for the public network.

Usage guidelines

Address conflicts occur when dynamically assigned IP addresses have been statically configured for other hosts. After you modify the address pool configuration, the conflicted addresses might become assignable. To assign these addresses, use the **reset dhcp server conflict** command to clear the conflict information first.

Examples

Clear all IP address conflict information.

```
<Sysname> reset dhcp server conflict
```

Related commands

display dhcp server conflict

reset dhcp server expired

Use **reset dhcp server expired** to clear binding information about expired IP addresses.

Syntax

reset dhcp server expired [[**ip** *ip-address*] [**vpn-instance** *vpn-instance-name*] | **pool** *pool-name*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

ip *ip-address*: Clears binding information about the specified expired IP address. If you do not specify an IP address, this command clears binding information about all expired IP addresses.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears lease expiration information about IP addresses for the public network.

pool *pool-name*: Clears binding information about the expired IP addresses in the specified address pool. The pool name is a case-insensitive string of 1 to 63 characters. If you do not specify an address pool, this command clears binding information about expired IP addresses in all address pools.

Examples

Clear binding information about all expired IP addresses.

```
<Sysname> reset dhcp server expired
```

Related commands

display dhcp server expired

reset dhcp server ip-in-use

Use **reset dhcp server ip-in-use** to clear binding information about assigned IP addresses.

Syntax

reset dhcp server ip-in-use [[**ip** *ip-address*] [**vpn-instance** *vpn-instance-name*] | **pool** *pool-name*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

ip *ip-address*: Clears binding information about the specified assigned IP address. If you do not specify an IP address, this command clears binding information about all assigned IP addresses.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears binding information for the public network.

pool *pool-name*: Clears binding information about assigned IP addresses in the specified address pool. The pool name is a case-insensitive string of 1 to 63 characters. If you do not specify an address pool, this command clears binding information about assigned IP addresses in all address pools.

Usage guidelines

If you use this command to clear information about an assigned static binding, the static binding becomes a free static binding.

Examples

Clear binding information about IP address 10.110.1.1.

```
<Sysname> reset dhcp server ip-in-use ip 10.110.1.1
```

Related commands

display dhcp server ip-in-use

reset dhcp server statistics

Use **reset dhcp server statistics** to clear DHCP server statistics.

Syntax

reset dhcp server statistics [**vpn-instance** *vpn-instance-name*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears DHCP server statistics for the public network.

Examples

Clear DHCP server statistics.

```
<Sysname> reset dhcp server statistics
```

Related commands

display dhcp server statistics

static-bind

Use **static-bind** to statically bind a client ID or MAC address to an IP address.

Use **undo static-bind** to remove a static binding.

Syntax

static-bind ip-address *ip-address* [*mask-length* | **mask** *mask*] { **client-identifier** *client-identifier* | **hardware-address** *hardware-address* [**ethernet** | **token-ring**] } [**description** *description-text*]

undo static-bind ip-address *ip-address*

Default

No static binding is specified in a DHCP address pool.

Views

DHCP address pool view

Predefined user roles

network-admin

context-admin

Parameters

ip-address *ip-address*: Specifies the IP address of the static binding. The natural mask is used if no mask length or mask is specified.

mask-length: Specifies the mask length in the range of 1 to 30.

mask *mask*: Specifies the mask, in dotted decimal format.

client-identifier *client-identifier*: Specifies the client ID of the static binding, a string of 4 to 254 characters. The string can contain only hexadecimal numbers and hyphen (-), in the format of H-H-H…. The last H can be a two-digit or four-digit hexadecimal number while the other Hs must be all four-digit hexadecimal numbers. For example, aabb-cccc-dd is correct, and aabb-c-dddd and aabb-cc-dddd are not correct.

hardware-address *hardware-address*: Specifies the client hardware address of the static binding, a string of 4 to 39 characters. The string can contain only hexadecimal numbers and hyphen (-), in the format of H-H-H…. The last H can be a two-digit or four-digit hexadecimal number while the other Hs must be all four-digit hexadecimal numbers. For example, aabb-cccc-dd is correct, and aabb-c-dddd and aabb-cc-dddd are not correct.

ethernet: Specifies the client hardware address type as Ethernet. The default type is Ethernet.

token-ring: Specifies the client hardware address type as token ring.

description *description-text*: Specifies a description for the static binding, a case-sensitive string of 1 to 255 characters.

Usage guidelines

The IP address of a static binding must not be an interface address of the DHCP server. Otherwise, an IP address conflict occurs, and the bound client cannot obtain the IP address.

You can specify multiple static bindings in an address pool. The total number of static bindings in all address pools cannot exceed 8192.

An IP address can be bound to only one DHCP client. To modify the binding for a DHCP client, first execute the **undo** form of the command to delete the existing binding and then create a new binding.

Examples

Bind IP address 10.1.1.1/24 to client ID **00aa-aabb** in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] static-bind ip-address 10.1.1.1 mask 255.255.255.0
client-identifier 00aa-aabb
```

Related commands

display dhcp server pool

tftp-server domain-name

Use **tftp-server domain-name** to specify a TFTP server name in a DHCP address pool.

Use **undo tftp-server domain-name** to restore the default.

Syntax

tftp-server domain-name *domain-name*

undo tftp-server domain-name

Default

No TFTP server name is specified.

Views

DHCP address pool view

Predefined user roles

network-admin

context-admin

Parameters

domain-name: Specifies the TFTP server name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify TFTP server name **aaa** in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] tftp-server domain-name aaa
```

Related commands

display dhcp server pool

tftp-server ip-address

tftp-server ip-address

Use **tftp-server ip-address** to specify a TFTP server address in a DHCP address pool.

Use **undo tftp-server ip-address** to restore the default.

Syntax

tftp-server ip-address *ip-address*

undo tftp-server ip-address

Default

No TFTP server address is specified.

Views

DHCP address pool view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the IP address of a TFTP server.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify TFTP server address 10.1.1.1 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] tftp-server ip-address 10.1.1.1
```

Related commands

display dhcp server pool

tftp-server domain-name

valid class

Use **valid class** to add DHCP user classes to the whitelist.

Use **undo valid class** to remove DHCP user classes from the whitelist.

Syntax

valid class *class-name*&<1-8>

undo valid class *class-name*&<1-8>

Default

No DHCP user class is listed on the whitelist.

Views

DHCP address pool view

Predefined user roles

network-admin

context-admin

Parameters

class-name&<1-8>: Specifies a space-separated list of up to eight DHCP user classes by their names, a case-insensitive string of 1 to 63 characters.

Usage guidelines

For this command to take effect, you must enable the DHCP user class whitelist.

Examples

Add DHCP user classes **test1** and **test2** to the whitelist in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] valid class test1 test2
```

Related commands

dhcp class

verify class

verify class

Use **verify class** to enable the DHCP user class whitelist.

Use **undo verify class** to disable the DHCP user class whitelist.

Syntax

verify class

undo verify class

Default

The DHCP user class whitelist is disabled.

Views

DHCP address pool view

Predefined user roles

network-admin

context-admin

Usage guidelines

After you enable the DHCP user class whitelist, the DHCP server processes requests only from clients on the DHCP user class whitelist.

The DHCP user class whitelist does not take effect on clients that request static IP addresses, and the server always processes their requests.

Examples

Enable the DHCP user class whitelist in DHCP address pool 0.

```
[Sysname] system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] verify class
```

Related commands

valid class

voice-config

Use **voice-config** to configure the content for Option 184 in a DHCP address pool.

Use **undo voice-config** to remove the Option 184 content from a DHCP address pool.

Syntax

voice-config { **as-ip** *ip-address* | **fail-over** *ip-address dialer-string* | **ncp-ip** *ip-address* | **voice-vlan** *vlan-id* { **disable** | **enable** } }

undo voice-config [**as-ip** | **fail-over** | **ncp-ip** | **voice-vlan**]

Default

No Option 184 content is configured in a DHCP address pool.

Views

DHCP address pool view

Predefined user roles

network-admin

context-admin

Parameters

as-ip *ip-address*: Specifies the IP address of the backup network calling processor.

fail-over *ip-address dialer-string*: Specifies the failover IP address and dialer string. The *dialer-string* is a string of 1 to 39 characters. Valid characters are digits and asterisk (*).

ncp-ip *ip-address*: Specifies the IP address of the primary network calling processor.

voice-vlan *vlan-id*: Specifies the voice VLAN ID in the range of 2 to 4094.

- **disable**: Disables the specified VLAN. DHCP clients will not take this VLAN as their voice VLAN.
- **enable**: Enables the specified VLAN. DHCP clients will take this VLAN as their voice VLAN.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure Option 184 in DHCP address pool 0. The primary and backup network calling processors are at 10.1.1.1 and 10.2.2.2, respectively. The voice VLAN 3 is enabled. The failover IP address is 10.3.3.3. The dialer string is 99*.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] voice-config ncp-ip 10.1.1.1
[Sysname-dhcp-pool-0] voice-config as-ip 10.2.2.2
[Sysname-dhcp-pool-0] voice-config voice-vlan 3 enable
[Sysname-dhcp-pool-0] voice-config fail-over 10.3.3.3 99*
```

Related commands

display dhcp server pool

vpn-instance

Use **vpn-instance** to apply a DHCP address pool to a VPN instance.

Use **undo vpn-instance** to restore the default.

Syntax

vpn-instance *vpn-instance-name*

undo vpn-instance

Default

The DHCP address pool is not applied to any VPN instance.

Views

DHCP address pool view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance-name: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

If a DHCP address pool is applied to a VPN instance, the DHCP server assigns IP addresses in this address pool to clients in the specified VPN instance.

The DHCP server identifies the VPN instance to which a DHCP client belongs according to the following information:

- The client's VPN information stored in authentication modules.
- The VPN information of the DHCP server's interface that receives DHCP packets from the client.

The VPN information from authentication modules takes priority over the VPN information of the receiving interface.

Examples

Apply DHCP address pool 0 to VPN instance **abc**.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] vpn-instance abc
```

DHCP relay agent commands

dhcp relay check mac-address

Use **dhcp relay check mac-address** to enable MAC address check on the relay agent.

Use **undo dhcp relay check mac-address** to disable MAC address check on the relay agent.

Syntax

dhcp relay check mac-address

undo dhcp relay check mac-address

Default

The MAC address check feature is disabled.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

This feature enables the DHCP relay agent to compare the **chaddr** field of a received DHCP request with the source MAC address in the frame header. If they are the same, the DHCP relay agent forwards the request to the DHCP server. If they are not the same, the DHCP relay agent discards the request.

The MAC address check feature takes effect only when the **dhcp select relay** command has already been configured on the interface.

Enable the MAC address check feature only on the DHCP relay agent directly connected to the DHCP clients. A DHCP relay agent changes the source MAC address of DHCP packets before sending them.

Examples

Enable MAC address check on the DHCP relay agent.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp relay check mac-address
```

Related commands

dhcp select relay

dhcp relay check mac-address aging-time

Use **dhcp relay check mac-address aging-time** to set the aging time for MAC address check entries on the DHCP relay agent.

Use **undo dhcp relay check mac-address aging-time** to restore the default.

Syntax

dhcp relay check mac-address aging-time *time*

undo dhcp relay check mac-address aging-time

Default

The aging time is 30 seconds.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

time: Specifies the aging time for MAC address check entries, in the range of 30 to 600 seconds.

Usage guidelines

This command takes effect only after you execute the **dhcp relay check mac-address** command.

Examples

Set the aging time to 60 seconds for MAC address check entries on the DHCP relay agent.

```
<Sysname> system-view
[Sysname] dhcp relay check mac-address aging-time 60
```

dhcp relay client-information record

Use **dhcp relay client-information record** to enable recording client information in relay entries.

Use **undo dhcp relay client-information record** to disable the feature.

Syntax

dhcp relay client-information record

undo dhcp relay client-information record

Default

The DHCP relay agent does not record client information in relay entries.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

Client information is recorded only when the DHCP relay agent is configured on the gateway of DHCP clients. A relay entry contains information about a client such as the client's IP and MAC addresses.

Disabling the recording of client information deletes all recorded relay entries.

Examples

Enable the recording of relay entries on the relay agent.

```
<Sysname> system-view
[Sysname] dhcp relay client-information record
```

Related commands

dhcp relay client-information refresh

dhcp relay client-information refresh enable

dhcp relay client-information refresh

Use **dhcp relay client-information refresh** to set the interval at which the DHCP relay agent refreshes relay entries.

Use **undo dhcp relay client-information refresh** to restore the default.

Syntax

dhcp relay client-information refresh [**auto** | **interval** *interval*]

undo dhcp relay client-information refresh

Default

The refresh interval is automatically calculated based on the number of relay entries.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

auto: Automatically calculates the refresh interval. The more the entries, the shorter the refresh interval. The shortest interval is 50 ms.

interval *interval*: Specifies the refresh interval in the range of 1 to 120 seconds.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the refresh interval to 100 seconds.

```
<Sysname> system-view
[Sysname] dhcp relay client-information refresh interval 100
```

Related commands

dhcp relay client-information record

dhcp relay client-information refresh enable

dhcp relay client-information refresh enable

Use **dhcp relay client-information refresh enable** to enable the DHCP relay agent to periodically refresh dynamic relay entries.

Use **undo dhcp relay client-information refresh enable** to disable the DHCP relay agent to periodically refresh dynamic relay entries.

Syntax

dhcp relay client-information refresh enable

undo dhcp relay client-information refresh enable

Default

The DHCP relay agent periodically refreshes relay entries.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

A DHCP client unicasts a DHCP-RELEASE message to the DHCP server to release its IP address. The DHCP relay agent conveys the message to the DHCP server and does not remove the IP-to-MAC entry of the client.

With this feature, the DHCP relay agent uses a client's IP address to periodically send a DHCP-REQUEST message to the DHCP server.

- If the server returns a DHCP-ACK message or does not return any message within an interval, the DHCP relay agent performs the following operations:
  - Removes the relay entry.
  - Sends a DHCP-RELEASE message to the DHCP server to release the IP address.
- If the server returns a DHCP-NAK message, the relay agent keeps the entry.

With this feature disabled, the DHCP relay agent does not remove relay entries automatically. After a DHCP client releases its IP address, you must use the **reset dhcp relay client-information** on the relay agent to remove the corresponding relay entry.

Examples

Disable periodic refresh of relay entries.

```
<Sysname> system-view
[Sysname] undo dhcp relay client-information refresh enable
```

Related commands

dhcp relay client-information record

dhcp relay client-information refresh

reset dhcp relay client-information

dhcp relay forward reply by-option82

Use **dhcp relay forward reply by-option82** to configure the DHCP relay agent to forward DHCP replies based on Option 82.

Use **undo dhcp relay forward reply by-option82** to restore the default.

Syntax

dhcp relay forward reply by-option82

undo dhcp relay forward reply by-option82

Default

The DHCP relay agent does not forward DHCP replies based on Option 82.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command takes effect only after you execute the **dhcp relay information enable** and **dhcp relay information circuit-id** commands.

Examples

Configure the DHCP relay agent to forward DHCP replies based on Option 82.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp relay forward reply by-option82
```

Related commands

dhcp relay information circuit-id

dhcp relay information enable

dhcp relay gateway

Use **dhcp relay gateway** to specify the DHCP relay agent address to be inserted in DHCP requests.

Use **undo dhcp relay gateway** to restore the default.

Syntax

dhcp relay gateway *ip-address*

undo dhcp relay gateway

Default

The primary IP address of the interface is inserted in DHCP requests as the DHCP relay agent address.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the DHCP relay agent address. It must be an IP address of the interface.

Usage guidelines

The DHCP relay agent uses the specified IP address instead of the primary IP address of the relay interface as the DHCP relay agent address.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify 10.1.1.1 as the DHCP relay agent address to be inserted in DHCP requests on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp relay gateway 10.1.1.1
```

Related commands

gateway-list

dhcp relay information circuit-id

Use **dhcp relay information circuit-id** to configure the padding mode and padding format for the Circuit ID sub-option of Option 82.

Use **undo dhcp relay information circuit-id** to restore the default.

Syntax

dhcp relay information circuit-id { **bas** [**sub-interface-vlan**] | **string** *circuit-id* | { **normal** | **verbose** [**node-identifier** { **mac** | **sysname** | **user-defined** *node-identifier* }] [**interface**] } [**sub-interface-vlan**] [**format** { **ascii** | **hex** }] }

undo dhcp relay information circuit-id

Default

The padding mode is **normal** and the padding format is **hex**.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

bas: Specifies the bas mode that fills in the Circuit ID sub-option with the interface and VLAN information. The device fills the information in the format of *interface-type slot/subslot/port vxlan_id.vlan_id.subvlan_id*.

sub-interface-vlan: Specifies the VLAN ID of the L2VE subinterface as the content for the Circuit ID sub-option. If you do not specify this keyword, the VLAN ID of the interface on which you configure this command is written to the sub-option. This keyword is available only for L3VE interfaces.

string *circuit-id*: Specifies the string mode that uses a case-sensitive string of 3 to 63 characters as the content of the Circuit ID sub-option.

normal: Specifies the normal mode, in which the padding content consists of the VLAN ID and port number.

verbose: Specifies the verbose mode. The padding content includes the node identifier, interface information, and VLAN ID. The default node identifier is the MAC address of the access node. The default interface information consists of the Ethernet type (fixed to **eth**), chassis number, slot number, sub-slot number, and interface number.

node-identifier { **mac** | **sysname** | **user-defined** *node-identifier* }: Specifies the access node identifier.

- **mac**: Uses the MAC address of the access node as the node identifier.
- **sysname**: Uses the device name as the node identifier. You can set the device name by using the **sysname** command in system view. The padding format for the device name is always ASCII regardless of the specified padding format. If you specify this keyword, do not include any spaces when you set the device name. Otherwise, the DHCP relay agent fails to add or replace Option 82.
- **user-defined** *node-identifier:* Uses a case-sensitive string of 1 to 50 characters as the node identifier. The padding format for the specified character string is always ASCII regardless of the specified padding format.

interface: Uses the interface name as the interface information. The padding format for the interface name is always ASCII regardless of the specified padding format.

format: Specifies the padding format for the Circuit ID sub-option.

ascii: Specifies the ASCII padding format.

hex: Specifies the hex padding format.

Usage guidelines

The Circuit ID sub-option cannot carry information about interface splitting or subinterfaces. For more information about interface splitting and subinterfaces, see *Interface Configuration Guide*.

If you execute this command multiple times, the most recent configuration takes effect.

The padding format for the string mode, the normal mode, or the verbose mode varies by command configuration. Table 8 shows how the padding format is determined for different modes.

Table 8 Padding format for different modes

Keyword (mode)	If no padding format is set	If the padding format is ascii	If the padding format is hex
string *circuit-id*	The padding format is ASCII, and is not configurable.	N/A	N/A
normal	Hex.	ASCII.	Hex.
verbose	Hex for the VLAN ID. ASCII for the node identifier, Ethernet type, chassis number, slot number, sub-slot number, and interface number.	ASCII.	ASCII for the node identifier and Ethernet type. Hex for the chassis number, slot number, sub-slot number, interface number, and VLAN ID.

Examples

Specify the content mode as verbose, node identifier as the device name, and the padding format as ASCII for the Circuit ID sub-option.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp relay information enable
[Sysname-GigabitEthernet1/0/1] dhcp relay information strategy replace
[Sysname-GigabitEthernet1/0/1] dhcp relay information circuit-id verbose node-identifier sysname format ascii
```

Related commands

dhcp relay forward reply by-option82

dhcp relay information enable

dhcp relay information strategy

display dhcp relay information

dhcp relay information enable

Use **dhcp relay information enable** to enable the DHCP relay agent to support Option 82.

Use **undo dhcp relay information enable** to disable Option 82 support.

Syntax

dhcp relay information enable

undo dhcp relay information enable

Default

The DHCP relay agent does not support Option 82.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command enables the DHCP relay agent to add Option 82 to DHCP requests that do not contain Option 82 before forwarding the requests to the DHCP server. The content of Option 82 is determined by the **dhcp relay information circuit-id** and **dhcp relay information remote-id** commands. If the DHCP requests contain Option 82, the relay agent handles the requests according to the strategy configured with the **dhcp relay information strategy** command.

If this feature is disabled, the relay agent forwards requests that contain or do not contain Option 82 to the DHCP server.

Examples

Enable Option 82 support on the relay agent.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp relay information enable
```

Related commands

dhcp relay forward reply by-option82

dhcp relay information circuit-id

dhcp relay information remote-id

dhcp relay information strategy

display dhcp relay information

dhcp relay information remote-id

Use **dhcp relay information remote-id** to configure the padding mode and padding format for the Remote ID sub-option of Option 82.

Use **undo dhcp relay information remote-id** to restore the default.

Syntax

dhcp relay information remote-id { **normal** [**format** { **ascii** | **hex** }] | **string** *remote-id* | **sysname** }

undo dhcp relay information remote-id

Default

The padding mode is **normal** and the padding format is **hex**.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

normal: Specifies the normal mode in which the padding content is the MAC address of the receiving interface.

format: Specifies the padding format for the Remote ID sub-option. The default padding format is hex.

ascii: Specifies the ASCII padding format.

hex: Specifies the hex padding format.

string *remote-id*: Specifies the string mode that uses a case-sensitive string of 1 to 63 characters as the content of the Remote ID sub-option.

sysname: Specifies the sysname mode that uses the device name as the content of the Remote ID sub-option. You can set the device name by using the **sysname** command.

Usage guidelines

The padding format is always ASCII for the specified character string (**string**), and the device name (**sysname**).

The padding format for the **normal** mode is determined by the command.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the padding content for the Remote ID sub-option of Option 82 as **device001**.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp relay information enable
[Sysname-GigabitEthernet1/0/1] dhcp relay information strategy replace
[Sysname-GigabitEthernet1/0/1] dhcp relay information remote-id string device001
```

Related commands

dhcp relay information enable

dhcp relay information strategy

display dhcp relay information

dhcp relay information strategy

Use **dhcp relay information strategy** to configure the strategy for the DHCP relay agent to handle messages containing Option 82.

Use **undo dhcp relay information strategy** to restore the default handling strategy.

Syntax

dhcp relay information strategy { **drop** | **keep** | **replace** }

undo dhcp relay information strategy

Default

The handling strategy for messages that contain Option 82 is **replace**.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

drop: Drops DHCP messages that contain Option 82 messages.

keep: Keeps the original Option 82 intact and forwards the DHCP messages.

replace: Replaces the original Option 82 with the configured Option 82 before forwarding the DHCP messages.

Usage guidelines

This command takes effect only on DHCP requests that contain Option 82.

For DHCP requests that do not contain Option 82, the DHCP relay agent always adds Option 82 to the requests before forwarding the requests to the DHCP server.

If the handling strategy is **replace**, configure a padding mode and padding format for Option 82. If the handling strategy is **keep** or **drop**, you do not need to configure any padding mode or padding format. The settings do not take effect even if you configure them.

Examples

Specify the handling strategy for Option 82 as **keep**.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp relay information enable
[Sysname-GigabitEthernet1/0/1] dhcp relay information strategy keep
```

Related commands

dhcp relay information enable

display dhcp relay information

dhcp relay release ip

Use **dhcp relay release ip** to release a client IP address.

Syntax

dhcp relay release ip *ip-address* [**vpn-instance** *vpn-instance-name*]

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the IP address to be released.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the specified IP address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command releases the IP address on the public network.

Usage guidelines

After you execute this command, the relay agent sends a DHCP-RELEASE packet to the DHCP server and removes the relay entry of the IP address. Upon receiving the packet, the server removes binding information about the specified IP address to release the IP address.

Examples

Release IP address 1.1.1.1.

```
<Sysname> system-view
[Sysname] dhcp relay release ip 1.1.1.1
```

dhcp relay server-address

Use **dhcp relay server-address** to specify DHCP servers on the DHCP relay agent.

Use **undo dhcp relay server-address** to remove DHCP servers.

Syntax

dhcp relay server-address *ip-address*

undo dhcp relay server-address [*ip-address*]

Default

No DHCP server is specified on the DHCP relay agent.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the IP address of a DHCP server. The DHCP relay agent forwards DHCP packets received from DHCP clients to this DHCP server.

Usage guidelines

The specified IP address of the DHCP server must not reside on the same subnet as the IP address of the DHCP relay agent interface. Otherwise, the DHCP clients might fail to obtain IP addresses.

You can specify a maximum of eight DHCP servers on an interface. After receiving a DHCP request, the DHCP relay agent forwards the packets to all the specified DHCP servers.

If you do not specify an IP address, the **undo dhcp relay server-address** command removes all DHCP servers on the interface.

Examples

Specify DHCP server address 1.1.1.1 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp relay server-address 1.1.1.1
```

Related commands

dhcp select relay

display dhcp relay interface

dhcp relay source-address

Use **dhcp relay source-address** to specify the source IP address for relayed DHCP requests.

Use **undo dhcp relay source-address** to restore the default.

Syntax

dhcp relay source-address { *ip-address* | **gateway** | **relay-interface** }

undo dhcp relay source-address

Default

The relay agent chooses the default source IP address for relayed requests depending on whether its server-side interface and the DHCP server belong to the same VPN instance:

- If they belong to the same VPN instance, the relay agent uses the IP address of the output interface for relayed requests as the default source IP address.
- If they belong to different VPN instances, the relay agent uses the lowest IP address that is in the same VPN instance as the DHCP server as the default source address.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the source IP address.

gateway: Uses the IP address in the **giaddr** field as the source IP address of the relayed DHCP requests. If the **giaddr** field is empty, the relay agent follows the default rule to specify the source IP address for relayed DHCP requests.

relay-interface: Uses the primary IP address of the relay interface as the source IP address. If this interface does not have an IP address, the relay agent follows the default rule to specify the source IP address for relayed DHCP requests.

Usage guidelines

This command is required if multiple relay interfaces share the same IP address or if a relay interface does not have routes to DHCP servers. You can use this command to specify the IP address of another interface, typically the loopback interface, on the DHCP relay agent as the source IP address for DHCP requests. The relay interface inserts the source IP address in the source IP address field as well as the **giaddr** field in DHCP requests.

If multiple relay interfaces share the same IP address, you must also configure the relay interface to support Option 82. Upon receiving a DHCP request, the relay interface inserts the subnet information in sub-option 5 in Option 82. The DHCP server assigns an IP address according to sub-option 5. The DHCP relay agent looks up the output interface in the MAC address table to forward the DHCP reply.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify 1.1.1.1 as the source IP address for relayed DHCP requests on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp relay source-address 1.1.1.1
```

Related commands

dhcp select relay

dhcp smart-relay enable

Use **dhcp smart-relay enable** to enable the DHCP smart relay feature.

Use **undo dhcp smart-relay enable** to disable the DHCP smart relay feature.

Syntax

dhcp smart-relay enable

undo dhcp smart-relay enable

Default

The DHCP smart relay feature is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

The smart relay feature allows the relay agent to use secondary IP addresses as the gateway address when the DHCP server does not reply the DHCP-OFFER message. The relay agent initially inserts its primary IP address in the **giaddr** field before forwarding a request to the DHCP server. If no DHCP-OFFER is returned after two retries, the relay agent switches to secondary IP addresses.

Without this feature, the relay agent always uses the primary IP address as the gateway address.

Examples

Enable the DHCP smart relay feature.

```
<Sysname> system-view
[Sysname] dhcp smart-relay enable
```

Related commands

dhcp select

gateway-list

display dhcp relay check mac-address

Use **display dhcp relay check mac-address** to display MAC address check entries on the relay agent.

Syntax

display dhcp relay check mac-address

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display MAC address check entries on the DHCP relay agent.

```
<Sysname> display dhcp relay check mac-address
Source-MAC        Interface                Aging-time
23f3-1122-adf1    GE1/0/1                  10
23f3-1122-2230    GE1/0/2                  30
```

Table 9 Command output

Field	Description
Source MAC	Source MAC address of the attacker.
Interface	Interface where the attack comes from.
Aging-time	Aging time of the MAC address check entry, in seconds.

display dhcp relay client-information

Use **display dhcp relay client-information** to display relay entries on the relay agent.

Syntax

display dhcp relay client-information [**interface** *interface-type interface-number* | **ip** *ip-address* [**vpn-instance** *vpn-instance-name*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface *interface-type interface-number*: Displays relay entries on the specified interface. If you do not specify an interface, this command displays relay entries on all interfaces.

ip *ip-address*: Displays the relay entry for the specified IP address. If you do not specify an IP address, this command displays relay entries for all IP addresses.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the specified IP address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays the relay entry for the specified IP address on the public network.

Usage guidelines

The DHCP relay agent records relay entries only after you configure the **dhcp relay client-information record** command.

Examples

Display all relay entries on the relay agent.

```
<Sysname> display dhcp relay client-information
Total number of client-information items: 2
Total number of dynamic items: 1
Total number of temporary items: 1
IP address       MAC address      Type        Interface           VPN name
10.1.1.1         00e0-0000-0001   Dynamic     GE1/0/1             N/A
10.1.1.5         00e0-0000-0000   Temporary   GE1/0/1             N/A
```

Table 10 Command output

Field	Description
Total number of client-information items	Total number of relay entries.
Total number of dynamic items	Total number of dynamic relay entries.
Total number of temporary items	Total number of temporary relay entries.
IP address	IP address of the DHCP client.
MAC address	MAC address of the DHCP client.
Type	Relay entry type: • **Dynamic**—The relay agent creates a dynamic relay entry upon receiving an ACK response from the DHCP server. • **Temporary**—The relay agent creates a temporary relay entry upon receiving a REQUEST packet from a DHCP client.
Interface	Layer 3 interface connected to the DHCP client. **N/A** is displayed for relay entries without interface information.
VPN name	Name of the VPN instance to which the DHCP client belongs. If the DHCP client does not belong to any VPN, this field displays **N/A**.

Related commands

dhcp relay client-information record

reset dhcp relay client-information

display dhcp relay information

Use **display dhcp relay information** to display Option 82 configuration information for the DHCP relay agent.

Syntax

display dhcp relay information [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface *interface-type interface-number*: Displays Option 82 configuration information for the specified interface. If you do not specify an interface, this command displays Option 82 configuration information about all interfaces.

Examples

Display Option 82 configuration information for all interfaces.

```
<Sysname> display dhcp relay information
Interface: GigabitEthernet1/0/1
   Status: Enable
   Strategy: Replace
   Circuit ID Pattern: Verbose
   Remote ID Pattern: Sysname
   Circuit ID format: Undefined
   Remote ID format: ASCII
   Node identifier: aabbcc
Interface: GigabitEthernet1/0/2
   Status: Enable
   Strategy: Replace
   Circuit ID Pattern: User Defined
   Remote ID Pattern: User Defined
   Circuit ID format: ASCII
   Remote ID format: ASCII
   User defined:
   Circuit ID: vlan100
   Remote ID: device001
```

Table 11 Command output

Field	Description
Interface	Interface name.
Status	Option 82 states: • **Enable**—DHCP relay agent support for Option 82 is enabled. • **Disable**—DHCP relay agent support for Option 82 is disabled.
Strategy	Handling strategy for request messages containing Option 82, **Drop**, **Keep**, or **Replace**.
Circuit ID Pattern	Padding content mode of the Circuit ID sub-option, **Verbose**, **Normal**, or **User Defined**.
Remote ID Pattern	Padding content mode of the Remote ID sub-option: **Sysname**, **Normal**, or **User Defined**.
Circuit ID format-type	Padding format of the Circuit ID sub-option, **ASCII**, **Hex**, or **Undefined**.
Remote ID format-type	Padding format of the Remote ID sub-option, **ASCII**, **Hex**, or **Undefined**.

Node identifier	Access node identifier.
User defined	Content of the user-defined sub-options.
Circuit ID	User-defined content of the Circuit ID sub-option.
Remote ID	User-defined content of the Remote ID sub-option.

display dhcp relay server-address

Use **display dhcp relay server-address** to display DHCP server addresses configured on an interface.

Syntax

display dhcp relay server-address [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface *interface-type interface-number*: Displays DHCP server addresses on the specified interface. If you do not specify an interface, this command displays DHCP server addresses on all interfaces.

Examples

Display DHCP server addresses on all interfaces.

```
<Sysname> display dhcp relay server-address
Interface name                Server IP address
GE1/0/1                       2.2.2.2
GE1/0/1                       2.2.2.3
```

Table 12 Command output

Field	Description
Interface name	Interface name.
Server IP address	DHCP server IP address.

Related commands

dhcp relay server-address

display dhcp relay statistics

Use **display dhcp relay statistics** to display DHCP packet statistics on the DHCP relay agent.

Syntax

display dhcp relay statistics [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface *interface-type interface-number*: Displays DHCP packet statistics on the specified interface. If you do not specify an interface, this command displays all DHCP packet statistics on the DHCP relay agent.

Examples

Display all DHCP packet statistics on the DHCP relay agent.

```
<Sysname> display dhcp relay statistics
DHCP packets dropped:                  0
DHCP packets received from clients:    0
   DHCPDISCOVER:                       0
   DHCPREQUEST:                        0
   DHCPINFORM:                         0
   DHCPRELEASE:                        0
   DHCPDECLINE:                        0
   BOOTPREQUEST:                       0
DHCP packets received from servers:    0
   DHCPOFFER:                          0
   DHCPACK:                            0
   DHCPNAK:                            0
   BOOTPREPLY:                         0
DHCP packets relayed to servers:       0
   DHCPDISCOVER:                       0
   DHCPREQUEST:                        0
   DHCPINFORM:                         0
   DHCPRELEASE:                        0
   DHCPDECLINE:                        0
   BOOTPREQUEST:                       0
DHCP packets relayed to clients:       0
   DHCPOFFER:                          0
   DHCPACK:                            0
   DHCPNAK:                            0
   BOOTPREPLY:                         0
DHCP packets sent to servers:          0
   DHCPDISCOVER:                       0
   DHCPREQUEST:                        0
   DHCPINFORM:                         0
```

```
   DHCPRELEASE:                        0
   DHCPDECLINE:                        0
   BOOTPREQUEST:                       0
DHCP packets sent to clients:          0
   DHCPOFFER:                          0
   DHCPACK:                            0
   DHCPNAK:                            0
   BOOTPREPLY:                         0
```

Related commands

reset dhcp relay statistics

gateway-list

Use **gateway-list** to specify gateway addresses for DHCP clients in a DHCP address pool.

Use **undo gateway-list** to remove gateway addresses from a DHCP address pool.

Syntax

gateway-list *ip-address*&<1-64> [**export-route**]

undo gateway-list [*ip-address*&<1-64>] [**export-route**]

Default

No gateway address is specified in a DHCP address pool.

Views

DHCP address pool view

Predefined user roles

network-admin

context-admin

Parameters

ip-address&<1-64>: Specifies a space-separated list of up to 64 addresses.

export-route: Binds the gateways to the device's MAC address in the address management module. The ARP module will use the entries to reply to ARP requests from the DHCP clients. If you do not specify this keyword, the gateways will not be bound to the device's MAC address.

Usage guidelines

DHCP clients of the same access type can be classified into different types by their locations. In this case, the relay interface typically has no IP address configured. You can use the **gateway-list** command to specify gateway addresses for clients matching the same DHCP address pool and bind the gateway addresses to the device's MAC address.

Upon receiving a DHCP DISCOVER or REQUEST from a client that matches a DHCP address pool, the relay agent processes the packet as follows:

1. Fills the **giaddr** field of the packet with the specified gateway address.
2. Forwards the packet to all DHCP servers in the matching DHCP address pool.

The DHCP servers select a DHCP address pool according to the gateway address.

Examples

Specify gateway address 10.1.1.1 in DHCP address pool 0.

```
<Sysname> system-view
```

```
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] gateway-list 10.1.1.1
```

Related commands

dhcp smart-relay enable

remote-server

Use **remote-server** to specify DHCP servers for a DHCP relay address pool.

Use **undo remote-server** to remove DHCP servers from a DHCP relay address pool.

Syntax

remote-server *ip-address*&<1-8>

undo remote-server [*ip-address*&<1-8>]

Default

No DHCP server is specified for the DHCP relay address pool.

Views

DHCP address pool view

Predefined user roles

network-admin

context-admin

Parameters

ip-address&<1-8>: Specifies a space-separated list of up to eight DHCP server addresses.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

If you do not specify a DHCP server address, the **undo remote-server** command removes all DHCP servers in the DHCP address pool.

Examples

Specify DHCP server 10.1.1.1 for DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] remote-server 10.1.1.1
```

reset dhcp relay client-information

Use **reset dhcp relay client-information** to clear relay entries on the DHCP relay agent.

Syntax

reset dhcp relay client-information [**interface** *interface-type interface-number* | **ip** *ip-address* [**vpn-instance** *vpn-instance-name*]]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

interface *interface-type interface-number*: Clears relay entries on the specified interface. If you do not specify an interface, this command clears relay entries on all interfaces.

ip *ip-address*: Clears the relay entry for the specified IP address. If you do not specify an IP address, this command clears relay entries for all IP addresses.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the specified IP address belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears the relay entry for the specified IP address on the public network.

Examples

Clear all relay entries on the DHCP relay agent.

```
<Sysname> reset dhcp relay client-information
```

Related commands

display dhcp relay client-information

reset dhcp relay statistics

Use **reset dhcp relay statistics** to clear relay agent statistics.

Syntax

reset dhcp relay statistics [**interface** *interface-type interface-number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command clears all DHCP relay agent statistics.

Examples

Clear all DHCP relay agent statistics.

```
<Sysname> reset dhcp relay statistics
```

Related commands

display dhcp relay statistics

DHCP client commands

dhcp client dad enable

Use **dhcp client dad enable** to enable duplicate address detection.

Use **undo dhcp client dad enable** to disable duplicate address detection.

Syntax

dhcp client dad enable

undo dhcp client dad enable

Default

Duplicate address detection is enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

DHCP client detects IP address conflict through ARP packets. An attacker can act as the IP address owner to send an ARP reply. This makes the client unable to use the IP address assigned by the server. As a best practice, disable duplicate address detection when ARP attacks exist on the network.

Examples

Disable the duplicate address.

```
<Sysname> system-view
[Sysname] undo dhcp client dad enable
```

dhcp client dscp

Use **dhcp client dscp** to set the DSCP value for DHCP packets sent by the DHCP client.

Use **undo dhcp client dscp** to restore the default.

Syntax

dhcp client dscp *dscp-value*

undo dhcp client dscp

Default

The DSCP value is 56 in DHCP packets sent by the DHCP client.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

dscp-value: Sets the DSCP value for DHCP packets, in the range of 0 to 63.

Usage guidelines

The DSCP value of a packet specifies the priority level of the packet and affects the transmission priority of the packet. A bigger DSCP value represents a higher priority.

Examples

Set the DSCP value to 30 for DHCP packets sent by the DHCP client.

```
<Sysname> system-view
[Sysname] dhcp client dscp 30
```

dhcp client identifier

Use **dhcp client identifier** to configure a DHCP client ID for an interface.

Use **undo dhcp client identifier** to restore the default.

Syntax

dhcp client identifier { **ascii** *ascii-string* | **hex** *hex-string* | **mac** *interface-type interface-number* }

undo dhcp client identifier

Default

An interface generates the DHCP client ID based on its MAC address. If the interface has no MAC address, it uses the MAC address of the first Ethernet interface to generate its client ID.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ascii *ascii-string*: Specifies a case-sensitive ASCII string of 1 to 63 characters as the client ID.

hex *hex-string*: Specifies a hexadecimal number of 4 to 64 characters as the client ID.

mac *interface-type interface-number*: Uses the MAC address of the specified interface as a DHCP client ID. The *interface-type interface-number* argument specifies an interface by its type and number.

Usage guidelines

A DHCP client ID is added to the DHCP option 61. A DHCP server can specify IP addresses for clients based on the DHCP client ID. You can specify a DHCP client ID by performing one of the following operations:

- Naming an ASCII string or hexadecimal number as the client ID.
- Using the MAC address of an interface to generate a client ID.

Whichever method you use, make sure the IDs for different DHCP clients are unique.

Examples

Use the MAC address of GigabitEthernet 1/0/2 as the DHCP client ID for GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp client identifier mac gigabitethernet 1/0/2
```

Related commands

display dhcp client

display dhcp client

Use **display dhcp client** to display DHCP client information.

Syntax

display dhcp client [**verbose**] [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

verbose: Displays detailed DHCP client information. If you do not specify this keyword, the command displays brief DHCP client information.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays DHCP client information on all interfaces.

Examples

Display brief DHCP client information on all interfaces.

```
<Sysname> display dhcp client
GigabitEthernet1/0/1 DHCP client information:
 Current state: BOUND
 Allocated IP: 40.1.1.20 255.255.255.0
 Allocated lease: 259200 seconds, T1: 129600 seconds, T2: 226800 seconds
 DHCP server: 40.1.1.2
```

Display detailed DHCP client information on all interfaces.

```
<Sysname> display dhcp client verbose
GigabitEthernet1/0/1 DHCP client information:
 Current state: BOUND
 Allocated IP: 40.1.1.20 255.255.255.0
 Allocated lease: 259200 seconds, T1: 129600 seconds, T2: 226800 seconds
 Lease from May 21 19:00:29 2012   to   May 31 19:00:29 2012
 DHCP server: 40.1.1.2
 Transaction ID: 0x1c09322d
 Default router: 40.1.1.2
Classless static routes:
   Destination: 1.1.0.1, Mask: 255.0.0.0, NextHop: 192.168.40.16
   Destination: 10.198.122.63, Mask: 255.255.255.255, NextHop: 192.168.40.16
 DNS servers: 44.1.1.11 44.1.1.12
 Domain name: ddd.com
 Boot servers: 200.200.200.200  1.1.1.1
 ACS parameter:
   URL: http://192.168.1.1:7547/acs
```

```
  Username: bims
  Password: ******
Client ID type: acsii(type value=00)
Client ID value: 000c.29d3.8659-GE1/0/1
Client ID (with type) hex: 0030-3030-632e-3239-
                           6433-2e38-3635-392d-
                           4574-6830-2f30-2f32
T1 will timeout in 1 day 11 hours 58 minutes 52 seconds.
```

Table 13 Command output

Field	Description
DHCP client information	Information about the interface that acts as the DHCP client.
Current state	Current state of the DHCP client: • **HALT**—The client stops applying for an IP address. • **INIT**—The initialization state. • **SELECTING**—The client has sent out a DHCP-DISCOVER message in search for a DHCP server and is waiting for the response from DHCP servers. • **REQUESTING**—The client has sent out a DHCP-REQUEST message requesting for an IP address and is waiting for the response from DHCP servers. • **BOUND**—The client has received the DHCP-ACK message from a DHCP server and obtained an IP address successfully. • **RENEWING**—The T1 timer expires. • **REBOUNDING**—The T2 timer expires.
Allocated IP	IP address allocated by the DHCP server.
Allocated lease	Allocated lease time.
T1	1/2 lease time (in seconds) of the DHCP client IP address.
T2	7/8 lease time (in seconds) of the DHCP client IP address.
Lease from….to….	Start and end time of the lease.
DHCP server	DHCP server IP address that assigned the IP address.
Transaction ID	Transaction ID, a random number chosen by the client to identify an IP address allocation.
Default router	Gateway address assigned to the client.
Classless static routes	Classless static routes assigned to the client.
Static routes	Classful static routes assigned to the client.
DNS servers	DNS server address assigned to the client.
Domain name	Domain name suffix assigned to the client.
Boot servers	PXE server addresses (up to 16 addresses) specified for the DHCP client, which are obtained through Option 43.
ACS parameter	Parameters about the ACS.
URL	URL of the ACS.
Username	Username for logging in to the ACS.

Field	Description
Password	Password for logging in to the ACS. If a password is configured, this field displays **********. If no password is configured, this field is not displayed.
Client ID type	DHCP client ID type: • If an ASCII string is used as the client ID value, the type value is 00. • If the MAC address of a specific interface is used as the client ID value, the type value is 01. • If a hexadecimal number is used as the client ID value, the type value is the first two characters in the string.
Client ID value	Value of the DHCP client ID.
Client ID (with type) hex	DHCP client ID with the type field, a hexadecimal number.
T1 will timeout in 1 day 11 hours 58 minutes 52 seconds.	How long the T1 (1/2 lease time) timer will timeout.

Related commands

dhcp client identifier

ip address dhcp-alloc

ip address dhcp-alloc

Use **ip address dhcp-alloc** to configure an interface to use DHCP for IP address acquisition.

Use **undo ip address dhcp-alloc** to cancel an interface from using DHCP.

Syntax

ip address dhcp-alloc

undo ip address dhcp-alloc

Default

An interface does not use DHCP for IP address acquisition.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

When you execute the **undo ip address dhcp-alloc** command, the interface sends a DHCP-RELEASE message to release the IP address obtained through DHCP. If the interface is down, the message cannot be sent out. This situation can occur when a subinterface obtained an IP address through DHCP, and the **shutdown** command is executed on its primary interface. The subinterface will fail to send a DHCP-RELEASE message.

Examples

Configure GigabitEthernet 1/0/1 to use DHCP for IP address acquisition.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ip address dhcp-alloc
```

BOOTP client commands

display bootp client

Use **display bootp client** to display information about a BOOTP client.

Syntax

display bootp client [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays BOOTP client information on all interfaces.

Examples

Display BOOTP client information on GigabitEthernet 1/0/1.

```
<Sysname> display bootp client interface gigabitethernet 1/0/1
GigabitEthernet1/0/1 BOOTP client information:
Allocated IP: 169.254.0.2 255.255.0.0
Transaction ID: 0x3d8a7431
MAC Address: 00e0-fc0a-c3ef
```

Table 14 Command output

Field	Description
BOOTP client information	Information about the interface that acts as a BOOTP client.
Allocated IP	BOOTP client's IP address allocated by the BOOTP server.
Transaction ID	Value of the **XID** field in a BOOTP message. The BOOTP client chooses a random number for the **XID** field when sending a BOOTP request to the BOOTP server. It is used to match a response message from the BOOTP server. If the values of the **XID** field are different in the BOOTP response and request, the BOOTP client drops the BOOTP response.
Mac Address	MAC address of a BOOTP client.

Related commands

ip address bootp-alloc

ip address bootp-alloc

Use **ip address bootp-alloc** to configure an interface to use BOOTP for IP address acquisition.

Use **undo ip address bootp-alloc** to cancel an interface from using BOOTP.

Syntax

ip address bootp-alloc

undo ip address bootp-alloc

Default

An interface does not use BOOTP for IP address acquisition.

Views

Interface view

Predefined user roles

network-admin

context-admin

Examples

Configure GigabitEthernet 1/0/1 to use BOOTP for IP address acquisition.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip address bootp-alloc
```

Related commands

display bootp client

Contents

DHCPv6 commands

Common DHCPv6 commands

display ipv6 dhcp duid

Use **display ipv6 dhcp duid** to display the DUID of the local device.

Syntax

display ipv6 dhcp duid

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Usage guidelines

A DHCP unique identifier (DUID) uniquely identifies a DHCPv6 device (DHCPv6 client, server, or relay agent). A DHCPv6 device adds its DUID in a sent packet.

This command displays output only after the DHCPv6 process is running on the device.

Examples

Display the DUID of the local device.

```
<Sysname> display ipv6 dhcp duid
The DUID of this device: 0003000100e0fc005552.
```

ipv6 dhcp dscp

Use **ipv6 dhcp dscp** to set the DSCP value for the DHCPv6 packets sent by the DHCPv6 server or the DHCPv6 relay agent.

Use **undo ipv6 dhcp dscp** to restore the default.

Syntax

ipv6 dhcp dscp *dscp-value*

undo ipv6 dhcp dscp

Default

The DSCP value is 56 in DHCPv6 packets sent by the DHCPv6 server or the DHCPv6 relay agent.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

dscp-value: Specifies the DSCP value for DHCPv6 packets, in the range of 0 to 63.

Usage guidelines

The DSCP value of a packet specifies the priority level of the packet and affects the transmission priority of the packet. A bigger DSCP value represents a higher priority.

Examples

Set the DSCP value to 30 for DHCPv6 packets sent by the DHCPv6 server or the DHCPv6 relay agent.

```
<Sysname> system-view
[Sysname] ipv6 dhcp dscp 30
```

ipv6 dhcp log enable

Use **ipv6 dhcp log enable** to enable DHCPv6 server logging.

Use **undo ipv6 dhcp log enable** to disable DHCPv6 server logging.

Syntax

ipv6 dhcp log enable

undo ipv6 dhcp log enable

Default

DHCPv6 server logging is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command enables the DHCPv6 server to generate DHCPv6 logs and send them to the information center. The log information helps administrators locate and solve problems. For information about the log destination and output rule configuration in the information center, see *Network Management and Monitoring Configuration Guide*.

As a best practice, disable this feature if the log generation affects the device performance or reduces the address and prefix allocation efficiency. For example, this situation might occur when a large number of clients frequently come online or go offline.

Examples

Enable DHCPv6 server logging.

```
<Sysname> system-view
[Sysname] ipv6 dhcp log enable
```

ipv6 dhcp select

Use **ipv6 dhcp select** to enable the DHCPv6 server or DHCPv6 relay agent on an interface.

Use **undo ipv6 dhcp select** to restore the default.

Syntax

ipv6 dhcp select { **relay** | **server** }

undo ipv6 dhcp select

Default

An interface does not work in the DHCPv6 server mode or in the DHCPv6 relay agent mode. It discards DHCPv6 packets from DHCPv6 clients.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

relay: Enables the DHCPv6 relay agent on the interface.

server: Enables the DHCPv6 server on the interface.

Usage guidelines

Before changing the DHCPv6 server mode to the DHCPv6 relay agent mode on an interface, use the following commands to remove IPv6 address/prefix bindings:

- **reset ipv6 dhcp server ip-in-use**
- **reset ipv6 dhcp server pd-in-use**

Do not configure the DHCPv6 client on the interface that has been configured as the DHCPv6 relay agent or DHCPv6 server.

Examples

Enable the DHCPv6 server on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp select server
```

Enable the DHCPv6 relay agent on GigabitEthernet 1/0/2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] ipv6 dhcp select relay
```

Related commands

display ipv6 dhcp relay server-address

display ipv6 dhcp server

DHCPv6 server commands

address range

Use **address range** to specify a non-temporary IPv6 address range in a DHCPv6 address pool for dynamic allocation.

Use **undo address range** to restore the default.

Syntax

address range *start-ipv6-address end-ipv6-address* [**preferred-lifetime** *preferred-lifetime* **valid-lifetime** *valid-lifetime*]

undo address range

Default

No non-temporary IPv6 address range exists.

Views

DHCPv6 address pool view

Predefined user roles

network-admin

context-admin

Parameters

start-ipv6-address: Specifies the start IPv6 address.

end-ipv6-address: Specifies the end IPv6 address.

preferred-lifetime *preferred-lifetime*: Specifies the preferred lifetime for the non-temporary IPv6 addresses. The value range is 60 to 4294967295 seconds, and the default is 604800 seconds (7 days).

valid-lifetime *valid-lifetime*: Specifies the valid lifetime for the non-temporary IPv6 addresses. The value range is 60 to 4294967295 seconds, and the default is 2592000 seconds (30 days). The valid lifetime cannot be shorter than the preferred lifetime.

Usage guidelines

If you do not specify a non-temporary IPv6 address range, all unicast addresses on the subnet specified by the **network** command in address pool view are assignable. If you specify a non-temporary IPv6 address range, only the IPv6 addresses in the specified IPv6 address range are assignable.

You can specify only one non-temporary IPv6 address range in an address pool. If you execute this command multiple times, the most recent configuration takes effect.

The non-temporary IPv6 address range specified by the **address range** command must be on the subnet specified by the **network** command.

Examples

Configure a non-temporary IPv6 address range from 3ffe:501:ffff:100::10 through 3ffe:501:ffff:100::31 in address pool 1.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] network 3ffe:501:ffff:100::/64
[Sysname-dhcp6-pool-1] address range 3ffe:501:ffff:100::10 3ffe:501:ffff:100::31
```

Related commands

display ipv6 dhcp pool

network

temporary address range

class pool

Use **class pool** to specify a DHCPv6 address pool for a DHCPv6 user class.

Use **undo class pool** to restore the default.

Syntax

class *class-name* **pool** *pool-name*

undo class *class-name* **pool**

Default

No DHCPv6 address pool is specified for a DHCPv6 user class.

Views

DHCPv6 policy view

Predefined user roles

network-admin

context-admin

Parameters

class-name: Specifies a DHCPv6 user class by its name, a case-insensitive string of 1 to 63 characters.

pool-name: Specifies a DHCPv6 address pool by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

You can specify only one DHCPv6 address pool for a DHCPv6 user class in a DHCPv6 policy. If you execute this command multiple times for a user class, the most recent configuration takes effect.

Examples

Specify DHCPv6 address pool **pool1** for DHCPv6 user class **test** in DHCPv6 policy 1.

```
<Sysname> system-view
[Sysname] ipv6 dhcp policy 1
[Sysname-dhcp6-policy-1] class test pool pool1
```

Related commands

default pool

ipv6 dhcp policy

ipv6 dhcp pool

default pool

Use **default pool** to specify the default DHCPv6 address pool.

Use **undo default pool** to restore the default.

Syntax

default pool *pool-name*

undo default pool

Default

No default DHCPv6 address pool is specified.

Views

DHCPv6 policy view

Predefined user roles

network-admin

context-admin

Parameters

pool-name: Specifies a DHCPv6 address pool by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

In a DHCPv6 policy, the DHCPv6 server uses the default address pool to assign IPv6 address, IPv6 prefix, or other parameters to clients that do not match any user classes. If no default address pool is specified or the default address pool does not have assignable IPv6 addresses or prefixes, the assignment fails.

You can specify only one default address pool in a DHCPv6 policy. If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the DHCPv6 address pool **pool1** as the default DHCPv6 address pool in DHCPv6 policy 1.

```
<Sysname> system-view
[Sysname] ipv6 dhcp policy 1
[Sysname-dhcp6-policy-1] default pool pool1
```

Related commands

class pool

ipv6 dhcp policy

display ipv6 dhcp option-group

Use **display ipv6 dhcp option-group** to display information about a DHCPv6 option group.

Syntax

display ipv6 dhcp option-group [*option-group-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

option-group-number: Specifies a static or dynamic DHCPv6 option group by its ID. The value range for the option group ID is 1 to 100. If you do not specify an option group, this command displays information about all DHCPv6 option groups.

Usage guidelines

A static DHCPv6 option group is created by using the **ipv6 dhcp option-group** command.

A dynamic DHCPv6 option group is created automatically by a DHCPv6 client after it obtains the DHCPv6 configuration parameters. Dynamic option groups cannot be manually modified or deleted.

Examples

Display information about all DHCPv6 option groups.

```
<Sysname> display ipv6 dhcp option-group
DHCPv6 option group: 1
  DNS server addresses:
    Type: Static
    Interface: N/A
    1::1
  DNS server addresses:
    Type: Dynamic (DHCPv6 address allocation)
    Interface: GigabitEthernet1/0/1
    1::1
  Domain name:
    Type: Static
    Interface: N/A
    aaa.com
  Domain name:
    Type: Dynamic (DHCPv6 address allocation)
    Interface: GigabitEthernet1/0/1
    aaa.com
  Options:
    Code: 23
      Type: Dynamic (DHCPv6 prefix allocation)
      Interface: GigabitEthernet1/0/1
      Length: 2 bytes
      Hex: ABCD
DHCPv6 option group: 20
  DNS server addresses:
    Type: Static
    Interface: N/A
    1::1
  DNS server addresses:
    Type: Dynamic (DHCPv6 address allocation)
    Interface: GigabitEthernet1/0/1
    1::1
  Domain name:
    Type: Static
    Interface: N/A
    aaa.com
  Domain name:
    Type: Dynamic (DHCPv6 address allocation)
    Interface: GigabitEthernet1/0/1
    aaa.com
  Options:
    Code: 23
      Type: Dynamic (DHCPv6 prefix allocation)
```

```
Interface: GigabitEthernet1/0/1
Length: 2 bytes
Hex: ABCD
```

Table 1 Command output

Field	Description
DHCPv6 option group	ID of the DHCPv6 option group.
Type	Types of the DHCPv6 option: • **Static**—Parameter in a static DHCPv6 option group. • **Dynamic (DHCPv6 address allocation)**—Parameter in a dynamic DHCPv6 option group created during IPv6 address acquisition. • **Dynamic (DHCPv6 prefix allocation)**—Parameters in a dynamic DHCPv6 option group created during IPv6 prefix acquisition. • **Dynamic (DHCPv6 address and prefix allocation)**—Parameters in a dynamic DHCPv6 option group created during IPv6 address and prefix acquisition.
Interface	Interface name.
DNS server addresses	IPv6 address of the DNS server.
Domain name	Domain name suffix.
SIP server addresses	IPv6 address of the SIP server.
SIP server domain names	Domain name of the SIP server.
Options	Self-defined options.
Code	Code of the self-defined option.
Length	Self-defined option length in bytes.
Hex	Self-defined option content represented by a hexadecimal number.

Related commands

ipv6 dhcp option-group

display ipv6 dhcp pool

Use **display ipv6 dhcp pool** to display information about a DHCPv6 address pool.

Syntax

display ipv6 dhcp pool [*pool-name* | **vpn-instance** *vpn-instance-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

pool-name: Displays information about the specified DHCPv6 address pool. The pool name is a case-insensitive string of 1 to 63 characters. If you do not specify a DHCPv6 address pool, this command displays information about all DHCPv6 address pools.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays information about DHCPv6 address pools for the public network.

Examples

Display information about DHCPv6 address pool 1.

```
<Sysname> display ipv6 dhcp pool 1
DHCPv6 pool: 1
  Network: 3FFE:501:FFFF:100::/64
    Preferred lifetime 604800 seconds, valid lifetime 2592000 seconds
  Prefix pool: 1
    Preferred lifetime 24000 seconds, valid lifetime 36000 seconds
  Addresses:
    Range: from 3FFE:501:FFFF:100::1
           to 3FFE:501:FFFF:100::99
    Preferred lifetime 70480 seconds, valid lifetime 200000 seconds
    Total address number: 153
    Available: 153
    In-use: 0
  Temporary addresses:
    Range: from 3FFE:501:FFFF:100::200
           to 3FFE:501:FFFF:100::210
    Preferred lifetime 60480 seconds, valid lifetime 259200 seconds
    Total address number: 17
    Available: 17
    In-use: 0
  Static bindings:
    DUID: 0003000100e0fc000001
    IAID: 0000003f
    Prefix: 3FFE:501:FFFF:200::/64
      Preferred lifetime 604800 seconds, valid lifetime 2592000 seconds
    Description: ClientA
    DUID: 0003000100e0fc00cff1
    IAID: 00000001
    Address: 3FFE:501:FFFF:2001::1/64
      Preferred lifetime 604800 seconds, valid lifetime 2592000 seconds
    Description: ClientB
  DNS server addresses:
    2::2
  Domain name:
    aaa.com
  SIP server addresses:
    5::1
  SIP server domain names:
    bbb.com
```

Display information about DHCPv6 address pool 1.

```
<Sysname> display ipv6 dhcp pool 1
DHCPv6 pool: 1
  Network: Not-available
    Preferred lifetime 604800 seconds, valid lifetime 2592000 seconds
```

Display information about DHCPv6 address pool 1.

```
<Sysname> display ipv6 dhcp pool 1
DHCPv6 pool: 1
  Network: 1::/64(Zombie)
    Preferred lifetime 604800 seconds, valid lifetime 2592000 seconds
```

Table 2 Command output

Field	Description
DHCPv6 pool	Name of the DHCPv6 address pool.
Network	IPv6 subnet for dynamic IPv6 address allocation. If the subnet prefix is ineffective, this field displays **Not-available**. If the subnet prefix becomes ineffective after a configuration recovery (for example, a switchover from the backup to the master), the prefix is marked **(Zombie)**.
Prefix pool	Prefix pool referenced by the address pool.
Preferred lifetime	Preferred lifetime in seconds.
valid lifetime	Valid lifetime in seconds.
Addresses	Non-temporary IPv6 address range.
Range	IPv6 address range for dynamic allocation.
Total address number	Total number of IPv6 addresses.
Available	Total number of available IPv6 addresses.
In-use	Total number of assigned IPv6 addresses.
Temporary addresses	Temporary IPv6 address range for dynamic allocation.
Static bindings	Static bindings configured in the address pool.
DUID	Client DUID.
IAID	Client IAID. If no IAID is configured, this field displays **Not configured**.
Prefix	IPv6 address prefix.
Address	Static IPv6 address.
Description	Description of the static binding.
DNS server addresses	DNS server address.
Domain name	Domain name.
SIP server addresses	SIP server address.
SIP server domain names	Domain name of the SIP server.

display ipv6 dhcp prefix-pool

Use **`display ipv6 dhcp prefix-pool`** to display information about a prefix pool.

Syntax

display ipv6 dhcp prefix-pool [*prefix-pool-number*] [**vpn-instance** *vpn-instance-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

prefix-pool-number: Displays detailed information about a prefix pool specified by its number in the range of 1 to 128. If you do not specify a prefix pool, this command displays brief information about all prefix pools.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays information about prefix pools for the public network.

Examples

Display brief information about all prefix pools.

```
<Sysname> display ipv6 dhcp prefix-pool
Prefix-pool Prefix                                  Available In-use Static
1           5::/64                                  64        0      0
```

Display brief information about all prefix pools.

```
<Sysname> display ipv6 dhcp  prefix-pool
Prefix-pool Prefix                                  Available In-use Static
2           Not-available                           0         0      0
```

Display brief information about all prefix pools.

```
<Sysname> display ipv6 dhcp  prefix-pool
Prefix-pool Prefix                                  Available In-use Static
11          21::/112(Zombie)                        0         64     0
```

Display detailed information about prefix pool 1.

```
<Sysname> display ipv6 dhcp prefix-pool 1
Prefix: 5::/64
Assigned length: 70
Total prefix number: 64
Available: 64
In-use: 0
Static: 0
```

Display detailed information about prefix pool 1.

```
<Sysname> display ipv6 dhcp prefix-pool 1
Prefix: Not-available
Assigned length: 70
Total prefix number: 0
Available: 0
In-use: 0
```

```
Static: 0
```

Display detailed information about prefix pool 1.

```
<Sysname> display ipv6 dhcp prefix-pool 1
Prefix: 5::/64(Zombie)
Assigned length: 70
Total prefix number: 10
Available: 0
In-use: 10
Static: 0
```

Table 3 Command output

Field	Description
Prefix-pool	Prefix pool number.
Prefix	Prefix specified in the prefix pool. If the prefix is ineffective, this field displays **Not-available**. If the prefix becomes ineffective after a configuration recovery (for example, a switchover from the backup to the master), the prefix is marked **(Zombie)**.
Available	Number of available prefixes.
In-use	Number of assigned prefixes.
Static	Number of statically bound prefixes.
Assigned length	Length of assigned prefixes.
Total prefix number	Number of prefixes.

display ipv6 dhcp server

Use **display ipv6 dhcp server** to display DHCPv6 server configuration information.

Syntax

display ipv6 dhcp server [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface *interface-type interface-number*: Displays DHCPv6 server configuration information for the specified interface. If you do not specify an interface, this command displays DHCPv6 server configuration information for all interfaces.

Examples

Display DHCPv6 server configuration information for all interfaces.

```
<Sysname> display ipv6 dhcp server
```

```
Interface             Pool
GigabitEthernet1/0/1  1
GigabitEthernet1/0/2  global
```

Display DHCPv6 server configuration information for the interface GigabitEthernet 1/0/1.

```
<Sysname> display ipv6 dhcp server interface gigabitethernet 1/0/1
Using pool: 1
Preference value: 0
Allow-hint: Enabled
Rapid-commit: Disabled
```

Table 4 Command output

Field	Description
Interface	Interface enabled with DHCPv6 server.
Pool	Address pool applied to the interface. If no address pool is applied to the interface, **global** is displayed. The DHCPv6 server selects a global address pool to assign a prefix, an address, and other configuration parameters to a client.
Using pool	Address pool applied to the interface. If no address pool is applied to the interface, **global** is displayed. The DHCPv6 server selects a global address pool to assign a prefix, an address, and other configuration parameters to a client.
Preference value	Server preference in the DHCPv6 Advertise message. The value range is 0 to 255. The bigger the value is, the higher preference the server has.
Allow-hint	Indicates whether desired address/prefix assignment is enabled.
Rapid-commit	Indicates whether rapid address/prefix assignment is enabled.

display ipv6 dhcp server conflict

Use **display ipv6 dhcp server conflict** to display information about IPv6 address conflicts.

Syntax

display ipv6 dhcp server conflict [**address** *ipv6-address*] [**vpn-instance** *vpn-instance-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

address *ipv6-address*: Displays conflict information for the specified IPv6 address. If you do not specify an IPv6 address, this command displays information about all IPv6 address conflicts.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays IPv6 address conflict information for the public network.

Usage guidelines

The DHCPv6 server creates IP address conflict information in the following conditions:

- The DHCPv6 client sends a DECLINE packet to the DHCPv6 server to inform the server of an IPv6 address conflict.
- The DHCPv6 server discovers that the only assignable address in the address pool is its own IPv6 address.

Examples

Display information about all address conflicts.

```
<Sysname> display ipv6 dhcp server conflict
IPv6 address                                Detect time
2001::1                                     Apr 25 16:57:20 2019
1::1:2                                      Apr 25 17:00:10 2019
```

Table 5 Command output

Field	Description
IPv6 address	Conflicted IPv6 address.
Detect time	Time when the conflict was discovered.

Related commands

reset ipv6 dhcp server conflict

display ipv6 dhcp server database

Use **display ipv6 dhcp server database** to display information about DHCPv6 binding auto backup.

Syntax

display ipv6 dhcp server database

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display information about DHCPv6 binding auto backup.

```
<Sysname> display ipv6 dhcp server database
 File name               :   database.dhcp
 Username                :
 Password                :
 Update interval         :   600 seconds
```

```
Latest write time       :   Feb  8 16:02:23 2014
Status                  :   Last write succeeded.
```

Table 6 Command output

Field	Description
File name	Name of the DHCPv6 binding backup file.
Username	Username for accessing the URL of the remote backup file.
Password	Password for accessing the URL of the remote backup file. This field displays ********** if a password is configured.
Update interval	Waiting time in seconds after a DHCPv6 binding change for the DHCPv6 server to update the backup file.
Latest write time	Time of the latest update.
Status	Status of the update: • **Writing**—The backup file is being updated. • **Last write succeeded**—The backup file was successfully updated. • **Last write failed**—The backup file failed to be updated.

display ipv6 dhcp server expired

Use **display ipv6 dhcp server expired** to display lease expiration information.

Syntax

display ipv6 dhcp server expired [[**address** *ipv6-address*] [**vpn-instance** *vpn-instance-name*] | **pool** *pool-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

address *ipv6-address*: Displays lease expiration information for the specified IPv6 address. If you do not specify an IPv6 address, this command displays lease expiration information for all IPv6 addresses.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays lease expiration information about IPv6 addresses for the public network.

pool *pool-name*: Displays lease expiration information for the DHCPv6 address pool specified by its name, a case-insensitive string of 1 to 63 characters. If you do not specify a DHCPv6 address pool, this command displays lease expiration information for all DHCPv6 address pools.

Usage guidelines

DHCPv6 assigns the expired IPv6 addresses to DHCPv6 clients when all available addresses have been assigned.

Examples

Display all lease expiration information.

```
<Sysname> display ipv6 dhcp server expired
IPv6 address           DUID                          Lease expiration
2001:3eff:fe80:4caa:   3030-3066-2e65-3230-302e-     Apr 25 17:10:47 2019
37ee:7::1              3130-3234-2d45-7468-6572-
                       6e65-7430-2f31
```

Table 7 Command output

Field	Description
IPv6 address	Expired IPv6 address.
DUID	Client DUID bound to the expired IPv6 address.
Lease expiration	Time when the lease expired.

Related commands

reset ipv6 dhcp server expired

display ipv6 dhcp server ip-in-use

Use **display ipv6 dhcp server ip-in-use** to display binding information for assigned IPv6 addresses.

Syntax

display ipv6 dhcp server ip-in-use [[**address** *ipv6-address*] [**vpn-instance** *vpn-instance-name*] | **pool** *pool-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

address *ipv6-address*: Displays binding information for the specified IPv6 address. If you do not specify an IPv6 address, this command displays binding information for all IPv6 addresses.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays binding information about IPv6 addresses for the public network.

pool *pool-name*: Displays IPv6 address binding information for the DHCPv6 address pool specified by its name, a case-insensitive string of 1 to 63 characters. If you do not specify a DHCPv6 address pool, this command displays IPv6 address binding information for all DHCPv6 address pools.

Examples

Display binding information for all assigned IPv6 address.

```
<Sysname> display ipv6 dhcp server ip-in-use
```

```
Pool: 1
 IPv6 address            Hardware address     Type      Lease expiration
 2:1::1                  0125-0354-aab2       Auto(O)   Jul 10 19:45:01 2019
Pool: 2
 IPv6 address            Hardware address     Type      Lease expiration
 1:1::2                  1325-0714-a3ec       Static(F) Not available
Pool: 3
 IPv6 address            Hardware address     Type      Lease expiration
 1:2::1F1                bb43-1314-bb32       Static(O) Oct  9 09:23:31 2019
Pool: 4
 IPv6 address            Hardware address     Type      Lease expiration
 2001:2F01:3EE3:3200:    ac22-5456-ee76       Auto(Z)   Oct  11 09:23:31 2019
 E013:7A86:5905:2012
```

Display binding information for all assigned IPv6 addresses for the specified DHCPv6 address pool.

```
<Sysname> display ipv6 dhcp server ip-in-use pool 1
Pool: 1
 IPv6 address            Hardware address     Type      Lease expiration
 2:1::1                  0125-0354-aab2       Auto(O)   Jul 10 22:22:22 2019
 3:1::2                  1563-8654-e2a3       Static(C) Jan  1 11:11:11 2019
```

Display binding information for the specified IPv6 address.

```
<Sysname> display ipv6 dhcp server ip-in-use address 2:1::3
Pool: 1
Client: FE80::C800:CFF0:FE18:0
Hardware address: 3674-0832-eab3
Type: Auto(O)
DUID: 00030001CA000C180000
IAID: 0x00030001
  IPv6 address: 2:1::3
  Preferred lifetime 400 seconds, valid lifetime 500 seconds
  Expires at Jul 10 09:45:01 2019 (288 seconds left)
```

Table 8 Command output

Field	Description
Pool	DHCPv6 address pool.
IPv6 address	IPv6 address assigned.
Hardware address	Hardware address of a DHCPv6 client. In a network with DHCPv6 relay agent, this field displays **N/A** because the DHCPv6 server cannot obtain the hardware address of the client.

Field	Description
Type	IPv6 address binding types: • **Static(F)**—Free static binding whose IPv6 address has not been assigned. • **Static(O)**—Offered static binding whose IPv6 address has been selected and sent by the DHCPv6 server in a DHCPv6-OFFER packet to the client. • **Static(C)**—Committed static binding whose IPv6 address has been assigned to the client. • **Auto(O)**—Offered dynamic binding whose IPv6 address has been dynamically selected by the DHCPv6 server and sent in a DHCPv6-OFFER packet to the DHCPv6 client. • **Auto(C)**—Committed dynamic binding whose IPv6 address has been dynamically assigned to the DHCPv6 client. • **Auto(Z)**—Zombie dynamic binding whose IPv6 address has been dynamically assigned to the DHCPv6 client. The binding becomes zombie because the subnet prefix goes invalid for address allocation after a configuration recovery, for example, after a switchover from the backup to the master.
Lease-expiration	Time when the lease of the IPv6 address will expire. If the lease expires after the year 2100, this field displays **Expires after 2100**. For an unassigned static binding, this field displays **Not available**.
Client	IPv6 address of the DHCPv6 client. For an unassigned static binding, this field is blank.
DUID	Client DUID.
IAID	Client IAID. For an unassigned static binding without IAID specified, this field displays **N/A**.
Preferred lifetime	Preferred lifetime in seconds of the IPv6 address.
valid lifetime	Valid lifetime in seconds of the IPv6 address.
Expires at	Time when the lease of an IPv6 address will expire. If the lease expires after the year 2100, this field displays **Expires after 2100**.

Related commands

`reset ipv6 dhcp server ip-in-use`

display ipv6 dhcp server pd-in-use

Use **`display ipv6 dhcp server pd-in-use`** to display binding information for the assigned IPv6 prefixes.

Syntax

`display ipv6 dhcp server pd-in-use` [**`pool`** *`pool-name`* | [**`prefix`** *`prefix/prefix-len`*] [**`vpn-instance`** *`vpn-instance-name`*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

pool *pool-name*: Displays IPv6 prefix binding information for the DHCPv6 address pool specified by its name, a case-insensitive string of 1 to 63 characters. If you do not specify a DHCPv6 address pool, this command displays IPv6 prefix binding information for all DHCPv6 address pools.

prefix *prefix/prefix-len*: Displays binding information for the specified IPv6 prefix. The value range for the prefix length is 1 to 128. If you do not specify an IPv6 prefix, this command displays binding information for all IPv6 prefixes.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays binding information about IPv6 prefixes for the public network.

Examples

Display all IPv6 prefix binding information.

```
<Sysname> display ipv6 dhcp server pd-in-use
Pool: 1
 IPv6 prefix             Hardware address     Type      Lease expiration
 2:1::/24                0125-0354-aab2       Auto(O)   Jul 10 19:45:01 2019
Pool: 2
 IPv6 prefix             Hardware address     Type      Lease expiration
 1:1::/64                1325-0714-a3ec       Static(F) Not available
Pool: 3
 IPv6 prefix             Hardware address     Type      Lease expiration
 1:2::/64                bb43-1314-bb32       Static(O) Oct  9 09:23:31 2019
Pool: 4
 IPv6 prefix             Hardware address     Type      Lease expiration
 12::/80                 ac22-5456-ee76       Auto(Z)   Oct 17 09:34:59 2019
```

Display IPv6 prefix binding information for DHCPv6 address pool 1.

```
<Sysname> display ipv6 dhcp server pd-in-use pool 1
Pool: 1
 IPv6 prefix             Hardware address     Type      Lease expiration
 2:1::/24                0125-0354-aab2       Auto(O)   Jul 10 22:22:22 2019
 3:1::/64                1563-8654-e2a3       Static(C) Jan  1 11:11:11 2019
```

Display binding information for the IPv6 prefix 2:1::3/24.

```
<Sysname> display ipv6 dhcp server pd-in-use prefix 2:1::3/24
Pool: 1
Client: FE80::C800:CFF:FE18:0
Hardware address: 3674-0832-eab3
Type: Auto(O)
DUID: 00030001CA000C180000
IAID: 0x00030001
  IPv6 prefix: 2:1::/24
   Preferred lifetime 400 seconds, valid lifetime 500 seconds
  Expires at Jul 10 09:45:01 2019 (288 seconds left)
```

Table 9 Command output

Field	Description
IPv6 prefix	IPv6 prefix assigned.

Field	Description
Hardware address	Hardware address of a DHCPv6 client. In a network with DHCPv6 relay agent, this field displays **N/A** because the DHCPv6 server cannot obtain the hardware address of the client.
Type	Prefix binding types: • **Static(F)**—Free static binding whose IPv6 prefix has not been assigned. • **Static(O)**—Offered static binding whose IPv6 prefix has been selected and sent by the DHCPv6 server in a DHCPv6-OFFER packet to the client. • **Static(C)**—Committed static binding whose IPv6 prefix has been assigned to the client. • **Auto(O)**—Offered dynamic binding whose IPv6 prefix has been dynamically selected by the DHCPv6 server and sent in a DHCPv6-OFFER packet to the DHCPv6 client. • **Auto(C)**—Committed dynamic binding whose IPv6 prefix has been dynamically assigned to the DHCPv6 client. • **Auto(Z)**—Zombie dynamic binding whose IPv6 prefix has been dynamically assigned to the DHCPv6 client. The binding becomes zombie because the prefix in the prefix pool goes invalid after a configuration recovery, for example, after a switchover from the backup to the master.
Pool	Address pool.
Lease-expiration	Time when the lease of the IPv6 prefix will expire. If the lease will expire after the year 2100, this field displays **Expires after 2100**. For an unassigned static binding, this field displays **Not available**.
Client	IPv6 address of the DHCPv6 client. For an unassigned static binding, this field is blank.
DUID	Client DUID.
IAID	Client IAID. For an unassigned static binding without IAID, this field displays **N/A**.
Preferred lifetime	Preferred lifetime in seconds of the IPv6 prefix.
valid lifetime	Valid lifetime in seconds of the IPv6 prefix.
Expires at	Time when the lease of the prefix will expire. If the lease expires after the year 2100, this field displays **Expires after 2100**.

Related commands

reset ipv6 dhcp server pd-in-use

display ipv6 dhcp server statistics

Use **display ipv6 dhcp server statistics to** display DHCPv6 packet statistics on the DHCPv6 server.

Syntax

display ipv6 dhcp server statistics [**pool** *pool-name* | **vpn-instance** *vpn-instance-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

pool *pool-name*: Displays DHCPv6 packet statistics for the DHCPv6 address pool specified by its name, a case-insensitive string of 1 to 63 characters. If you do not specify an address pool, this command displays DHCPv6 packet statistics for all address pools.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays DHCPv6 server statistics for the public network.

Examples

Display all DHCPv6 packet statistics on the DHCPv6 server.

```
<Sysname> display ipv6 dhcp server statistics
Bindings:
    Ip-in-use               :  1
    Pd-in-use               :  0
    Expired                 :  0
Conflict                    :  0
Packets received            :  1
    Solicit                 :  1
    Request                 :  0
    Confirm                 :  0
    Renew                   :  0
    Rebind                  :  0
    Release                 :  0
    Decline                 :  0
    Information-request     :  0
    Relay-forward           :  0
Packets dropped             :  0
Packets sent                :  0
    Advertise               :  0
    Reconfigure             :  0
    Reply                   :  0
    Relay-reply             :  0
```

Table 10 Command output

Field	Description
Bindings	Number of bindings: • **Ip-in-use**—Total number of address bindings. • **Pd-in-use**—Total number of prefix bindings. • **Expired**—Total number of expired address bindings.
Conflict	Total number of conflicted addresses. If statistics about an address pool are displayed, this field is not displayed.

Field	Description
Packets received	Number of messages received by the DHCPv6 server. The message types include: • Solicit. • Request. • Confirm. • Renew. • Rebind. • Release. • Decline. • Information-request. • Relay-forward. If statistics about an address pool are displayed, this field is not displayed.
Packets dropped	Number of packets discarded. If statistics about an address pool are displayed, this field is not displayed.
Packets sent	Number of messages sent by the DHCPv6 server. The message types include: • Advertise. • Reconfigure. • Reply. • Relay-reply. If statistics about an address pool are displayed, this field is not displayed.

Related commands

`reset ipv6 dhcp server statistics`

dns-server

Use **`dns-server`** to specify a DNS server in a DHCPv6 address pool.

Use **`undo dns-server`** to remove the specified DNS server from a DHCPv6 address pool.

Syntax

`dns-server` *`ipv6-address`*

`undo dns-server` *`ipv6-address`*

Default

No DNS server address is specified.

Views

DHCPv6 address pool view

DHCPv6 option group view

Predefined user roles

network-admin

context-admin

Parameters

`ipv6-address`: Specifies the IPv6 address of a DNS server.

Usage guidelines

You can use the **dns-server** command to specify up to eight DNS servers in an address pool. A DNS server specified earlier has a higher preference.

Examples

Specify the DNS server address 2:2::3 in DHCPv6 address pool 1.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] dns-server 2:2::3
```

Related commands

display ipv6 dhcp pool

domain-name

Use **domain-name** to specify a domain name in a DHCPv6 address pool.

Use **undo domain-name** to restore the default.

Syntax

domain-name *domain-name*

undo domain-name

Default

No domain name is specified.

Views

DHCPv6 address pool view

DHCPv6 option group view

Predefined user roles

network-admin

context-admin

Parameters

domain-name: Specifies a domain name, a case-sensitive string of 1 to 50 characters.

Usage guidelines

You can configure only one domain name in an address pool. If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the domain name **aaa.com** in DHCPv6 address pool 1.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] domain-name aaa.com
```

Related commands

display ipv6 dhcp pool

if-match

Use **if-match** to configure a match rule for a DHCPv6 user class.

Use **undo if-match** to delete a match rule for a DHCP user class.

Syntax

if-match rule *rule-number* { **option** *option-code* [**ascii** *ascii-string* [**offset** *offset* | **partial**] | **hex** *hex-string* [**mask** *mask* | **offset** *offset* **length** *length* | **partial**]] | **relay-agent** *gateway-ipv6-address* }

undo if-match rule *rule-number*

Default

No match rules are configured for the DHCPv6 user class.

Views

DHCPv6 user class view

Predefined user roles

network-admin

context-admin

Parameters

rule *rule-number*: Assigns the match rule an ID in the range of 1 to 128. A smaller ID represents a higher match priority.

option *option-code*: Specifies a DHCPv6 option by its number in the range of 1 to 65535.

ascii *ascii-string*: Specifies an ASCII string of 1 to 128 characters.

offset *offset*: Specifies the offset in bytes after which the match operation starts. The value range is 0 to 65534. If you specify an ASCII string, a packet matches the rule if the option content after the offset is the same as the ASCII string. If you specify a hexadecimal number, a packet matches the rule if the option content of the specified length after the offset is the same as the hexadecimal number.

partial: Enables partial match. A packet matches the rule if the specified option in the packet contains the ASCII string or hexadecimal number specified in the rule. For example, if you specify **abc** in the rule, option content **xabc**, **xyzabca**, **xabcyz**, and **abcxyz** all match the rule.

hex *hex-string*: Specifies a hexadecimal number. The length of the hexadecimal number must be an even number in the range of 2 to 256.

mask *mask*: Specifies the mask for the match operation. The mask is a hexadecimal number whose length is an even number in the range of 2 to 256 and must be the same as the *hex-string* length. The DHCPv6 server selects option content of the mask length from the start and ANDs the selected option content and the specified hexadecimal number with the mask. The packet matches the rule if the two AND operation results are the same.

length *length*: Specifies the length of the option content to be matched, in the range of 1 to 128 bytes. The length must be the same as the *hex-string* length.

relay-agent *gateway-ipv6-address*: Specifies a **link-address** field value. The value is an IPv6 address. A packet matches the rule if its **link-address** field value is the same as that in the rule.

Usage guidelines

If a DHCPv6 request sent by a DHCPv6 client matches a rule in a DHCPv6 user class, the DHCPv6 client matches the user class.

You can configure multiple match rules for a DHCPv6 user class. Each match rule is uniquely identified by a rule ID within its type (option or relay agent address).

- If the rule that you are configuring has the same ID and type as an existing rule, the new rule overwrites the existing rule.

- If the rule that you are configuring has the same ID as an existing rule but a different type, the new rule takes effect and coexists with the existing rule. As a best practice, do not assign the same ID to rules of different types.
- Rules of different IDs cannot have the same rule content.

When you configure an **if-match option** rule, follow these guidelines:

- To match packets that contain an option, specify only the *option-code* argument.
- To match a hexadecimal number by AND operations, specify the **option** *option-code* **hex** *hex-string* **mask** *mask* options.
- To match a hexadecimal number directly, specify the **option** *option-code* **hex** *hex-string* [**offset** *offset* **length** *length* | **partial**] options. If you do not specify the **offset**, **length**, or **partial** parameter, a packet matches a rule if the option content starts with the hexadecimal number.
- To match an ASCII string, specify the **option** *option-code* **ascii** *ascii-string* [**offset** *offset* | **partial**] options. If you do not specify the **offset** or **partial** parameter, a packet matches a rule if the option content starts with the ASCII string.

Examples

Configure match rule **1** for the DHCPv6 user class **exam** to match DHCPv6 requests that contain Option 16.

```
<Sysname> system-view
[Sysname] ipv6 dhcp class exam
[Sysname-dhcp6-class-exam] if-match rule 1 option 16
```

Configure match rule **2** for the DHCPv6 user class **exam**. The rule matches DHCPv6 requests in which the highest bit of the fourth byte in Option 16 is the hexadecimal number **1**.

```
<Sysname> system-view
[Sysname] ipv6 dhcp class exam
[Sysname-dhcp6-class-exam] if-match rule 2 option 16 hex 00000080 mask 00000080
```

Configure match rule **3** for the DHCPv6 user class **exam**. The rule matches DHCPv6 requests in which the first three bytes of Option 16 are the hexadecimal number **13ae92**.

```
<Sysname> system-view
[Sysname] ipv6 dhcp class exam
[Sysname-dhcp6-class-exam] if-match rule 3 option 16 hex 13ae92 offset 0 length 3
```

Configure match rule **4** for the DHCPv6 user class **exam**. The rule matches DHCPv6 requests in which the Option 16 contains the hexadecimal number **13ae**.

```
<Sysname> system-view
[Sysname] ipv6 dhcp class exam
[Sysname-dhcp6-class-exam] if-match rule 5 option 16 hex 13ae partial
```

Configure match rule **5** for the DHCPv6 user class **exam** to match DHCPv6 requests in which the **link-address** field is 2001::1.

```
<Sysname> system-view
[Sysname] ipv6 dhcp class exam
[Sysname-dhcp6-class-exam] if-match rule 5 relay-agent 2001::1
```

Related commands

ipv6 dhcp class

ipv6 dhcp apply-policy

Use **ipv6 dhcp apply-policy** to apply a DHCPv6 policy to an interface.

Use **undo ipv6 dhcp apply-policy** to restore the default.

Syntax

ipv6 dhcp apply-policy *policy-name*

undo ipv6 dhcp apply-policy

Default

No DHCPv6 policy is applied to an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies a DHCPv6 policy by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

You can apply only one DHCPv6 policy to an interface. If you execute this command multiple times, the most recent configuration takes effect.

Examples

Apply the DHCPv6 policy **test** to GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp apply-policy test
```

Related commands

ipv6 dhcp class

ipv6 dhcp class

Use **ipv6 dhcp class** to create a DHCPv6 user class and enter its view, or enter the view of an existing DHCPv6 user class.

Use **undo ipv6 dhcp class** to delete the specified DHCPv6 user class.

Syntax

ipv6 dhcp class *class-name*

undo ipv6 dhcp class *class-name*

Default

No DHCPv6 user classes exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

class-name: Specifies a name for the DHCPv6 user class, a case-insensitive string of 1 to 63 characters.

Usage guidelines

In the DHCPv6 user class view, you can use the **if-match** command to configure match rules for user classification.

Examples

Create a DHCPv6 user class **test** and enter DHCPv6 user class view.

```
<Sysname> system-view
[Sysname] ipv6 dhcp class test
[Sysname-dhcp6-class-test]
```

Related commands

class pool

ipv6 dhcp policy

if-match

ipv6 dhcp option-group

Use **ipv6 dhcp option-group** to create a static DHCPv6 option group and enter its view.

Use **undo ipv6 dhcp option-group** to delete the specified static DHCPv6 option group.

Syntax

ipv6 dhcp option-group *option-group-number*

undo ipv6 dhcp option-group *option-group-number*

Default

No static DHCPv6 option groups exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

option-group-number: Assigns an ID to the static option group, in the range of 1 to 100.

Usage guidelines

A static DHCPv6 option group can use the same ID as a dynamic DHCPv6 option group. If a static DHCPv6 option group and a dynamic DHCPv6 option group use the same ID, the static one takes precedence over the dynamic one.

Examples

Create static DHCPv6 option group 1 and enter its view.

```
<Sysname> system-view
[Sysname] ipv6 dhcp option-group 1
[Sysname-dhcp6-option-group-1]
```

Related commands

display ipv6 dhcp option-group

ipv6 dhcp policy

Use **ipv6 dhcp policy** to create a DHCPv6 policy and enter its view, or enter the view of an existing DHCPv6 policy.

Use **undo ipv6 dhcp policy** to delete a DHCPv6 policy.

Syntax

ipv6 dhcp policy *policy-name*

undo ipv6 dhcp policy *policy-name*

Default

No DHCPv6 policies exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Assigns a name to the DHCPv6 policy. The policy name is a case-insensitive string of 1 to 63 characters.

Usage guidelines

In DHCP policy view, you can specify address pools for different user classes. Clients matching a user class will obtain IPv6 addresses and other parameters from the specified address pool.

For a DHCPv6 policy to take effect, you must apply it to an interface.

Examples

Create DHCPv6 policy **test** and enter its view.

```
<Sysname> system-view
[Sysname] ipv6 dhcp policy test
[Sysname-dhcp6-policy-test]
```

Related commands

class pool

default pool

ipv6 dhcp apply-policy

ipv6 dhcp class

ipv6 dhcp pool

Use **ipv6 dhcp pool** to create a DHCPv6 address pool and enter its view, or enter the view of an existing DHCPv6 address pool.

Use **undo ipv6 dhcp pool** to delete the specified DHCPv6 address pool.

Syntax

ipv6 dhcp pool *pool-name*

undo ipv6 dhcp pool *pool-name*

Default

No DHCPv6 address pools exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

pool-name: Specifies a name for the DHCPv6 address pool, a case-insensitive string of 1 to 63 characters.

Usage guidelines

A DHCPv6 address pool stores IPv6 address/prefix and other configuration parameters to be assigned to DHCPv6 clients.

When you delete a DHCPv6 address pool, binding information for the assigned IPv6 addresses and prefixes in the address pool is also deleted.

Examples

Create a DHCPv6 address pool named **pool1** and enter its view.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool pool1
[Sysname-dhcp6-pool-pool1]
```

Related commands

class pool

display ipv6 dhcp pool

ipv6 dhcp server apply pool

ipv6 dhcp prefix-pool

Use **ipv6 dhcp prefix-pool** to create a prefix pool and specify the prefix and the assigned prefix length for the pool.

Use **undo ipv6 dhcp prefix-pool** to delete the specified prefix pool.

Syntax

ipv6 dhcp prefix-pool *prefix-pool-number* **prefix** { *prefix-number* | *prefix/prefix-len* } **assign-len** *assign-len* [**vpn-instance** *vpn-instance-name*]

undo ipv6 dhcp prefix-pool *prefix-pool-number* [**vpn-instance** *vpn-instance-name*]

Default

No prefix pools exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

prefix-pool-number: Specifies a prefix pool number in the range of 1 to 128.

prefix { *prefix-number* | *prefix/prefix-len* }: Specifies a prefix by its ID or in the format of *prefix*/*prefix length*. The value range for the *prefix-number* argument is 1 to 1024. The value range for the *prefix-len* argument is 1 to 128.

assign-len *assign-len*: Specifies the assigned prefix length. The value range is 1 to 128, and the value must be greater than or equal to *prefix-len*. The difference between *assign-len* and *prefix-len* must be no more than 16.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. To create a prefix pool for the public network, do not specify this option.

Usage guidelines

Different prefix pools cannot overlap.

To modify a prefix pool, execute the **undo ipv6 dhcp prefix-pool** command to delete the prefix pool, and then execute the **ipv6 dhcp prefix-pool** command.

Deleting a prefix pool clears all prefix bindings from the prefix pool.

When you specify a prefix by its ID, follow these restrictions and guidelines:

- This command does not take effect if the prefix does not exist. This command takes effect after the prefix is created.
- Do not specify the same prefix for different prefix pools in a VPN.
- If the prefix that the ID represents is changed, the prefix range in the prefix pool accordingly changes.

Examples

Create IPv6 prefix 88:99::/32 with ID 3. Configure prefix pool 2 with IPv6 prefix 3 and an assigned prefix length of 42. Prefix pool 2 contains 1024 prefixes from 88:99::/42 to 88:99:FFC0::/42.

```
<Sysname> system-view
[Sysname] ipv6 prefix 3 88:99::/32
[Sysname] ipv6 dhcp prefix-pool 2 prefix 3 assign-len 42
```

Create prefix pool 1, and specify prefix 2001:0410::/32 with an assigned prefix length of 42. Prefix pool 1 contains 1024 prefixes from 2001:0410::/42 to 2001:0410:FFC0::/42.

```
<Sysname> system-view
[Sysname] ipv6 dhcp prefix-pool 1 prefix 2001:0410::/32 assign-len 42
```

Related commands

display ipv6 dhcp prefix-pool

prefix-pool

ipv6 dhcp server

Use **ipv6 dhcp server** to configure global address assignment on an interface. The server on the interface uses a global address pool to assign configuration information to a client.

Use **undo ipv6 dhcp server** to restore the default.

Syntax

ipv6 dhcp server { **allow-hint** | **preference** *preference-value* | **rapid-commit** } *

undo ipv6 dhcp server

Default

The server supports global address assignment on an interface, but does not support desired address/prefix assignment or rapid address/prefix assignment. No server preference is set.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

allow-hint: Enables desired address/prefix assignment.

preference *preference-value*: Specifies the server preference in Advertise messages, in the range of 0 to 255. A greater value represents a higher preference.

rapid-commit: Enables rapid address/prefix assignment involving two messages.

Usage guidelines

The **allow-hint** keyword enables the server to assign the desired address or prefix to the requesting client. If the desired address or prefix is not included in any global address pool, or is already assigned to another client, the server assigns the client a free address or a prefix. If the **allow-hint** keyword is not specified, the server ignores the desired address or prefix, and selects an address or prefix from a global address pool.

If you use the **ipv6 dhcp server** and **ipv6 dhcp server apply pool** commands on the same interface, the **ipv6 dhcp server apply pool** command takes effect.

Examples

Configure global address assignment on the interface GigabitEthernet 1/0/1. Use the desired address/prefix assignment and rapid address/prefix assignment, and set the server preference to the highest 255.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp server allow-hint preference 255 rapid-commit
```

Related commands

display ipv6 dhcp server

ipv6 dhcp select

ipv6 dhcp server apply pool

Use **ipv6 dhcp server apply pool** to apply a DHCPv6 address pool to an interface.

Use **undo ipv6 dhcp server apply pool** to restore the default.

Syntax

ipv6 dhcp server apply pool *pool-name* [**allow-hint** | **preference** *preference-value* | **rapid-commit**] *

undo ipv6 dhcp server apply pool

Default

No DHCPv6 address pool is applied to an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

pool-name: Specifies a DHCPv6 address pool by its name, a case-insensitive string of 1 to 63 characters.

allow-hint: Enables desired address/prefix assignment.

preference *preference-value*: Specifies the server preference in Advertise messages, in the range of 0 to 255. A greater value represents a higher preference. By default, no server preference is set.

rapid-commit: Enables rapid address/prefix assignment involving two messages.

Usage guidelines

Upon receiving a DHCPv6 request, the DHCPv6 server selects an IPv6 address or prefix from the address pool applied to the receiving interface. If no address pool is applied, the server selects an IPv6 address or prefix from a global address pool that matches the IPv6 address of the receiving interface or the DHCPv6 relay agent.

The **allow-hint** keyword enables the server to assign the desired address or prefix to the client. If the desired address or prefix does not exist or is already assigned to another client, the server assigns a free address or prefix. If **allow-hint** is not specified, the server ignores the desired address or prefix, and assigns a free address or prefix.

Only one address pool can be applied to an interface. If you execute this command multiple times, the most recent configuration takes effect.

A non-existing address pool can be applied to an interface, but the server cannot assign any prefix, address, or other configuration information from the address pool until the address pool is created.

Examples

Apply address pool 1 to GigabitEthernet 1/0/1, configure the address pool to support desired address/prefix assignment and address/prefix rapid assignment, and set the preference to 255.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp server apply pool 1 allow-hint preference 255
rapid-commit
```

Related commands

display ipv6 dhcp server

ipv6 dhcp pool

ipv6 dhcp select

ipv6 dhcp server database filename

Use **ipv6 dhcp server database filename** to configure the DHCPv6 server to back up the DHCPv6 bindings to a file.

Use **undo ipv6 dhcp server database filename** to restore the default.

Syntax

ipv6 dhcp server database filename { *filename* | **url** *url* [**username** *username* [**password** { **cipher** | **simple** } *string*]] }

undo ipv6 dhcp server database filename

Default

The DHCPv6 server does not back up the DHCPv6 bindings.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

filename: Specifies the name of a local backup file. For information about the *filename* argument, see *Fundamentals Configuration Guide*.

url *url*: Specifies the URL of a remote backup file. The URL is a case-sensitive string of 1 to 255 characters. Do not include a username or password in the URL.

username *username*: Specifies the username for accessing the URL of the remote backup file, a case-sensitive string of 1 to 32 characters. Do not specify this option if a username is not required for accessing the URL of the remote backup file.

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 32 characters. Its encrypted form is a case-sensitive string of 1 to 73 characters. Do not specify this argument if a password is not required for accessing the URL of the remote backup file.

Usage guidelines

The command automatically creates the file if you specify a nonexistent file.

With this command executed, the DHCPv6 server backs up its bindings immediately and runs auto backup. The server, by default, waits 300 seconds after a binding change to update the backup file. You can use the **ipv6 dhcp server database update interval** command to change the waiting time. If no DHCPv6 binding changes, the backup file is not updated.

As a best practice, back up the bindings to a remote file. If you use the local storage medium, the frequent erasing and writing might damage the medium and then cause the DHCPv6 server to malfunction.

When the backup file is on a remote device, follow these restrictions and guidelines to specify the URL, username, and password:

- If the file is on an FTP server, enter URL in the format of ftp:*//server address:port/file path*, where the port number is optional.
- If the file is on a TFTP server, enter URL in the format of tftp:*//server address:port/file path*, where the port number is optional.
- The username and password must be the same as those configured on the FTP server. If the server authenticates only the username, the password can be omitted.
- If the IP address of the server is an IPv6 address, enclose the address in a pair of brackets, for example, **ftp://[1::1]/database.dhcp**.
- You can also specify the DNS domain name for the server address field, for example, **ftp://company/database.dhcp**.

Examples

Configure the DHCPv6 server to back up its bindings to the file **database.dhcp**

```
<Sysname> system-view
[Sysname] ipv6 dhcp server database filename database.dhcp
```

Configure the DHCPv6 server to back up its bindings to the file **database.dhcp** in the working directory of the FTP server at 10::1.

```
<Sysname> system-view
[Sysname] ipv6 dhcp server database filename url ftp://[10::1]/database.dhcp username 1
password simple 1
```

Related commands

ipv6 dhcp server database update interval

ipv6 dhcp server database update now

ipv6 dhcp server database update stop

ipv6 dhcp server database update interval

Use **ipv6 dhcp server database update interval** to set the waiting time for the DHCPv6 server to update the backup file after a DHCPv6 binding change.

Use **undo ipv6 dhcp server database update interval** to restore the default.

Syntax

ipv6 dhcp server database update interval *interval*

undo ipv6 dhcp server database update interval

Default

The DHCPv6 server waits 300 seconds to update the backup file after a DHCPv6 binding change. If no DHCPv6 binding changes, the backup file is not updated.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interval: Sets the waiting time in the range of 60 to 864000 seconds.

Usage guidelines

When a DHCPv6 binding is created, updated, or removed, the waiting period starts. The DHCPv6 server updates the backup file when the waiting period is reached. All bindings changed during the period will be saved to the backup file.

The waiting time takes effect only after you configure the DHCPv6 binding auto backup by using the **ipv6 dhcp server database filename** command.

Examples

Set the waiting time to 600 seconds for the DHCPv6 server to update the backup file.

```
<Sysname> system-view
[Sysname] ipv6 dhcp server database update interval 600
```

Related commands

ipv6 dhcp server database filename

ipv6 dhcp server database update now

ipv6 dhcp server database update stop

ipv6 dhcp server database update now

Use **ipv6 dhcp server database update now** to manually save the DHCPv6 bindings to the backup file.

Syntax

ipv6 dhcp server database update now

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

Each time this command is executed, the DHCPv6 bindings are saved to the backup file.

For this command to take effect, you must configure the DHCPv6 auto backup by using the **ipv6 dhcp server database filename** command.

Examples

Manually save the DHCPv6 bindings to the backup file.

```
<Sysname> system-view
[Sysname] ipv6 dhcp server database update now
```

Related commands

ipv6 dhcp server database filename

ipv6 dhcp server database update interval

ipv6 dhcp server database update stop

ipv6 dhcp server database update stop

Use **ipv6 dhcp server database update stop** to terminate the download of DHCPv6 bindings from the backup file.

Syntax

ipv6 dhcp server database update stop

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

The DHCPv6 server does not provide services during the binding download process. If the connection breaks up during the process, the waiting timeout timer is 60 minutes. When the timer expires, the DHCPv6 server stops waiting and starts providing address allocation services. You can execute this command to terminate the download immediately.

Manual termination allows the DHCPv6 server to provide services without waiting for the connection to be repaired. The IPv6 addresses and prefixes associated with the undownloaded bindings will be assigned to clients and address conflicts might occur.

Examples

Terminate the download of the backup DHCPv6 bindings.

```
<Sysname> system-view
[Sysname] ipv6 dhcp server database update stop
```

Related commands

ipv6 dhcp server database filename

ipv6 dhcp server database update interval

ipv6 dhcp server database update now

ipv6 dhcp server forbidden-address

Use **ipv6 dhcp server forbidden-address** to exclude IPv6 addresses in the DHCPv6 address pool from dynamic allocation.

Use **undo ipv6 dhcp server forbidden-address** to remove the configuration.

Syntax

ipv6 dhcp server forbidden-address *start-ipv6-address* [*end-ipv6-address*] [**vpn-instance** *vpn-instance-name*]

undo ipv6 dhcp server forbidden-address *start-ipv6-address* [*end-ipv6-address*] [**vpn-instance** *vpn-instance-name*]

Default

Except for the DHCPv6 server address, all IPv6 addresses in a DHCPv6 address pool are assignable.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

start-ipv6-address: Specifies the start IPv6 address.

end-ipv6-address: Specifies the end IPv6 address, which cannot be lower than *start-ipv6-address*. If you do not specify an end IPv6 address, only the start IPv6 address is excluded from dynamic allocation. If you specify an end IPv6 address, the IP addresses from *start-ipv6-address* through *end-ipv6-address* are all excluded from dynamic allocation.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If the excluded IPv6 addresses belong to the public network, do not specify this option.

Usage guidelines

The IPv6 addresses of some devices such as the gateway and FTP server cannot be assigned to clients. Use this command to exclude such addresses from dynamic allocation.

If the excluded IPv6 address is in a static DHCPv6 binding, the address can still be assigned to the client.

The address or address range specified in the **undo** form of the command must be the same as the address or address range specified in the command. To remove an IP address that has been specified as part of an address range, you must remove the entire address range.

You can execute this command multiple times to exclude multiple IPv6 address ranges from dynamic allocation.

Examples

Exclude IPv6 addresses of 2001:10:110::1 through 2001:10:110::20 from dynamic assignment.

```
<Sysname> system-view
[Sysname] ipv6 dhcp server forbidden-address 2001:10:110::1 2001:10:110::20
```

Related commands

ipv6 dhcp server forbidden-prefix

static-bind

ipv6 dhcp server forbidden-prefix

Use **ipv6 dhcp server forbidden-prefix** to exclude IPv6 prefixes in the DHCPv6 prefix pool from dynamic allocation.

Use **undo ipv6 dhcp server forbidden-prefix** to remove the configuration.

Syntax

ipv6 dhcp server forbidden-prefix *start-prefix/prefix-len* [*end-prefix/prefix-len*] [**vpn-instance** *vpn-instance-name*]

undo ipv6 dhcp server forbidden-prefix *start-prefix/prefix-len* [*end-prefix/prefix-len*] [**vpn-instance** *vpn-instance-name*]

Default

No IPv6 prefixes in the DHCPv6 prefix pool are excluded from dynamic allocation.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

start-prefix/prefix-len: Specifies the start IPv6 prefix. The *prefix-len* argument specifies the prefix length in the range of 1 to 128.

end-prefix/prefix-len: Specifies the end IPv6 prefix. The *prefix-len* argument specifies the prefix length in the range of 1 to 128. The value for *end-prefix* cannot be lower than that for *start-prefix*. If you do not specify this argument, only the *start-prefix/prefix-len* is excluded from dynamic allocation. If you specify this argument, the prefixes from *start-prefix/prefix-len* to *end-prefix/prefix-len* are all excluded.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If the excluded IPv6 prefixes belong to the public network, do not specify this option.

Usage guidelines

If the excluded IPv6 prefix is in a static binding, the prefix can still be assigned to the client.

The prefix or prefix range specified in the **undo** form of the command must be the same as the prefix or prefix range specified in the command. To remove a prefix that has been specified as part of a prefix range, you must remove the entire prefix range.

You can execute this command multiple times to exclude multiple IPv6 prefix ranges from dynamic allocation.

Examples

Exclude IPv6 prefixes from 2001:3e11::/32 through 2001:3eff::/32 from dynamic allocation.

```
<Sysname> system-view
[Sysname] ipv6 dhcp server forbidden-prefix 2001:3e11::/32 2001:3eff::/32
```

Related commands

ipv6 dhcp server forbidden-address

static-bind

network

Use **network** to specify an IPv6 subnet for dynamic allocation in a DHCPv6 address pool.

Use **undo network** to restore the default.

Syntax

network { *prefix/prefix-length* | **prefix** *prefix-number* [*sub-prefix/sub-prefix-length*] } [**preferred-lifetime** *preferred-lifetime* **valid-lifetime** *valid-lifetime*] [**export-route**]

undo network

Default

No IPv6 subnet is specified in a DHCPv6 address pool.

Views

DHCPv6 address pool view

Predefined user roles

network-admin

context-admin

Parameters

prefix/prefix-length: Specifies the IPv6 subnet for dynamic allocation. The value range for the *prefix-length* argument is 1 to 128.

prefix *prefix-number*: Specifies an IPv6 prefix by its ID in the range of 1 to 1024.

sub-prefix/*sub-prefix-length*: Specifies an IPv6 sub-prefix and its length. The value range for the *sub-prefix-length* argument is 1 to 128. If the IPv6 prefix is longer than the IPv6 sub-prefix or if you do not specify an IPv6 sub-prefix, the IPv6 subnet defined by the IPv6 prefix is used for dynamic allocation.

preferred-lifetime *preferred-lifetime*: Sets the preferred lifetime. The value range is 60 to 4294967295 seconds, and the default is 604800 seconds (7 days).

valid-lifetime *valid-lifetime*: Sets the valid lifetime. The value range is 60 to 4294967295 seconds, and the default is 2592000 seconds (30 days). The valid lifetime must be longer than or equal to the preferred lifetime.

export-route: Advertises the subnet assigned to DHCPv6 clients. If you do not specify this keyword, the subnet will not be advertised.

Usage guidelines

You can specify only one subnet for a DHCPv6 address pool. If you execute the **network** command multiple times, the most recent configuration takes effect.

Modifying or removing the **network** command configuration removes assigned addresses in the current address pool.

If you execute the **network export-route** command multiple times, the most recent configuration takes effect.

The **network prefix** command does not take effect if the specified IPv6 prefix does not exist. This command takes effect after the IPv6 prefix is created.

The **network** command defines the IPv6 subnet for dynamic allocation through the *prefix/prefix-length* arguments or the *prefix-number* [*sub-prefix*/*sub-prefix-length*] arguments. The IPv6 subnets cannot be the same in different DHCPv6 address pools.

If the prefix that the ID represents is changed, the IPv6 subnet in this command accordingly changes, and the assigned prefix and address bindings are cleared.

Examples

Specify the subnet 3ffe:501:ffff:100::/64 in DHCPv6 address pool 1.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] network 3ffe:501:ffff:100::/64
```

Create IPv6 prefix 88:99::/32 with the prefix ID 3. Create DHCPv6 address pool 1 and use the IPv6 subnet defined by the IPv6 prefix for dynamic allocation.

```
<Sysname> system-view
[Sysname] ipv6 prefix 3 88:99::/32
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] network prefix 3
```

Create IPv6 prefix 88:99::/32 with the prefix ID 3. Create DHCPv6 address pool 1 and use IPv6 subnet 88:99:ffff:100::/64 defined by IPv6 prefix 3 and IPv6 sub-prefix 3ffe:501:ffff:100::/64 for dynamic allocation. The first 32 bits of the IPv6 subnet are determined by IPv6 prefix 3. The bits 33 to 64 of the IPv6 subnet are determined by the IPv6 sub-prefix and its length. The prefix length of the IPv6 subnet is the IPv6 sub-prefix length.

```
<Sysname> system-view
```

```
[Sysname] ipv6 prefix 3 88:99::/32
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] network prefix 3 3ffe:501:ffff:100::/64
```

Related commands

address range

display ipv6 dhcp pool

temporary address range

option

Use **option** to configure a self-defined DHCPv6 option in a DHCPv6 address pool.

Use **undo option** to remove a self-defined DHCPv6 option from a DHCPv6 address pool.

Syntax

option *code* **hex** *hex-string*

undo option *code*

Default

No self-defined DHCPv6 option is configured in a DHCPv6 address pool.

Views

DHCPv6 address pool view

DHCPv6 option group view

Predefined user roles

network-admin

context-admin

Parameters

code: Specifies a number for the self-defined option, in the range of 21 to 65535, excluding 25 through 26, 37 through 40, and 43 through 48.

hex *hex-string*: Specifies the content of the option, a hexadecimal number whose length is an even number in the range of 2 to 256.

Usage guidelines

The DHCPv6 server fills the self-defined option with the specified hexadecimal number and sends it in a response to the client.

You can self-define options for the following purposes:

- Add newly released options.
- Add options for which the vendor defines the contents, for example, Option 43.
- Add options for which the CLI does not provide a dedicated configuration command like **dns-server**. For example, you can use the **option 31 hex 02000000000000000000000000000001** command to define the NTP server address 200::1 for DHCP clients.

If a DHCPv6 option is specified by both the dedicated command and the **option** command, the DHCPv6 server preferentially assigns the content specified by the dedicated command. For example, if a DNS server address is specified by the **dns-server** command and the **option 23** command, the server uses the address specified by **dns-server** command.

If you execute this command multiple times with the same *code* specified, the most recent configuration takes effect.

Examples

Configure Option 23 that specifies a DNS server address 2001:f3e0::1 in DHCPv6 address pool 1.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] option 23 hex 2001f3e000000000000000000000001
```

Related commands

display ipv6 dhcp pool

dns-server

domain-name

sip-server

option-group

Use **option-group** to specify a DHCPv6 option group for a DHCPv6 address pool.

Use **undo option-group** to restore the default.

Syntax

option-group *option-group-number*

undo option-group

Default

No DHCPv6 option group is specified for a DHCPv6 address pool.

Views

DHCPv6 address pool view

Predefined user roles

network-admin

context-admin

Parameters

option-group--number: Specifies a DHCPv6 option group by its number in the range of 1 to 100.

Examples

Specify DHCPv6 option group 1 for DHCPv6 address pool 1.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] option-group 1
```

Related commands

display ipv6 dhcp pool

ipv6 dhcp option-group

prefix-pool

Use **prefix-pool** to apply a prefix pool to a DHCPv6 address pool, so the DHCPv6 server can dynamically select a prefix from the prefix pool for a client.

Use **undo prefix-pool** to remove the prefix pool.

Syntax

prefix-pool *prefix-pool-number* [**preferred-lifetime** *preferred-lifetime* **valid-lifetime** *valid-lifetime*]

undo prefix-pool *prefix-pool-number*

Default

No prefix pool is applied to a DHCPv6 address pool.

Views

DHCPv6 address pool view

Predefined user roles

network-admin

context-admin

Parameters

prefix-pool-number: Specifies a prefix pool by its number in the range of 1 to 128.

preferred-lifetime *preferred-lifetime*: Sets the preferred lifetime in the range of 60 to 4294967295 seconds. The default value is 604800 seconds (7 days).

valid-lifetime *valid-lifetime*: Sets the valid lifetime in the range of 60 to 4294967295 seconds. The default value is 2592000 seconds (30 days). The valid lifetime must be longer than or equal to the preferred lifetime.

Usage guidelines

Only one prefix pool can be applied to an address pool.

You can apply a prefix pool that has not been created to an address pool. The setting takes effect after the prefix pool is created.

To modify the prefix pool in a DHCPv6 address pool, execute the **undo prefix-pool** command to remove the prefix pool, and then execute the **prefix-pool** command.

Examples

Apply prefix pool 1 to address pool 1, and use the default preferred lifetime and valid lifetime.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] prefix-pool 1
```

Apply prefix pool 2 to address pool 2, and set the preferred lifetime to one day and the valid lifetime to three days.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 2
[Sysname-dhcp6-pool-2] prefix-pool 2 preferred-lifetime 86400 valid-lifetime 259200
```

Related commands

display ipv6 dhcp pool

ipv6 dhcp prefix-pool

reset ipv6 dhcp server conflict

Use **reset ipv6 dhcp server conflict** to clear IPv6 address conflict information.

Syntax

reset ipv6 dhcp server conflict [**address** *ipv6-address*] [**vpn-instance** *vpn-instance-name*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

address *ipv6-address*: Clears conflict information for the specified IPv6 address. If you do not specify an IPv6 address, this command clears all IPv6 address conflict information.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears conflict information about IPv6 addresses for the public network.

Usage guidelines

Address conflicts occur when dynamically assigned IP addresses have been statically configured for other hosts. After the conflicts are resolved, you can use the **reset ipv6 dhcp server conflict** command to clear conflict information so that the conflicted addresses can be assigned to clients.

Examples

Clear all IPv6 address conflict information.

```
<Sysname> reset ipv6 dhcp server conflict
```

Related commands

display ipv6 dhcp server conflict

reset ipv6 dhcp server expired

Use **reset ipv6 dhcp server expired** to clear binding information for lease-expired IPv6 addresses.

Syntax

reset ipv6 dhcp server expired [[**address** *ipv6-address*] [**vpn-instance** *vpn-instance-name*] | **pool** *pool-name*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

address *ipv6-address*: Clears binding information for the specified lease-expired IPv6 address. If you do not specify an IPv6 address, this command clears binding information for all lease-expired IPv6 address.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears binding information about lease-expired IPv6 addresses for the public network.

pool *pool-name*: Clears binding information for lease-expired IPv6 addresses in the address pool specified by its name, a case-insensitive string of 1 to 63 characters. If you do not specify an address pool, this command clears binding information for lease-expired IPv6 addresses in all address pools.

Examples

Clear binding information for expired IPv6 address 2001:f3e0::1.

```
<Sysname> reset ipv6 dhcp server expired address 2001:f3e0::1
```

Related commands

display ipv6 dhcp server expired

reset ipv6 dhcp server ip-in-use

Use **reset ipv6 dhcp server ip-in-use** to clear binding information for assigned IPv6 addresses.

Syntax

reset ipv6 dhcp server ip-in-use [[**address** *ipv6-address*] [**vpn-instance** *vpn-instance-name*] | **pool** *pool-name*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

address *ipv6-address*: Clears binding information for the specified assigned IPv6 address. If you do not specify an IPv6 address, this command clears binding information for all assigned IPv6 addresses.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears binding information about assigned IPv6 addresses for the public network.

pool *pool-name*: Clears binding information for assigned IPv6 addresses in the address pool specified by its name, a case-insensitive string of 1 to 63 characters. If you do not specify an address pool, this command clears binding information for assigned IPv6 addresses in all address pools.

Usage guidelines

If you execute this command to clear information about an assigned static binding, the static binding becomes a free static binding.

Examples

Clear binding information for all assigned IPv6 addresses.

```
<Sysname> reset ipv6 dhcp server ip-in-use
```

Clears binding information for assigned IPv6 addresses in DHCPv6 address pool 1.

```
<Sysname> reset ipv6 dhcp server ip-in-use pool 1
```

Clears binding information for the assigned IPv6 address 2001:0:0:1::1.

```
<Sysname> reset ipv6 dhcp server ip-in-use address 2001:0:0:1::1
```

Related commands

display ipv6 dhcp server ip-in-use

reset ipv6 dhcp server pd-in-use

Use **reset ipv6 dhcp server pd-in-use** to clear binding information for assigned IPv6 prefixes.

Syntax

reset ipv6 dhcp server pd-in-use [**pool** *pool-name* | [**prefix** *prefix/prefix-len*] [**vpn-instance** *vpn-instance-name*]]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

pool *pool-name*: Clears binding information for assigned IPv6 prefixes in the address pool specified by its name, a case-insensitive string of 1 to 63 characters. If you do not specify an address pool, this command clears binding information for assigned IPv6 prefixes in all address pools.

prefix *prefix/prefix-len*: Clears binding information for the specified assigned IPv6 prefix. The value range for the prefix length is 1 to 128. If you do not specify an IPv6 prefix, this command clears binding information for all assigned IPv6 prefixes.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears binding information about assigned IPv6 prefixes for the public network.

Usage guidelines

If you execute this command to clear information about an assigned static binding, the static binding becomes a free static binding.

Examples

Clear binding information for all assigned IPv6 prefixes.

```
<Sysname> reset ipv6 dhcp server pd-in-use
```

Clears binding information for assigned IPv6 prefixes in DHCPv6 address pool 1.

```
<Sysname> reset ipv6 dhcp server pd-in-use pool 1
```

Clears binding information for the assigned IPv6 prefix 2001:0:0:1::/64.

```
<Sysname> reset ipv6 dhcp server pd-in-use prefix 2001:0:0:1::/64
```

Related commands

display ipv6 dhcp server pd-in-use

reset ipv6 dhcp server statistics

Use **reset ipv6 dhcp server statistics** to clear DHCPv6 server statistics.

Syntax

reset ipv6 dhcp server statistics [**vpn-instance** *vpn-instance-name*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears DHCPv6 server statistics for the public network.

Examples

Clear DHCPv6 server statistics.

```
<Sysname> reset ipv6 dhcp server statistics
```

Related commands

display ipv6 dhcp server statistics

sip-server

Use **sip-server** to specify the IPv6 address or domain name of a SIP server in the DHCPv6 address pool.

Use **undo sip-server** to remove a SIP server.

Syntax

sip-server { **address** *ipv6-address* | **domain-name** *domain-name* }

undo sip-server { **address** *ipv6-address* | **domain-name** *domain-name* }

Default

No SIP server address or domain name is specified.

Views

DHCPv6 address pool view

DHCPv6 option group view

Predefined user roles

network-admin

context-admin

Parameters

address *ipv6-address*: Specifies the IPv6 address of a SIP server.

domain-name *domain-name*: Specifies the domain name of a SIP server, a case-insensitive string of 1 to 50 characters.

Usage guidelines

You can specify up to eight SIP server addresses and eight SIP server domain names in an address pool. A SIP server that is specified earlier has a higher preference.

Examples

Specify the SIP server address **2:2::4** in DHCPv6 address pool 1.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] sip-server address 2:2::4
```

Specify the SIP server domain name **bbb.com** in DHCPv6 address pool 1.

```
[Sysname-dhcp6-pool-1] sip-server domain-name bbb.com
```

Related commands

display ipv6 dhcp pool

static-bind

Use **static-bind** to statically bind an IPv6 address or prefix to a client in the DHCPv6 address pool.

Use **undo static-bind** to delete a static binding.

Syntax

static-bind { **address** *ipv6-address*/*addr-prefix-length* | **prefix** *prefix*/*prefix-len* } **duid** *duid* [**iaid** *iaid*] [**preferred-lifetime** *preferred-lifetime* **valid-lifetime** *valid-lifetime*] [**description** *description-text*]

undo static-bind { **address** *ipv6-address*/*addr-prefix-length* | **prefix** *prefix*/*prefix-len* }

Default

No static binding is configured in a DHCPv6 address pool.

Views

DHCPv6 address pool view

Predefined user roles

network-admin

context-admin

Parameters

address *ipv6-address*/*addr-prefix-length*: Specifies the IPv6 address and prefix length. The value range for the prefix length is 1 to 128.

prefix *prefix*/*prefix-len*: Specifies the prefix and prefix length. The value range for the prefix length is 1 to 128.

duid *duid*: Specifies a client DUID. The value is an even hexadecimal number in the range of 2 to 256.

iaid *iaid*: Specifies a client IAID. The value is a hexadecimal number in the range of 0 to FFFFFFFF. If you do not specify an IAID, the server does not match the client IAID for prefix assignment.

preferred-lifetime *preferred-lifetime*: Sets the preferred lifetime of the address or prefix. The value range is 60 to 4294967295 seconds, and the default is 604800 seconds (7 days).

valid-lifetime *valid-lifetime*: Sets the valid lifetime of the address or prefix. The value range is 60 to 4294967295 seconds, and the default is 2592000 seconds (30 days). The valid lifetime cannot be shorter than the preferred lifetime.

description *description-text*: Specifies a description for the static binding, a case-sensitive string of 1 to 255 characters.

Usage guidelines

You can specify multiple static bindings in a DHCPv6 address pool.

An IPv6 address or prefix can be bound to only one DHCPv6 client.

To modify a static binding, execute the **undo static-bind** command to delete the binding, and then execute the **static-bind** command.

Examples

In address pool 1, bind IPv6 address 2001:0410::/35 to the client DUID 0003000100e0fc005552 and IAID A1A1A1A1.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] static-bind address 2001:0410::/35 duid 0003000100e0fc005552 iaid A1A1A1A1
```

In address pool 1, bind prefix 2001:0410::/35 to the client DUID 00030001CA0006A400 and IAID A1A1A1A1.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] static-bind prefix 2001:0410::/35 duid 00030001CA0006A400 iaid A1A1A1A1
```

Related commands

display ipv6 dhcp pool

temporary address range

Use **temporary address range** to configure a temporary IPv6 address range in a DHCPv6 address pool for dynamic allocation.

Use **undo temporary address range** to restore the default.

Syntax

temporary address range *start-ipv6-address end-ipv6-address* [**preferred-lifetime** *preferred-lifetime* **valid-lifetime** *valid-lifetime*]

undo temporary address range

Default

No temporary IPv6 address range is configured in a DHCPv6 address pool.

Views

DHCPv6 address pool view

Predefined user roles

network-admin

context-admin

Parameters

start-ipv6-address: Specifies the start IPv6 address.

end-ipv6-address: Specifies the end IPv6 address.

preferred-lifetime *preferred-lifetime*: Sets the preferred lifetime. The value range is 60 to 4294967295 seconds, and the default is 604800 seconds (7 days).

valid-lifetime *valid-lifetime*: Sets the valid lifetime. The value range is 60 to 4294967295 seconds, and the default is 2592000 seconds (30 days). The valid lifetime cannot be shorter than the preferred lifetime.

Usage guidelines

If you do not execute the **temporary address range** command, the DHCPv6 server does not support temporary address assignment.

You can configure only one temporary IPv6 address range in an address pool. If you execute this command multiple times, the most recent configuration takes effect.

Examples

In DHCPv6 address pool 1, configure a temporary IPv6 address range from 3ffe:501:ffff:100::50 to 3ffe:501:ffff:100::60.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] network 3ffe:501:ffff:100::/64
[Sysname-dhcp6-pool-1] temporary address range 3ffe:501:ffff:100::50
3ffe:501:ffff:100::60
```

Related commands

display ipv6 dhcp pool

address range

network

vpn-instance

Use **vpn-instance** to apply a DHCPv6 address pool to a VPN instance.

Use **undo vpn-instance** to restore the default.

Syntax

vpn-instance *vpn-instance-name*

undo vpn-instance

Default

The DHCPv6 address pool is not applied to any VPN instance.

Views

DHCPv6 address pool view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance-name: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the DHCPv6 address pool belongs to the public network.

Usage guidelines

If a DHCPv6 address pool is applied to a VPN instance, the DHCPv6 server assigns IPv6 addresses in this address pool to clients in the specified VPN instance.

The DHCPv6 server identifies the VPN instance to which a DHCPv6 client belongs according to the following information:

- The client's VPN information stored in authentication modules.
- The VPN information of the DHCPv6 server's interface that receives DHCPv6 packets from the client.

The VPN information from authentication modules takes priority over the VPN information of the receiving interface.

Examples

Apply DHCPv6 address pool 0 to the VPN instance **abc**.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 0
[Sysname-dhcp6-pool-0] vpn-instance abc
```

DHCPv6 relay agent commands

display ipv6 dhcp relay server-address

Use **display ipv6 dhcp relay server-address** to display DHCPv6 server addresses specified on the DHCPv6 relay agent.

Syntax

display ipv6 dhcp relay server-address [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays DHCPv6 server addresses on all interfaces enabled with DHCPv6 relay agent.

Examples

Display DHCPv6 server addresses on all interfaces enabled with DHCPv6 relay agent.

```
<Sysname> display ipv6 dhcp relay server-address
Interface: GigabitEthernet1/0/1
 Server address                              Outgoing Interface
 2::3
 3::4                                        GigabitEthernet1/0/3
```

```
Interface: GigabitEthernet1/0/2
 Server address                              Outgoing Interface
 2::3
 3::4                                        GigabitEthernet1/0/3
```

Display DHCPv6 server addresses on GigabitEthernet 1/0/1.

```
<Sysname> display ipv6 dhcp relay server-address interface gigabitethernet 1/0/1
Interface: GigabitEthernet1/0/1
 Server address                              Outgoing Interface
 2::3
 3::4                                        GigabitEthernet1/0/3
```

Table 11 Command output

Field	Description
Server address	DHCPv6 server address specified on the DHCP relay agent.
Outgoing Interface	Output interface of DHCPv6 packets. If no output interface is specified, the device searches the routing table for the output interface.

Related commands

ipv6 dhcp relay server-address

ipv6 dhcp select

display ipv6 dhcp relay statistics

Use **display ipv6 dhcp relay statistics** to display DHCPv6 packet statistics on the DHCPv6 relay agent.

Syntax

display ipv6 dhcp relay statistics [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays DHCPv6 packets statistics on all interfaces enabled with DHCPv6 relay agent.

Examples

Display DHCPv6 packet statistics on all interfaces enabled with DHCPv6 relay agent.

```
<Sysname> display ipv6 dhcp relay statistics
Packets dropped              :  4
Packets received             :  14
    Solicit                  :  0
```

```
    Request                  :  0
    Confirm                  :  0
    Renew                    :  0
    Rebind                   :  0
    Release                  :  0
    Decline                  :  0
    Information-request      :  7
    Relay-forward            :  0
    Relay-reply              :  7
Packets sent                 :  14
    Advertise                :  0
    Reconfigure              :  0
    Reply                    :  7
    Relay-forward            :  7
    Relay-reply              :  0
```

Display DHCPv6 packet statistics on the DHCPv6 relay agent on GigabitEthernet 1/0/1.

```
<Sysname> display ipv6 dhcp relay statistics interface gigabitethernet 1/0/1
Packets dropped              :  4
Packets received             :  16
    Solicit                  :  0
    Request                  :  0
    Confirm                  :  0
    Renew                    :  0
    Rebind                   :  0
    Release                  :  0
    Decline                  :  0
    Information-request      :  8
    Relay-forward            :  0
    Relay-reply              :  8
Packets sent                 :  16
    Advertise                :  0
    Reconfigure              :  0
    Reply                    :  8
    Relay-forward            :  8
    Relay-reply              :  0
```

Table 12 Command output

Field	Description
Packets dropped	Number of discarded packets.
Packets received	Number of received packets.
Solicit	Number of received solicit packets.
Request	Number of received request packets.
Confirm	Number of received confirm packets.
Renew	Number of received renew packets.
Rebind	Number of received rebind packets.
Release	Number of received release packets.

Field	Description
Decline	Number of received decline packets.
Information-request	Number of received information request packets.
Relay-forward	Number of received relay-forward packets.
Relay-reply	Number of received relay-reply packets.
Packets sent	Number of sent packets.
Advertise	Number of sent advertise packets.
Reconfigure	Number of sent reconfigure packets.
Reply	Number of sent reply packets.
Relay-forward	Number of sent Relay-forward packets.
Relay-reply	Number of sent Relay-reply packets.

Related commands

reset ipv6 dhcp relay statistics

gateway-list

Use **gateway-list** to specify gateway addresses for DHCPv6 clients in a DHCPv6 address pool.

Use **undo gateway-list** to remove gateway addresses from a DHCPv6 address pool.

Syntax

gateway-list *ipv6-address*&<1-8>

undo gateway-list [*ipv6-address*&<1-8>]

Default

No gateway address is specified in a DHCPv6 address pool.

Views

DHCPv6 address pool view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address&<1-8>: Specifies a space-separated list of up to eight addresses.

Usage guidelines

DHCPv6 clients of the same access type can be classified into different types by their locations. In this case, the relay interface typically has no IPv6 address configured. You can use the **gateway-list** command to specify gateway addresses for clients matching the same DHCPv6 address pool.

Upon receiving a DHCPv6 Solicit or Request from a client that matches a DHCPv6 address pool, the relay agent processes the packet as follows:

- Fills the **link-address** field of the packet with a specified gateway address.
- Forwards the packet to all DHCPv6 servers in the matching DHCPv6 address pool.

The DHCPv6 servers select a DHCPv6 address pool according to the gateway address.

Examples

Specify the gateway address 10::1 in the DHCPv6 address pool **p1**.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool p1
[Sysname-dhcp6-pool-p1] gateway-list 10::1
```

ipv6 dhcp relay gateway

Use **ipv6 dhcp relay gateway** to specify a gateway address for DHCPv6 clients on the DHCPv6 relay interface.

Use **undo ipv6 dhcp relay gateway** to restore the default.

Syntax

ipv6 dhcp relay gateway *ipv6-address*

undo ipv6 dhcp relay gateway

Default

The first IPv6 address of the relay interface is used as the gateway address for DHCPv6 clients.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address: Specifies a gateway address. The IPv6 address must be an IPv6 address of the relay interface.

Usage guidelines

The DHCPv6 relay agent uses the specified IPv6 address instead of the first IPv6 address of the relay interface as the gateway address for DHCPv6 clients.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify 10::1 as the gateway address for DHCPv6 clients on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp relay gateway 10::1
```

Related commands

gateway-list

ipv6 dhcp relay interface-id

Use **ipv6 dhcp relay interface-id** to specify a padding mode for the Interface-ID option.

Use **undo ipv6 dhcp relay interface-id** to restore the default.

Syntax

ipv6 dhcp relay interface-id { **bas** | **interface** }

undo ipv6 dhcp relay interface-id

Default

The DHCPv6 relay agent fills the Interface-ID option with the interface index of the interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

bas: Specifies the BAS mode.

interface: Specifies the interface name mode. This mode pads the Interface-ID option in ASCII code with the interface name and VLAN ID of the interface.

Usage guidelines

Enable the DHCPv6 relay agent on the interface before executing this command. Otherwise, the command does not take effect.

Examples

Specify the BAS mode as the padding mode for the Interface-ID option on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp relay interface-id bas
```

Specify the interface name mode as the padding mode for the Interface-ID option on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp relay interface-id interface
```

ipv6 dhcp relay server-address

Use **ipv6 dhcp relay server-address** to specify a DHCPv6 server on the DHCPv6 relay agent.

Use **undo ipv6 dhcp relay server-address** to remove DHCPv6 server addresses.

Syntax

ipv6 dhcp relay server-address *ipv6-address* [**interface** *interface-type interface-number*]

undo ipv6 dhcp relay server-address [*ipv6-address* [**interface** *interface-type interface-number*]]

Default

No DHCPv6 server address is specified on the DHCPv6 relay agent.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address: Specifies the IPv6 address of a DHCPv6 server.

interface *interface-type interface-number*: Specifies an output interface through which the relay agent forwards the DHCPv6 requests to the DHCPv6 server. If you do not specify an output interface, the relay agent looks up the routing table for an output interface.

Usage guidelines

Upon receiving a request from a DHCPv6 client, the interface encapsulates the request into a Relay-forward message and forwards the message to the specified DHCPv6 server.

You can specify a maximum of eight DHCPv6 servers on an interface. The DHCPv6 relay agent forwards DHCP requests to all the specified DHCPv6 servers.

If the DHCPv6 server address is a link-local address or multicast address, you must specify an output interface. If you do not specify an output interface, DHCPv6 packets might fail to reach the DHCPv6 server.

If you do not specify an IPv6 address, the **undo ipv6 dhcp relay server-address** command removes all DHCPv6 server addresses specified on the interface.

Do not enable the DHCPv6 client and the DHCPv6 relay agent on the same interface.

Examples

Enable the DHCPv6 relay agent on GigabitEthernet 1/0/1 and specify the DHCPv6 server address 2001:1::3.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp select relay
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp relay server-address 2001:1::3
```

Related commands

display ipv6 dhcp relay server-address

ipv6 dhcp select

remote-server

Use **remote-server** to specify DHCPv6 servers for a DHCPv6 address pool.

Use **undo remote-server** to remove DHCPv6 servers from a DHCPv6 address pool.

Syntax

remote-server *ipv6-address* [**interface** *interface-type interface-number*]

undo remote-server [*ipv6-address* [**interface** *interface-type interface-number*]]

Default

No DHCPv6 server is specified for the DHCPv6 address pool.

Views

DHCPv6 address pool view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address: Specifies a DHCPv6 server address.

interface *interface-type interface-number*: Specifies the outgoing interface by its type and number for the DHCPv6 relay agent to forward packets to the DHCPv6 server. If you do not specify an outgoing interface, the DHCPv6 relay agent performs a routing table lookup.

Usage guidelines

You can specify a maximum of eight DHCPv6 servers in one DHCPv6 address pool.

If you do not specify any parameters, the **undo remote-server** command removes all DHCPv6 servers in the DHCPv6 address pool.

If a DHCPv6 server address is a link-local address, you must specify an outgoing interface by using the **interface** keyword in this command. If you do not specify an outgoing interface, DHCPv6 packets might fail to reach the DHCPv6 server.

Examples

Specify DHCPv6 server 10::1 for DHCPv6 address pool 0.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 0
[Sysname-dhcp6-pool-0] remote-server 10::1
```

reset ipv6 dhcp relay statistics

Use **reset ipv6 dhcp relay statistics** to clear packets statistics on the DHCPv6 relay agent.

Syntax

reset ipv6 dhcp relay statistics [**interface** *interface-type interface-number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command clears all relay agent statistics.

Examples

Clear packet statistics on the DHCPv6 relay agent.

```
<Sysname> reset ipv6 dhcp relay statistics
```

Related commands

display ipv6 dhcp relay statistics

DHCPv6 client commands

display ipv6 dhcp client

Use **display ipv6 dhcp client** to display DHCPv6 client information.

Syntax

display ipv6 dhcp client [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays information about all DHCPv6 clients.

Examples

Display the DHCPv6 client information on GigabitEthernet 1/0/1.

```
<Sysname> display ipv6 dhcp client interface gigabitethernet 1/0/1
GigabitEthernet1/0/1:
  Type: Stateful client requesting address and prefix
    State: OPEN
    Client DUID: 0003000100e002000000
    Preferred server
      Reachable via address: FE80::2E0:1FF:FE00:18
      Server DUID: 0003000100e001000000
    IA_NA: IAID 0x00000642, T1 50 sec, T2 80 sec
      Address: 1:1::2/128
        Preferred lifetime 100 sec, valid lifetime 200 sec
        Will expire on Feb 4 2014 at 15:37:20(288 seconds left)
    IA_PD: IAID 0x00000642, T1 50 sec, T2 80 sec
      Prefix: 12:34::/48
        Preferred lifetime 100 sec, valid lifetime 200 sec
        Will expire on Mar 27 2014 at 08:13:24 (199 seconds left)
    DNS server addresses:
      2:2::3
    Domain name:
      aaa.com
    SIP server addresses:
      2:2::4
    SIP server domain names:
      bbb.com
```

```
Options:
  Code: 88
    Length: 3 bytes
    Hex: AABBCC
```

Table 13 Command output

Field	Description
Type	Types of DHCPv6 client: • **Stateful client requesting address**—A DHCPv6 client that requests an IPv6 address. • **Stateful client requesting prefix**—A DHCPv6 client that requests an IPv6 prefix. • **Stateful client requesting address and prefix**—A DHCPv6 client that requests an IPv6 address and prefix. • **Stateless client**—A DHCPv6 client that requests configuration parameters other than an IPv6 address and prefix through stateless DHCPv6.
State	Current state of the DHCPv6 client: • **IDLE**—The client is in idle state. • **SOLICIT**—The client is locating a DHCPv6 server. • **REQUEST**—The client is requesting an IPv6 address or prefix. • **OPEN**—The client has obtained an IPv6 address or prefix. • **RENEW**—The client is extending the lease (after T1 and before T2). • **REBIND**—The client is extending the lease (after T2 and before the lease expires). • **RELEASE**—The client is releasing an IPv6 address or prefix. • **DECLINE**—The client is declining an IPv6 address or prefix because of an address or prefix conflict. • **INFO-REQUESTING**—The client is requesting configuration parameters through stateless DHCPv6.
Client DUID	DUID of the DHCPv6 client.
Preferred server	Information about the DHCPv6 server selected by the DHCPv6 client.
Reachable via address	Reachable address for the DHCPv6 client. It is the link local address of the DHCPv6 server or DHCPv6 relay agent.
Server DUID	DUID of the DHCPv6 server.
IA_NA	IA_NA information.
IA_PD	IA_PD information.
IAID	IA identifier.
T1	T1 value in seconds.
T2	T2 value in seconds.
Address	IPv6 address obtained. This field is displayed only when the DHCPv6 client type is **Stateful client requesting address**.
Prefix	IPv6 prefix obtained. This field is displayed only when the DHCPv6 client type is **Stateful client requesting prefix**.
Preferred lifetime	Preferred lifetime in seconds.
valid lifetime	Valid lifetime in seconds.

Field	Description
Will expire on Feb 4 2014 at 15:37:20 (288 seconds left)	Time when the lease expires and the remaining time of the lease. If the lease expires after the year 2100, this field displays **Will expire after 2100**.
DNS server addresses	IPv6 address of the DNS server.
Domain name	Domain name suffix.
SIP server addresses	IPv6 address of the SIP server.
SIP server domain names	Domain name of the SIP server.
Options	Self-defined options.
Code	Code of the self-defined option.
Length	Self-defined option length in bytes.
Hex	Self-defined option content represented by a hexadecimal number.

Related commands

ipv6 address dhcp-alloc

ipv6 dhcp client duid

ipv6 dhcp client pd

display ipv6 dhcp client statistics

Use **display ipv6 dhcp client statistics** to display DHCPv6 client statistics.

Syntax

display ipv6 dhcp client statistics [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays statistics for all DHCPv6 clients.

Examples

Display DHCPv6 client statistics on GigabitEthernet 1/0/1.

```
<Sysname> display ipv6 dhcp client statistics interface gigabitethernet 1/0/1
Interface                    :  GigabitEthernet1/0/1
Packets received             :  1
        Reply                :  1
        Advertise            :  0
```

```
         Reconfigure         :   0
         Invalid             :  0
Packets sent                 :  5
         Solicit             :  0
         Request             :  0
         Renew               :  0
         Rebind              :  0
         Information-request  :  5
         Release             :  0
         Decline             :  0
```

Table 14 Command output

Field	Description
Interface	Interface that acts as the DHCPv6 client.
Packets Received	Number of received packets.
Reply	Number of received reply packets.
Advertise	Number of received advertise packets.
Reconfigure	Number of received reconfigure packets.
Invalid	Number of invalid packets.
Packets sent	Number of sent packets.
Solicit	Number of sent solicit packets.
Request	Number of sent request packets.
Renew	Number of sent renew packets.
Rebind	Number of sent rebind packets.
Information-request	Number of sent information request packets.
Release	Number of sent release packets.
Decline	Number of sent decline packets.

Related commands

`reset ipv6 dhcp client statistics`

ipv6 address dhcp-alloc

Use **`ipv6 address dhcp-alloc`** to configure an interface to use DHCPv6 for IPv6 address acquisition.

Use **`undo ipv6 address dhcp-alloc`** to cancel an interface from using DHCPv6, and clear the obtained IPv6 address and other configuration parameters.

Syntax

`ipv6 address dhcp-alloc` [**`option-group`** *`option-group-number`* | **`rapid-commit`**] *

`undo ipv6 address dhcp-alloc`

Default

An interface does not use DHCPv6 for IPv6 address acquisition.

Views

Layer 3 Ethernet interface view

Layer 3 Ethernet subinterface view

Layer 3 aggregate interface view

Layer 3 aggregate subinterface view

VLAN interface view

Reth interface view

Reth subinterface view

Predefined user roles

network-admin

context-admin

Parameters

option-group *option-group-number*: Enables the DHCPv6 client to create a dynamic DHCPv6 option group for saving the configuration parameters, and assigns an ID to the option group. The value range for the ID is 1 to 100. If you do not specify this option, the DHCPv6 client does not create any dynamic DHCPv6 option groups.

rapid-commit: Supports rapid address or prefix assignment.

Examples

Configure GigabitEthernet 1/0/1 to use DHCPv6 for IPv6 address acquisition. Configure the DHCPv6 client to support rapid address assignment and create dynamic DHCPv6 option group 1 for the configuration parameters obtained.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 address dhcp-alloc rapid-commit option-group 1
```

Related commands

display ipv6 dhcp client

ipv6 dhcp client dscp

Use **ipv6 dhcp client dscp** to set the DSCP value for DHCPv6 packets sent by the DHCPv6 client.

Use **undo ipv6 dhcp client dscp** to restore the default.

Syntax

ipv6 dhcp client dscp *dscp-value*

undo ipv6 dhcp client dscp

Default

The DSCP value in DHCPv6 packets is 56.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

dscp-value: Sets the DSCP value for DHCP packets, in the range of 0 to 63.

Usage guidelines

The DSCP value is carried in the Traffic class field of a DHCPv6 packet. It specifies the priority level of the packet and affects the transmission priority of the packet. A bigger DSCP value represents a higher priority.

Examples

Set the DSCP value to 30 for DHCPv6 packets sent by the DHCPv6 client.

```
<Sysname> system-view
[Sysname] ipv6 dhcp client dscp 30
```

ipv6 dhcp client duid

Use **ipv6 dhcp client duid** to configure the DHCPv6 client DUID for an interface.

Use **undo ipv6 dhcp client duid** to restore the default.

Syntax

ipv6 dhcp client duid { **ascii** *ascii-string* | **hex** *hex-string* | **mac** *interface-type interface-number* }

undo ipv6 dhcp client duid

Default

The interface uses the device bridge MAC address to generate its DHCPv6 client DUID.

Views

Layer 3 Ethernet interface view

Layer 3 Ethernet subinterface view

Layer 3 aggregate interface view

Layer 3 aggregate subinterface view

VLAN interface view

Reth interface view

Reth subinterface view

Predefined user roles

network-admin

context-admin

Parameters

ascii *ascii-string*: Specifies a case-sensitive ASCII string of 1 to 130 characters as the DHCPv6 client DUID.

hex *hex-string*: Specifies a hexadecimal number of 2 to 260 characters as the DHCPv6 client DUID.

mac *interface-type interface-number*: Specifies the MAC address of the specified interface as the DHCPv6 client DUID. The *interface-type interface-number* arguments specify an interface by its type and number.

Usage guidelines

A DHCPv6 client pads its DUID into the Option 1 of the DHCPv6 packet that it sends to the DHCPv6 server. The DHCPv6 server can assign specific IPv6 addresses or prefixes to DHCPv6 clients with specific DUIDs.

The DUID of a DHCPv6 client is the globally unique identifier of the client, so make sure the DUID that you configure is unique.

Examples

Specify the MAC address of GigabitEthernet 1/0/2 as the DHCPv6 client DUID for GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp client duid mac gigabitethernet 1/0/2
```

Related commands

display ipv6 dhcp client

ipv6 dhcp client pd

Use **ipv6 dhcp client pd** to configure an interface to use DHCPv6 for IPv6 prefix acquisition.

Use **undo ipv6 dhcp client pd** to cancel an interface from using DHCPv6, and clear the obtained IPv6 prefix and other configuration parameters.

Syntax

ipv6 dhcp client pd *prefix-number* [**option-group** *option-group-number* | **rapid-commit**]*

undo ipv6 dhcp client pd

Default

An interface does not use DHCPv6 for IPv6 prefix acquisition.

Views

Layer 3 Ethernet interface view

Layer 3 Ethernet subinterface view

Layer 3 aggregate interface view

Layer 3 aggregate subinterface view

VLAN interface view

Reth interface view

Reth subinterface view

Predefined user roles

network-admin

context-admin

Parameters

prefix-number: Specifies an IPv6 prefix ID in the range of 1 to 1024. After obtaining an IPv6 prefix, the client assigns the ID to the IPv6 prefix.

rapid-commit: Supports rapid address or prefix assignment.

option-group *option-group-number*: Enables the DHCPv6 client to create a dynamic DHCPv6 option group for saving the configuration parameters, and assigns an ID to the option group. The value range for the ID is 1 to 100. If you do not specify this option, the DHCPv6 client does not create any dynamic DHCPv6 option groups.

Examples

Configure GigabitEthernet 1/0/1 to use DHCPv6 for IPv6 prefix acquisition. Specify IDs for the dynamic IPv6 prefix and dynamic DHCPv6 option group, and configure the client to support rapid prefix assignment.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp client pd 1 rapid-commit option-group 1
```

Related commands

display ipv6 dhcp client

ipv6 dhcp client stateful

Use **ipv6 dhcp client stateful** to configure an interface to use DHCPv6 for IPv6 address and prefix acquisition.

Use **undo ipv6 dhcp client stateful** to cancel an interface from using DHCPv6, and clear the obtained IPv6 address, prefix, and other configuration parameters.

Syntax

ipv6 dhcp client stateful prefix *prefix-number* [**option-group** *option-group-number* | **rapid-commit**] *

undo ipv6 dhcp client stateful

Default

An interface does not use DHCPv6 for IPv6 address and prefix acquisition.

Views

Layer 3 Ethernet interface view

Layer 3 Ethernet subinterface view

Layer 3 aggregate interface view

Layer 3 aggregate subinterface view

VLAN interface view

Reth interface view

Reth subinterface view

Predefined user roles

network-admin

context-admin

Parameters

prefix *prefix-number*: Specifies an IPv6 prefix ID in the range of 1 to 1024. After obtaining an IPv6 prefix, the client assigns the ID to the IPv6 prefix.

rapid-commit: Supports rapid address and prefix assignment.

option-group *option-group-number*: Enables the DHCPv6 client to create a dynamic DHCPv6 option group for saving the configuration parameters, and assigns an ID to the option group.

The value range for the ID is 1 to 100. If you do not specify this option, the DHCPv6 client does not create any dynamic DHCPv6 option groups.

Usage guidelines

The **ipv6 dhcp client stateful** command takes effect if it is configured with the **ipv6 address dhcp-alloc** and **ipv6 dhcp client pd** commands on an interface. You must execute the **undo ipv6 dhcp client stateful** command to have the **ipv6 address dhcp-alloc** and **ipv6 dhcp client pd** commands take effect.

Examples

Configure GigabitEthernet 1/0/1 to use DHCPv6 for IPv6 address and prefix acquisition. Specify IDs for the dynamic IPv6 prefix and dynamic DHCPv6 option group, and configure the client to support rapid address and prefix assignment.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp client stateful prefix 1 rapid-commit
option-group 1
```

Related commands

ipv6 address dhcp-alloc

ipv6 dhcp client pd

ipv6 dhcp client stateless enable

Use **ipv6 dhcp client stateless enable** to enable stateless DHCPv6.

Use **undo ipv6 dhcp client stateless enable** to disable stateless DHCPv6.

Syntax

ipv6 dhcp client stateless enable

undo ipv6 dhcp client stateless enable

Default

Stateless DHCPv6 is disabled.

Views

Layer 3 Ethernet interface view

Layer 3 Ethernet subinterface view

Layer 3 aggregate interface view

Layer 3 aggregate subinterface view

VLAN interface view

Reth interface view

Reth subinterface view

Predefined user roles

network-admin

context-admin

Usage guidelines

Stateless DHCPv6 enables the interface to send an Information-request message to the multicast address of all DHCPv6 servers and DHCPv6 relay agents for configuration parameters.

Examples

Enable stateless DHCPv6 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp client stateless enable
```

reset ipv6 dhcp client statistics

Use **reset ipv6 dhcp client statistics** to clear DHCPv6 client statistics.

Syntax

reset ipv6 dhcp client statistics [**interface** *interface-type interface-number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command clears all DHCPv6 client statistics.

Examples

Clear all DHCPv6 client statistics.

```
<Sysname> reset ipv6 dhcp client statistics
```

Related commands

display ipv6 dhcp client statistics

Contents

DNS commands

display dns domain

Use **display dns domain** to display the domain name suffixes.

Syntax

display dns domain [**dynamic**] [**vpn-instance** *vpn-instance-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

dynamic: Displays the domain name suffixes dynamically obtained through DHCP or other protocols. If you do not specify this keyword, the command displays the statically configured and dynamically obtained domain name suffixes.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays domain name suffixes for the public network.

Examples

Display the statically configured and dynamically obtained domain name suffixes for the public network.

```
<Sysname> display dns domain
Type:
  D: Dynamic    S: Static

No.    Type   Domain suffix
1      S      com
2      D      net
```

Table 1 Command output

Field	Description
No.	Sequence number.
Type	Domain name suffix type: • **S**—A statically configured domain name suffix. • **D**—A domain name suffix dynamically obtained through DHCP or other protocols.
Domain suffix	Domain name suffixes.

Related commands

dns domain

display dns host

Use **display dns host** to display information about domain name-to-IP address mappings.

Syntax

display dns host [**ip** | **ipv6**] [**vpn-instance** *vpn-instance-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ip: Specifies type A queries. A type A query resolves a domain name to the mapped IPv4 address.

ipv6: Specifies type AAAA queries. A type AAAA query resolves a domain name to the mapped IPv6 address.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays domain name-to-IP address mappings for the public network.

Usage guidelines

If you do not specify the **ip** or **ipv6** keyword, this command displays domain name-to-IP address mappings of all query types.

Examples

Display domain name-to-IP address mappings of all query types.

```
<Sysname> display dns host
Type:
  D: Dynamic    S: Static

Total number: 3
No.  Host name         Type  TTL        Query type   IP addresses
1    sample.com        D     3132       A            192.168.10.1
                                                     192.168.10.2
                                                     192.168.10.3
2    zig.sample.com    S     -          A            192.168.1.1
3    sample.net        S     -          AAAA         FE80::4904:4448
```

Table 2 Command output

Field	Description
No.	Sequence number.
Host name	Domain name.
Type	Domain name-to-IP address mapping type: • **S**—A static mapping configured by the **ip host** or **ipv6 host** command.

Field	Description
	• **D**—A mapping dynamically obtained through dynamic domain name resolution.
TTL	Time in seconds that a mapping can be stored in the cache. For a static mapping, a hyphen (-) is displayed.
Query type	Query type: A and AAAA.
IP addresses	Replied IP address: • For a type A query, the replied IP address is an IPv4 address. • For a type AAAA query, the replied IP address is an IPv6 address.

Related commands

ip host

ipv6 host

reset dns host

display dns server

Use **display dns server** to display IPv4 DNS server information.

Syntax

display dns server [**dynamic**] [**vpn-instance** *vpn-instance-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

dynamic: Displays IPv4 DNS server information dynamically obtained through DHCP or other protocols. If you do not specify this keyword, the command displays statically configured and dynamically obtained IPv4 DNS server information.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays IPv4 DNS server information for the public network.

Examples

Display IPv4 DNS server information for the public network.

```
<Sysname> display dns server
Type:
  D: Dynamic    S: Static

No. Type  IP address
1   S     202.114.0.124
2   S     169.254.65.125
```

Table 3 Command output

Field	Description
No.	Sequence number.
Type	DNS server type: • **S**—A manually configured DNS server. • **D**—DNS server information dynamically obtained through DHCP or other protocols.
IP address	IPv4 address of the DNS server.

Related commands

dns server

display ipv6 dns server

Use **display ipv6 dns server** to display IPv6 DNS server information.

Syntax

display ipv6 dns server [**dynamic**] [**vpn-instance** *vpn-instance-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

dynamic: Displays IPv6 DNS server information dynamically obtained through DHCP or other protocols. If you do not specify this keyword, the command displays the statically configured and dynamically obtained IPv6 DNS server information.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays IPv6 DNS server information for the public network.

Examples

Display IPv6 DNS server information for the public network.

```
<Sysname> display ipv6 dns server
Type:
  D: Dynamic    S: Static

No. Type  IPv6 address                            Outgoing Interface
1   S     2::2
```

Table 4 Command output

Field	Description
No.	Sequence number.

Field	Description
Type	DNS server type: • **S**—A manually configured DNS server. • **D**—DNS server information dynamically obtained through DHCP or other protocols.
IPv6 address	IPv6 address of the DNS server.
Outgoing Interface	Output interface.

Related commands

ipv6 dns server

dns cache ttl

Use **dns cache ttl** to set the TTL value for DNS entries.

Use **undo dns cache ttl** to cancel the TTL configuration for DNS entries.

Syntax

dns cache ttl { **maximum** *max-value* | **minimum** *min-value* } *

undo dns cache ttl { **maximum** | **minimum** }

Default

The TTL value for DNS entries is the TTL value in the DNS reply.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

maximum *max-value*: Specifies the maximum TTL value for DNS entries, in the range of 60 to 3600 seconds.

minimum *min-value*: Specifies the minimum TTL value for DNS entries, in the range of 60 to 3600 seconds. The value for the *min-value* argument must be smaller than that for the *max-value* argument.

Usage guidelines

The device periodically sends a DNS request to the DNS server according to the TTL for DNS entries, which consumes CPU resources. If the TTL value is too small, the device sends DNS requests frequently to the DNS server, which consumes more CPU resources. If the TTL value is too large, DNS mappings cannot be updated in time. To avoid such issues, you can use this command to set the TTL value for DNS entries.

By default, the DNS client obtains the TTL for the following DNS entries from the DNS reply:

- DNS entries generated from DNS transparent proxy.
- DNS entries generated from DNS snooping.
- Dynamic domain name resolution cache generated from the DNS server/DNS server group.

After you set the TTL value for DNS entries, the device specifies the TTL for DNS entries as follows:

- If the TTL value in the DNS reply is smaller than the minimum TTL value, the device uses the minimum TTL value as the TTL for DNS entries. Otherwise, the device uses the TTL value in the DNS reply as the TTL for DNS entries.
- If the TTL value in the DNS reply is larger than the maximum TTL value, the device uses the maximum TTL value as the TTL for DNS entries. Otherwise, the device uses the TTL value in the DNS reply as the TTL for DNS entries.

After you execute this command, the configuration only takes effect on the subsequent DNS entries generated from DNS transparent proxy, DNS snooping, and DNS server/DNS server group.

After you execute the **undo dns cache ttl** command, the current TTL for the existing DNS entries still works.

If you execute the **dns cache ttl minimum**, **dns cache ttl maximum**, or **dns cache ttl minimum maximum** command multiple times, the most recent configuration takes effect.

Examples

Set the minimum TTL value for DNS entries to 180 seconds and the maximum TTL value for DNS entries to 3600 seconds.

```
<Sysname> system-view
[Sysname] dns cache ttl maximum 3600 minimum 180
```

Related commands

dns server
dns snooping enable
dns transparent-proxy enable

dns domain

Use **dns domain** to configure a domain name suffix.

Use **undo dns domain** to delete the specified domain name suffix.

Syntax

dns domain *domain-name* [**vpn-instance** *vpn-instance-name*]

undo dns domain *domain-name* [**vpn-instance** *vpn-instance-name*]

Default

No domain name suffix is configured. Only the provided domain name is resolved.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

domain-name: Specifies a domain name suffix. It is a dot-separated, case-insensitive string that can include letters, digits, hyphens (-), underscores (_), and dots (.), for example, aabbcc.com. The domain name suffix can include a maximum of 253 characters, and each separated string includes no more than 63 characters.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. To configure a domain name suffix for the public network, do not specify this option.

Usage guidelines

For domain name resolution, the resolver automatically uses the suffix list to supply the missing part of an incomplete name entered by a user.

A domain name suffix applies to both IPv4 DNS and IPv6 DNS.

The system allows a maximum of 16 domain name suffixes for the public network or each VPN instance. You can specify domain name suffixes for both public network and VPN instances.

Examples

Configure domain name suffix **com** for the public network.

```
<Sysname> system-view
[Sysname] dns domain com
```

Related commands

display dns domain

dns dscp

Use **dns dscp** to set the DSCP value for DNS packets sent by a DNS client or DNS proxy.

Use **undo dns dscp** to restore the default.

Syntax

dns dscp *dscp-value*

undo dns dscp

Default

The DSCP value is 0 in DNS packets sent by a DNS client or DNS proxy.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

dscp-value: Specifies the DSCP value in the range of 0 to 63.

Usage guidelines

The DSCP value of a packet specifies the priority level of the packet and affects the transmission priority of the packet. A bigger DSCP value represents a higher priority.

Examples

Set the DSCP value to 30 for outgoing DNS packets.

```
<Sysname> system-view
[Sysname] dns dscp 30
```

dns filter

Use **dns filter** to enable DNS filtering and add a host name to the denylist or allowlist.

Use **undo dns filter** to disable DNS filtering and delete a host name from the denylist or allowlist.

Syntax

dns filter { **allowlist** | **denylist** } *hostname*

undo dns filter { **allowlist** | **denylist** } *hostname*

Default

DNS filtering is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

allowlist: Adds a host name to the allowlist.

denylist: Adds a host name to the denylist.

hostname: Specifies a host name, a case-insensitive string of 1 to 253 characters. The string can contain letters, digits, hyphens (-), underscores (_), and dots (.). This argument supports fuzzy match by adding the character (*) to the start or end of the string. For example, to match a host name including **abc**, specify the *hostname* argument as **abc**, **abc*, or *abc**. To exactly match a host name, do not add the character (*).

Usage guidelines

The DNS proxy uses DNS filtering to filter DNS requests as follows:

- If the allowlist has a matching host name or the denylist has no matching host name with the domain name in the received DNS request, the DNS proxy filters in the request. After receiving a DNS reply, the DNS proxy records the DNS mapping and forwards the reply to the DNS client.
- If the denylist has a matching host name or the allowlist has no matching host name with the domain name in the received DNS request, the DNS proxy discards the DNS request.

To implement a strict access control, use an allowlist to filter DNS requests. To implement a loose access control, use a denylist to filter DNS requests.

To add multiple host names to the allowlist or denylist, repeat this command. However, a host name cannot be added to both the denylist and allowlist.

Examples

Enable DNS filtering and add the host names with **.abc** to the allowlist.

```
<Sysname> system-view
[Sysname] dns filter allowlist *.abc
```

dns proxy enable

Use **dns proxy enable** to enable DNS proxy.

Use **undo dns proxy enable** to disable DNS proxy.

Syntax

dns proxy enable

undo dns proxy enable

Default

DNS proxy is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This configuration applies to both IPv4 DNS and IPv6 DNS.

Examples

Enable DNS proxy.

```
<Sysname> system-view
[Sysname] dns proxy enable
```

dns server

Use **dns server** to specify the IPv4 address of a DNS server.

Use **undo dns server** to remove the IPv4 address of a DNS server.

Syntax

dns server *ip-address* [**vpn-instance** *vpn-instance-name*]

undo dns server [*ip-address*] [**vpn-instance** *vpn-instance-name*]

Default

No DNS server IPv4 address is specified.

Views

System view

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the IPv4 address of a DNS server. When you execute the **undo** form of the command in interface view, you must specify this argument.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. To specify a DNS server IPv4 address for the public network, do not use this option.

Usage guidelines

The device sends a DNS query request to the DNS servers in the order their IPv4 addresses are specified.

The system allows a maximum of six DNS server IPv4 addresses for the public network or each VPN instance. You can specify DNS server IPv4 addresses for both public network and VPN instances.

If you do not specify an IPv4 address, the **undo dns server** command removes all DNS server IPv4 addresses for the public network or the specified VPN instance.

Examples

Specify DNS server IPv4 address 172.16.1.1.

```
<Sysname> system-view
[Sysname] dns server 172.16.1.1
```

Specify DNS server IPv4 address 172.16.1.1 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dns server 172.16.1.1
```

Related commands

display dns server

dns snooping enable

Use **dns snooping enable** to enable DNS snooping.

Use **undo dns snooping enable** to disable DNS snooping.

Syntax

dns snooping enable

undo dns snooping enable

Default

DNS snooping is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

DNS snooping is applicable to the scenario where traffic filtering is based on domain names. To filter traffic based on domain names, the DNS mapping is required. The device enabled with DNS snooping monitors received DNS requests and replies. If the domain name in a DNS request matches a filtering rule, the device records the DNS mapping after receiving a DNS reply and reports the mapping to the rule for traffic filtering. If the domain name does not match a filtering rule, the device does not record the DNS mapping.

DNS snooping only works between the DNS client and DNS server, or the DNS client and DNS proxy.

The DNS snooping and DNS transparent proxy features cannot be both configured.

The DNS snooping feature is not VPN-aware. The input interface and output interface of DNS packets must belong to the same VPN.

Examples

Enable DNS snooping.

```
<Sysname> system-view
[Sysname] dns snooping enable
```

Related commands

dns transparent-proxy enable

dns snooping log enable

Use **dns snooping log enable** to enable DNS snooping logging.

Use **undo dns snooping log enable** to disable DNS snooping logging.

Syntax

dns snooping log enable

undo dns snooping log enable

Default

DNS snooping logging is enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

The DNS proxy searches the static domain name resolution table and dynamic domain name resolution cache after receiving a request.

- If the requested information is found, the DNS proxy returns a DNS reply to the client.
- If the requested information is not found, the DNS proxy sends the request to the designated DNS server.

Too many requests received at the same time will increase network load and affect the performance of the DNS proxy and DNS server.

To avoid this issue, you can have DNS snooping work between the DNS client and DNS proxy, or the DNS client and DNS server. The DNS snooping logging feature enables the DNS snooping device to generate DNS snooping logs and send them to the fast log module. The administrator can locate and troubleshoot issues based on the logs. For information about the fast log output configuration, see *Network Management and Monitoring Configuration Guide*.

Examples

Enable DNS snooping logging.

```
<Sysname> system-view
[Sysname] dns snooping log enable
```

dns snooping rate-limit

Use **dns snooping rate-limit** to configure a rate limit of incoming DNS packets on interfaces.

Use **undo dns snooping rate-limit** to disable DNS snooping packet rate limit.

Syntax

dns snooping rate-limit *rate*

undo dns snooping rate-limit

Default

The rate of incoming DNS packets is not limited.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

rate: Specifies the maximum rate in pps. The value range for this argument is 64 to 512

Usage guidelines

An interface will discard DNS packets exceeding the specified rate limit.

This command takes effect only when the DNS transparent proxy or DNS snooping logging feature is enabled.

Examples

Set the DNS packet rate limit to 64 pps.

```
<Sysname> system-view
[Sysname] dns snooping rate-limit 64
```

Related commands

dns snooping log enable

dns transparent-proxy enable

dns source-interface

Use **dns source-interface** to specify the source interface for DNS packets.

Use **undo dns source-interface** to restore the default.

Syntax

dns source-interface *interface-type interface-number* [**vpn-instance** *vpn-instance-name*]

undo dns source-interface *interface-type interface-number* [**vpn-instance** *vpn-instance-name*]

Default

No source interface is specified for DNS packets. The device uses the primary IP address of the output interface of the matching route as the source IP address for a DNS request.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. To specify a source interface for the public network, do not use this option.

Usage guidelines

This configuration applies to both IPv4 and IPv6.

In IPv4 DNS, the device uses the primary IPv4 address of the specified source interface as the source IP address of a DNS query. In IPv6 DNS, the device selects an IPv6 address of the specified source interface as the source IP address of a DNS query. The method of selecting the IPv6 address is defined in RFC 3484.

The system allows only one source interface for the public network or each VPN instance. If you execute this command multiple times, the most recent configuration takes effect. You can specify source interfaces for both public network and VPN instances.

This command takes effect whether the source interface belongs to the VPN instance or not. As a best practice, specify an interface that belongs to the VPN instance as the source interface.

Examples

Specify GigabitEthernet 1/0/1 as the source interface for DNS packets on the public network.

```
<Sysname> system-view
[Sysname] dns source-interface gigabitethernet 1/0/1
```

dns spoofing

Use **dns spoofing** to enable DNS spoofing and specify the IPv4 address for spoofing DNS requests.

Use **undo dns spoofing** to disable DNS spoofing.

Syntax

dns spoofing *ip-address* [**vpn-instance** *vpn-instance-name*]

undo dns spoofing *ip-address* [**vpn-instance** *vpn-instance-name*]

Default

DNS spoofing is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the IPv4 address used to spoof DNS requests.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. To enable DNS spoofing for the public network, do not specify this option.

Usage guidelines

Use the **dns spoofing** command together with the **dns proxy enable** command.

DNS spoofing functions when the DNS proxy does not know the DNS server address or cannot reach the DNS server. It enables the DNS proxy to spoof DNS queries of type A by responding with the specified IPv4 address.

The system allows only one replied IPv4 address for the public network or each VPN instance. If you execute this command multiple times, the most recent configuration takes effect. You can configure DNS spoofing for both public network and VPN instances.

Examples

Enable DNS spoofing for the public network and specify IPv4 address 1.1.1.1 for spoofing DNS requests.

```
<Sysname> system-view
[Sysname] dns proxy enable
[Sysname] dns spoofing 1.1.1.1
```

Related commands

dns proxy enable

dns transparent-proxy enable

Use **dns transparent-proxy enable** to enable DNS transparent proxy.

Use **undo dns transparent-proxy enable** to disable DNS transparent proxy.

Syntax

dns transparent-proxy enable

undo dns transparent-proxy enable

Default

DNS transparent proxy is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

DNS transparent proxy modifies the source address in the DNS request so that the DNS client seems to receive a DNS reply directly from the DNS server. This feature is applicable to domain name-based policies, such as security policies and bandwidth policies.

The DNS client does not configure the DNS server address as the DNS transparent proxy address, which simplifies DNS client configurations. As a best practice, enable DNS transparent proxy in some load balancing scenarios.

The device enabled with DNS transparent proxy monitors received DNS requests and replies and records the DNS mapping as follows:

1. The DNS transparent proxy monitors all received DNS packets. After receiving a DNS request, the DNS transparent proxy specifies a local IP address that can reach the DNS server as the source IP address in the request.
2. After receiving the DNS reply, the DNS transparent proxy records the DNS mapping and forwards the reply to the DNS client.
3. The DNS transparent proxy searches the local entries after receiving another request. If the requested information is found, the DNS transparent proxy returns a DNS reply to the client. If the requested information is not found, the DNS proxy forwards the query to the DNS server for domain name resolution.

The DNS transparent proxy and DNS snooping features cannot be both configured.

The DNS transparent proxy is not VPN-aware. The input interface and output interface of DNS packets must belong to the same VPN.

Examples

Enable DNS transparent proxy.

```
<Sysname> system-view
[Sysname] dns transparent-proxy enable
```

Related commands

dns proxy enable

dns snooping enable

dns trust-interface

Use **dns trust-interface** to specify a DNS trusted interface.

Use **undo dns trust-interface** to remove a DNS trusted interface.

Syntax

dns trust-interface *interface-type interface-number*

undo dns trust-interface [*interface-type interface-number*]

Default

No DNS trusted interface is specified.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

By default, an interface obtains DNS suffix and DNS server information from DHCP. A network attacker might act as the DHCP server to assign a wrong DNS suffix and DNS server address to the device. As a result, the device fails to obtain the resolved IP address or might get the wrong IP address. With the DNS trusted interface specified, the device only uses the DNS suffix and DNS server information obtained through the trusted interface to avoid attacks.

This configuration applies to both IPv4 DNS and IPv6 DNS.

You can configure a maximum of 128 DNS trusted interfaces on the device.

If you do not specify an interface, the **undo dns trust-interface** command removes all DNS trusted interfaces and restores the default.

Examples

Specify GigabitEthernet 1/0/1 as a DNS trusted interface.

```
<Sysname> system-view
[Sysname] dns trust-interface gigabitethernet 1/0/1
```

ip host

Use **ip host** to create a host name-to-IPv4 address mapping.

Use **undo ip host** to remove a host name-to-IPv4 address mapping.

Syntax

ip host *host-name ip-address* [**vpn-instance** *vpn-instance-name*]

undo ip host *host-name ip-address* [**vpn-instance** *vpn-instance-name*]

Default

No host name-to-IPv4 address mappings exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

host-name: Specifies a host name, a case-insensitive string of 1 to 253 characters. Valid characters are letters, digits, hyphens (-), underscores (_), and dots (.).

ip-address: Specifies the IPv4 address of the host.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. To create a host name-to-IP address mapping for the public network, do not specify this option.

Usage guidelines

The system allows a maximum of 1024 host name-to-IPv4 address mappings for the public network or each VPN instance. You can configure host name-to-IPv4 address mappings for both public network and VPN instances.

For the public network or a VPN instance, each host name maps to only one IPv4 address. If you execute this command multiple times, the most recent configuration takes effect.

Do not use the **ping** command parameter **ip**, **-a**, **-c**, **-f**, **-h**, **-i**, **-m**, **-n**, **-p**, **-q**, **-r**, **-s**, **-t**, **-tos**, **-v**, or **-vpn-instance** as the host name. For more information about the **ping** command parameters, see *Network Management and Monitoring Command Reference*.

Examples

Map IPv4 address 10.110.0.1 to host name **aaa** for the public network.

```
<Sysname> system-view
[Sysname] ip host aaa 10.110.0.1
```

Related commands

display dns host

ipv6 dns dscp

Use **ipv6 dns dscp** to set the DSCP value for IPv6 DNS packets sent by an IPv6 DNS client or IPv6 DNS proxy.

Use **undo ipv6 dns dscp** to restore the default.

Syntax

ipv6 dns dscp *dscp-value*

undo ipv6 dns dscp

Default

The DSCP value is 0 in IPv6 DNS packets sent by an IPv6 DNS client or IPv6 DNS proxy.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

dscp-value: Specifies the DSCP value in the range of 0 to 63.

Usage guidelines

The DSCP value of a packet specifies the priority level of the packet and affects the transmission priority of the packet. A bigger DSCP value represents a higher priority.

Examples

Set the DSCP value to 30 for outgoing IPv6 DNS packets.

```
<Sysname> system-view
[Sysname] ipv6 dns dscp 30
```

ipv6 dns server

Use **ipv6 dns server** to specify the IPv6 address of a DNS server.

Use **undo ipv6 dns server** to remove the IPv6 address of a DNS server.

Syntax

ipv6 dns server *ipv6-address* [*interface-type interface-number*] [**vpn-instance** *vpn-instance-name*]

undo ipv6 dns server [*ipv6-address* [*interface-type interface-number*]] [**vpn-instance** *vpn-instance-name*]

Default

No DNS server IPv6 address is specified.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address: Specifies the IPv6 address of a DNS server.

interface-type interface-number: Specifies the output interface by its type and number. If you do not specify an interface, the device forwards DNS packets out of the output interface of the

matching route. Specify this argument if the IPv6 address of the DNS server is a link-local address. Do not specify this argument if the IPv6 address of the DNS server is a global unicast address.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. To specify a DNS server IPv6 address for the public network, do not use this option.

Usage guidelines

The device sends a DNS query request to the DNS servers in the order their IPv6 addresses are specified.

The system allows a maximum of six DNS server IPv6 addresses for the public network or each VPN instance. You can specify DNS server IPv6 addresses for both public network and VPN instances.

If you do not specify an IPv6 address, the **undo ipv6 dns server** command removes all DNS server IPv6 addresses for the public network or the specified VPN instance.

Examples

Specify DNS server IPv6 address 2002::1 for the public network.

```
<Sysname> system-view
[Sysname] ipv6 dns server 2002::1
```

Related commands

display ipv6 dns server

ipv6 dns spoofing

Use **ipv6 dns spoofing** to enable DNS spoofing and specify the IPv6 address to spoof DNS requests.

Use **undo ipv6 dns spoofing** to disable DNS spoofing.

Syntax

ipv6 dns spoofing *ipv6-address* [**vpn-instance** *vpn-instance-name*]

undo ipv6 dns spoofing *ipv6-address* [**vpn-instance** *vpn-instance-name*]

Default

DNS spoofing is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address: Specifies the IPv6 address used to spoof DNS requests.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. To enable DNS spoofing for the public network, do not specify this option.

Usage guidelines

Use the **ipv6 dns spoofing** command together with the **dns proxy enable** command.

DNS spoofing functions when the DNS proxy does not know the DNS server address or cannot reach the DNS server. It enables the DNS proxy to spoof DNS queries of type AAAA by responding with the specified IPv6 address.

The system allows only one replied IPv6 address for the public network or each VPN instance. If you execute this command multiple times, the most recent configuration takes effect. You can configure DNS spoofing for both public network and VPN instances.

Examples

Enable DNS spoofing for the public network and specify IPv6 address 2001::1 for spoofing DNS requests.

```
<Sysname> system-view
[Sysname] dns proxy enable
[Sysname] ipv6 dns spoofing 2001::1
```

Related commands

dns proxy enable

ipv6 host

Use **ipv6 host** to create a host name-to-IPv6 address mapping.

Use **undo ipv6 host** to remove a host name-to-IPv6 address mapping.

Syntax

ipv6 host *host-name ipv6-address* [**vpn-instance** *vpn-instance-name*]

undo ipv6 host *host-name ipv6-address* [**vpn-instance** *vpn-instance-name*]

Default

No host name-to-IPv6 address mappings exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

host-name: Specifies a host name, a case-insensitive string of 1 to 253 characters. It can include letters, digits, hyphens (-), underscores (_), and dots (.).

ipv6-address: Specifies the IPv6 address of the host.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. To create a host name-to-IPv6 address mapping for the public network, do not specify this option.

Usage guidelines

The system allows a maximum of 1024 host name-to-IPv6 address mappings for the public network or each VPN instance. You can configure host name-to-IPv6 address mappings for both public network and VPN instances.

For the public network or a VPN instance, each host name maps to only one IPv6 address. If you execute this command multiple times, the most recent configuration takes effect.

Do not use the **ping ipv6** command parameter **-a**, **-c**, **-i**, **-m**, **-q**, **-s**, **-t**, **-tc**, **-v**, or **-vpn-instance** as the host name. For more information about the **ping ipv6** command parameters, see *Network Management and Monitoring Command Reference*.

Examples

Map IPv6 address 2001::1 to host name **aaa** for the public network.

```
<Sysname> system-view
[Sysname] ipv6 host aaa 2001::1
```

Related commands

ip host

reset dns host

Use **reset dns host** to clear dynamic DNS entries.

Syntax

reset dns host [**ip** | **ipv6**] [**vpn-instance** *vpn-instance-name*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

ip: Specifies type A queries. A type A query resolves a domain name to the mapped IPv4 address.

ipv6: Specifies type AAAA queries. A type AAAA query resolves a domain name to the mapped IPv6 address.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears dynamic DNS entries for the public network.

Usage guidelines

If you do not specify the **ip** or **ipv6** keyword, the **reset dns host** command clears dynamic DNS entries of all query types.

Use this command to clear the following dynamic DNS entries:

- Dynamic DNS entries on the DNS client.
- Dynamic DNS entries on the device enabled with DNS transparent proxy.

Examples

Clear dynamic DNS entries of all query types for the public network.

```
<Sysname> reset dns host
```

Related commands

display dns host

reset dns snooping log statistics

Use **reset dns snooping log statistics** to clear log statistics for incoming DNS packets.

Syntax

reset dns snooping log statistics

Views

User view

Predefined user roles

network-admin

context-admin

Examples

Clear log statistics for incoming DNS packets.

```
<Sysname> reset dns snooping log statistics
```

DDNS commands

ddns apply policy

Use **ddns apply policy** to apply a DDNS policy to an interface and enable DDNS update. DDNS updates the mapping between the FQDN and the primary IP address of the interface.

Use **undo ddns apply policy** to remove the application of a DDNS policy from an interface and to stop DDNS update.

Syntax

ddns apply policy *policy-name* [**fqdn** *domain-name*]

undo ddns apply policy *policy-name*

Default

No DDNS policy and FQDN are specified on the interface, and DDNS update is disabled.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies a DDNS policy by its name, a case-insensitive string of 1 to 32 characters.

fqdn *domain-name*: Specifies the FQDN to replace <h> in the URL for DDNS update. The *domain-name* argument specifies a case-insensitive string of 1 to 253 characters. It can include letters, digits, hyphens (-), underscores (_), and dots (.).

Usage guidelines

You can apply a maximum of four DDNS policies to an interface.

If you execute this command multiple times with the same DDNS policy name but different FQDNs, both of the following occur:

- The most recent configuration takes effect.
- The device initiates a DDNS update request immediately.

Examples

Apply DDNS policy **steven_policy** to GigabitEthernet 1/0/1 to update the domain name-to-IP address mapping for FQDN **www.whatever.com** and enable DDNS update.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ddns apply policy steven_policy fqdn www.whatever.com
```

Related commands

ddns policy

display ddns policy

ddns dscp

Use **ddns dscp** to set the DSCP value for outgoing DDNS packets.

Use **undo ddns dscp** to restore the default.

Syntax

ddns dscp *dscp-value*

undo ddns dscp

Default

The DSCP value for outgoing DDNS packets is 0.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

dscp-value: Specifies the DSCP value in the range of 0 to 63.

Usage guidelines

The DSCP value of a packet specifies the priority level of the packet and affects the transmission priority of the packet. A bigger DSCP value represents a higher priority.

Examples

Set the DSCP value to 30 for outgoing DDNS packets.

```
<Sysname> system-view
[Sysname] ddns dscp 30
```

ddns policy

Use **ddns policy** to create a DDNS policy and enter its view, or enter the view of an existing DDNS policy.

Use **undo ddns policy** to delete a DDNS policy.

Syntax

ddns policy *policy-name*

undo ddns policy *policy-name*

Default

No DDNS policies exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies the DDNS policy name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

You can create a maximum of 16 DDNS policies on the device.

Examples

Create a DDNS policy named **steven_policy** and enter its view.

```
<Sysname> system-view
[Sysname] ddns policy steven_policy
```

Related commands

ddns apply policy

display ddns policy

display ddns policy

Use **display ddns policy** to display information about DDNS policies.

Syntax

display ddns policy [*policy-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

policy-name: Specifies a DDNS policy by its name, a case-insensitive string of 1 to 32 characters. If you do not specify a DDNS policy, this command displays information about all DDNS policies.

Examples

Display information about DDNS policy **steven_policy**.

```
<Sysname> display ddns policy steven_policy
DDNS policy: steven_policy
  URL              : http://members.3322.org/dyndns/update?
                     system=dyndns&hostname=<h>&myip=<a>
  Username         : steven
  Password         : ******
  Method           : GET
  SSL client policy:
  Interval         : 1 days 0 hours 1 minutes
```

Display information about all DDNS policies.

```
<Sysname> display ddns policy
DDNS policy: steven_policy
  URL              : http://members.3322.org/dyndns/update?system=
                     dyndns&hostname=<h>&myip=<a>
```

```
  Username         : steven
  Password         : ******
  Method           : GET
  SSL client policy:
  Interval         : 0 days 0 hours 30 minutes

DDNS policy: tom-policy
  URL              : http://members.3322.org/dyndns/update?system=
                     dyndns&hostname=<h>&myip=<a>
  Username         :
  Password         :
  Method           : GET
  SSL client policy:
  Interval         : 0 days 0 hours 15 minutes

DDNS policy: u-policy
  URL              : oray://phddns60.oray.net
  Username         : username
  Password         :
  Method           : -
  SSL client policy:
  Interval         : 0 days 0 hours 15 minutes
```

Table 5 Command output

Field	Description
DDNS policy	DDNS policy name.
URL	URL address for a DDNS update request. This field is empty if no URL address is configured.
Username	Username for logging in to the DDNS server. This field is empty if no username is configured.
Password	Password for logging in to the DDNS server. This field is empty if no password is configured and displays ********** if a password is configured.
Method	Parameter transmission method used to send HTTP/HTTPS-based DDNS update requests. Method types include GET and POST.
SSL client policy	Name of the associated SSL client policy. This field is empty if no SSL client policy is associated.
Interval	Interval for sending DDNS update requests.

Related commands

ddns policy

interval

Use **interval** to set the interval for sending DDNS update requests.

Use **undo interval** to restore the default.

Syntax

interval *days* [*hours* [*minutes*]]

undo interval

Default

The DDNS update request interval is 1 hour.

Views

DDNS policy view

Predefined user roles

network-admin

context-admin

Parameters

days: Days in the range of 0 to 365.

hours: Hours in the range of 0 to 23.

minutes: Minutes in the range of 0 to 59.

Usage guidelines

The interface always sends a DDNS update request in one of the following conditions:

- The primary IP address of the interface changes.
- The link state of the interface changes from down to up.

If you set the interval to 0, the device does not periodically initiate DDNS update requests.

If you execute this command multiple times, the most recent configuration takes effect. If you change the interval for an applied DDNS policy, the device immediately initiates a DDNS update request and sets the interval as the update interval.

Examples

Set the interval to 1 day and 1 minute for sending DDNS update requests for DDNS policy **steven_policy**.

```
<Sysname> system-view
[Sysname] ddns policy steven_policy
[Sysname-ddns-policy-steven_policy] interval 1 0 1
```

Related commands

ddns policy

display ddns policy

method

Use **method** to specify the parameter transmission method for sending DDNS update requests to HTTP/HTTPS-based DDNS servers.

Use **undo method** to restore the default.

Syntax

method { **http-get** | **http-post** }

undo method

Default

The method **http-get** applies.

Views

DDNS policy view

Predefined user roles

network-admin

context-admin

Parameters

http-get: Uses the get operation.

http-post: Uses the post operation.

Usage guidelines

This command applies to DDNS updates in HTTP/HTTPS. If the DDNS server uses HTTP or HTTPS service, choose a parameter transmission method compatible with the DDNS server. For example, a DHS server supports the **http-post** method.

If the DDNS policy has been applied to an interface, a DDNS update is sent immediately after the parameter transmission is changed.

Examples

Specify the parameter transmission method as **http-post** for DDNS update requests for DDNS policy **steven_policy**.

```
<Sysname> system-view
[Sysname] ddns policy steven_policy
[Sysname-ddns-policy-steven_policy] method http-post
```

Related commands

ddns policy

display ddns policy

password

Use **password** to specify the password for logging in to the DDNS server.

Use **undo password** to restore the default.

Syntax

password { **cipher** | **simple** } *string*

undo password

Default

No password is specified for logging in to the DDNS server.

Views

DDNS policy view

Predefined user roles

network-admin

context-admin

Parameters

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 32 characters. Its encrypted form is a case-sensitive string of 1 to 73 characters.

Examples

In DDNS policy **steven_policy**, specify **nevets** as the password for logging in to the DDNS server.

```
<Sysname> system-view
[Sysname] ddns policy steven_policy
[Sysname-ddns-policy-steven_policy] password simple nevets
```

Related commands

ddns policy

display ddns policy

url

username

ssl-client-policy

Use **ssl-client-policy** to associate an SSL client policy with a DDNS policy.

Use **undo ssl-client-policy** to restore the default.

Syntax

ssl-client-policy *policy-name*

undo ssl-client-policy

Default

No SSL client policy is associated with a DDNS policy.

Views

DDNS policy view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies a SSL client policy by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

The SSL client policy is effective only for HTTPS-based DDNS update requests.

If you execute this command multiple times with different SSL client policies, the most recent configuration takes effect.

Examples

Associate SSL client policy **ssl_policy** with DDNS policy **steven_policy**.

```
<Sysname> system-view
```

```
[Sysname] ddns policy steven_policy
[Sysname-ddns-policy-steven_policy] ssl-client-policy ssl_policy
```

Related commands

ddns policy

display ddns policy

ssl-client-policy (*Security Command Reference*)

url

Use **url** to specify the URL address for DDNS update requests.

Use **undo url** to restore the default.

Syntax

url *request-url*

undo url

Default

No URL address is specified for DDNS update requests.

Views

DDNS policy view

Predefined user roles

network-admin

context-admin

Parameters

request-url: Specifies the URL address, a case-sensitive string of 1 to 240 characters.

Usage guidelines

The URL addresses configured for update requests vary by DDNS server. Common DDNS server URL address formats are shown in Table 6.

Table 6 Common URL addresses for DDNS update request

DDNS server	URL addresses for DDNS update requests
www.3322.org	http://members.3322.org/dyndns/update?system=dyndns&hostname=<h>&myip=<a>
DYNDNS	http://members.dyndns.org/nic/update?system=dyndns&hostname=<h>&myip=<a>
DYNS	http://www.dyns.cx/postscript.php?host=<h>&ip=<a>
ZONEEDIT	http://dynamic.zoneedit.com/auth/dynamic.html?host=<h>&dnsto=<a>
TZO	http://cgi.tzo.com/webclient/signedon.html?TZOName=<h>IPAddress=<a>
EASYDNS	http://members.easydns.com/dyn/ez-ipupdate.php?action=edit&myip=<a>&host_id=<h>
HEIPV6TB	http://dyn.dns.he.net/nic/update?hostname=<h>&myip=<a>
CHANGE-IP	http://nic.changeip.com/nic/update?hostname=<h>&offline=1
NO-IP	http://dynupdate.no-ip.com/nic/update?hostname=<h>&myip=<a>

DDNS server	URL addresses for DDNS update requests
DHS	http://members.dhs.org/nic/hosts?domain=dyn.dhs.org&hostname=<h>&hostscmd=edit&hostscmdstage=2&type=1&ip=<a>
HP	https://*server-name*/nic/update?group=*group-name*&myip=<a>
ODS	ods://update.ods.org
GNUDIP	gnudip://*server-name*
PeanutHull	• oray://phddns60.oray.net • oray://phservice2.oray.net • http://ddns.oray.com/ph/update?hostname=<h>&myip=<a>

The URL address cannot contain the username or password. To configure the username and password, use the **username** command and the **password** command.

HP and GNUDIP are common DDNS update protocols. The *server-name* parameter is the domain name or IP address of the service provider's server using one of the update protocols.

The URL address for an update request can start with:

- **http://**—The HTTP-based DDNS server.
- **https://**—The HTTPS-based DDNS server.
- **ods://**—The TCP-based ODS server.
- **gnudip://**—The TCP-based GNUDIP server.
- **oray://**—The TCP-based DDNS server.

The domain names of DDNS servers are members.3322.org and phddns60.oray.net. The domain names of PeanutHull DDNS servers can be phddns60.oray.net and phservice2.oray.net. The domain name phservice2.oray.net maps to the public IP address of the old version PeanutHull DDNS server, which is not maintained any more. You might need to try several times upon failures to connect to the server. As a best practice, register a new account and a domain name on the PeanutHull DDNS of a new version. Determine the domain name in the URL according to the actual situation.

The port number in the URL address is optional. If you do not specify a port number, the default port number is used. HTTP uses port 80, HTTPS uses port 443, and the PeanutHull server uses port 6060.

The system automatically performs the following tasks:

- Fills <h> with the FQDN that is specified when the DDNS policy is applied to an interface.
- Fills <a> with the primary IP address of the interface to which the DDNS policy is applied.

You can also manually specify an FQDN and an IP address in <h> and <a>, respectively. In this case, the FQDN that is specified when the DDNS policy is applied to an interface will not take effect. As a best practice, do not manually change the <h> and <a> because your configuration might be incorrect.

You cannot specify an FQDN and IP address in the URL address for contacting the PeanutHull server. Alternatively, you can specify an FQDN when applying the DDNS policy to an interface. The system automatically uses the primary IP address of the interface to which the DDNS policy is applied as the IP address for DDNS update.

To avoid misinterpretation, do not include colons (:), at signs (@), and question marks (?) in your login username or password, even if you can do so.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the URL address for DDNS update requests for DDNS policy **steven_policy**. The device contacts **www.3322.org** for DDNS update.

```
<Sysname> system-view
[Sysname] ddns policy steven_policy
[Sysname-ddns-policy-steven_policy] url http://
members.3322.org/dyndns/update?system=dyndns&hostname=<h>&myip=<a>
```

Related commands

ddns policy

display ddns policy

password

username

username

Use **username** to specify the username for logging in to the DDNS server.

Use **undo username** to restore the default.

Syntax

username *username*

undo username

Default

No username is specified for logging in to the DDNS server.

Views

DDNS policy view

Predefined user roles

network-admin

context-admin

Parameters

username: Specifies the username, a case-sensitive string of 1 to 32 characters.

Examples

In DDNS policy **steven_policy**, specify **steven** as the username for logging in to the DDNS server.

```
<Sysname> system-view
[Sysname] ddns policy steven_policy
[Sysname-ddns-policy-steven_policy] username steven
```

Related commands

ddns policy

display ddns policy

password

url

Contents

IP performance optimization commands

display icmp statistics

Use **display icmp statistics** to display ICMP statistics.

Syntax

display icmp statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays ICMP statistics for all member devices.

Usage guidelines

ICMP statistics include information about received and sent ICMP packets.

Examples

Display ICMP statistics.

```
<Sysname> display icmp statistics
  Input: bad formats   0                   bad checksum            0
         echo          175                 destination unreachable 0
         source quench 0                   redirects               0
         echo replies  201                 parameter problem       0
         timestamp     0                   information requests    0
         mask requests 0                   mask replies            0
         time exceeded 0                   invalid type            0
         router advert 0                   router solicit          0
         broadcast/multicast echo requests ignored            0
         broadcast/multicast timestamp requests ignored       0
 Output: echo          0                   destination unreachable 0
         source quench 0                   redirects               0
         echo replies  175                 parameter problem       0
         timestamp     0                   information replies     0
         mask requests 0                   mask replies            0
         time exceeded 0                   bad address             0
         packet error  1442                router advert           3
```

display ip statistics

Use **display ip statistics** to display IP packet statistics.

Syntax

display ip statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IP packet statistics for all member devices.

Usage guidelines

IP statistics include information about received and sent packets, fragments, and reassembly.

Examples

Display IP packet statistics.

```
<Sysname> display ip statistics
  Input:           sum            7120          local             112
                   bad protocol   0             bad format        0
                   bad checksum   0             bad options       0
                   dropped        0
  Output:          forwarding     0             local             27
                   dropped        0             no route          2
                   compress fails 0
  Reassembling:    fragments      0             reassembled       0
                   dropped        0             timeouts          0
  Fragment:        fragmented     0             couldn't fragment 0
                   output frags   0
  Forwarded Frags: sum            0
```

Table 1 Command output

Field	Description
Input	Statistics about received packets: • **sum**—Total number of packets received. • **local**—Total number of packets destined for the device. • **bad protocol**—Total number of unknown protocol packets. • **bad format**—Total number of packets with incorrect format. • **bad checksum**—Total number of packets with incorrect checksum. • **bad options**—Total number of packets with incorrect option.
Reassembling	Statistics about reassembling: • **fragments**—Total number of fragments that need reassembling. • **reassembled**—Total number of packets that are reassembled. • **dropped**—Total number of dropped fragments that fail the reassembling. • **timeouts**—Total number of reassembly timeouts.

Field	Description
Fragment	Statistics about fragments: • **fragmented**—Total number of packets successfully fragmented. • **couldn't fragment**—Total number of packets that failed to be fragmented. • **output**—Total number of fragments sent.
Forwarded Frags	Statistics about forwarded fragments: **sum**—Total number of fragments that are directly forwarded.

Related commands

`display ip interface`

`reset ip statistics`

display rawip

Use **`display rawip`** to display brief information about RawIP connections.

Syntax

`display rawip` [**`slot`** *`slot-number`*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

`slot` *`slot-number`*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays brief information about RawIP connections for all member devices.

Usage guidelines

Brief RawIP connection information includes local and peer addresses, protocol, and PCB.

Examples

Display brief information about RawIP connections.

```
<Sysname> display rawip
 Local Addr       Foreign Addr     Protocol  Slot  PCB
 0.0.0.0          0.0.0.0          1         1     0x0000000000000009
 0.0.0.0          0.0.0.0          1         1     0x0000000000000008
 0.0.0.0          0.0.0.0          1         5     0x0000000000000002
```

Table 2 Command output

Field	Description
Local Addr	Local IP address.
Foreign Addr	Peer IP address.

Field	Description
Protocol	Protocol number.
PCB	Protocol control block.

display rawip verbose

Use **display rawip verbose** to display detailed information about RawIP connections.

Syntax

display rawip verbose [**slot** *slot-number* [**pcb** *pcb-index*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

pcb *pcb-index*: Displays detailed RawIP connection information for the specified PCB. The *pcb-index* argument specifies the index of the PCB. The index value range is 1 to 16.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays detailed information about RawIP connections for all member devices.

Usage guidelines

The detailed information includes socket creator, state, option, type, protocol number, and the source and destination IP addresses of RawIP connections.

Examples

Display detailed information about RawIP connections.

```
<Sysname> display rawip verbose
Total RawIP socket number: 1

 Connection info: src = 0.0.0.0, dst = 0.0.0.0
 Location: slot 6
 Creator: ping[320]
 State: N/A
 Options: N/A
 Error: 0
 Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 9216 / 1 / 0 / N/A
 Sending buffer(cc/hiwat/lowat/state): 0 / 9216 / 512 / N/A
 Type: 3
 Protocol: 1
 Inpcb flags: N/A
 Inpcb extflag: N/A
 Inpcb vflag: INP_IPV4
```

```
TTL: 255(minimum TTL: 0)
Send VRF: 0xffff
Receive VRF: 0xffff
```

Table 3 Command output

Field	Description
Total RawIP socket number	Total number of RawIP sockets.
Connection info	Connection information, including source IP address and destination IP address.
Location	Socket location.
Creator	Name of the operation that created the socket. The number in brackets is the process number of the creator.
State	Socket state: • **NOFDREF**—The user has closed the connection. • **ISCONNECTED**—The connection has been established. • **ISCONNECTING**—The connection is being established. • **ISDISCONNECTING**—The connection is being interrupted. • **ISSMOOTHING**—Cross-card data smoothing is in progress. • **CANBIND**—The socket supports the bind operation. • **ASYNC**—Asynchronous mode. • **ISDISCONNECTED**—The connection has been terminated. • **PROTOREF**—Indicates strong protocol reference. • **ISPCBSYNCING**—Cross-card PCB synchronization is in progress. • **N/A**—None of above state.

Field	Description
Options	Socket options: • **SO_DEBUG**—Records socket debugging information. • **SO_ACCEPTCONN**—Enables the server to listen connection requests. • **SO_REUSEADDR**—Allows the local address reuse. • **SO_KEEPALIVE**—Requires the protocol to test whether the connection is still alive. • **SO_DONTROUTE**—Bypasses the routing table query for outgoing packets because the destination is in a directly connected network. • **SO_BROADCAST**—Supports broadcast packets. • **SO_LINGER**—Closes the socket. The system can still send remaining data in the socket send buffer. • **SO_OOBINLINE**—Stores the out-of-band data in the input queue. • **SO_REUSEPORT**—Allows the local port reuse. • **SO_TIMESTAMP**—Records the timestamps of the incoming packets, accurate to milliseconds. This option is applicable to protocols that are not connection orientated. • **SO_NOSIGPIPE**—Disables the socket from sending data. As a result, a sigpipe cannot be established when a return failure occurs. • **SO_FILTER**—Supports setting the packet filter criterion. This option takes effect on the incoming packets. • **SO_TIMESTAMPNS**—Has a similar function with the timestamp, accurate to nanoseconds. • **SO_SEQPACKET**—Preserves the boundaries of packets sent to the socket buffer. • **SO_FILLTWAMPTIME**—Sets the timestamp for TWAMP. • **SO_LOCAL**—Local socket option. • **SO_NBMAADDR**—Obtains the remote NBMA address of the ADVPN tunnel. • **SO_DONTDELIVER**—Do not deliver the data to the application. • **N/A**—No options are set.
Error	Error code.

Receiving buffer (cc/hiwat/lowat/drop/state)	Displays receive buffer information in the following order:
	• **cc**—Used space.
	• **hiwat**—Maximum space.
	• **lowat**—Minimum space.
	• **drop**—Number of dropped packets.
	• **state**—Buffer state:
	  ○ **CANTSENDMORE**—Unable to send data to the peer.
	  ○ **CANTRCVMORE**—Unable to receive data from the peer.
	  ○ **RCVATMARK**—Receiving tag.
	  ○ **N/A**—None of the above states.

Field	Description

Sending buffer (cc/hiwat/lowat/state)	Displays send buffer information in the following order:
	• **cc**—Used space.
	• **hiwat**—Maximum space.
	• **lowat**—Minimum space.
	• **state**—Buffer state:
	  ○ **CANTSENDMORE**—Unable to send data to the peer.
	  ○ **CANTRCVMORE**—Unable to receive data from the peer.
	  ○ **RCVATMARK**—Receiving tag.
	  ○ **N/A**—None of the above states.

Type	Socket type: • **1**—**SOCK_STREAM**. This socket uses TCP to provide reliable transmission of byte streams. • **2**—**SOCK_DGRAM**. This socket uses UDP to provide datagram transmission. • **3**—**SOCK_RAW**. This socket allows an application to change the next upper-layer protocol header. • **N/A**—None of the above types.
Protocol	Number of the protocol using the socket.
Inpcb flags	Flags in the Internet PCB: • **INP_RECVOPTS**—Receives IP options. • **INP_RECVRETOPTS**—Receives replied IP options. • **INP_RECVDSTADDR**—Receives destination IP address. • **INP_HDRINCL**—Provides the entire IP header. • **INP_REUSEADDR**—Reuses the IP address. • **INP_REUSEPORT**—Reuses the port number. • **INP_ANONPORT**—Port number not specified. • I**NP_RECVIF**—Records the input interface of the packet. • **INP_RECVTTL**—Receives TTL of the packet. Only UDP and RawIP support this flag. • **INP_DONTFRAG**—Sets the **Don't Fragment** flag. • **INP_ROUTER_ALERT**—Receives packets with the router alert option. Only RawIP supports this flag. • **INP_PROTOCOL_PACKET**—Identifies a protocol packet. • **INP_RCVVLANID**—Receives the VLAN ID of the packet. Only UDP and RawIP support this flag. • **INP_RCVMACADDR**—Receives the MAC address of the frame. • **INP_RECVTOS**—Receives TOS of the packet. Only UDP and RawIP support this flag. • **INP_USEICMPSRC**—Uses the specified IP address as the source IP address for outgoing ICMP packets. • **INP_SYNCPCB**—Waits until Internet PCB is synchronized. • **INP_LOCAL**—Preferentially matches the INPCB with this flag on the same card. • **N/A**—None of the above flags.

Field	Description
Inpcb extflag	Extension flags in the Internet PCB: • **INP_EXTRCVPVCIDX**—Records the PVC index of the received packet. • **INP_RCVPWID**—Records the PW ID of the received packet. • **INP_EXTRCVICMPERR**—Receives an ICMP error packet. • **INP_EXTFILTER**—Filters the contents in the received packet. • **INP_EXTDONTDROP**—Do not drop the received packet. • **INP_EXLISTEN**—Adds the INPCB carrying this flag to the listen hash table. • **INP_SELECTMATCHSRCBYFIB**—Uses the FIB table to select a matching source. • **INP_EXTPRIVATESOCKET**—Associates the INPCB with the NSR private socket. • **INP_EXLISTENNET**—Sets this flag when the connection information is added to the network segment linked list. • **N/A**—None of the above flags.
Inpcb vflag	IP version flags in the Internet PCB: • **INP_IPV4**—IPv4 protocol. • **INP_TIMEWAIT**—In **TIMEWAIT** state. • **INP_ONESBCAST**—Sends broadcast packets. • **INP_DROPPED**—Protocol dropped flag. • **INP_SOCKREF**—Strong socket reference. • **INP_DONTBLOCK**—Do not block synchronization of the Internet PCB. • **N/A**—None of the above flags.
TTL	TTL value in the Internet PCB.
Send VRF	VRF from which packets are sent.
Receive VRF	VRF from which packets are received.

display tcp

Use **`display tcp`** to display brief information about TCP connections.

Syntax

`display tcp` [**`slot`** *`slot-number`*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

`slot` *`slot-number`*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays brief information about TCP connections for all member devices.

Usage guidelines

Brief TCP connection information includes local IP address, local port number, peer IP address, peer port number, and TCP connection state.

Examples

Display brief information about TCP connections.

```
<Sysname> display tcp
 *: TCP MD5 Connection
 Local Addr:port       Foreign Addr:port     State       Slot  PCB
*0.0.0.0:21            0.0.0.0:0             LISTEN      1     0x000000000000c387
 192.168.20.200:23     192.168.20.14:1284    ESTABLISHED 1     0x0000000000000009
 192.168.20.200:23     192.168.20.14:1283    ESTABLISHED 1     0x0000000000000002
```

Table 4 Command output

Field	Description
*	Indicates that the TCP connection uses authentication.
Local Addr:port	Local IP address and port number.
Foreign Addr:port	Peer IP address and port number.
State	TCP connection state.
PCB	PCB index.

display tcp statistics

Use **display tcp statistics** to display TCP traffic statistics.

Syntax

display tcp statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays TCP traffic statistics for all member devices.

Usage guidelines

TCP traffic statistics include information about received and sent TCP packets and Syncache/syncookie.

Examples

Display TCP traffic statistics.

```
<Sysname> display tcp statistics
Received packets:
```

```
    Total: 4150
    packets in sequence: 1366 (134675 bytes)
    window probe packets: 0, window update packets: 0
    checksum error: 0, offset error: 0, short error: 0
    packets dropped for lack of memory: 0
    packets dropped due to PAWS: 0
    duplicate packets: 12 (36 bytes), partially duplicate packets: 0 (0 bytes)
    out-of-order packets: 0 (0 bytes)
    packets with data after window: 0 (0 bytes)
    packets after close: 0
    ACK packets: 3531 (795048 bytes)
    duplicate ACK packets: 33, ACK packets for unsent data: 0

Sent packets:
    Total: 4058
    urgent packets: 0
    control packets: 50
    window probe packets: 3, window update packets: 11
    data packets: 3862 (795012 bytes), data packets retransmitted: 0 (0 bytes)
    ACK-only packets: 150 (52 delayed)
    unnecessary packet retransmissions: 0

Syncache/syncookie related statistics:
    entries added to syncache: 12
    syncache entries retransmitted: 0
    duplicate SYN packets: 0
    reply failures: 0
    successfully build new socket: 12
    bucket overflows: 0
    zone failures: 0
    syncache entries removed due to RST: 0
    syncache entries removed due to timed out: 0
    ACK checked by syncache or syncookie failures: 0
    syncache entries aborted: 0
    syncache entries removed due to bad ACK: 0
    syncache entries removed due to ICMP unreachable: 0
    SYN cookies sent: 0
    SYN cookies received: 0

SACK related statistics:
    SACK recoveries: 1
    SACK retransmitted segments: 0 (0 bytes)
    SACK blocks (options) received: 0
    SACK blocks (options) sent: 0
    SACK scoreboard overflows: 0

Other statistics:
    retransmitted timeout: 0, connections dropped in retransmitted timeout: 0
```

```
    persist timeout: 0
    keepalive timeout: 21, keepalive probe: 0
    keepalive timeout, so connections disconnected: 0
    fin_wait_2 timeout, so connections disconnected: 0
    initiated connections: 29, accepted connections: 12, established connections:
23
    closed connections: 50051 (dropped: 0, initiated dropped: 0)
    bad connection attempt: 0
    ignored RSTs in the window: 0
    listen queue overflows: 0
    RTT updates: 3518(attempt segment: 3537)
    correct ACK header predictions: 0
    correct data packet header predictions: 568
    resends due to MTU discovery: 0
    packets dropped due to MD5 authentication failure: 0
    packets that passed MD5 authentication: 0
    sent Keychain-encrypted packets: 0
    packets that passed Keychain authentication: 0
    packets dropped due to Keychain authentication failure: 0
    packets dropped with MD5 authentication: 0
    packets permitted with MD5 authentication: 0
```

Related commands

reset tcp statistics

display tcp verbose

Use **display tcp verbose** to display detailed information about TCP connections.

Syntax

display tcp verbose [**slot** *slot-number* [**pcb** *pcb-index*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

pcb *pcb-index*: Displays detailed TCP connection information for the specified PCB. The index value range is 1 to 16.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays detailed information about TCP connections for all member devices.

Usage guidelines

The detailed TCP connection information includes socket creator, state, option, type, protocol number, source IP address and port number, destination IP address and port number, and connection state.

Examples

Display detailed information about TCP connections.

```
<Sysname> display tcp verbose
TCP inpcb number: 1(tcpcb number: 1)

 Connection info: src = 192.168.20.200:179 ,  dst = 192.168.20.14:4181
 Location: slot 6
 NSR standby: N/A
 Creator: bgpd[199]
 State: ISCONNECTED
 Options: N/A
 Error: 0
 Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 65700 / 1 / 0 / N/A
 Sending buffer(cc/hiwat/lowat /state): 0 / 65700 / 512 / N/A
 Type: 1
 Protocol: 6
 Inpcb flags: N/A
 Inpcb extflag: N/A
 Inpcb vflag: INP_IPV4
 TTL: 255(minimum TTL: 0)
 Connection state: ESTABLISHED
 TCP options: TF_REQ_SCALE TF_REQ_TSTMP TF_SACK_PERMIT TF_NSR
 NSR state: READY(M)
 Send VRF: 0x0
 Receive VRF: 0x0
```

Table 5 Command output

Field	Description
TCP inpcb number	Number of TCP IP PCBs.
Connection info	Connection information, including source IP address, source port number, destination IP address, and destination port number.
Location	Socket location.
NSR standby	ID of the IRF member device and number of the slot where the NSR standby card resides. This field displays **N/A** if no NSR standby card is present.
tcpcb number	Number of TCP PCBs. This field is not displayed if the state of the TCP connection is **TIME_WAIT**.
Creator	Name of the operation that created the socket. The number in brackets is the process number of the creator.

Field	Description
State	Socket state: • **NOFDREF**—The user has closed the connection. • **ISCONNECTED**—The connection has been established. • **ISSMOOTHING**—Cross-card data smoothing is in progress. • **CANBIND**—The socket supports the bind operation. • **ISCONNECTING**—The connection is being established. • **ISDISCONNECTING**—The connection is being interrupted. • **ASYNC**—Asynchronous mode. • **ISDISCONNECTED**—The connection has been terminated. • **PROTOREF**—Indicates strong protocol reference. • **ISPCBSYNCING**—Cross-card PCB synchronization is in progress. • **N/A**—None of above state.
Options	Socket options: • **SO_DEBUG**—Records socket debugging information. • **SO_ACCEPTCONN**—Enables the server to listen connection requests. • **SO_REUSEADDR**—Allows the local address reuse. • **SO_KEEPALIVE**—Requires the protocol to test whether the connection is still alive. • **SO_DONTROUTE**—Bypasses the routing table query for outgoing packets because the destination is in a directly connected network. • **SO_BROADCAST**—Supports broadcast packets. • **SO_LINGER**—Closes the socket. The system can still send remaining data in the socket send buffer. • **SO_OOBINLINE**—Stores the out-of-band data in the input queue. • **SO_REUSEPORT**—Allows the local port reuse. • **SO_TIMESTAMP**—Records the timestamps of the incoming packets, accurate to milliseconds. This option is applicable to protocols that are not connection orientated. • **SO_NOSIGPIPE**—Disables the socket from sending data. As a result, a sigpipe cannot be established when a return failure occurs. • **SO_TIMESTAMPNS**—Has a similar function with the timestamp, accurate to nanoseconds. • **SO_KEEPALIVETIME**—Sets a keepalive time. • **SO_SEQPACKET**—Preserves the boundaries of packets sent to the socket buffer. • **SO_FILLTWAMPTIME**—Sets the timestamp for TWAMP. • **SO_LOCAL**—Local socket option. • **SO_NBMAADDR**—Obtains the remote NBMA address of the ADVPN tunnel. • **SO_DONTDELIVER**—Do not deliver the data to the application. • **N/A**—No options are set.
Error	Error code.

Field	Description

Receiving buffer (cc/hiwat/lowat/drop/state)	Displays receive buffer information in the following order:
	• **cc**—Used space.
	• **hiwat**—Maximum space.
	• **lowat**—Minimum space.
	• **drop**—Number of dropped packets.
	• **state**—Buffer state:
	  ○ **CANTSENDMORE**—Unable to send data to the peer.
	  ○ **CANTRCVMORE**—Unable to receive data from the peer.
	  ○ **RCVATMARK**—Receiving tag.
	  ○ **N/A**—None of the above states.

Sending buffer (cc/hiwat/lowat/state)	Displays send buffer information in the following order:
	• **cc**—Used space.
	• **hiwat**—Maximum space.
	• **lowat**—Minimum space.
	• **state**—Buffer state:
	  ○ **CANTSENDMORE**—Unable to send data to the peer.
	  ○ **CANTRCVMORE**—Unable to receive data from the peer.
	  ○ **RCVATMARK**—Receiving tag.
	  ○ **N/A**—None of the above states.

Type	Socket type: • **1**—**SOCK_STREAM**. This socket uses TCP to provide reliable transmission of byte streams. • **2**—**SOCK_DGRAM**. This socket uses UDP to provide datagram transmission. • **3**—**SOCK_RAW**. This socket allows an application to change the next upper-layer protocol header. • **N/A**—None of the above types.
Protocol	Number of the protocol using the socket.

Field	Description
Inpcb flags	Flags in the Internet PCB: • **INP_RECVOPTS**—Receives IP options. • **INP_RECVRETOPTS**—Receives replied IP options. • **INP_RECVDSTADDR**—Receives destination IP address. • **INP_HDRINCL**—Provides the entire IP header. • **INP_REUSEADDR**—Reuses the IP address. • **INP_REUSEPORT**—Reuses the port number. • **INP_ANONPORT**—Port number not specified. • I**NP_RECVIF**—Records the input interface of the packet. • **INP_RECVTTL**—Receives TTL of the packet. Only UDP and RawIP support this flag. • **INP_DONTFRAG**—Sets the **Don't Fragment** flag. • **INP_ROUTER_ALERT**—Receives packets with the router alert option. Only RawIP supports this flag. • **INP_PROTOCOL_PACKET**—Identifies a protocol packet. • **INP_RCVVLANID**—Receives the VLAN ID of the packet. Only UDP and RawIP support this flag. • **INP_RCVMACADDR**—Receives the MAC address of the frame. • **INP_RECVTOS**—Receives TOS of the packet. Only UDP and RawIP support this flag. • **INP_SYNCPCB**—Waits until Internet PCB is synchronized. • **INP_LOCAL**—Preferentially matches the INPCB with this flag on the same card. • **N/A**—None of the above flags.
Inpcb extflag	Extension flags in the Internet PCB: • **INP_EXTRCVPVCIDX**—Records the PVC index of the received packet. • **INP_RCVPWID**—Records the PW ID of the received packet. • **INP_EXTFILTER**—Filters the contents in the received packets. • **INP_SELECTMATCHSRCBYFIB**—Uses the FIB table to select a matching source. • **INP_EXTRCVICMPERR**—Receives an ICMP error packet. • **INP_EXTPRIVATESOCKET**—Associates the INPCB with the NSR private socket. • **INP_EXLISTENNET**—Sets this flag when the connection information is added to the network segment linked list. • **N/A**—None of the above flags.
Inpcb vflag	IP version flags in the Internet PCB: • **INP_IPV4**—IPv4 protocol. • **INP_TIMEWAIT**—In **TIMEWAIT** state. • **INP_ONESBCAST**—Sends broadcast packets. • **INP_DROPPED**—Protocol dropped flag. • **INP_SOCKREF**—Strong socket reference. • **INP_DONTBLOCK**—Do not block synchronization of the Internet PCB. • **N/A**—None of the above flags.
TTL	TTL value in the Internet PCB.

Field	Description
TCP options	TCP options: • **TF_ACKNOW**—Immediately replies an ACK packet to the peer. • **TF_DELACK**—Delays sending ACK packets. • **TF_SENTFIN**—A FIN packet has been sent. • **TF_RCVD_SCALE**—Requests the receive window size scale factor. • **TF_RCVD_TSTMP**—A timestamp was received in the SYN packet. • **TF_NEEDSYN**—Sends a SYN packet. • **TF_NEEDFIN**—Sends a FIN packet. • **TF_MORETOCOME**—More data is to be added to the socket. • **TF_LQ_OVERFLOW**—The listening queue overflows. • **TF_LASTIDLE**—Idle connection. • **TF_RXWIN0SENT**—A reply with receive window size 0 was sent. • **TF_FASTRECOVERY**—Enters NewReno fast recovery mode. • **TF_WASFRECOVERY**—In NewReno fast recovery mode. • **TF_SIGNATURE**—MD5 signature. • **TF_FORCEDATA**—Forces to send one byte. • **TF_TSO**—TSO is enabled. • **TF_PMTU**—Supports RFC 1191. • **TF_PMTUD**—Starts Path MTU discovery. • **TF_PASSIVE_CONN**—Passive connection. • **TF_APP_SEND**—The application sends data. • **TF_NODELAY**—Disables the Nagle algorithm that buffers the sent data inside the TCP. • **TF_NOOPT**—No TCP options. • **TF_NOPUSH**—Forces TCP to delay sending any TCP data until a full sized segment is buffered in the TCP buffers. • **TF_NSR**—Enables TCP NSR. • **TF_REQ_SCALE**—Enables the TCP window scale option. • **TF_REQ_TSTMP**—Enables the time stamp option. • **TF_SACK_PERMIT**—Enables the TCP selective acknowledgement option. • **TF_ENHANCED_AUTH**—Enables the enhanced authentication option.
NSR state	State of the TCP connections. Between the parentheses is the role of the connection: • **M**—Main connection. • **S**—Standby connection.
Send VRF	VRF from which packets are sent.
Receive VRF	VRF from which packets are received.

display tcp-proxy

Use **display tcp-proxy** to display brief information about TCP proxy.

Syntax

display tcp-proxy slot *slot-number*

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID.

Usage guidelines

TCP proxy splits every TCP connection that passes through it into two TCP connections to relay data packets between clients and servers. The split is transparent to the servers and clients. This feature reduces bandwidth use and improves TCP performance. It is used for services such as load balancing and SSL VPN.

Examples

Display brief information about TCP proxy for the specified slot.

```
<Sysname> display tcp-proxy slot 1
Local Addr:port       Foreign Addr:port     State        Service type
192.168.56.25:1111    111.111.111.125:8080  ESTABLISHED  LB
111.111.111.125:8080  192.168.56.25:1111    ESTABLISHED  LB
```

Table 6 Command output

Field	Description
Local Addr:port	Local IP address and port number.
Foreign Addr:port	Peer IP address and port number.
State	TCP connection state.
Service type	Type of services that the TCP proxy is used for: • **LB**—Load balancing services. • **SSL VPN**—SSL VPN services. • **WAAS**—WAAS services. • **APPPROXY**—Application proxy services.

display tcp-proxy port-info

Use **display tcp-proxy port-info** to display the usage of non-well known ports for TCP proxy.

Syntax

display tcp-proxy port-info slot *slot-number*

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays non-well known port usage for all member devices.

Usage guidelines

The TCP ports are divided into well-known ports (port numbers from 0 through 1023) and non-well known ports (port numbers from 1024 through 65535).

- Well known ports are for certain services, for example, port 23 for Telnet service, ports 20 and 21 for FTP service, and port 80 for HTTP service.
- Non-well known ports are available for various services. You can use the **display tcp-proxy port-info** command to display the usage of these ports.

Examples

Display the usage of non-well known ports for TCP proxy for the specified slot.

```
<Sysname> display tcp-proxy port-info slot 1
Index  Range            State
16     [1024, 1087]     USABLE
17     [1088, 1151]     USABLE
18     [1152, 1215]     USABLE
19     [1216, 1279]     USABLE
20     [1280, 1343]     USABLE
...
1020   [65280, 65343]   USABLE
1021   [65344, 65407]   USABLE
1022   [65408, 65471]   USABLE
1023   [65472, 65535]   USABLE
```

Table 7 Command output

Field	Description
Index	Index of the port range.
Range	Start port number and end port number.
State	State of the port range: • **USABLE**—The ports are assignable. • **ASSIGNED**—Some ports are dynamically assigned and some ports are not. • **ALLASSIGNED**—All ports are dynamically assigned. The assigned ports can be reclaimed. • **TO RECLAIM**—Some ports are statically assigned. The assigned ports can be reclaimed. • **RESERVED**—The ports are reserved. The reserved ports cannot be dynamically assigned.

display udp

Use **display udp** to display brief information about UDP connections.

Syntax

display udp [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays brief information about UDP connections for all member devices.

Usage guidelines

Brief UDP connection information includes local IP address and port number, and peer IP address and port number.

Examples

Display brief information about UDP connections.

```
<Sysname> display udp
 Local Addr:port        Foreign Addr:port     Slot  PCB
 0.0.0.0:69             0.0.0.0:0             1     0x0000000000000003
 192.168.20.200:1024    192.168.20.14:69      5     0x0000000000000002
```

Table 8 Command output

Field	Description
Local Addr:port	Local IP address and port number.
Foreign Addr:port	Peer IP address and port number.
PCB	PCB index.

display udp statistics

Use **display udp statistics** to display UDP traffic statistics.

Syntax

display udp statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays UDP traffic statistics for all member devices.

Usage guidelines

UDP traffic statistics include information about received and sent UDP packets.

Examples

Display UDP traffic statistics.

```
<Sysname> display udp statistics
Received packets:
     Total: 240
     checksum error: 0, no checksum: 0
     shorter than header: 0, data length larger than packet: 0
     no socket on port(unicast): 0
     no socket on port(broadcast/multicast): 240
     not delivered, input socket full: 0
Sent packets:
     Total: 0
```

Related commands

reset udp statistics

display udp verbose

Use **display udp verbose** to display detailed information about UDP connections.

Syntax

display udp verbose [**slot** *slot-number* [**pcb** *pcb-index*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

pcb *pcb-index*: Displays detailed UDP connection information for the specified PCB. The value range for the *pcb-index* argument is 1 to 16.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays detailed information about UDP connections for all member devices.

Usage guidelines

The detailed information includes socket creator, status, option, type, protocol number, source IP address and port number, and destination IP address and port number for UDP connections.

Examples

Display detailed UDP connection information.

```
<Sysname> display udp verbose
Total UDP socket number: 1

 Connection info: src = 0.0.0.0:69, dst = 0.0.0.0:0
 Location: slot 6
 Creator: sock_test_mips[250]
 State: N/A
 Options: N/A
 Error: 0
 Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 41600 / 1 / 0 / N/A
 Sending buffer(cc/hiwat/lowat/state): 0 / 9216 / 512 / N/A
 Type: 2
 Protocol: 17
 Inpcb flags: N/A
 Inpcb extflag: N/A
 Inpcb vflag: INP_IPV4
 TTL: 255(minimum TTL: 0)
 Send VRF: 0xffff
 Receive VRF: 0xffff
```

Table 9 Command output

Field	Description
Total UDP socket number	Total number of UDP sockets.
Connection info	Connection information, including source IP address, source port number, destination IP address, and destination port number.
Location	Socket location.
Creator	Name of the operation that created the socket. The number in brackets is the process number of the creator.
State	Socket state: • **NOFDREF**—The user has closed the connection. • **ISCONNECTED**—The connection has been established. • **ISCONNECTING**—The connection is being established. • **ISDISCONNECTING**—The connection is being interrupted. • **ASYNC**—Asynchronous mode. • **ISDISCONNECTED**—The connection has been terminated. • **ISSMOOTHING**—Cross-card data smoothing is in progress. • **CANBIND**—The socket supports the bind operation. • **PROTOREF**—Indicates strong protocol reference. • **ISPCBSYNCING**—Cross-card PCB synchronization is in progress. • **N/A**—None of above state.

Field	Description
Options	Socket options: • **SO_DEBUG**—Records socket debugging information. • **SO_ACCEPTCONN**—Enables the server to listen connection requests. • **SO_REUSEADDR**—Allows the local address reuse. • **SO_KEEPALIVE**—Requires the protocol to test whether the connection is still alive. • **SO_DONTROUTE**—Bypasses the routing table query for outgoing packets because the destination is in a directly connected network. • **SO_BROADCAST**—Supports broadcast packets. • **SO_LINGER**—Closes the socket. The system can still send remaining data in the socket send buffer. • **SO_OOBINLINE**—Stores the out-of-band data in the input queue. • **SO_REUSEPORT**—Allows the local port reuse. • **SO_TIMESTAMP**—Records the timestamps of the incoming packets, accurate to milliseconds. This option is applicable to protocols that are not connection orientated. • **SO_NOSIGPIPE**—Disables the socket from sending data. As a result, a sigpipe cannot be established when a return failure occurs. • **SO_TIMESTAMPNS**—Has a similar function with the timestamp, accurate to nanoseconds. • **SO_SEQPACKET**—Preserves the boundaries of packets sent to the socket buffer. • **SO_FILLTWAMPTIME**—Sets the timestamp for TWAMP. • **SO_LOCAL**—Local socket option. • **SO_NBMAADDR**—Obtains the remote NBMA address of the ADVPN tunnel. • **SO_DONTDELIVER**—Do not deliver the data to the application. • **N/A**—No options are set.
Error	Error code.

Receiving buffer(cc/hiwat/lowat/drop/state)	Displays receive buffer information in the following order:
	• **cc**—Used space.
	• **hiwat**—Maximum space.
	• **lowat**—Minimum space.
	• **drop**—Number of dropped packets.
	• **state**—Buffer state:
	  ○ **CANTSENDMORE**—Unable to send data to the peer.
	  ○ **CANTRCVMORE**—Unable to receive data from the peer.
	  ○ **RCVATMARK**—Receiving tag.
	  ○ **N/A**—None of the above states.

Sending buffer(cc/hiwat/lowat/state)	Displays send buffer information in the following order:
	• **cc**—Used space.
	• **hiwat**—Maximum space.
	• **lowat**—Minimum space.
	• **state**—Buffer state:
	  ○ **CANTSENDMORE**—Unable to send data to the peer.
	  ○ **CANTRCVMORE**—Unable to receive data from the peer.
	  ○ **RCVATMARK**—Receiving tag.
	  ○ **N/A**—None of the above states.

Field	Description
Type	Socket type: • **1**—**SOCK_STREAM**. This socket uses TCP to provide reliable transmission of byte streams. • **2**—**SOCK_DGRAM**. This socket uses UDP to provide datagram transmission. • **3**—**SOCK_RAW**. This socket allows an application to change the next upper-layer protocol header. • **N/A**—None of the above types.
Protocol	Number of the protocol using the socket.
Connection info	Connection information, including source IP address, source port number, destination IP address, and destination port number.
Inpcb flags	Flags in the Internet PCB: • **INP_RECVOPTS**—Receives IP options. • **INP_RECVRETOPTS**—Receives replied IP options. • **INP_RECVDSTADDR**—Receives destination IP address. • **INP_HDRINCL**—Provides the entire IP header. • **INP_REUSEADDR**—Reuses the IP address. • **INP_REUSEPORT**—Reuses the port number. • **INP_ANONPORT**—Port number not specified. • I**NP_RECVIF**—Records the input interface of the packet. • **INP_RECVTTL**—Receives TTL of the packet. Only UDP and RawIP support this flag. • **INP_DONTFRAG**—Sets the **Don't Fragment** flag. • **INP_ROUTER_ALERT**—Receives packets with the router alert option. Only RawIP supports this flag. • **INP_PROTOCOL_PACKET**—Identifies a protocol packet. • **INP_RCVVLANID**—Receives the VLAN ID of the packet. Only UDP and RawIP support this flag. • **INP_RCVMACADDR**—Receives the MAC address of the frame. • **INP_RECVTOS**—Receives TOS of the packet. Only UDP and RawIP support this flag. • **INP_SYNCPCB**—Waits until Internet PCB is synchronized. • **INP_LOCAL**—Preferentially matches the INPCB with this flag on the same card. • **N/A**—None of the above flags.
Inpcb extflag	Extension flags in the Internet PCB: • **INP_EXTRCVPVCIDX**—Records the PVC index of the received packet. • **INP_RCVPWID**—Records the PW ID of the received packet. • **INP_EXTDONTDROP**—Do not drop the received packet. • **INP_EXLISTEN**—Adds the INPCB carrying this flag to the listen hash table. • **INP_EXTFILTER**—Filters the contents in the received packets. • **INP_SELECTMATCHSRCBYFIB**—Uses the FIB table to select a matching source. • **INP_EXTRCVICMPERR**—Receives an ICMP error packet. • **INP_EXTPRIVATESOCKET**—Associates the INPCB with the NSR private socket. • **INP_EXLISTENNET**—Sets this flag when the connection information is added to the network segment linked list. • **N/A**—None of the above flags.

Field	Description
Inpcb vflag	IP version flags in the Internet PCB: • **INP_IPV4**—IPv4 protocol. • **INP_TIMEWAIT**—In **TIMEWAIT** state. • **INP_ONESBCAST**—Sends broadcast packets. • **INP_DROPPED**—Protocol dropped flag. • **INP_SOCKREF**—Strong socket reference. • **INP_DONTBLOCK**—Do not block synchronization of the Internet PCB. • **N/A**—None of the above flags.
TTL	TTL value in the Internet PCB.
Send VRF	VRF from which packets are sent.
Receive VRF	VRF from which packets are received.

ip df-bit

Use **ip df-bit** to configure the DF bit for IP packets.

Use **undo ip df-bit** to restore the default.

Syntax

ip df-bit { **clear** | **set** }

undo ip df-bit

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB1180, NFNX3-HDB1480	No

Default

The DF bit value of IP packets is retained as it is.

Views

System view

Predefined user roles

network-admin

context-adminn

Parameters

clear: Sets the DF bit to 0 for IP packets. The IP packets can be fragmented.

set: Sets the DF bit to 1 for IP packets. The IP packets cannot be fragmented.

Examples

Clear the DF bit for IP packets.

```
<Sysname> system-view
```

```
[Sysname] ip df-bit clear
```

ip forward-broadcast

Use **ip forward-broadcast** to enable an interface to receive and forward directed broadcast packets destined for the directly connected network.

Use **undo ip forward-broadcast** to disable an interface from receiving and forwarding directed broadcast packets destined for the directly connected network.

Syntax

ip forward-broadcast

undo ip forward-broadcast

Default

An interface cannot forward directed broadcasts destined for the directly connected network, and can receive directed broadcasts destined for the directly connected network.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

acl *acl-number*: Specifies an ACL by its number. The interface forwards only the directed broadcasts permitted by the ACL. The value range for basic ACLs is 2000 to 2999. The value range for advanced ACLs is 3000 to 3999.

Usage guidelines

A directed broadcast packet is destined for all hosts on a specific network. In the destination IP address of the directed broadcast, the network ID identifies the target network, and the host ID is made up of all ones.

Examples

Enable GigabitEthernet 1/0/1 to receive and forward directed broadcast packets destined for the directly connected network.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip forward-broadcast
```

ip icmp error-interval

Use **ip icmp error-interval** to set the interval for tokens to arrive in the bucket and the bucket size for ICMP error messages.

Use **undo ip icmp error-interval** to restore the default.

Syntax

ip icmp error-interval *interval* [*bucketsize*]

undo ip icmp error-interval

Default

A token is placed in the bucket every 100 milliseconds, and the bucket allows a maximum of 10 tokens.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies the interval for tokens to arrive in the bucket. The value range is 0 to 2147483647 milliseconds. To disable the ICMP rate limit, set the value to 0.

bucketsize: Specifies the maximum number of tokens allowed in the bucket. The value range is 1 to 200.

Usage guidelines

This command limits the rate at which ICMP error messages are sent. Use this command to avoid sending excessive ICMP error messages within a short period that might cause network congestion. A token bucket algorithm is used with one token representing one ICMP error message.

A token is placed in the bucket at intervals until the maximum number of tokens that the bucket can hold is reached.

A token is removed from the bucket when an ICMP error message is sent. When the bucket is empty, ICMP error messages are not sent until a new token is placed in the bucket.

Examples

Set the interval to 200 milliseconds for tokens to arrive in the bucket and set the bucket size to 40 tokens for ICMP error messages.

```
<Sysname> system-view
[Sysname] ip icmp error-interval 200 40
```

ip icmp source

Use **ip icmp source** to specify the source address for outgoing ICMP packets.

Use **undo ip icmp source** to remove the specified source address for outgoing ICMP packets.

Syntax

ip icmp source [**vpn-instance** *vpn-instance-name*] *ip-address*

undo ip icmp source [**vpn-instance** *vpn-instance-name*]

Default

No source address is specified for outgoing ICMP packets. The default source IP addresses for different types of ICMP packets vary as follows:

- For an ICMP error message, the source IP address is the IP address of the receiving interface of the packet that triggers the ICMP error message. ICMP error messages include Time Exceeded, Port Unreachable, and Parameter Problem messages.
- For an ICMP echo request, the source IP address is the IP address of the sending interface.
- For an ICMP echo reply, the source IP address is the destination IP address of the ICMP echo request specific to this reply.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance to which the specified address belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. The specified VPN instance must exist. If you do not specify a VPN instance, the *ip-address* argument specifies an IP address on the public network.

ip-address: Specifies an IP address.

Usage guidelines

It is a good practice to specify the IP address of the loopback interface as the source IP address for outgoing ping echo request and ICMP error messages. This feature helps users to locate the sending device easily.

Examples

Specify 1.1.1.1 as the source address for outgoing ICMP packets.

```
<Sysname> system-view
[Sysname] ip icmp source 1.1.1.1
```

ip mtu

Use **ip mtu** to set the interface MTU for IPv4 packets. The MTU defines the largest size of an IPv4 packet that an interface can transmit without fragmentation.

Use **undo ip mtu** to restore the default.

Syntax

ip mtu *mtu-size*

undo ip mtu

Default

The interface MTU is not set.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

mtu-size: Specifies the MTU in bytes. The value range for the *mtu-size* argument depends on the interface type.

Usage guidelines

When a packet exceeds the MTU of the sending interface, the device processes the packet in one of the following ways:

- If the packet disallows fragmentation, the device discards it.
- If the packet allows fragmentation, the device fragments it and forwards the fragments.

Fragmentation and reassembling consume system resources, so set an appropriate MTU to avoid fragmentation.

If an interface supports both the **mtu** and **ip mtu** commands, the device fragments a packet based on the MTU set by the **ip mtu** command.

Examples

Set the interface MTU to 1280 bytes for GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip mtu 1280
```

ip reassemble local enable

Use **ip reassemble local enable** to enable IPv4 local fragment reassembly.

Use **undo ip reassemble local enable** to disable local fragment reassembly.

Syntax

ip reassemble local enable

undo ip reassemble local enable

Default

IPv4 local fragment reassembly is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

Use this feature on a multichassis IRF fabric to improve fragment reassembly efficiency. This feature enables a subordinate to reassemble the IPv4 fragments of a packet if all the fragments arrive at it. If this feature is disabled, all IPv4 fragments are delivered to the master device for reassembly. The feature applies only to fragments destined for the same subordinate.

Examples

Enable IPv4 local fragment reassembly.

```
<Sysname> system-view
[Sysname] ip reassemble local enable
```

ip redirects enable

Use **ip redirects enable** to enable sending ICMP redirect messages.

Use **undo ip redirects enable** to disable sending ICMP redirect messages.

Syntax

ip redirects enable

undo ip redirects enable

Default

Sending ICMP redirect messages is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

ICMP redirect messages simplify host management and enable hosts to gradually optimize their routing tables.

A host that has only one route destined for the default gateway sends all packets to the default gateway. The default gateway sends an ICMP redirect message to inform the host of a correct next hop when the following conditions are met:

- The receiving and sending interfaces are the same.
- The packet source IP address and the IP address of the packet receiving interface are on the same segment.
- There is no source route option in the received packet.

Examples

Enable sending ICMP redirect messages.

```
<Sysname> system-view
[Sysname] ip redirects enable
```

ip ttl-expires enable

Use **ip ttl-expires enable** to enable sending ICMP time exceeded messages.

Use **undo ip ttl-expires enable** to disable sending ICMP time exceeded messages.

Syntax

ip ttl-expires enable

undo ip ttl-expires enable

Default

Sending ICMP time exceeded messages is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

A device sends ICMP time exceeded messages by following these rules:

- The device sends an ICMP TTL exceeded in transit message to the source when the following conditions are met:
  - The received packet is not destined for the device.
  - The TTL field of the packet is 1.

- When the device receives the first fragment of an IP datagram destined for the device itself, it starts a timer. If the timer expires before all the fragments of the datagram are received, the device sends an ICMP fragment reassembly time exceeded message to the source.

A device disabled from sending ICMP time exceeded messages does not send ICMP TTL exceeded in transit messages but can still send ICMP fragment reassembly time exceeded messages.

Examples

Enable sending ICMP time exceeded messages.

```
<Sysname> system-view
[Sysname] ip ttl-expires enable
```

ip unreachables enable

Use **ip unreachables enable** to enable sending ICMP destination unreachable messages.

Use **undo ip unreachables enable** to disable sending ICMP destination unreachable messages.

Syntax

ip unreachables enable

undo ip unreachables enable

Default

Sending ICMP destination unreachable messages is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

A device sends ICMP destination unreachable messages by following these rules:

- The device sends the source an ICMP network unreachable message when the following conditions are met:
  - The received packet does not match any route.
  - No default route exists in the routing table.
- The device sends the source an ICMP protocol unreachable message when the following conditions are met:
  - The received packet is destined for the device.
  - The transport layer protocol of the packet is not supported by the device.
- The device sends the source an ICMP port unreachable message when the following conditions are met:
  - The received UDP packet is destined for the device.
  - The packet's port number does not match the running process.
- The device sends the source an ICMP source route failed message when the following conditions are met:
  - The source uses Strict Source Routing to send packets.
  - The intermediate device finds that the next hop specified by the source is not directly connected.

- The device sends the source an ICMP fragmentation needed and DF set message when the following conditions are met:
  - The MTU of the sending interface is smaller than the packet.
  - The packet has Don't Fragment set.

Examples

Enable sending ICMP destination unreachable messages.

```
<Sysname> system-view
[Sysname] ip unreachables enable
```

ip virtual-reassembly centralize

Use **ip virtual-reassembly centralize** to enable fragment centralization for IPv4 VFR.

Use **undo ip virtual-reassembly centralize** to disable fragment centralization for IPv4 VFR.

Syntax

ip virtual-reassembly centralize

undo ip virtual-reassembly centralize

Default

Fragment centralization is disabled for IPv4 VFR.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

On an HA network, if an HA device enabled with IPv4 VFR does not receive all fragments of a datagram, it cannot reassemble the datagram and will discard the received fragments. To resolve this issue, you can enable this feature. Devices that do not receive the first fragment of a datagram forward the received fragments of this datagram to the device that receives the first fragment for VFR.

This feature is applicable to devices enabled with IPv4 VFR on an HA network.

For more information about HA networking, see high availability group configuration in *High Availability Configuration Guide*.

Examples

Enable fragment centralization for IPv4 VFR.

```
<Sysname> system-view
[Sysname] ip virtual-reassembly centralize
```

Related commands

undo ip virtual-reassembly suppress

ip virtual-reassembly enable

Use **ip virtual-reassembly enable** to enable IPv4 virtual fragment reassembly (VFR).

Use **undo ip virtual-reassembly enable** to disable IPv4 virtual fragment reassembly.

Syntax

ip virtual-reassembly enable

undo ip virtual-reassembly enable

Default

IPv4 virtual fragment reassembly is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

To prevent each service module from processing packet fragments that do not arrive in order, you can enable the virtual fragment reassembly feature. This feature virtually reassembles the fragments of a datagram through fragment check, sequencing, and caching, ensuring fragments arrive at each service module in order.

VFR can detect and prevent the following types of attacks:

- **Tiny fragment attack**—The first fragment size is too small to hold the Layer 4 (such as TCP and UDP) header field, which is forced into the second fragment. VFR discards all tiny fragments.
- **Overlapping fragment attack**—Two consecutive incoming fragments are identical or overlap with each other. If an overlapping fragment is detected, VFR discards all fragments within a fragment chain.
- **Fragment flooding attack**—The maximum number of concurrent preassemblies or the number of fragments per datagram exceeds the upper limits. VFR discards subsequent fragments if the upper limit is reached.

The enabling status of VFR can be managed at CLI or the enabling status of a service module that can call VFR. VRF is enabled in either of the following conditions:

- A service module that can call it is enabled.
- The **ip virtual-reassembly enable** command is executed.

If fragment reassembly is required, but a service module cannot call it, execute this command at CLI.

Examples

Enable IPv4 virtual fragment reassembly

```
<Sysname> system-view
[Sysname] ip virtual-reassembly enable
```

ip virtual-reassembly suppress

Use **ip virtual-reassembly suppress** to forcibly disable IPv4 VFR.

Use **undo ip virtual-reassembly suppress** to restore the default.

Syntax

ip virtual-reassembly suppress

undo ip virtual-reassembly suppress

Default

Forcibly disabling IPv4 VFR is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

IMPORTANT:

Use this feature according to the demands of VFR.

IPv4 VFR checks, sequences, and caches fragments upon fragment receiving to ensure that these fragments will be assembled in the correct order. By default, IPv4 VFR is enabled.

On an HA network, if an HA device does not receive all fragments of a datagram, it cannot reassemble the datagram and will discard the received fragments. For the device to permit the received fragments to pass, you can forcibly disable IPv4 VFR.

After you enable VFR through service calling or CLI, you can use the **ip virtual-reassembly suppress** command to forcibly disable VFR.

With IPv4 VFR forcibly disabled, ASPF and connection limit do not take effect on the received IPv4 fragments and the fragments will be forwarded directly.

For more information about HA networking, see high availability group configuration in *High Availability Configuration Guide*.

Examples

Forcibly disable IPv4 VFR.

```
<Sysname> system-view
[Sysname] ip virtual-reassembly suppress
```

ipv6 virtual-reassembly centralize

Use **ipv6 virtual-reassembly centralize** to enable fragment centralization for IPv6 VFR.

Use **undo ipv6 virtual-reassembly centralize** to disable fragment centralization for IPv6 VFR.

Syntax

ipv6 virtual-reassembly centralize

undo ipv6 virtual-reassembly centralize

Default

Fragment centralization is disabled for IPv6 VFR.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

On an HA network, if an HA device enabled with IPv6 VFR does not receive all fragments of a datagram, it cannot reassemble the datagram and will discard all the received fragments. To resolve this issue, you can enable this feature. Devices that do not receive the first fragment of a datagram forward the received fragments of this datagram to the device that receives the first fragment for VFR.

This feature is applicable to devices enabled with IPv6 VFR on an HA network.

For more information about HA networking, see high availability group configuration in *High Availability Configuration Guide*.

Examples

Enable fragment centralization for IPv6 VFR.

```
<Sysname> system-view
[Sysname] ipv6 virtual-reassembly centralize
```

ipv6 virtual-reassembly suppress

Use **ipv6 virtual-reassembly suppress** to forcibly disable IPv6 VFR.

Use **undo ipv6 virtual-reassembly suppress** to restore the default.

Syntax

ipv6 virtual-reassembly suppress

undo ipv6 virtual-reassembly suppress

Default

Forcibly disabling IPv6 VFR is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

IMPORTANT:

Use this feature according to the demands of VFR.

IPv6 VFR checks, sequences, and caches fragments upon fragment receiving to ensure that these fragments will be assembled in the correct order. By default, IPv6 VFR is enabled.

In an HA network, if an HA device does not receive all fragments of a datagram, it cannot reassemble the datagram and will discard the received fragments. For the devices to permit the received fragments to pass, you can forcibly disable IPv6 VFR.

With IPv6 VFR disabled forcibly, ASPF and connection limit do not take effect on the received IPv6 fragments and the fragments will be forwarded directly.

For more information about HA networking, see high availability group configuration in *High Availability Configuration Guide*.

Examples

Forcibly disable IPv6 VFR.

```
<Sysname> system-view
```

```
[Sysname] ipv6 virtual-reassembly suppress
```

reset ip statistics

Use **reset ip statistics** to clear IP traffic statistics.

Syntax

reset ip statistics [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears IP traffic statistics for all member devices.

Usage guidelines

Use this command to clear history IP traffic statistics before you collect IP traffic statistics for a time period.

Examples

Clear IP traffic statistics.

```
<Sysname> reset ip statistics
```

Related commands

display ip interface

display ip statistics

reset tcp statistics

Use **reset tcp statistics** to clear TCP traffic statistics.

Syntax

reset tcp statistics

Views

User view

Predefined user roles

network-admin

context-admin

Examples

Clear TCP traffic statistics.

```
<Sysname> reset tcp statistics
```

Related commands

display tcp statistics

reset udp statistics

Use **reset udp statistics** to clear UDP traffic statistics.

Syntax

reset udp statistics

Views

User view

Predefined user roles

network-admin

context-admin

Examples

Clear UDP traffic statistics.

```
<Sysname> reset udp statistics
```

Related commands

display udp statistics

tcp mss

Use **tcp mss** to set the TCP maximum segment size (MSS).

Use **undo tcp mss** to restore the default.

Syntax

tcp mss *value*

undo tcp mss

Default

The TCP MSS is not set.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

value: Specifies the TCP MSS in bytes. The minimum value is 128 bytes. The maximum value equals the maximum MTU that the interface supports minus 40.

Usage guidelines

The MSS option informs the receiver of the largest segment that the sender can accept. Each end announces its MSS during TCP connection establishment. If the size of a TCP segment is smaller than the MSS of the receiver, TCP sends the TCP segment without fragmentation. If not, TCP fragments the segment according to the receiver's MSS.

If you set the TCP MSS on an interface, the size of each TCP segment received or sent on the interface cannot exceed the MSS value.

This configuration takes effect only on TCP connections that are established after the configuration and not on the TCP connections that already exist.

This configuration is effective only on IP packets.

Examples

Set the TCP MSS to 300 bytes on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] tcp mss 300
```

tcp path-mtu-discovery

Use **tcp path-mtu-discovery** to enable TCP path MTU discovery.

Use **undo tcp path-mtu-discovery** to disable TCP path MTU discovery.

Syntax

tcp path-mtu-discovery [**aging** *age-time* | **no-aging**]

undo tcp path-mtu-discovery

Default

TCP path MTU discovery is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

aging *age-time*: Specifies the aging time for the path MTU, in the range of 10 to 30 minutes. The default aging time is 10 minutes.

no-aging: Does not age out the path MTU.

Usage guidelines

After you enable TCP path MTU discovery, all new TCP connections detect the path MTU. The device uses the path MTU to calculate the MSS to avoid IP fragmentation.

After you disable TCP path MTU discovery, the system stops all path MTU timers. The TCP connections established later do not detect the path MTU, but the TCP connections previously established still can detect the path MTU.

Examples

Enable TCP path MTU discovery and set the path MTU aging time to 20 minutes.

```
<Sysname> system-view
[Sysname] tcp path-mtu-discovery aging 20
```

tcp syn-cookie enable

Use **tcp syn-cookie enable** to enable SYN Cookie to protect the device from SYN flood attacks.

Use **undo tcp syn-cookie enable** to disable SYN Cookie.

Syntax

tcp syn-cookie enable

undo tcp syn-cookie enable

Default

SYN Cookie is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

A TCP connection is established through a three-way handshake:

1. The sender sends a SYN packet to the server.
2. The server receives the SYN packet, establishes a TCP semi-connection in SYN_RECEIVED state, and replies with a SYN ACK packet to the sender.
3. The sender receives the SYN ACK packet and replies with an ACK packet. Then, a TCP connection is established.

An attacker can exploit this mechanism to mount SYN flood attacks. The attacker sends a large number of SYN packets, but they do not respond to the SYN ACK packets from the server. As a result, the server establishes a large number of TCP semi-connections and cannot handle normal services.

SYN Cookie can protect the server from SYN flood attacks. When the server receives a SYN packet, it responds to the request with a SYN ACK packet without establishing a TCP semi-connection.

The server establishes a TCP connection and enters ESTABLISHED state only when it receives an ACK packet from the sender.

Examples

Enable SYN Cookie.

```
<Sysname> system-view
[Sysname] tcp syn-cookie enable
```

tcp timer fin-timeout

Use **tcp timer fin-timeout** to set the TCP FIN wait timer.

Use **undo tcp timer fin-timeout** to restore the default.

Syntax

tcp timer fin-timeout *time-value*

undo tcp timer fin-timeout

Default

The TCP FIN wait timer is 675 seconds.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

time-value: Specifies the TCP FIN wait timer in the range of 76 to 3600 seconds.

Usage guidelines

TCP starts the FIN wait timer when the state of a TCP connection changes to FIN_WAIT_2. If no FIN packet is received within the timer interval, the TCP connection is terminated.

If a FIN packet is received, TCP changes the connection state to TIME_WAIT. If a non-FIN packet is received, TCP restarts the timer and tears down the connection when the timer expires.

Examples

Set the TCP FIN wait timer to 800 seconds.

```
<Sysname> system-view
[Sysname] tcp timer fin-timeout 800
```

tcp timer syn-timeout

Use **tcp timer syn-timeout** to set the TCP SYN wait timer.

Use **undo tcp timer syn-timeout** to restore the default.

Syntax

tcp timer syn-timeout *time-value*

undo tcp timer syn-timeout

Default

The TCP SYN wait timer is 75 seconds.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

time-value: Specifies the TCP SYN wait timer in the range of 2 to 600 seconds.

Usage guidelines

TCP starts the SYN wait timer after sending a SYN packet. Within the SYN wait timer if no response is received or the upper limit on TCP connection tries is reached, TCP fails to establish the connection.

Examples

Set the TCP SYN wait timer to 80 seconds.

```
<Sysname> system-view
[Sysname] tcp timer syn-timeout 80
```

tcp timestamps enable

Use **tcp timestamps enable** to enable carrying the TCP timestamp option in outgoing TCP packets.

Use **undo tcp timestamps enable** to disable carrying the TCP timestamp option in outgoing TCP packets.

Syntax

tcp timestamps enable

undo tcp timestamps enable

Default

The device adds the TCP timestamp option in outgoing TCP packets.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

The TCP timestamp option in TCP packets is used to calculate the RTT between two communicating devices. In some networks, it is required to prevent the intermediate devices from obtaining the TCP timestamps in packets passing through. Then you can disable carrying the TCP timestamp option in outgoing packets on a device at either end.

This command takes effect on TCP connections established only after the execution of the command.

Examples

Enable carrying the TCP timestamp option in outgoing TCP packets.

```
<Sysname> system-view
[Sysname] undo tcp timestamps enable
```

tcp window

Use **tcp window** to set the size of the TCP receive/send buffer.

Use **undo tcp window** to restore the default.

Syntax

tcp window *window-size*

undo tcp window

Default

The size of the TCP receive/send buffer is 63 KB.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

window-size: Specifies the size of the TCP receive/send buffer, in the range of 1 to 64 KB.

Examples

Set the size of the TCP receive/send buffer to 3 KB.

```
<Sysname> system-view
[Sysname] tcp window 3
```

Contents

Multi-CPU packet distribution commands

forwarding policy

Use **forwarding policy** to specify a multi-CPU packet distribution policy.

Use **undo forwarding policy** to restore the default.

Syntax

forwarding policy { **per-flow** [**three-tuple | mode { source-ip | destination-ip | source-port | destination-port }**] | **per-packet** }

undo forwarding policy

Default

The device uses the flow-based policy that identifies a flow by source IP address, destination IP address, source port number, destination port number, and protocol number.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

per-flow: Specifies the flow-based forwarding. The device identifies a data flow by the five-tuple, and forwards packets of the same flow to one CPU. The CPU processes flow packets by following the first-in first-out rule.

three-tuple: Identifies a data flow by the three-tuple (source IP address, destination IP address, and protocol number). If you do not specify this keyword, the device identifies a data flow by the five-tuple.

The following compatibility matrixes show the support of hardware platforms for the **three-tuple** keyword:

Models	Parameter compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	No

mode: Specifies a flow-based forwarding mode.

source-ip: Identifies a flow by source IP address.

destination-ip: Identifies a flow by destination IP address.

source-port: Identifies a flow by source port.

destination-port: Identifies a flow by destination port.

per-packet: Specifies the packet-based forwarding. The device forwards packets in sequence to different CPUs, even though they are the same flow. This policy does not ensure packet order.

Usage guidelines

If you do not specify any keyword for flow identification, the device identifies a flow by source IP address, destination IP address, source port number, destination port number, and protocol number.

Examples

Specify the flow-based policy.

```
<Sysname> system-view
[Sysname] forwarding policy per-flow
```

Contents

Adjacency table commands

IPv4 adjacency table commands

display adjacent-table

Use **display adjacent-table** to display IPv4 adjacency entries.

Syntax

display adjacent-table { **all** | **physical-interface** *interface-type interface-number* | **routing-interface** *interface-type interface-number* | **slot** *slot-number* } [**count** | **verbose**]

View

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

all: Displays all IPv4 adjacency entries.

physical-interface *interface-type interface-number*: Displays IPv4 adjacency entries about the specified physical interface.

routing-interface *interface-type interface-number*: Displays IPv4 adjacency entries about the specified routing interface.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv4 adjacency entries for all member devices.

count: Displays the number of IPv4 adjacency entries.

verbose: Displays detailed information about IPv4 adjacency entries.

Examples

Display detailed information about all IPv4 adjacency entries.

```
<Sysname> display adjacent-table all verbose
   IP address                      : 0.0.0.0
   Routing interface               : Tunnel1
   Physical interface              : Tunnel1
   Logical interface               : N/A
   Service type                    : Tunnel
   Action type                     : Forwarding
   Link media type                 : P2P
   Slot                            : 0
   Cpu                             : 0
   VPN index                       : 0
```

```
  Virtual circuit information   : N/A
  Link head information(IP)      : 450000000000000ff2f0000020202010202020200000
                                   0800
  Link head information(MPLS)    : 450000000000000ff2f0000020202010202020200000
                                   0800
```

Display IPv4 adjacency entries for the specified slot.

```
<Sysname> display adjacent-table slot 1
IP address        Routing interface         Physical interface      Type
0.0.0.0           Tun1                         Tun1                       Tunnel
```

Display the number of IPv4 adjacency entries for the specified slot.

```
<Sysname> display adjacent-table slot 1 count
 Total entries on slot 1: 1
```

Table 1 Command output

Field	Description
IP address	IP address of the next hop. • For a P2P link, the IP address of the next hop is not needed. This field displays **0.0.0.0**. • For an NBMA link, the value 0.0.0.0 indicates the default adjacency entry. Packets are forwarded through the default virtual circuit.
Routing interface	Output interface of the matching route entry.
Physical interface	Physical interface of which the outgoing packets are sent out.
Logical interface	Logical interface for sending the packets. If the entry has no logical interface, this field displays **N/A**.
Service type/Type	Link layer protocol type.
Action type	Packet processing type, **Forwarding** or **Drop**.
Link media type	Link media type: • **P2P**—Point-to-point link. • **NBMA**—Non-broadcast multi-access link.
Cpu	This field is not supported in the current software version. Number of the CPU.
VPN index	Index of the VPN.
Virtual circuit information	Information about the virtual circuit, such as PVC or DLCI. If the entry has no virtual circuit, this field displays **N/A**.
Link head information(IP)	Link layer header for IPv4.
Link head information(MPLS)	This field is not supported in the current software version. Link layer header for MPLS.

IPv6 adjacency table commands

display ipv6 adjacent-table

Use **display ipv6 adjacent-table** to display IPv6 adjacency entries.

Syntax

display ipv6 adjacent-table { **all** | **physical-interface** *interface-type interface-number* | **routing-interface** *interface-type interface-number* | **slot** *slot-number* } [**count** | **verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

all: Displays all IPv6 adjacency entries.

physical-interface *interface-type interface-number*: Displays IPv6 adjacency entries about the specified physical interface.

routing-interface *interface-type interface-number*: Displays IPv6 adjacency entries about the specified routing interface.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv6 adjacency entries for all member devices.

count: Displays the number of IPv6 adjacency entries.

verbose: Displays detailed information about IPv6 adjacency entries.

Examples

Display detailed information about all IPv6 adjacency entries.

```
<Sysname> display ipv6 adjacent-table all verbose
   IPv6 address                    : N/A
   Routing interface               : Tunnel1
   Physical interface              : Tunnel1
   Logical interface               : N/A
   Service type                     : Tunnel
   Action type                      : Forwarding
   Link media type                 : P2P
   Slot                              : 1
   Cpu                               : 0
   VPN index                         : 0
   Virtual circuit information   : N/A
   Link head information(IPv6)   : 450000000000000ff2f000002020201020202020000
                                   86dd
   Link head information(MPLS)   : 450000000000000ff2f000002020201020202020000
```

```
                                    86dd
```

Display IPv6 adjacency entries for the specified slot.

```
<Sysname> display ipv6 adjacent-table slot 1
IPv6 address          Routing interface     Physical interface    Type
N/A                     Tun1                     Tun1                    Tunnel
```

Display the number of IPv6 adjacency entries for the specified slot.

```
<Sysname> display ipv6 adjacent-table slot 1 count
 Total entries on slot 1: 1
```

Table 2 Command output

Field	Description
IPv6 address	IPv6 address of the next hop. • For a P2P link, the IPv6 address of the next hop is not needed. This field has the value 0::0, and displays **N/A**. • For an NBMA link, the value 0.0.0.0 indicates a default adjacency table. Packets are forwarded through the default virtual circuit.
Routing interface	Output interface of the matching route entry.
Physical interface	Physical interface of which the outgoing packets are sent out.
Logical interface	Logical interface that sends the packets. If the entry has no logical interface, this field displays **N/A**.
Service type/Type	Link layer protocol type.
Action type	Packet processing type, **Forwarding** or **Drop**.
Link media type	Link media type: • **P2P**—Point-to-point link. • **NBMA**—Non-broadcast multi-access link.
Cpu	This field is not supported in the current software version. Number of the CPU.
VPN index	Index of the VPN.
Virtual circuit information	Information about the virtual circuit, such as PVC or DLCI. If the entry has no virtual circuit, this field displays **N/A**.
Link head information(IPv6)	Link layer header for IPv6.
Link head information(MPLS)	This field is not supported in the current software version. Link layer header for MPLS.

Contents

Web caching commands

Web caching is supported only in RXX60P20 and later.

backup

Use **backup** to specify a backup Web caching slot.

Use **undo backup** to restore the default.

Syntax

backup slot *slot-number*

undo backup

Default

No backup Web caching slot is specified.

Views

Web cache view

Predefined user roles

network-admin

context-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID.

Usage guidelines

To enhance the high availability of Web caching, configure the Web cache backup feature. You can use this command to specify a backup Web caching slot. When the primary slot (specified by using the **web-cache** command) fails, the backup slot will take over to provide the Web caching service to ensure service continuity. When the primary slot recovers, the Web caching service switches back to the primary slot.

Examples

Specify slot 1 as the backup Web caching slot.

```
<Sysname> system-view
[Sysname] web-cache slot 1
[Sysname-web-cache-slot1] backup slot 2
```

cached-data

Use **cached-data** to specify the types of the webpage files to be cached.

Use **undo cached-data** to restore the default.

Syntax

cached-data { **apk** | **bmp** | **doc** | **docx** | **gif** | **gzip** | **ipa** | **jar** | **jpg** | **jpeg** | **mp4** | **pdf** | **png** | **ppt** | **pptx** | **rar** | **swf** | **tar** | **txt** | **xls** | **xlsx** | **zip** } *

undo cached-data

Default

No webpage file types are specified.

Views

Web cache view

Predefined user roles

network-admin

context-admin

Parameters

`apk`: Specifies .apk files.

`bmp`: Specifies .bmp files.

`doc`: Specifies .doc files.

`docx`: Specifies .docx files.

`gif`: Specifies .gif files.

`gzip`: Specifies .gzip files.

`ipa`: Specifies .ipa files.

`jar`: Specifies .jar files.

`jpg`: Specifies .jpg files.

`jpeg`: Specifies .jpeg files.

`mp4`: Specifies .mp4 files.

`pdf`: Specifies .pdf files.

`png`: Specifies .png files.

`ppt`: Specifies .ppt files.

`pptx`: Specifies .pptx files.

`rar`: Specifies .rar files.

`swf`: Specifies .swf files.

`tar`: Specifies .tar files.

`txt`: Specifies .txt files.

`xls`: Specifies .xls files.

`xlsx`: Specifies .xlsx files.

`zip`: Specifies .zip files.

Usage guidelines

If you do not specify the types of the webpage files to be cached, the Web caching feature does not cache any types of files on webpages.

Execute this command before enabling Web caching.

Before configuring or modifying file type settings, you must disable Web caching. After configuring or modifying file type settings, enable Web caching again.

Execution of the **`undo cached-data`** command will not delete webpage files saved in the Web cache directory. The Web caching feature can still cache webpage files specified by using the **`cached-file`** command.

Examples

Configure the Web caching feature to cache .doc and .docx files on webpages.

```
<Sysname> system-view
[Sysname] web-cache slot 1
[Sysname-web-cache-slot1] cached-data doc docx
```

Related commands

http enable

https enable

cached-file

Use **cached-file** to specify a webpage file to be cached.

Use **undo cached-file** to remove a webpage file to be cached.

Syntax

cached-file *file-name*

undo cached-file [*file-name*]

Default

No webpage files can be cached.

Views

Web cache view

Predefined user roles

network-admin

context-admin

Parameters

file-name: Specifies a webpage file by its name, a case-sensitive string of 1 to 127 characters.

Usage guidelines

You can repeat this command to specify multiple webpage files to be cached.

If you specify both webpage files and types of the webpage files to be cached, the device caches the matching webpage files of the specified types.

Before you add or delete a webpage file to be cached, you must disable Web caching. After adding or deleting the webpage file, enable Web caching again.

Execution of the **undo cached-data** command will not delete webpage files saved in the Web cache directory.

Examples

Specify file **test1.doc** as a webpage file to be cached.

```
<Sysname> system-view
[Sysname] web-cache slot 1
[Sysname-web-cache-slot1] cached-file test1.doc
```

Related commands

cached-data

cache-limit

Use **cache-limit** to set the maximum total size for Web cache files.

Use **undo cache-limit** to restore the default.

Syntax

cache-limit *size*

undo cache-limit

Default

The maximum total size of Web cache files is 4 GB.

Views

Web cache view

Predefined user roles

network-admin

context-admin

Parameters

size: Specifies the maximum total size for Web cache files in GB. The value range is 1 to 4095. The default is 4.

Usage guidelines

Before changing the maximum total file size setting, you must disable Web caching. After changing the maximum total file size setting, enable Web caching again.

The maximum total size for Web cache files must be smaller than the maximum storage space size in the working directory. To display the maximum size of storage space in the working directory, execute the **display web-cache** command. After the effective maximum total size is reached, the device deletes the oldest Web cache file to save the new Web cache file.

The aging time for Web cache files is fixed at 30 days. When the device reboots or receives a request for the content in a Web cache file, it restarts the aging timer. If no users request the content in a file before the aging timer expires, the device deletes the file.

Examples

Set the maximum total size for Web cache files to 3 GB.

```
<Sysname> system-view
[Sysname] web-cache slot 1
[Sysname-web-cache-slot1] cache-limit 3
```

display web-cache

Use **display web-cache** to display Web caching information.

Syntax

display web-cache [**history** [**last** { **day** | **30-days** | **365-days** | **hour** | **minute** | **week** } | **verbose**]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

history: Displays history information. If you specify this keyword but do not specify any following keywords, the command displays the current statistics, which is collected at 1-second intervals. If you do not specify this keyword, the command displays Web cache configuration and statistics for the most recent time ranges.

last: Displays statistics for a specific period of time in the past.

minute: Displays statistics for the most recent one minute.

hour: Displays statistics for the most recent one hour.

day: Displays statistics for the most recent one day.

week: Displays statistics for the most recent one week.

30-days: Displays statistics for the most recent 30 days.

365-days: Displays statistics for the most recent 365 days.

verbose: Displays detailed information. If you do not specify this keyword, the command displays brief information.

Examples

Display the current Web caching statistics.

```
<Sysname> display web-cache history
Date TimeRange ConnectTop CacheTop BandwidthSaved CacheHitRate
2018/06/20 14:43:02-14:43:03 3 16.0KB 0 0%
2018/06/20 14:43:01-14:43:02 3 16.0KB 96.0Kbps 100%
```

Display all Web caching information.

```
<Sysname> display web-cache
Web-cache configurations
  Cache path: flash:/var/web-cache/proxy/cache
  Max connections: 1022
  Max cache size: 3GB

Current state information
  Cache memory: 0
  Cache count: 0

Statistics for past 1 minute
  ConnectTop: 2
  CacheTop: 0
  Bandwidth saved:                      0
  Cached data transmission speed:       0
  Cached data transmitted:              0
  Download speed:                       0
  Download size:                        0
```

```
  CacheHitRate: 0%
    Hit count: 0                    Miss count: 0

Statistics for past 1 hour
  ConnectTop: 2
  CacheTop: 0
  Bandwidth saved:                      0
  Cached data transmission speed:       0
  Cached data transmitted:              0
  Download speed:                       0
  Download size:                        0
  CacheHitRate: 0%
    Hit count: 0                    Miss count: 0

Statistics for past 1 day
  ConnectTop: 2
  CacheTop: 463.4MB
  Bandwidth saved:                      0
  Cached data transmission speed:       0
  Cached data transmitted:              0
  Download speed:                       0
  Download size:                        0
  CacheHitRate: 0%
    Hit count: 0                    Miss count: 0

Statistics for past 30 days
  ConnectTop: 2
  CacheTop: 463.4MB
  Bandwidth saved:                      0
  Cached data transmission speed:       0
  Cached data transmitted:              0
  Download speed:                       0
  Download size:                        0
  CacheHitRate: 0%
    Hit count: 0                    Miss count: 0

Statistics for past 365 days
  ConnectTop: 2
  CacheTop: 463.4MB
  Bandwidth saved:                      0
  Cached data transmission speed:       120 Kbps
  Cached data transmitted:              400MB
  Download speed:                       0
  Download size:                        0
  CacheHitRate: 0%
Hit count: 0                    Miss count: 0
```

Display detailed current Web caching statistics.

```
<Sysname> display web-cache history verbose
```

```
2018/06/05 09:02:47-09:02:48
  ConnectTop: 2
  CacheTop: 0
  Bandwidth saved:                        0
  Cached data transmission speed:         0
  Cached data transmitted:                0
  Download speed:                         0
  Download size:                          0
  CacheHitRate: 0%
    Hit count: 0                     Miss count: 0

2018/06/05 09:02:46-09:02:47
  ConnectTop: 2
  CacheTop: 0
  Bandwidth saved:                        0
  Cached data transmission speed:         0
  Cached data transmitted:                0
  Download speed:                         0
  Download size:                          0
  CacheHitRate: 0%
    Hit count: 0                     Miss count: 0
```

Table 1 Command output

Field	Description
Cache path	Web cache directory.
Max connections	Maximum number of connections allowed.
Max cache size	Current maximum storage space size.
Cache memory	Current total size of Web cache files.
Cache count	Number of Web cache files.
Statistics for past 1 minute	Web caching statistics for the most recent one minute.
Statistics for past 1 hour	Web caching statistics for the most recent one hour.
Statistics for past 1 day	Web caching statistics for the most recent one day.
Statistics for past 30 days	Web caching statistics for the most recent 30 days.
Statistics for past 365 days	Web caching statistics for the most recent 365 days.
ConnectTop	Maximum number of connections during the specified period of time.
CacheTop	Maximum total size of Web cache files during the specified period of time, in KB, MB, GB, or TB.
Bandwidth saved	Bandwidth saved during the specified period of time, in Kbps, Mbps, Gbps, or Tbps.
Cached data transmission speed	Speed at which cached data was transferred to users during the specified period of time, in Kbps, Mbps, Gbps, or Tbps.
Cached data transmitted	Amount of cached data that was transferred to users during the specified period of time, in KB, MB, GB, or TB.
Download speed	Speed at which cached data was downloaded from Web servers during the specified period of time, in Kbps, Mbps, Gbps, or Tbps.

Field	Description
Download size	Amount of cached data that was downloaded from Web servers during the specified period of time, in KB, MB, GB, or TB.
CacheHitRate	Percentage of hits of cached data.
Hit count	Number of hits of cached data.
Miss count	Number of times that cached data was not matched.

file-directory

Use **file-directory** to set the primary Web cache directory.

Use **undo file-directory** to restore the default.

Syntax

file-directory *directory*

undo file-directory

Default

The primary Web cache directory is not set.

Views

Web cache view

Predefined user roles

network-admin

context-admin

Parameters

directory: Specifies the primary Web cache directory, starting from the storage medium location information **slot***n*#. The slot number *n* must be the same as the slot number of the Web cache view.

Usage guidelines

Before changing the Web cache directory, you must disable Web caching. After changing the Web cache directory, enable Web caching again.

Make sure the storage medium where the Web cache directory resides has sufficient storage space. The Web caching feature saves its operation data and the Web content to be cached to files in the directory. The directory typically needs a storage space of over 1 GB.

Before specifying a Web cache directory, make sure all files in the upper-level directory are using a different name than the Web cache directory or have a file extension. For example, if you want to specify **flash:/web-cache** as the Web cache directory, files without a file extension in the **flash:** directory cannot use **web-cache** as the file name.

The primary Web cache directory for a Web cache view must reside on the same slot as the Web view.

Examples

Set the primary Web cache directory.

```
<Sysname> system-view
[Sysname] web-cache slot 1
[Sysname-web-cache-slot1] file-directory slot1#flash:/aaa
```

file-directory backup

Use **file-directory backup** to set the backup Web cache directory.

Use **undo file-directory backup** to restore the default.

Syntax

file-directory backup *directory*

undo file-directory backup

Default

No backup Web cache directory is set.

Views

Web cache view

Predefined user roles

network-admin

context-admin

Parameters

directory: Specifies the backup Web cache directory, starting from the storage medium location information **slot***n*#. The slot number *n* must be the same as the slot number of the Web cache view.

Usage guidelines

To implement Web cache backup, use this command to specify the backup Web cache directory. When the device uses the primary slot for Web caching, it saves webpage files to the primary Web cache directory. When the device uses the backup Web caching slot, it saves webpage files to the backup Web cache directory.

Make sure the storage medium where the Web cache directory resides has sufficient storage space. The Web caching feature saves its operation data and the Web content to be cached to files in the directory. The directory typically needs a storage space of over 1 GB.

The backup Web cache directory for a Web cache view must reside on the backup slot. After the backup Web cache directory is created, the device will not synchronize cache files under the primary directory to the backup directory.

Before specifying a Web cache directory, make sure all files in the upper-level directory are using a different name than the Web cache directory or have a file extension. For example, if you want to specify **flash:/web-cache** as the Web cache directory, files without a file extension in the **flash:** directory cannot use **web-cache** as the file name.

Before changing the Web cache directory, you must disable Web caching. After changing the Web cache directory, enable Web caching again.

You must specify a directory on the slot same as the backup Web caching slot specified by using the **backup** command.

Examples

Set the backup Web cache directory.

```
<Sysname> system-view
[Sysname] web-cache slot 1
[Sysname-web-cache-slot1] file-directory backup slot4#flash:/webcache
```

Related commands

backup

http enable

Use **http enable** to enable HTTP-based Web caching.

Use **undo http enable** to disable HTTP-based Web caching.

Syntax

http enable

undo http enable

Default

HTTP-based Web caching is disabled.

Views

Web cache view

Predefined user roles

network-admin

context-admin

Usage guidelines

Before enabling HTTP-based Web caching, you must configure the types of the webpage files to be cached and the Web cache directory.

Examples

Enable HTTP-based Web caching.

```
<Sysname> system-view
[Sysname] web-cache slot 1
[Sysname-web-cache-slot1] http enable
```

Related commands

cached-data

file-directory

listen-port

https enable

Use **https enable** to enable HTTPS-based Web caching.

Use **undo https enable** to disable HTTP-based Web caching.

Syntax

https enable

undo https enable

Default

HTTPS-based Web caching is disabled.

Views

Web cache view

Predefined user roles

network-admin

context-admin

Usage guidelines

Before enabling HTTPS-based Web caching, you must configure the types of the webpage files to be cached and the Web cache directory.

Examples

Enable HTTPS-based Web caching.

```
<Sysname> system-view
[Sysname] web-cache slot 1
[Sysname-web-cache-slot1] https enable
```

Related commands

file-directory

cached-data

https listen-port

Use **https listen-port** to set the port number for Web caching to listen for HTTPS packets.

Use **undo https listen-port** to restore the default.

Syntax

https listen-port *port-number*

undo https listen-port

Default

Web caching listens to port 443 for HTTPS packets.

Views

Web cache view

Predefined user roles

network-admin

context-admin

Parameters

port-number: Specifies a TCP port number in the range of 1 to 65535.

Usage guidelines

Make sure the specified TCP port number is not being used by any other services on the device. To display TCP port numbers in use, execute the **display tcp verbose** command.

Before changing the listening port setting, you must disable Web caching. After changing the listening port setting, enable Web caching again.

Examples

Set the port number to 655 for Web caching to listen for HTTPS packets.

```
<Sysname> system-view
[Sysname] web-cache slot 1
[Sysname-web-cache-slot1] https listen-port 655
```

Related commands

https enable

listen-port

Use **listen-port** to set the port number for Web caching to listen for HTTP packets.

Use **undo listen-port** to restore the default.

Syntax

listen-port *port-number*

undo listen-port

Default

Web caching listens to port 80 for HTTP packets.

Views

Web cache view

Predefined user roles

network-admin

context-admin

Parameters

port-number: Specifies a TCP port number in the range of 1 to 65535.

Usage guidelines

Make sure the specified TCP port number is not being used by any other services on the device. To display TCP port numbers in use, execute the **display tcp verbose** command.

Before changing the listening port setting, you must disable Web caching. After changing the listening port setting, enable Web caching again.

Examples

Set the port number to 655 for Web caching to listen for HTTP packets.

```
<Sysname> system-view
[Sysname] web-cache slot 1
[Sysname-web-cache-slot1] listen-port 655
```

Related commands

http enable

object-group

Use **object-group** to specify an IPv4 object group used to filter Web content to be cached.

Use **undo object-group** to remove an IPv4 object group used to filter Web content to be cached.

Syntax

object-group [**source**] **ip** *object-group-name*

undo object-group [**source**]

Default

No IPv4 object group is specified for filtering Web content. The Web caching feature caches webpage content from all Web servers.

Views

Web cache view

Predefined user roles

network-admin

context-admin

Parameters

source: Caches Web content requested by specific Web clients. If you do not specify this keyword, the Web caching feature caches Web content from specific Web servers.

ip: Uses an IPv4 object group to specify Web clients or Web servers. For more information about IPv4 object groups, see *Security Configuration Guide*.

object-group-name: Specifies an IPv4 object group by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

Use this command to configure the Web caching feature to cache only Web content requested by specific Web clients or sent from specific Web servers.

This command requires the cooperation of the IPv4 object group feature. For more information about the IPv4 object group feature, see object group configuration in *Security Configuration Guide*.

Execute this command before enabling Web caching.

Before changing the IPv4 object group setting, you must disable Web caching. After changing the IPv4 object group setting, enable Web caching again.

Examples

Configure the Web caching feature to cache only Web content from Web servers specified by IPv4 object group **aaa**.

```
<Sysname> system-view
[Sysname] web-cache slot 1
[Sysname-web-cache-slot1] object-group ip aaa
```

Related commands

object-group (*Security Command Reference*)

web-cache

Use **web-cache** to create a Web cache view and enter its view, or enter an existing Web cache view.

Use **undo web-cache** to delete a Web cache view and all settings in the view.

Syntax

web-cache slot *slot-number*

undo web-cache slot

Default

No Web cache views exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID.

Examples

Create a Web cache view and enter its view.

```
<Sysname> system-view
[Sysname] web-cache slot 1
[Sysname-web-cache-slot1]
```

NSFOCUS Firewall Series

NF Layer 3—IP Routing

Command Reference

NSFOCUS Technologies, Inc.

Document version: 6W600-20230221

Preface

This command reference describes the commands for configuring routing protocols, including basic IP routing, static routing, RIP, OSPF, IS-IS, BGP, policy-based routing, IPv6 static routing, IPv6 policy-based routing, RIPng, OSPFv3, Guard route , RIR and routing policies.

This preface includes the following topics about the documentation:

- Audience.
- Conventions.

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators.

Conventions

The following information describes the conventions used in the documentation.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select a minimum of one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
CAUTION:	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Contents

Basic IP routing commands

address-family ipv4

Use **address-family ipv4** to create the RIB IPv4 address family and enter its view, or enter the view of the existing RIB IPv4 address family.

Use **undo address-family ipv4** to delete the RIB IPv4 address family and all settings in the view.

Syntax

address-family ipv4

undo address-family ipv4

Default

No RIB IPv4 address family exists.

Views

RIB view

Predefined user roles

network-admin

context-admin

Examples

Create the RIB IPv4 address family and enter its view.

```
<Sysname> system-view
[Sysname] rib
[Sysname-rib] address-family ipv4
[Sysname-rib-ipv4]
```

address-family ipv6

Use **address-family ipv6** to create the RIB IPv6 address family and enter its view, or enter the view of the existing RIB IPv6 address family.

Use **undo address-family ipv6** to delete the RIB IPv6 address family and all settings in the view.

Syntax

address-family ipv6

undo address-family ipv6

Default

No RIB IPv6 address family exists.

Views

RIB view

Predefined user roles

network-admin

context-admin

Examples

Create the RIB IPv6 address family and enter its view.

```
<Sysname> system-view
[Sysname] rib
[Sysname-rib] address-family ipv6
[Sysname-rib-ipv6]
```

display ip routing-table

Use **display ip routing-table** to display routing table information.

Syntax

display ip routing-table [**vpn-instance** *vpn-instance-name*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters.

verbose: Displays detailed routing table information, including information about both active and inactive routes. If you do not specify this keyword, the command displays only brief information about active routes.

Usage guidelines

If you do not specify any parameters, the command displays routing table information for the public network.

Examples

Display brief information about active routes in the routing table.

```
<Sysname> display ip routing-table

Destinations : 10        Routes : 10

Destination/Mask   Proto   Pre Cost        NextHop         Interface
0.0.0.0/32         Direct  0   0           127.0.0.1       InLoop0
1.1.1.1/32         Guard   254 0           0.0.0.0         NULL0
1.1.1.0/24         Static  60  0           192.168.47.4    GE1/0/1
127.0.0.0/8        Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/32       Direct  0   0           127.0.0.1       InLoop0
127.0.0.1/32       Direct  0   0           127.0.0.1       InLoop0
127.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
192.168.1.40/32    Direct  0   0           127.0.0.1       InLoop0
224.0.0.0/4        Direct  0   0           0.0.0.0         NULL0
```

```
224.0.0.0/24       Direct  0   0           0.0.0.0         NULL0
255.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
```

Table 1 Command output

Field	Description
Destinations	Number of destination addresses.
Routes	Number of routes.
Destination/Mask	Destination address/mask length.
Proto	Protocol that installed the route.
Pre	Preference of the route.
Cost	Cost of the route.
NextHop	Next hop address of the route.
Interface	Output interface for packets to be forwarded along the route.
Summary count	Number of routes.

Display detailed information about all routes in the routing table.

```
<Sysname> display ip routing-table verbose

Destinations : 2        Routes : 2

Destination: 0.0.0.0/32
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                  Age: 08h34m37s
       Cost: 0              Preference: 0
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                 State: Active NoAdv
  OrigTblID: 0x0              OrigVrf: default-vrf
    TableID: 0x2               OrigAs: 0
      NibID: 0x10000000        LastAs: 0
     AttrID: 0xffffffff       Neighbor: 0.0.0.0
      Flags: 0x1000c       OrigNextHop: 127.0.0.1
      Label: NULL          RealNextHop: 127.0.0.1
    BkLabel: NULL            BkNextHop: N/A
    SRLabel: NULL            BkSRLabel: NULL
   SIDIndex: NULL              InLabel: NULL
  Tunnel ID: Invalid         Interface: InLoopBack0
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A              VpnPeerId: N/A
       Dscp: N/A                    Exp: N/A

Destination: 1.1.1.0/24
   Protocol: Static
 Process ID: 0
  SubProtID: 0x0                  Age: 04h20m37s
```

```
      Cost: 0              Preference: 60
     IpPre: N/A            QosLocalID: N/A
       Tag: 0                   State: Active Adv
 OrigTblID: 0x0              OrigVrf: default-vrf
   TableID: 0x2               OrigAs: 0
     NibID: 0x10000003        LastAs: 0
    AttrID: 0xffffffff      Neighbor: 0.0.0.0
     Flags: 0x1008c       OrigNextHop: 192.168.47.4
     Label: NULL          RealNextHop: 192.168.47.4
   BkLabel: NULL            BkNextHop: N/A
   SRLabel: NULL            BkSRLabel: NULL
  SIDIndex: NULL              InLabel: NULL
 Tunnel ID: Invalid         Interface: GigabitEthernet1/0/1
BkTunnel ID: Invalid      BkInterface: N/A
  FtnIndex: 0x0          TrafficIndex: N/A
 Connector: N/A             VpnPeerId: N/A
      Dscp: N/A                   Exp: N/A
```

Table 2 Command output

Field	Description
Destinations	Number of destination addresses.
Routes	Number of routes.
Destination	Destination address/mask length.
Protocol	Protocol that installed the route.
SubProtID	ID of the subprotocol for routing.
Age	Time for which the route has been in the routing table.
Cost	Cost of the route.
Preference	Preference of the route.
IpPre	IP precedence.
QosLocalID	Local QoS ID.
Tag	Route tag.
State	Route status: • **Active**—Active unicast route. • **Adv**—Route that can be advertised. • **Inactive**—Inactive route. • **NoAdv**—Route that the router must not advertise. • **Vrrp**—Routes generated by VRRP. This state is not supported in the current software version. • **Nat**—Routes generated by NAT. • **TunE**—Tunnel.
OrigTblID	Original routing table ID.
OrigVrf	Original VPN instance that the route belongs to. This field displays **default-vrf** if the route is on the public network.
TableID	ID of the routing table.
OrigAs	Original AS number.

Field	Description
NibID	ID of the next hop.
LastAs	Last AS number.
AttrID	Attribute ID.
Neighbor	Address of the neighbor determined by the routing protocol.
Flags	Flags of the route.
OrigNextHop	Next hop address of the route.
Label	This field is not supported in the current software version. Label of the route.
RealNextHop	Real next hop of the route.
BkLabel	This field is not supported in the current software version. Backup label.
BkNexthop	Backup next hop.
SRLabel	This field is not supported in the current software version. Segment routing (SR) label.
BkSRLabel	This field is not supported in the current software version. Backup segment routing (SR) label.
SIDIndex	This field is not supported in the current software version. SID index value.
InLabel	This field is not supported in the current software version. Input label.
Tunnel ID	Tunnel ID.
Interface	Output interface for packets to be forwarded along the route.
BkTunnel ID	Backup tunnel ID.
BkInterface	Backup output interface.
FtnIndex	Index of the FTN entry.
TrafficIndex	Traffic index in the range of 1 to 64. This field displays **N/A** when the value is invalid.
Connector	BGP connector attribute exchanged between BGP peers along with a VPN IPv4 route. The value of the attribute is the IP address of the remote PE device. The BGP connector attribute is used for MD VPN. This field displays **N/A** if the BGP connector attribute is not supported.
VpnPeerId	This field is not supported in the current software version. ID of the VPN peer to which the route belongs, in the range of 1 to 134217727. This field displays **N/A** when the value is invalid.
Dscp	DSCP value of the route, in the range of 0 to 63. This field displays **N/A** when the value is invalid.
Exp	MPLS EXP value of the route, which is supported only by BGP. This field displays **N/A** when the value is invalid.
Summary count	Number of routes.

display ip routing-table acl

Use **display ip routing-table acl** to display information about routes permitted by a basic ACL.

Syntax

display ip routing-table [**vpn-instance** *vpn-instance-name*] **acl** *ipv4-acl-number* [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays routing information for the public network.

ipv4-acl-number: Specifies a basic ACL by its number in the range of 2000 to 2999.

verbose: Displays detailed information about all routes permitted by the basic ACL. If you do not specify this keyword, the command displays only brief information about active routes permitted by the basic ACL.

Usage guidelines

If the specified ACL does not exist or has no rules configured, the command displays information about all routes.

Examples

Define basic ACL 2000 and set the route filtering rules.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Sysname-acl-ipv4-basic-2000] rule deny source any
```

Display brief information about active routes permitted by basic ACL 2000.

```
[Sysname-acl-ipv4-basic-2000] display ip routing-table acl 2000

Summary count : 4

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
192.168.1.0/24      Direct 0    0            192.168.1.111   GE1/0/1
192.168.1.0/32      Direct 0    0            192.168.1.111   GE1/0/1
192.168.1.111/32    Direct 0    0            127.0.0.1       InLoop0
192.168.1.255/32    Direct 0    0            192.168.1.111   GE1/0/1
```

For command output, see Table 1.

Display detailed information about all routes permitted by basic ACL 2000.

```
<Sysname> display ip routing-table acl 2000 verbose
```

```
Summary count : 4

Destination: 192.168.1.0/24
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x1                    Age: 04h20m37s
       Cost: 0                Preference: 0
      IpPre: N/A              QosLocalID: N/A
        Tag: 0                    State: Active Adv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0x2                 OrigAs: 0
      NibID: 0x10000003          LastAs: 0
     AttrID: 0xffffffff        Neighbor: 0.0.0.0
      Flags: 0x10080         OrigNextHop: 192.168.1.111
      Label: NULL            RealNextHop: 192.168.1.111
    BkLabel: NULL              BkNextHop: N/A
    SRLabel: NULL              BkSRLabel: NULL
   SIDIndex: NULL                InLabel: NULL
  Tunnel ID: Invalid           Interface: GigabitEthernet1/0/1
BkTunnel ID: Invalid         BkInterface: N/A
   FtnIndex: 0x0            TrafficIndex: N/A
  Connector: N/A                VpnPeerId: N/A
       Dscp: N/A                    Exp: N/A

Destination: 192.168.1.0/32
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                    Age: 04h20m37s
       Cost: 0                Preference: 0
      IpPre: N/A              QosLocalID: N/A
        Tag: 0                    State: Active NoAdv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0x2                 OrigAs: 0
      NibID: 0x10000003          LastAs: 0
     AttrID: 0xffffffff        Neighbor: 0.0.0.0
      Flags: 0x1008c         OrigNextHop: 192.168.1.111
      Label: NULL            RealNextHop: 192.168.1.111
    BkLabel: NULL              BkNextHop: N/A
    SRLabel: NULL              BkSRLabel: NULL
   SIDIndex: NULL                InLabel: NULL
  Tunnel ID: Invalid           Interface: GigabitEthernet1/0/1
BkTunnel ID: Invalid         BkInterface: N/A
   FtnIndex: 0x0            TrafficIndex: N/A
  Connector: N/A                VpnPeerId: N/A
       Dscp: N/A                    Exp: N/A

Destination: 192.168.1.111/32
```

```
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x1                    Age: 04h20m37s
       Cost: 0                Preference: 0
      IpPre: N/A              QosLocalID: N/A
        Tag: 0                    State: Active NoAdv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0x2                 OrigAs: 0
      NibID: 0x10000000          LastAs: 0
     AttrID: 0xffffffff        Neighbor: 0.0.0.0
      Flags: 0x10004        OrigNextHop: 127.0.0.1
      Label: NULL           RealNextHop: 127.0.0.1
    BkLabel: NULL             BkNextHop: N/A
    SRLabel: NULL             BkSRLabel: NULL
   SIDIndex: NULL               InLabel: NULL
  Tunnel ID: Invalid          Interface: InLoopBack0
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0            TrafficIndex: N/A
  Connector: N/A               VpnPeerId: N/A
       Dscp: N/A                    Exp: N/A

Destination: 192.168.1.255/32
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                    Age: 04h20m37s
       Cost: 0                Preference: 0
      IpPre: N/A              QosLocalID: N/A
        Tag: 0                    State: Active NoAdv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0x2                 OrigAs: 0
      NibID: 0x10000003          LastAs: 0
     AttrID: 0xffffffff        Neighbor: 0.0.0.0
      Flags: 0x1008c        OrigNextHop: 192.168.1.111
      Label: NULL           RealNextHop: 192.168.1.111
    BkLabel: NULL             BkNextHop: N/A
    SRLabel: NULL             BkSRLabel: NULL
   SIDIndex: NULL               InLabel: NULL
  Tunnel ID: Invalid          Interface: GigabitEthernet1/0/1
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0            TrafficIndex: N/A
  Connector: N/A               VpnPeerId: N/A
       Dscp: N/A                    Exp: N/A
```

For command output, see Table 2.

display ip routing-table *ip-address*

Use **display ip routing-table** *ip-address* to display information about routes to a specific destination address.

Use **display ip routing-table** *ip-address1* **to** *ip-address2* to display information about routes to a range of destination addresses.

Syntax

display ip routing-table [**vpn-instance** *vpn-instance-name*] *ip-address* [*mask-length* | *mask*] [**longer-match**] [**verbose**]

display ip routing-table [**vpn-instance** *vpn-instance-name*] *ip-address1* **to** *ip-address2* [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays routing information for the public network.

ip-address: Specifies a destination IP address in dotted decimal notation.

mask-length: Specifies the mask length, an integer in the range of 0 to 32.

mask: Specifies the IP address mask in dotted decimal notation.

longer-match: Displays the route entry with the longest mask.

ip-address1 **to** *ip-address2*: Specifies a destination IP address range.

verbose: Displays detailed routing table information, including information about both active and inactive routes. If you do not specify this keyword, the command displays brief information about active routes.

Usage guidelines

Executing the command with different parameters yields different outputs.

- **display ip routing-table** *ip-address*
  - The system ANDs the entered destination IP address with the subnet mask in each active route entry.
  - The system ANDs the destination IP address in each active route entry with its own subnet mask.

  If the two operations yield the same result for an entry, the entry is displayed.
- **display ip routing-table** *ip-address mask*
  - The system ANDs the entered destination IP address with the entered subnet mask.
  - The system ANDs the destination IP address in each active route entry with the entered subnet mask.

  If the two operations yield the same result for an entry with a subnet mask not greater than the entered subnet mask, the entry is displayed.
- **display ip routing-table** *ip-address* **longer-match**
  - The system ANDs the entered destination IP address with the subnet mask in each active route entry.

- The system ANDs the destination IP address in each active route entry with its own subnet mask.

If the two operations yield the same result for multiple entries, the entry with the longest mask length is displayed.

- **display ip routing-table** *ip-address mask* **longer-match**
  - The system ANDs the entered destination IP address with the entered subnet mask.
  - The system ANDs the destination IP address in each active route entry with the entered subnet mask.

  If the two operations yield the same result for multiple entries with a mask not greater than the entered subnet mask, the entry with the longest mask length is displayed.
- **display ip routing-table** *ip-address1* **to** *ip-address2*

  The system displays active route entries with destinations in the range of *ip-address1*/32 to *ip-address2*/32.

Examples

Display brief information about the routes to the destination IP address 11.0.0.1.

```
<Sysname> display ip routing-table 11.0.0.1

Summary count : 3

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
11.0.0.0/8          Static 60   0            0.0.0.0         NULL0
11.0.0.0/16         Static 60   0            0.0.0.0         NULL0
11.0.0.0/24         Static 60   0            0.0.0.0         NULL0
```

Display brief information about the routes to the destination IP address 11.0.0.1 and mask length 20.

```
<Sysname> display ip routing-table 11.0.0.1 20

Summary count : 2

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
11.0.0.0/8          Static 60   0            0.0.0.0         NULL0
11.0.0.0/16         Static 60   0            0.0.0.0         NULL0
```

Display brief information about the most specific route to the destination address 11.0.0.1.

```
<Sysname> display ip routing-table 11.0.0.1 longer-match

Summary count : 1

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
11.0.0.0/24         Static 60   0            0.0.0.0         NULL0
```

Display brief information about the most specific route to the destination IP address 11.0.0.1 and mask length 20.

```
<Sysname> display ip routing-table 11.0.0.1 20 longer-match

Summary count : 1

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
11.0.0.0/16         Static 60   0            0.0.0.0         NULL0
```

Display brief information about the routes to destination addresses in the range of 1.1.1.0 to 5.5.5.0.

```
<Sysname> display ip routing-table 1.1.1.0 to 5.5.5.0

Summary count : 5

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
1.1.1.1/32          Direct 0    0            127.0.0.1       InLoop0
3.3.3.0/24          Direct 0    0            3.3.3.1         GE1/0/2
3.3.3.1/32          Direct 0    0            127.0.0.1       InLoop0
4.4.4.0/24          Direct 0    0            4.4.4.1         GE1/0/1
4.4.4.1/32          Direct 0    0            127.0.0.1       InLoop0
```

Display detailed information about the routes to the destination IP address 1.2.3.4.

```
<Sysname> display ip routing-table 1.2.3.4 verbose

Summary count : 1

Destination: 1.2.3.4/32
   Protocol: O_INTRA
 Process ID: 0
  SubProtID: 0x1                  Age: 00h00m37s
       Cost: 0              Preference: 255
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                  State: Active Adv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0x2                OrigAs: 200
      NibID: 0x15000000         LastAs: 200
     AttrID: 0x0              Neighbor: 192.168.47.2
      Flags: 0x10060       OrigNextHop: 192.168.47.2
      Label: NULL          RealNextHop: 192.168.47.2
    BkLabel: NULL            BkNextHop: N/A
    SRLabel: NULL            BkSRLabel: NULL
   SIDIndex: NULL              InLabel: NULL
  Tunnel ID: Invalid          Interface: GigabitEthernet1/0/1
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A              VpnPeerId: N/A
       Dscp: N/A                    Exp: N/A
```

For command output, see Table 2.

display ip routing-table prefix-list

Use **display ip routing-table prefix-list** to display routes permitted by an IP prefix list.

Syntax

display ip routing-table [**vpn-instance** *vpn-instance-name*] **prefix-list** *prefix-list-name* [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays routing information for the public network.

prefix-list-name: Specifies an IP prefix list by its name, a case-sensitive string of 1 to 63 characters.

verbose: Displays detailed information about all routes permitted by the IP prefix list. If you do not specify this keyword, the command displays brief information about active routes permitted by the IP prefix list.

Usage guidelines

If the specified IP prefix list does not exist, the command displays information about all routes.

Examples

Create an IP prefix list named **test** to permit the route 1.1.1.0/24.

```
<Sysname> system-view
[Sysname] ip prefix-list test permit 1.1.1.0 24
```

Display brief information about the active route permitted by the IP prefix list.

```
[Sysname] display ip routing-table prefix-list test

Summary count : 1

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
1.1.1.0/24          Direct 0    0            1.1.1.2         GE1/0/2
```

For command output, see Table 1.

Display detailed information about all routes permitted by the IP prefix list.

```
[Sysname] display ip routing-table prefix-list test verbose

Summary count : 1

Destination: 1.1.1.0/24
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x1                  Age: 04h20m37s
       Cost: 0              Preference: 0
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                   State: Active Adv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0x2                OrigAs: 0
```

```
      NibID: 0x10000003          LastAs: 0
     AttrID: 0xffffffff        Neighbor: 0.0.0.0
      Flags: 0x1008c        OrigNextHop: 1.1.1.2
      Label: NULL           RealNextHop: 1.1.1.2
    BkLabel: NULL             BkNextHop: N/A
    SRLabel: NULL             BkSRLabel: NULL
   SIDIndex: NULL               InLabel: NULL
  Tunnel ID: Invalid          Interface: GigabitEthernet1/0/2
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A              VpnPeerId: N/A
       Dscp: N/A                    Exp: N/A
```

For command output, see Table 2.

display ip routing-table protocol

Use **display ip routing-table protocol** to display information about routes installed by a protocol.

Syntax

display ip routing-table [**vpn-instance** *vpn-instance-name*] **protocol** *protocol* [**inactive** | **verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays routing information for the public network.

protocol: Specifies a routing protocol.

inactive: Displays information about inactive routes. If you do not specify this keyword, the command displays information about both active and inactive routes.

verbose: Displays detailed routing table information. If you do not specify this keyword, the command displays brief routing information.

Examples

Display brief information about direct routes.

```
<Sysname> display ip routing-table protocol direct

Summary count : 9

Direct Routing table status : <Active>
Summary count : 9
```

```
Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
192.168.80.0/24     Direct 0    0            192.168.80.10   GE1/0/1
192.168.80.0/32     Direct 0    0            192.168.80.10   GE1/0/1
192.168.80.10/32    Direct 0    0            127.0.0.1       InLoop0
192.168.80.255/32   Direct 0    0            192.168.80.10   GE1/0/1

Direct Routing table status : <Inactive>
Summary count : 0
```

Display brief information about static routes.

```
<Sysname> display ip routing-table protocol static

Summary count : 1

Static Routing table status : <Active>
Summary count : 0

Static Routing table status : <Inactive>
Summary count : 1

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
3.0.0.0/8           Static 60   0            2.2.2.2         GE1/0/1
```

Display detailed information about OSPF routes.

```
<Sysname> display ip routing-table protocol ospf verbose

Summary count : 1

Destination: 1.1.1.2/32
   Protocol: O_INTRA
 Process ID: 0
  SubProtID: 0x6                  Age: 00h03m54s
       Cost: 0              Preference: 255
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                 State: Active Adv
  OrigTblID: 0x0              OrigVrf: default-vrf
    TableID: 0x2               OrigAs: 200
      NibID: 0x16000000        LastAs: 200
     AttrID: 0x0             Neighbor: 192.168.47.2
      Flags: 0x10060       OrigNextHop: 192.168.47.2
      Label: NULL          RealNextHop: 192.168.47.2
    BkLabel: NULL            BkNextHop: N/A
    SRLabel: NULL            BkSRLabel: NULL
   SIDIndex: NULL              InLabel: NULL
```

```
  Tunnel ID: Invalid          Interface: GigabitEthernet1/0/1
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A              VpnPeerId: N/A
       Dscp: N/A                    Exp: N/A
```

For command output, see Table 2.

display ip routing-table statistics

Use **display ip routing-table statistics** to display IPv4 route statistics, including numbers of total routes, routes installed by the protocol, routes marked as deleted, and active routes.

Syntax

display ip routing-table [**vpn-instance** *vpn-instance-name*] **statistics**

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

If you do not specify any parameters, the command displays IPv4 route statistics for the public network.

Examples

Display IPv4 route statistics for the public network.

```
<Sysname> display ip routing-table statistics

Total prefixes: 15        Active prefixes: 15

Proto      route       active      added       deleted
DIRECT     12          12          30          18
STATIC     3           3           5           2
RIP        0           0           0           0
OSPF       0           0           0           0
IS-IS      0           0           0           0
LISP       0           0           0           0
BGP        0           0           0           0
Total      15          15          35          20
```

Table 3 Command output

Field	Description
Proto	Protocol that installed the route.
route	Number of routes installed by the protocol.
active	Number of active routes.
added	Number of routes added to the routing table after the router started up or the routing table was cleared most recently.
deleted	Number of routes marked as deleted, which will be cleared after a period.
Total	Total number of routes.

display ip routing-table summary

Use **display ip routing-table summary** to display brief routing table information, including maximum number of ECMP routes, maximum number of active routes, and number of remaining active routes.

Syntax

display ip routing-table [**vpn-instance** *vpn-instance-name*] **summary**

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays brief routing table information for the public network.

Examples

Display brief routing table information for the public network.

```
<Sysname> display ip routing-table summary

Max ECMP: 32
Max Active Route: 262144
Remain Active Route: 262126
```

Display brief routing table information for the MPLS L3VPN instance **vpn1**.

```
<Sysname> display ip routing-table vpn-instance vpn1 summary

Max ECMP: 32
Max Active Route: 262144
Remain Active Route: 262134
Threshold value percentage of max active routes: 100%
```

Table 4 Command output

Field	Description
Max ECMP	Maximum number of ECMP routes supported by the system.
Max Active Route	Maximum number of supported routes.
Remain Active Route	Number of the remaining inactive routes.
Threshold value xxx	Alarm threshold of active routes specified by using the **routing-table limit** command in a VPN instance: • **Threshold value of active routes alert**—This field is displayed when the alarm threshold is specified by using the **routing-table limit** *number* **simply-alert** command. When the number of active routes exceeds the alarm threshold, the system logs the event and sends traps but still accepts active routes. • **Threshold value percentage of max active routes**—This field is displayed when the **routing-table limit** *number* **simply-alert** command is not configured or when the alarm threshold is specified by using the **routing-table limit** *number* *warn-threshold* command. The value range for the alarm threshold is 1 to 100 in percentage. When the percentage of active routes exceeds the alarm threshold, the system logs the event and sends traps but still accepts active routes. If the number of active routes reaches the maximum number, no more routes can be added. The percentage of active routes equals the number of active routes divided by the maximum number of active routes supported in a VPN instance, and multiplied by 100.

display ipv6 rib attribute

Use **display ipv6 rib attribute** to display route attribute information in the IPv6 RIB.

Syntax

display ipv6 rib attribute [*attribute-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

attribute-id: Specifies a route attribute by its ID, a hexadecimal string in the range of 0 to ffffffff.

Examples

Display route attribute information in the IPv6 RIB.

```
<Sysname> display ipv6 rib attribute
Total number of attribute(s): 1
```

```
Detailed information of attribute 0x9:
                  Flag: 0x0
              Protocol: BGP4+ instance default
        Address family: IPv6
       Reference count: 0
      Local preference: 0
Ext-communities number: 0
 Ext-communities value: N/A
    Communities number: 0
     Communities value: N/A
        AS-path number: 0
         AS-path value: N/A
```

For command output, see Table 8.

display ipv6 rib graceful-restart

Use **`display ipv6 rib graceful-restart`** to display IPv6 RIB GR state information.

Syntax

`display ipv6 rib graceful-restart`

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display IPv6 RIB GR state information.

```
<Sysname> display ipv6 rib graceful-restart
RIB GR state     : Phase2-calculation end
RCOM GR state    : Flush end
Protocol GR state:
 No.  Protocol   Lifetime FD   State    Start/End
-------------------------------------------------
 1    DIRECT6    480      29   End      No/No
 2    STATIC6    480      32   End      No/No
 3    ISISV6     480      30   End      No/No
 4    BGP4+ instance default
                 480      31   End      No/No
 5    BGP4+ instance ebcdefg
                 480      32   End      No/No
```

For command output, see Table 9.

display ipv6 rib nib

Use **display ipv6 rib nib** to display next hop information in the IPv6 RIB.

Syntax

display ipv6 rib nib [**self-originated**] [*nib-id*] [**verbose**]

display ipv6 rib nib protocol *protocol* [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

self-originated: Displays information about next hops of self-originated routes in the IPv6 RIB.

nib-id: Specifies a NIB by its ID, a hexadecimal string in the range of 1 to ffffffff.

verbose: Displays detailed next hop information in the IPv6 RIB. If you do not specify this keyword, the command displays brief next hop information in the IPv6 RIB.

protocol *protocol*: Specifies a protocol by its name.

Examples

Display brief next hop information in the IPv6 RIB.

```
<Sysname> display ipv6 rib nib
Total number of nexthop(s): 151

      NibID: 0x20000000        Sequence: 0
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: ::
    IFIndex: 0x111            LocalAddr: ::
   TopoNthp: Invalid

      NibID: 0x20000001        Sequence: 1
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: ::1
    IFIndex: 0x112            LocalAddr: ::1
   TopoNthp: Invalid

...
```

Display detailed next hop information in the IPv6 RIB.

```
<Sysname> display ipv6 rib nib verbose
Total number of nexthop(s): 151
```

```
      NibID: 0x20000000        Sequence: 0
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: ::
    IFIndex: 0x111            LocalAddr: ::
   TopoNthp: Invalid
     RefCnt: 4              FlushRefCnt: 1
       Flag: 0x84               Version: 1
 1 nexthop(s):
PrefixIndex: 0              OrigNexthop: ::
  RelyDepth: 0              RealNexthop: ::
  Interface: NULL0            LocalAddr: ::
  TunnelCnt: 0                      Vrf: default-vrf
   TunnelID: N/A               Topology:
     Weight: 0

      NibID: 0x20000001        Sequence: 1
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: ::1
    IFIndex: 0x112            LocalAddr: ::1
   TopoNthp: Invalid
     RefCnt: 4              FlushRefCnt: 1
       Flag: 0x84               Version: 1
 1 nexthop(s):
PrefixIndex: 0              OrigNexthop: ::1
  RelyDepth: 0              RealNexthop: ::1
  Interface: InLoop0          LocalAddr: ::1
  TunnelCnt: 0                      Vrf: default-vrf
   TunnelID: N/A               Topology:
     Weight: 0

      NibID: 0x26000001        Sequence: 1
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: 121::2
    IFIndex: 0x112            LocalAddr: ::
   TopoNthp: Invalid
   Instance: default

      NibID: 0x26000002        Sequence: 1
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: 122::2
    IFIndex: 0x112            LocalAddr: ::
   TopoNthp: Invalid
   Instance: abc
```

...

For command output, see Table 10 and Table 11.

display ipv6 route-direct nib

Use **display ipv6 route-direct nib** to display next hop information for IPv6 direct routes.

Syntax

display ipv6 route-direct nib [*nib-id*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

nib-id: Specifies a NIB by its ID, a hexadecimal string in the range of 1 to ffffffff.

verbose: Displays detailed next hop information for IPv6 direct routes. If you do not specify this keyword, the command displays brief next hop information for IPv6 direct routes.

Examples

Display brief next hop information for IPv6 direct routes.

```
<Sysname> display ipv6 route-direct nib
Total number of nexthop(s): 115

      NibID: 0x20000000        Sequence: 0
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: ::
    IFIndex: 0x111             LocalAddr: ::
   TopoNthp: Invalid

      NibID: 0x20000001        Sequence: 1
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: ::1
    IFIndex: 0x112             LocalAddr: ::1
   TopoNthp: Invalid

...
```

Display detailed next hop information for IPv6 direct routes.

```
<Sysname> display ipv6 route-direct nib verbose
Total number of nexthop(s): 115

      NibID: 0x20000000        Sequence: 0
```

```
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: ::
    IFIndex: 0x111            LocalAddr: ::
     RefCnt: 1              FlushRefCnt: 0
       Flag: 0x2                Version: 1
 1 nexthop(s):
PrefixIndex: 0              OrigNexthop: ::
  RelyDepth: 0              RealNexthop: ::
  Interface: NULL0            LocalAddr: ::
  TunnelCnt: 0                      Vrf: default-vrf
   TunnelID: N/A               Topology:
     Weight: 0

      NibID: 0x20000001        Sequence: 1
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: ::1
    IFIndex: 0x112            LocalAddr: ::1
     RefCnt: 1              FlushRefCnt: 0
       Flag: 0x2                Version: 1
 1 nexthop(s):
PrefixIndex: 0              OrigNexthop: ::1
  RelyDepth: 0              RealNexthop: ::1
  Interface: InLoop0          LocalAddr: ::1
  TunnelCnt: 0                      Vrf: default-vrf
   TunnelID: N/A               Topology:
     Weight: 0

...
```

For command output, see Table 12 and Table 13.

display ipv6 routing-table

Use **display ipv6 routing-table** to display IPv6 routing table information.

Syntax

display ipv6 routing-table [**vpn-instance** *vpn-instance-name*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters.

verbose: Displays detailed routing table information, including information about both active and inactive routes. If you do not specify this keyword, the command displays only brief information about active routes.

Usage guidelines

If you do not specify any parameters, the command displays IPv6 routing table information for the public network.

Examples

Display brief information about active routes in the IPv6 routing table.

```
<Sysname> display ipv6 routing-table

Destinations : 4        Routes : 4

Destination: ::1/128                                    Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0

Destination: 1:1:2::/64                                 Protocol  : Guard
NextHop    : ::                                         Preference: 254
Interface  : NULL0                                      Cost      : 0

Destination: FE80::/10                                  Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : InLoop0                                    Cost      : 0

Destination: FF00::/8                                   Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : NULL0                                      Cost      : 0
```

Table 5 Command output

Field	Description
Destinations	Number of destination addresses.
Routes	Number of routes.
Destination	IPv6 address and prefix of the destination network or host.
NextHop	Next hop address of the route.
Preference	Preference of the route.
Interface	Output interface for packets to be forwarded along the route.
Protocol	Protocol that installed the route.
Cost	Cost of the route.
Summary count	Number of routes.

Display detailed information about all routes in the IPv6 routing table.

```
<Sysname> display ipv6 routing-table verbose
```

```
Destinations : 2 Routes : 2

Destination: ::1/128
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                    Age: 19h23m02s
       Cost: 0                Preference: 0
      IpPre: N/A              QosLocalID: N/A
        Tag: 0                    State: Active NoAdv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0xa                 OrigAs: 0
      NibID: 0x20000000          LastAs: 0
     AttrID: 0xffffffff        Neighbor: ::
      Flags: 0x10004        OrigNextHop: ::1
      Label: NULL           RealNextHop: ::1
    BkLabel: NULL             BkNextHop: N/A
    SRLabel: NULL             BkSRLabel: NULL
   SIDIndex: NULL               InLabel: NULL
  Tunnel ID: Invalid          Interface: InLoopBack0
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A              VpnPeerId: N/A
       Dscp: N/A                    Exp: N/A

Destination: 12::/96
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                    Age: 00h01m47s
       Cost: 0                Preference: 0
      IpPre: N/A              QosLocalID: N/A
        Tag: 0                    State: Active Adv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0xa                 OrigAs: 0
      NibID: 0x20000003          LastAs: 0
     AttrID: 0xffffffff        Neighbor: ::
      Flags: 0x10080        OrigNextHop: ::
      Label: NULL           RealNextHop: ::
    BkLabel: NULL             BkNextHop: N/A
    SRLabel: NULL             BkSRLabel: NULL
   SIDIndex: NULL               InLabel: NULL
  Tunnel ID: Invalid          Interface: GigabitEthernet1/0/2
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A              VpnPeerId: N/A
       Dscp: N/A                    Exp: N/A
```

Table 6 Command output

Field	Description
Destination	IPv6 address and prefix of the destination network or host.
Protocol	Protocol that installed the route.
SubProtID	ID of the subprotocol for routing.
Age	Time for which the route has been in the routing table.
Cost	Cost of the route.
Preference	Preference of the route.
IpPre	IP precedence.
QosLocalID	Local QoS ID.
Tag	Tag of the route.
State	Route status: • **Active**—Active unicast route. • **Adv**—Route that can be advertised. • **Inactive**—Inactive route. • **NoAdv**—Route that the router must not advertise. • **Vrrp**—Routes generated by VRRP. This state is not supported in the current software version. • **Nat**—Routes generated by NAT. • **TunE**—Tunnel.
OrigTblID	Original routing table ID.
OrigVrf	Original VPN instance that the route belongs to. This field displays **default-vrf** if the route is on the public network.
TableID	ID of the routing table.
OrigAs	Original AS number.
NibID	ID of the next hop.
LastAs	Last AS number.
AttrID	Attribute ID.
Neighbor	Address of the neighbor determined by the routing protocol.
Flags	Flags of the route.
OrigNextHop	Next hop address of the route.
Label	This field is not supported in the current software version. Label of the route.
RealNextHop	Real next hop of the route.
BkLabel	This field is not supported in the current software version. Backup label.
BkNexthop	Backup next hop.
SRLabel	This field is not supported in the current software version. SR label.
BkSRLabel	This field is not supported in the current software version. Backup SR label.

Field	Description
Tunnel ID	Tunnel ID.
Interface	Output interface for packets to be forwarded along the route.
BkTunnel ID	Backup tunnel ID.
BkInterface	Backup output interface.
FtnIndex	Index of the FTN entry.
TrafficIndex	Traffic index in the range of 1 to 64. This field displays **N/A** when the value is invalid.
Connector	BGP connector attribute exchanged between BGP peers along with a VPN IPv4 route. The value of the attribute is the IP address of the remote PE device. The BGP connector attribute is used for MD VPN. This field displays **N/A** if BGP connector attribute is not supported.
VpnPeerId	This field is not supported in the current software version. ID of the VPN peer to which the route belongs, in the range of 1 to 134217727. This field displays **N/A** when the value is invalid.
Dscp	DSCP value of the route, in the range of 0 to 63. This field displays **N/A** when the value is invalid.
Exp	MPLS EXP value of the route, which is supported only by BGP. This field displays **N/A** when the value is invalid.
Summary count	Number of routes.

display ipv6 routing-table acl

Use **display ipv6 routing-table acl** to display routing information permitted by an IPv6 basic ACL.

Syntax

display ipv6 routing-table [**vpn-instance** *vpn-instance-name*] **acl** *ipv6-acl-number* [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays routing information for the public network.

ipv6-acl-number: Specifies a basic IPv6 ACL by its number in the range of 2000 to 2999.

verbose: Displays detailed information about all routes permitted by the basic IPv6 ACL. If you do not specify this keyword, the command displays only brief information about active routes permitted by the basic IPv6 ACL.

Usage guidelines

If the specified IPv6 ACL does not exist or has no rules configured, the command displays information about all IPv6 routes.

Examples

Display brief information about active routes permitted by IPv6 ACL 2000.

```
<Sysname> display ipv6 routing-table acl 2000

Summary count : 6

Destination : ::1/128                                   Protocol  : Direct
NextHop     : ::1                                       Preference: 0
Interface   : InLoop0                                   Cost      : 0

Destination: 12::/96                                    Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : GE1/0/1                                    Cost      : 0

Destination: 12::1/128                                  Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0

Destination: FF::11/128                                 Protocol  : O_INTER
NextHop    : 12::2                                      Preference: 255
Interface  : GE1/0/2                                    Cost      : 0

Destination: FE80::/10                                  Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : InLoop0                                    Cost      : 0

Destination: FF00::/8                                   Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : NULL0                                      Cost      : 0
```

For command output, see Table 5.

Display detailed information about all routes permitted by IPv6 ACL 2000.

```
<Sysname> display ipv6 routing-table acl 2000 verbose

Summary count : 6

Destination: ::1/128
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                  Age: 19h29m12s
       Cost: 0              Preference: 0
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                   State: Active NoAdv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0xa                OrigAs: 0
```

```
      NibID: 0x20000000          LastAs: 0
     AttrID: 0xffffffff        Neighbor: ::
      Flags: 0x10004        OrigNextHop: ::1
      Label: NULL           RealNextHop: ::1
    BkLabel: NULL             BkNextHop: N/A
    SRLabel: NULL             BkSRLabel: NULL
   SIDIndex: NULL               InLabel: NULL
  Tunnel ID: Invalid          Interface: InLoopBack0
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0            TrafficIndex: N/A
  Connector: N/A              VpnPeerId: N/A
       Dscp: N/A                    Exp: N/A

Destination: 12::/96
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                   Age: 00h07m57s
       Cost: 0               Preference: 0
      IpPre: N/A             QosLocalID: N/A
        Tag: 0                    State: Active Adv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0xa                 OrigAs: 0
      NibID: 0x20000003          LastAs: 0
     AttrID: 0xffffffff        Neighbor: ::
      Flags: 0x10080        OrigNextHop: ::
      Label: NULL           RealNextHop: ::
    BkLabel: NULL             BkNextHop: N/A
    SRLabel: NULL             BkSRLabel: NULL
   SIDIndex: NULL               InLabel: NULL
  Tunnel ID: Invalid          Interface: GigabitEthernet1/0/2
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0            TrafficIndex: N/A
  Connector: N/A              VpnPeerId: N/A
       Dscp: N/A                    Exp: N/A

Destination: 12::1/128
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                   Age: 00h07m55s
       Cost: 0               Preference: 0
      IpPre: N/A             QosLocalID: N/A
        Tag: 0                    State: Active NoAdv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0xa                 OrigAs: 0
      NibID: 0x20000000          LastAs: 0
     AttrID: 0xffffffff        Neighbor: ::
      Flags: 0x10004        OrigNextHop: ::1
      Label: NULL           RealNextHop: ::1
```

```
    BkLabel: NULL             BkNextHop: N/A
    SRLabel: NULL             BkSRLabel: NULL
   SIDIndex: NULL               InLabel: NULL
  Tunnel ID: Invalid          Interface: InLoopBack0
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A              VpnPeerId: N/A
       Dscp: N/A                    Exp: N/A

Destination: FF::11/128
   Protocol: O_INTER
 Process ID: 0
  SubProtID: 0x6                   Age: 00h06m43s
       Cost: 0               Preference: 255
      IpPre: N/A             QosLocalID: N/A
        Tag: 0                    State: Active Adv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0xa                 OrigAs: 200
      NibID: 0x26000000          LastAs: 200
     AttrID: 0x1               Neighbor: 12::2
      Flags: 0x10060        OrigNextHop: 12::2
      Label: NULL           RealNextHop: 12::2
    BkLabel: NULL             BkNextHop: N/A
    SRLabel: NULL             BkSRLabel: NULL
   SIDIndex: NULL               InLabel: NULL
  Tunnel ID: Invalid          Interface: GigabitEthernet1/0/2
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A              VpnPeerId: N/A
       Dscp: N/A                    Exp: N/A

Destination: FE80::/10
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                   Age: 19h29m12s
       Cost: 0               Preference: 0
      IpPre: N/A             QosLocalID: N/A
        Tag: 0                    State: Active NoAdv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0xa                 OrigAs: 0
      NibID: 0x20000002          LastAs: 0
     AttrID: 0xffffffff        Neighbor: ::
      Flags: 0x10084        OrigNextHop: ::
      Label: NULL           RealNextHop: ::
    BkLabel: NULL             BkNextHop: N/A
    SRLabel: NULL             BkSRLabel: NULL
   SIDIndex: NULL               InLabel: NULL
  Tunnel ID: Invalid          Interface: InLoopBack0
```

```
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A              VpnPeerId: N/A
       Dscp: N/A                    Exp: N/A

Destination: FF00::/8
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                    Age: 19h29m12s
       Cost: 0               Preference: 0
      IpPre: N/A             QosLocalID: N/A
        Tag: 0                    State: Active NoAdv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0xa                 OrigAs: 0
      NibID: 0x20000001          LastAs: 0
     AttrID: 0xffffffff        Neighbor: ::
      Flags: 0x10014        OrigNextHop: ::
      Label: NULL           RealNextHop: ::
    BkLabel: NULL             BkNextHop: N/A
    SRLabel: NULL             BkSRLabel: NULL
   SIDIndex: NULL               InLabel: NULL
  Tunnel ID: Invalid          Interface: NULL0
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A              VpnPeerId: N/A
       Dscp: N/A                    Exp: N/A
```

For command output, see Table 6.

display ipv6 routing-table *ipv6-address*

Use **display ipv6 routing-table** *ipv6-address* to display information about routes to an IPv6 destination address.

Use **display ipv6 routing-table** *ipv6-address1* **to** *ipv6-address2* to display information about routes to a range of IPv6 destination addresses.

Syntax

display ipv6 routing-table [**vpn-instance** *vpn-instance-name*] *ipv6-address* [*prefix-length*] [**longer-match**] [**verbose**]

display ipv6 routing-table [**vpn-instance** *vpn-instance-name*] *ipv6-address1* **to** *ipv6-address2* [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays routing information for the public network.

ipv6-address: Specifies a destination IPv6 address.

prefix-length: Specifies the prefix length in the range of 0 to 128.

longer-match: Displays the route entry with the longest prefix.

ipv6-address1 **to** *ipv6-address2*: Specifies a destination IPv6 address range.

verbose: Displays detailed routing table information, including information about both active and inactive routes. If you do not specify this keyword, the command displays only brief information about active routes.

Usage guidelines

Executing the command with different parameters yields different output.

- **display ipv6 routing-table** *ipv6-address*
  - The system ANDs the entered destination IPv6 address with the prefix length in each active route entry.
  - The system ANDs the destination IPv6 address in each active route entry with the prefix length in the entry.

  If the two operations yield the same result for an entry, the entry is displayed.
- **display ipv6 routing-table** *ipv6-address prefix-length*
  - The system ANDs the entered destination IPv6 address with the entered prefix length.
  - The system ANDs the destination IPv6 address in each active route entry with the entered prefix length.

  If the two operations yield the same result for an entry with a prefix length not greater than the entered prefix length, the entry is displayed.
- **display ipv6 routing-table** *ipv6-address* **longer-match**
  - The system ANDs the entered destination IPv6 address with the prefix length in each active route entry.
  - The system ANDs the destination IPv6 address in each active route entry with the prefix length in the entry.

  If the two operations yield the same result for multiple entries, the entry with the longest prefix length is displayed.
- **display ipv6 routing-table** *ipv6-address prefix-length* **longer-match**
  - The system ANDs the entered destination IPv6 address with the entered prefix length.
  - The system ANDs the destination IPv6 address in each active route entry with the entered prefix length.

  If the two operations yield the same result for multiple entries with a prefix length not greater than the entered prefix length, the entry with the longest prefix length is displayed.
- **display ipv6 routing-table** *ipv6-address1* **to** *ipv6-address2*

  The system displays route entries with destinations in the range of *ipv6-address1*/128 to *ipv6-address2*/128.

Examples

Display brief information about the routes to the destination IPv6 address 10::1 127.

```
<Sysname> display ipv6 routing-table 10::1 127
```

```
Summary count: 3

Destination: 10::/64                                    Protocol  : Static
NextHop    : ::                                         Preference: 60
Interface  : NULL0                                      Cost      : 0

Destination: 10::/68                                    Protocol  : Static
NextHop    : ::                                         Preference: 60
Interface  : NULL0                                      Cost      : 0

Destination: 10::/120                                   Protocol  : Static
NextHop    : ::                                         Preference: 60
Interface  : NULL0                                      Cost      : 0
```

Display brief information about the most specific route to the destination IPv6 address 10::1 and prefix length 127.

```
<Sysname> display ipv6 routing-table 10::1 127 longer-match

Summary count : 1

Destination: 10::/120                                   Protocol  : Static
NextHop    : ::                                         Preference: 60
Interface  : NULL0                                      Cost      : 0
```

Display brief information about the routes to destination addresses in the range of 100:: to 300::.

```
<Sysname> display ipv6 routing-table 100:: to 300::

Summary count : 3

Destination: 100::/64                                   Protocol  : Static
NextHop    : ::                                         Preference: 60
Interface  : NULL0                                      Cost      : 0

Destination: 200::/64                                   Protocol  : Static
NextHop    : ::                                         Preference: 60
Interface  : NULL0                                      Cost      : 0

Destination: 300::/64                                   Protocol  : Static
NextHop    : ::                                         Preference: 60
Interface  : NULL0                                      Cost      : 0
```

Display detailed information about the routes to destination IPv6 addresses 1:2::3:4/128.

```
<Sysname> display ipv6 routing-table 1:2::3:4 128 verbose

Summary count : 1

Destination: 1:2::3:4/128
   Protocol: O_INTER
 Process ID: 0
  SubProtID: 0x1                  Age: 00h01m14s
       Cost: 0              Preference: 255
```

```
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                   State: Active Adv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0x1                OrigAs: 200
      NibID: 0x26000000         LastAs: 200
     AttrID: 0x0              Neighbor: 2:2::3:4
      Flags: 0x10060       OrigNextHop: 2:2::3:4
      Label: NULL          RealNextHop: 2:2::3:4
    BkLabel: NULL            BkNextHop: N/A
    SRLabel: NULL            BkSRLabel: NULL
   SIDIndex: NULL              InLabel: NULL
  Tunnel ID: Invalid         Interface: GigabitEthernet1/0/1
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0          TrafficIndex: N/A
  Connector: N/A             VpnPeerId: N/A
       Dscp: N/A                   Exp: N/A
```

For command output, see Table 6.

display ipv6 routing-table prefix-list

Use **display ipv6 routing-table prefix-list** to display information about IPv6 routes permitted by an IPv6 prefix list.

Syntax

display ipv6 routing-table [**vpn-instance** *vpn-instance-name*] **prefix-list** *prefix-list-name* [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays routing information for the public network.

prefix-list-name: Specifies an IPv6 prefix list by its name, a case-sensitive string of 1 to 63 characters.

verbose: Displays detailed information about all IPv6 routes permitted by the IPv6 prefix list. If you do not specify this keyword, the command displays brief information about active IPv6 routes permitted by the IPv6 prefix list.

Usage guidelines

If the specified IPv6 prefix list does not exist, the command displays information about all routes.

Examples

Create an IPv6 prefix list named test to permit the prefix ::1/128.

```
<Sysname> system-view
[Sysname] ipv6 prefix-list test permit ::1 128
```

Display brief information about the active IPv6 route permitted by the IPv6 prefix list.

```
[Sysname] display ipv6 routing-table prefix-list test

Summary count : 1

Destination: ::1/128                                    Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0
```

For command output, see Table 5.

Display detailed information about all routes permitted by the IPv6 prefix list.

```
[Sysname] display ipv6 routing-table prefix-list test verbose

Summary count : 1

Destination: ::1/128
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                  Age: 08h57m19s
       Cost: 0              Preference: 0
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                   State: Active NoAdv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0xa                OrigAs: 0
      NibID: 0x20000000         LastAs: 0
     AttrID: 0xffffffff       Neighbor: ::
      Flags: 0x10004       OrigNextHop: ::1
      Label: NULL          RealNextHop: ::1
    BkLabel: NULL            BkNextHop: N/A
    SRLabel: NULL            BkSRLabel: NULL
   SIDIndex: NULL              InLabel: NULL
  Tunnel ID: Invalid         Interface: InLoopBack0
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0          TrafficIndex: N/A
  Connector: N/A              VpnPeerId: N/A
       Dscp: N/A                   Exp: N/A
```

For command output, see Table 6.

display ipv6 routing-table protocol

Use **display ipv6 routing-table protocol** to display information about IPv6 routes installed by a protocol.

Syntax

display ipv6 routing-table [**vpn-instance** *vpn-instance-name*] **protocol** *protocol* [**inactive** | **verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays routing information for the public network.

protocol: Specifies a routing protocol.

inactive: Displays information about inactive routes. If you do not specify this keyword, the command displays information about both active and inactive routes.

verbose: Displays detailed routing table information. If you do not specify this keyword, the command displays brief routing information.

Examples

Display brief information about IPv6 direct routes.

```
<Sysname> display ipv6 routing-table protocol direct

Summary count : 3

Direct Routing table status : <Active>
Summary count : 3

Destination: ::1/128                                Protocol  : Direct
NextHop    : ::1                                    Preference: 0
Interface  : InLoop0                                Cost      : 0

Destination: FE80::/10                              Protocol  : Direct
NextHop    : ::                                     Preference: 0
Interface  : InLoop0                                Cost      : 0

Destination: FF00::/8                               Protocol  : Direct
NextHop    : ::                                     Preference: 0
Interface  : NULL0                                  Cost      : 0

Direct Routing table status : <Inactive>
Summary count : 0
```

Display brief information about IPv6 static routes.

```
<Sysname> display ipv6 routing-table protocol static

Summary count : 3

Static Routing table status : <Active>
```

```
Summary count : 3

Destination: 2::2/128                                   Protocol  : Static
NextHop    : fe80::2                                    Preference: 60
Interface  : GE1/0/2                                    Cost      : 0

Destination: 2::2/128                                   Protocol  : Static
NextHop    : fe80::3                                    Preference: 60
Interface  : GE1/0/2                                    Cost      : 0

Destination: 3::3/128                                   Protocol  : Static
NextHop    : 2::2                                       Preference: 60
Interface  : GE1/0/2                                    Cost      : 0

Static Routing table status : <Inactive>
Summary count : 0
```

Display detailed information about OSPFv3 routes.

```
<Sysname> display ipv6 routing-table protocol ospfv3 verbose

Summary count : 1

Destination: 22::22/128
   Protocol: O_INTER
 Process ID: 0
  SubProtID: 0x6                  Age: 00h04m15s
       Cost: 0              Preference: 255
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                 State: Active Adv
  OrigTblID: 0x0              OrigVrf: default-vrf
    TableID: 0xa               OrigAs: 200
      NibID: 0x25000001         LastAs: 200
     AttrID: 0x3              Neighbor: 121::2
      Flags: 0x10060       OrigNextHop: 121::2
      Label: NULL          RealNextHop: 121::2
    BkLabel: NULL            BkNextHop: N/A
    SRLabel: NULL            BkSRLabel: NULL
   SIDIndex: NULL              InLabel: NULL
  Tunnel ID: Invalid         Interface: GigabitEthernet1/0/1
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0          TrafficIndex: N/A
  Connector: N/A              VpnPeerId: N/A
       Dscp: N/A                   Exp: N/A
```

For command output, see Table 6.

display ipv6 routing-table statistics

Use **`display ipv6 routing-table statistics`** to display IPv6 route statistics, including numbers of total routes, routes installed and deleted by the protocol, and active routes.

Syntax

display ipv6 routing-table [**vpn-instance** *vpn-instance-name*] **statistics**

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

If you do not specify any parameters, the command displays IPv6 route statistics for the public network.

Examples

Display IPv6 route statistics for the public network.

```
<Sysname> display ipv6 routing-table statistics

Total prefixes: 8        Active prefixes: 8

Proto      route       active      added       deleted
DIRECT     5           5           5           0
STATIC     3           3           3           0
RIPng      0           0           0           0
OSPFv3     0           0           0           0
IS-ISv6    0           0           0           0
LISP       0           0           0           0
BGP4+      0           0           0           0
Total      8           8           8           0
```

Table 7 Command output

Field	Description
Proto	Protocol that installed the route.
route	Number of routes installed by the protocol.
active	Number of active routes.
added	Number of routes added to the routing table after the router started up or the routing table was cleared most recently.
deleted	Number of routes marked as deleted, which will be cleared after a period.
Total	Total number of routes.

display ipv6 routing-table summary

Use **display ipv6 routing-table summary** to display brief IPv6 routing table information, including maximum number of ECMP routes, maximum number of active routes, and number of remaining active routes.

Syntax

display ipv6 routing-table [**vpn-instance** *vpn-instance-name*] **summary**

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays brief IPv6 routing table information for the public network.

Examples

Display brief IPv6 routing table information for the public network.

```
<Sysname> display ipv6 routing-table summary

Max ECMP: 32
Max Active Route: 262144
Remain Active Route: 262126
```

Display brief IPv6 routing table information for the MPLS L3VPN instance **vpn1**.

```
<Sysname> display ipv6 routing-table vpn-instance vpn1 summary

Max ECMP: 32
Max Active Route: 262144
Remain Active Route: 262134
Threshold value of active routes alert: 65100
```

For command output, see Table 4.

display rib attribute

Use **display rib attribute** to display route attribute information in the RIB.

Syntax

display rib attribute [*attribute-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

attribute-id: Specifies a route attribute by its ID, a hexadecimal string in the range of 0 to ffffffff.

Examples

Display route attribute information in the RIB.

```
<Sysname> display rib attribute
Total number of attribute(s): 10

Detailed information of attribute 0x0:
                  Flag: 0x0
              Protocol: BGP instance default
        Address family: IPv4
       Reference count: 0
      Local preference: 0
Ext-communities number: 26
 Ext-communities value: <RT: 1:1> <RT: 2:2> <RT: 3:3> <RT: 123.123.123.123:65535
                        > <RT: 1234567890:65535> <RT: 123.123.123.123:65534> <RT
                        : 4:4> <RT: 5:5> <RT: 6:6> <RT: 7:7> <RT: 8:8> <RT: 9:9>
                         <RT: 10:10> <RT: 10:1> <RT: 10:11> <RT: 10:12> <RT: 10:
                        13> <RT: 10:14> <RT: 10:15> <RT: 10:16> ...
    Communities number: 0
     Communities value: N/A
        AS-path number: 0
         AS-path value: N/A

Detailed information of attribute 0x1:
                  Flag: 0x0
              Protocol: BGP
        Address family: IPv4
       Reference count: 0
      Local preference: 0
Ext-communities number: 1
 Ext-communities value: <RT: 1:2>
    Communities number: 0
     Communities value: N/A
        AS-path number: 0
         AS-path value: N/A
```

Table 8 Command output

Field	Description
Protocol	Protocol that generates the attribute.
Ext-communities number	Number of the extended community attribute values.
Ext-communities value	Values of the extended community attribute. This field displays **N/A** when no values exist, and it can display a maximum of 20 values.

Field	Description
Communities number	Number of the COMMUNITY attribute values.
Communities value	Values of the COMMUNITY attribute. This field displays **N/A** when no values exist, and it can display a maximum of 20 values.
AS-path number	Number of ASs in the AS_PATH attribute.
AS-path value	Values of the AS_PATH attribute, including AS_SET, AS_SEQUENCE, confederation AS_SET, and confederation AS_SEQUENCE. This field displays **N/A** when no values exist, and it can display a maximum of 20 values.

display rib graceful-restart

Use **display rib graceful-restart** to display RIB GR state information.

Syntax

display rib graceful-restart

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display RIB GR state information.

```
<Sysname> display rib graceful-restart
RIB GR state     : Phase2-calculation end
RCOM GR state    : Flush end
Protocol GR state:
 No.  Protocol   Lifetime FD   State    Start/End
-------------------------------------------------
 1    DIRECT     100      30   End      No/No
 2    STATIC     480      34   End      No/No
 3    OSPF       480      36   End      No/No
 4    ISIS       480      32   End      No/No
```

Table 9 Command output

Field	Description
RIB GR state	RIB GR status: • **Start**—GR starts. • **IGP end**—All IGP protocols complete GR. • **VPN-triggering end**—Optimal route selection triggered by VPN routes completes. • **VPN-calculation end**—Optimal VPN route selection completes. • **Routing protocol end**—All routing protocols complete GR. • **NSR-calculation unfinished**—NSR has not finished optimal route selection. • **Triggering start**—All triggered optimal route selection starts. • **Triggering end**—All triggered optimal route selection completes. • **Phase1-calculation end**—Optimal route selection phase 1 completes. • **All end**—All protocols complete GR. • **Phase2-calculation end**—Optimal route selection phase 2 completes.
RCOM GR state	RCOM GR status: • **Start**—GR starts. • **VPN-calculation end**—Optimal VPN route selection completes. • **VPN-notification end**—VPN routes have been delivered to the route management module. • **Routing protocol end**—All routing protocols complete GR. • **NSR-calculation unfinished**—NSR has not finished optimal route selection. • **Phase1-calculation end**—Optimal route selection phase 1 completes. • **Notification end**—All routes have been delivered to the route management module. • **Phase2-calculation end**—Optimal route selection phase 2 completes. • **Flush start**—Starts to flush routes to the FIB. • **Flush end**—Completes flushing routes to the FIB.
No.	Protocol number.
Lifetime	Lifetime (in seconds) of routes in the RIB during GR.
FD	Handle between the protocol and the RIB.
State	Protocol GR state: • **Init**—Initialization state. • **Listen**—Listening state. • Idle. • Active. • **Start**—GR starts. • **End**—GR completes.
Start/End	Message sending state: • **No**—The message has not been sent. • **Yes**—The message has been sent.

display rib nib

Use **display rib nib** to display next hop information in the RIB.

Syntax

display rib nib [**self-originated**] [*nib-id*] [**verbose**]

display rib nib protocol *protocol* [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

self-originated: Displays information about next hops of self-originated routes in the RIB.

nib-id: Specifies a NIB by its ID, a hexadecimal string in the range of 1 to ffffffff.

verbose: Displays detailed next hop information in the RIB. If you do not specify this keyword, the command displays brief next hop information in the RIB.

protocol *protocol*: Specifies a protocol by its name.

Examples

Display brief next hop information in the RIB.

```
<Sysname> display rib nib
Total number of nexthop(s): 176

      NibID: 0x10000000        Sequence: 0
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: 0.0.0.0
    IFIndex: 0x111           LocalAddr: 0.0.0.0
   TopoNthp: 0

      NibID: 0x10000001        Sequence: 1
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: 127.0.0.1
    IFIndex: 0x112           LocalAddr: 127.0.0.1
   TopoNthp: 0

      NibID: 0x10000002        Sequence: 2
       Type: 0x5                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: 127.0.0.1
    IFIndex: 0x112           LocalAddr: 127.0.0.1
```

```
   TopoNthp: 0

      NibID: 0x16000000        Sequence: 3
       Type: 0x21               Flushed: No
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: 12.1.1.2
    IFIndex: 0x0               LocalAddr: 0.0.0.0
   TopoNthp: 0
   Instance: abc

...
```

Table 10 Command output

Field	Description
NibID	ID of the next hop.
Sequence	Sequence number of the next hop.
Type	Type of the next hop.
Flushed	Indicates whether the route with the next hop has been flushed to the FIB.
UserKey0	Reserved data 1.
UserKey1	Reserved data 2.
VrfNthp	Index of the VPN instance that the next hop belongs to. This field displays **0** if the next hop is on the public network.
Nexthop	Next hop address.
IFIndex	Interface index.
LocalAddr	Local interface address.
TopoNthp	Non-base topologies are not supported in the current software version. Index of the topology that contains the next hop. This field displays **0** if the next hop is on the IPv4 public network. This field displays **Invalid** if the next hop is on an IPv6 network, because the router does not support multiple IPv6 topologies.
Instance	BGP instance name.
SubNibID	ID of the sub-next hop.
SubSeq	Sequence number of the sub-next hop.
NthpCnt	Number of sub-next hops.
Samed	Number of the same sub-next hops.
NthpType	Type of the sub-next hop: **IP**—IP forwarding.

Display detailed next hop information in the RIB.

```
<Sysname> display rib nib verbose
Total number of nexthop(s): 176

      NibID: 0x10000000        Sequence: 0
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
```

```
   UserKey1: 0x0               Nexthop: 0.0.0.0
    IFIndex: 0x111           LocalAddr: 0.0.0.0
   TopoNthp: 0
     RefCnt: 6             FlushRefCnt: 2
       Flag: 0x84              Version: 1
 1 nexthop(s):
PrefixIndex: 0             OrigNexthop: 0.0.0.0
  RelyDepth: 0             RealNexthop: 0.0.0.0
  Interface: NULL0           LocalAddr: 0.0.0.0
  TunnelCnt: 0                    Vrf: default-vrf
   TunnelID: N/A              Topology: base
     Weight: 0

      NibID: 0x10000001        Sequence: 1
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: 127.0.0.1
    IFIndex: 0x112           LocalAddr: 127.0.0.1
   TopoNthp: 0
     RefCnt: 13            FlushRefCnt: 5
       Flag: 0x84              Version: 1
 1 nexthop(s):
PrefixIndex: 0             OrigNexthop: 127.0.0.1
  RelyDepth: 0             RealNexthop: 127.0.0.1
  Interface: InLoop0         LocalAddr: 127.0.0.1
  TunnelCnt: 0                    Vrf: default-vrf
   TunnelID: N/A              Topology: base
     Weight: 0

      NibID: 0x15000003        Sequence: 3
       Type: 0x43               Flushed: Yes
   UserKey0: 0x100010000        VrfNthp: 0
   UserKey1: 0x0                Nexthop: 22.22.22.22
    IFIndex: 0x0             LocalAddr: 0.0.0.0
   TopoNthp: 0
   Instance: default
     RefCnt: 9             FlushRefCnt: 3
       Flag: 0x84              Version: 1
 1 nexthop(s):
PrefixIndex: 0             OrigNexthop: 22.22.22.22
  RelyDepth: 1             RealNexthop: 13.1.1.2
  Interface: GE1/0/3         LocalAddr: 13.1.1.1
  TunnelCnt: 1                    Vrf: default-vrf
   TunnelID: 1025             Topology: base
     Weight: 0

...
```

Table 11 Command output

Field	Description
x nexthop (s)	Number of next hops.
PrefixIndex	Prefix index of the next hop for an ECMP route.
Vrf	VPN instance name. For the public network, this field displays **default-vrf**.
OrigNexthop	Original next hop.
RealNexthop	Real next hop.
Interface	Output interface.
LocalAddr	Local interface address.
RelyDepth	Recursion depth.
TunnelCnt	Number of tunnels after route recursion.
TunnelID	ID of the tunnel after route recursion.
Topology	Non-base topologies are not supported in the current software version. Topology name. The topology name for the IPv4 public network is **base**. This field is blank for IPv6, because IPv6 does not support multiple topologies.
Weight	ECMP route weight. This field displays 0 for non-ECMP routes.
Instance	BGP instance name.
RefCnt	Reference count of the next hop.
FlushRefCnt	Reference count of the next hop that is flushed to the FIB.
Flag	Flag of the next hop.
Version	Version of the next hop.

display route-direct nib

Use **`display route-direct nib`** to display next hop information for direct routes.

Syntax

`display route-direct nib` [*`nib-id`*] [**`verbose`**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

`nib-id`: Specifies a NIB by its ID, a hexadecimal string in the range of 1 to ffffffff.

`verbose`: Displays detailed next hop information for direct routes. If you do not specify this keyword, the command displays brief next hop information for direct routes.

Examples

Display brief next hop information for direct routes.

```
<Sysname> display route-direct nib
Total number of nexthop(s): 116

      NibID: 0x10000000        Sequence: 0
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: 0.0.0.0
    IFIndex: 0x111             LocalAddr: 0.0.0.0
   TopoNthp: 0

      NibID: 0x10000001        Sequence: 1
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: 127.0.0.1
    IFIndex: 0x112             LocalAddr: 127.0.0.1
   TopoNthp: 0

...
```

Table 12 Command output

Field	Description
NibID	ID of the NIB.
Sequence	Sequence number of the NIB.
Type	Type of the NIB.
Flushed	Indicates whether the route with the NIB has been flushed to the FIB.
UserKey0	Reserved data 1.
UserKey1	Reserved data 2.
VrfNthp	Index of the VPN instance that the next hop belongs to. This field displays **0** if the next hop is on the public network.
Nexthop	Next hop address.
IFIndex	Interface index.
LocalAddr	Local interface IP address.
TopoNthp	This field is not supported in the current software version. Index of the topology that contains the next hop. This field displays **0** if the next hop is on the IPv4 public network. This field displays **Invalid** if the next hop is on an IPv6 network, because the router does not support multiple IPv6 topologies.

Display detailed next hop information for direct routes.

```
<Sysname> display route-direct nib verbose
Total number of nexthop(s): 116

      NibID: 0x10000000        Sequence: 0
       Type: 0x1                Flushed: Yes
```

```
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: 0.0.0.0
    IFIndex: 0x111            LocalAddr: 0.0.0.0
     RefCnt: 2              FlushRefCnt: 0
       Flag: 0x2                Version: 1
 1 nexthop(s):
PrefixIndex: 0              OrigNexthop: 0.0.0.0
  RelyDepth: 0              RealNexthop: 0.0.0.0
  Interface: NULL0            LocalAddr: 0.0.0.0
  TunnelCnt: 0                      Vrf: default-vrf
   TunnelID: N/A               Topology: base
     Weight: 0

      NibID: 0x10000001         Sequence: 1
       Type: 0x1                 Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: 127.0.0.1
    IFIndex: 0x112            LocalAddr: 127.0.0.1
     RefCnt: 5              FlushRefCnt: 0
       Flag: 0x2                Version: 1
 1 nexthop(s):
PrefixIndex: 0              OrigNexthop: 127.0.0.1
  RelyDepth: 0              RealNexthop: 127.0.0.1
  Interface: InLoop0          LocalAddr: 127.0.0.1
  TunnelCnt: 0                      Vrf: default-vrf
   TunnelID: N/A               Topology: base
     Weight: 0
...
```

Table 13 Command output

Field	Description
x nexthop(s)	Number of next hops.
PrefixIndex	Prefix index of the next hop for an ECMP route.
Vrf	VPN instance name. For the public network, this field displays **default-vrf**.
OrigNexthop	Original next hop.
RealNexthop	Real next hop.
Interface	Output interface.
localAddr	Local interface address.
RelyDepth	Recursion depth.
TunnelCnt	Number of tunnels after route recursion.
TunnelID	ID of the tunnel after route recursion.
Topology	Non-base topologies are not supported in the current software version. Topology name. The topology name for the IPv4 public network is **base**. This field is blank for IPv6, because IPv6 does not support multiple topologies.

Field	Description
Weight	ECMP route weight. This field displays 0 for non-ECMP routes.
RefCnt	Reference count of the next hop.
FlushRefCnt	Reference count of the next hop that is flushed to the FIB.
Flag	Flag of the next hop.
Version	Version of the next hop.

fib lifetime

Use **fib lifetime** to set the maximum lifetime for IPv4 or IPv6 routes in the FIB.

Use **undo fib lifetime** to restore the default.

Syntax

fib lifetime *seconds*

undo fib lifetime

Default

The maximum lifetime for IPv4 or IPv6 routes in the FIB is 600 seconds.

Views

RIB IPv4 address family view

RIB IPv6 address family view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies the maximum lifetime for routes in the FIB, in the range of 0 to 6000 seconds. When this argument is set to 0, FIB entries immediately age out after a protocol or RIB process switchover.

Usage guidelines

When a protocol or RIB process switchover occurs and GR or NSR is not configured, FIB entries age out after the time specified in this command.

Examples

Set the maximum lifetime for IPv4 routes in the FIB to 60 seconds.

```
<Sysname> system-view
[Sysname] rib
[Sysname-rib] address-family ipv4
[Sysname-rib-ipv4] fib lifetime 60
```

inter-protocol fast-reroute

Use **inter-protocol fast-reroute** to enable IPv4 or IPv6 RIB inter-protocol FRR.

Use **undo inter-protocol fast-reroute** to disable IPv4 or IPv6 RIB inter-protocol FRR.

Syntax

inter-protocol fast-reroute [**vpn-instance** *vpn-instance-name*]

undo inter-protocol fast-reroute [**vpn-instance** *vpn-instance-name*]

Default

Inter-protocol FRR is disabled.

Views

RIB IPv4 address family view

RIB IPv6 address family view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command enables IPv4 or IPv6 RIB inter-protocol FRR for the public network.

Usage guidelines

This command allows a device to perform fast rerouting between routes of different protocols. A backup next hop is automatically selected to reduce the service interruption time caused by unreachable next hops. When the next hop of the primary link fails, the traffic is redirected to the backup next hop.

This command uses the next hop of a route from a different protocol as the backup next hop for the faulty route, which might cause loops.

Inter-protocol FRR cannot select a backup next hop from routes in the RIB that have the same next hop, output interface, and destination as those of the faulty route.

Examples

Enable IPv4 RIB inter-protocol FRR for the public network.

```
<Sysname> system-view
[Sysname] rib
[Sysname-rib] address-family ipv4
[Sysname-rib-ipv4] inter-protocol fast-reroute
```

ipv6 max-ecmp-num

Use **ipv6 max-ecmp-num** to set the maximum number of IPv6 ECMP routes.

Syntax

ipv6 max-ecmp-num *number*

Default

Models	Default
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1180, NFNX3-HDB1480	16
NFNX3-HDB1780, NFNX3-HDB3080	Not supported
NFNX3-HDB680, NFNX3-HDB1080	32

Views

System view

Predefined user roles

network-admin

Parameters

number: Specifies the maximum number of IPv6 ECMP routes. The value range for this argument is 1 to 128.

Usage guidelines

This command takes effect after a device reboot. Before you reboot the device, make sure you understand the potential impact on the network.

This command is supported only on the default context.

Examples

Set the maximum number of IPv6 ECMP routes to 10.

```
<Sysname> system-view
[Sysname] ipv6 max-ecmp-num 10
The configuration will take effect at the next reboot. Continue? [Y/N]:y
Reboot device to make the configuration take effect.
```

After reboot, the maximum number of IPv6 ECMP routes is 10.

Related commands

display ipv6 max-ecmp-num

max-ecmp-num

Use **max-ecmp-num** to set the maximum number of IPv4 ECMP routes.

Syntax

max-ecmp-num *number*

Default

Models	Default
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1180, NFNX3-HDB1480	16
NFNX3-HDB1780, NFNX3-HDB3080	Not supported
NFNX3-HDB680, NFNX3-HDB1080	32

Views

System view

Predefined user roles

network-admin

Parameters

number: Specifies the maximum number of IPv4 ECMP routes. The value range for this argument is 1 to 128.

Usage guidelines

This command takes effect after a device reboot. Before you reboot the device, make sure you understand the potential impact on the network.

This command is supported only on the default context.

Examples

Set the maximum number of IPv4 ECMP routes to 10.

```
<Sysname> system-view
[Sysname] max-ecmp-num 10
The configuration will take effect at the next reboot. Continue? [Y/N]:y
Reboot device to make the configuration take effect.
```

After reboot, the maximum number of IPv4 ECMP routes is 10.

Related commands

display max-ecmp-num

non-stop-routing

Use **non-stop-routing** to enable RIB NSR.

Use **undo non-stop-routing** to disable RIB NSR.

Syntax

non-stop-routing

undo non-stop-routing

Default

RIB NSR is disabled.

Views

RIB IPv4 address family view

RIB IPv6 address family view

Predefined user roles

network-admin

context-admin

Examples

Enable NSR for the RIB IPv4 address family.

```
<Sysname> system-view
[Sysname] rib
[Sysname-rib] address-family ipv4
[Sysname-rib-ipv4] non-stop-routing
```

protocol lifetime

Use **protocol lifetime** to set the maximum lifetime for IPv4 or IPv6 routes in the RIB.

Use **undo protocol lifetime** to restore the default.

Syntax

protocol *protocol* [**instance** *instance-name*] **lifetime** *seconds*

undo protocol *protocol* [**instance** *instance-name*] **lifetime**

Default

The maximum lifetime for IPv4 or IPv6 routes in the RIB is 480 seconds.

Views

RIB IPv4 address family view

RIB IPv6 address family view

Predefined user roles

network-admin

context-admin

Parameters

protocol: Specifies a routing protocol.

instance *instance-name*: Specifies a BGP instance by its name, a case-sensitive string of 1 to 31 characters. This argument applies only to the BGP protocol. If you do not specify a BGP instance, this command sets the maximum lifetime for all BGP routes and labels in the RIB.

seconds: Specifies the maximum lifetime for routes and labels in the RIB, in the range of 1 to 6000 seconds.

Usage guidelines

When GR is enabled, make sure the protocol can complete GR and install all route entries to the RIB within the lifetime configured in this command.

Examples

Set the maximum lifetime for RIP routes in the RIB to 60 seconds.

```
<Sysname> system-view
[Sysname] rib
[Sysname-rib] address-family ipv4
[Sysname-rib-ipv4] protocol rip lifetime 60
```

reset ip routing-table statistics protocol

Use **reset ip routing-table statistics protocol** to clear IPv4 route statistics.

Syntax

reset ip routing-table statistics protocol [**vpn-instance** *vpn-instance-name*] { *protocol* | **all** }

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command clears IPv4 route statistics for the public network.

protocol: Clears route statistics for a routing protocol.

all: Clears route statistics for all IPv4 routing protocols.

Usage guidelines

This command clears only statistics of added and deleted routes for the specified routing protocols.

Examples

Clear all IPv4 route statistics for the public network.

```
<Sysname> reset ip routing-table statistics protocol all
```

reset ipv6 routing-table statistics protocol

Use **reset ipv6 routing-table statistics protocol** to clear IPv6 route statistics.

Syntax

reset ipv6 routing-table statistics protocol [**vpn-instance** *vpn-instance-name*] { *protocol* | **all** }

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command clears the IPv6 route statistics for the public network.

protocol: Clears route statistics for an IPv6 routing protocol.

all: Clears route statistics for all IPv6 routing protocols.

Usage guidelines

This command clears only statistics of added and deleted routes for the specified routing protocols.

Examples

Clear all IPv6 route statistics for the public network.

```
<Sysname> reset ipv6 routing-table statistics protocol all
```

rib

Use **rib** to enter RIB view.

Use **undo rib** to remove all configurations in RIB view.

Syntax

rib

undo rib

Views

System view

Predefined user roles

network-admin

context-admin

Examples

Enter RIB view.

```
<Sysname> system-view
[Sysname] rib
[Sysname-rib]
```

Contents

Static routing commands

delete static-routes all

Use **delete static-routes all** to delete all static routes.

Syntax

delete [**vpn-instance** *vpn-instance-name*] **static-routes all**

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command deletes all static routes for the public network.

Usage guidelines

CAUTION:

This command might interrupt network communication and cause packet forwarding failure. Before executing the command, make sure you fully understand the potential impact on the network.

When you use this command, the system will prompt you to confirm the operation before deleting all the static routes.

To delete one static route, use the **undo ip route-static** command. To delete all static routes, including the default route, use the **delete static-routes all** command.

Examples

Delete all static routes.

```
<Sysname> system-view
[Sysname] delete static-routes all
This will erase all IPv4 static routes and their configurations, you must reconfigure all static routes.
Are you sure?[Y/N]:y
```

Related commands

ip route-static

display route-static nib

Use **display route-static nib** to display static route next hop information.

Syntax

display route-static nib [*nib-id*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

nib-id: Specifies a NIB by its ID, a hexadecimal string of 1 to ffffffff. If you do not specify this argument, the command displays all static route next hop information.

verbose: Displays detailed static route next hop information. If you do not specify this keyword, the command displays brief static route next hop information.

Examples

Displays brief static route next hop information.

```
<Sysname> display route-static nib
Total number of nexthop(s): 44

     NibID: 0x11000000       Sequence: 0
      Type: 0x21             Flushed: Yes
  UserKey0: 0x111             VrfNthp: 0
  UserKey1: 0x0               Nexthop: 0.0.0.0
   IFIndex: 0x111           LocalAddr: 0.0.0.0
  TopoNthp: 0

     NibID: 0x11000001       Sequence: 1
      Type: 0x41             Flushed: Yes
  UserKey0: 0x0               VrfNthp: 5
  UserKey1: 0x0               Nexthop: 2.2.2.2
   IFIndex: 0x0             LocalAddr: 0.0.0.0
  TopoNthp: 0

...
```

Table 1 Command output

Field	Description
NibID	ID of the NIB.
Sequence	Sequence number of the NIB.
Type	Type of the NIB.
Flushed	Indicates whether the route with the NIB has been flushed to the FIB.
UserKey0	Reserved data 1.
UserKey1	Reserved data 2.
VrfNthp	Index of the VPN instance that the next hop belongs to. This field displays **0** if the next hop is on the public network.

Field	Description
Nexthop	Next hop address.
IFIndex	Interface index
LocalAddr	Local interface address.
TopoNthp	This field is not supported in the current software version. Index of the topology that contains the next hop. This field displays **0** if the next hop is on the public network.

Displays detailed static route next hop information.

```
<Sysname> display route-static nib verbose
Total number of nexthop(s): 44

     NibID: 0x11000000      Sequence: 0
      Type: 0x21            Flushed: Yes
   UserKey0: 0x111           VrfNthp: 0
   UserKey1: 0x0             Nexthop: 0.0.0.0
    IFIndex: 0x111         LocalAddr: 0.0.0.0
   TopoNthp: 0
     RefCnt: 2           FlushRefCnt: 0
       Flag: 0x2            Version: 1
 1 nexthop(s):
PrefixIndex: 0           OrigNexthop: 0.0.0.0
  RelyDepth: 0           RealNexthop: 0.0.0.0
  Interface: NULL0         LocalAddr: 0.0.0.0
  TunnelCnt: 0                 Vrf: default-vrf
   TunnelID: N/A           Topology: base
     Weight: 1000000

     NibID: 0x11000001      Sequence: 1
      Type: 0x41            Flushed: Yes
   UserKey0: 0x0             VrfNthp: 5
   UserKey1: 0x0             Nexthop: 2.2.2.2
    IFIndex: 0x0           LocalAddr: 0.0.0.0
   TopoNthp: 0
     RefCnt: 1           FlushRefCnt: 0
       Flag: 0x12           Version: 1
 2 nexthop(s):
PrefixIndex: 0           OrigNexthop: 2.2.2.2
  RelyDepth: 7           RealNexthop: 8.8.8.8
  Interface: GE1/0/2       LocalAddr: 12.12.12.12
  TunnelCnt: 0                 Vrf: default-vrf
   TunnelID: N/A           Topology: base
     Weight: 1000000
PrefixIndex: 0           OrigNexthop: 2.2.2.2
  RelyDepth: 9           RealNexthop: 0.0.0.0
  Interface: NULL0         LocalAddr: 0.0.0.0
  TunnelCnt: 0                 Vrf: default-vrf
```

```
  TunnelID: N/A            Topology: base
    Weight: 1000000

...
```

Table 2 Command output

Field	Description
NibID	ID of the NIB.
Sequence	Sequence number of the NIB.
Type	Type of the NIB.
Flushed	Indicates whether the route with the NIB has been flushed to the FIB.
UserKey0	Reserved data 1.
VrfNthp	Index of the VPN instance that the next hop belongs to. This field displays **0** if the next hop is on the public network.
UserKey1	Reserved data 2.
Nexthop	Next hop address.
IFIndex	Interface index
LocalAddr	Local interface address.
TopoNthp	Index of the topology that contains the next hop. This field displays **0** if the next hop is on the public network.
RefCnt	Reference count of the next hop.
FlushRefCnt	Reference count of the next hop that is flushed to the FIB.
Flag	Flag of the next hop.
Version	Version of the next hop.
x nexthop(s)	Number of next hops.
PrefixIndex	Prefix index of the next hop for an ECMP route.
OrigNexthop	Original next hop.
RelyDepth	Recursion depth.
RealNexthop	Real next hop.
Interface	Output interface.
localAddr	Local interface address.
TunnelCnt	Number of tunnels after route recursion.
Vrf	VPN instance name. For the public network, this field displays **default-vrf**.
TunnelID	ID of the tunnel after route recursion.
Topology	This field is not supported in the current software version. Topology name. The topology name for the public network is **base**.
Weight	ECMP route weight. This field displays 0 for non-ECMP routes.

display route-static routing-table

Use **display route-static routing-table** to display static routing table information.

Syntax

display route-static routing-table [**vpn-instance** *vpn-instance-name*] [*ip-address* { *mask-length* | *mask* }]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays static routing table information for the public network.

ip-address: Specifies the destination IP address in dotted decimal notation. If you do not specify this argument, the command displays all static routing table information.

mask-length: Specifies the mask length, an integer in the range of 0 to 32.

mask: Specifies the subnet mask in dotted decimal notation.

Examples

Display static routing table information.

```
<Sysname> display route-static routing-table
Total number of routes: 24

Status: * - valid

*Destination: 0.0.0.0/0
      NibID: 0x1100000a       NextHop: 2.2.2.10
   MainNibID: N/A           BkNextHop: N/A
     BkNibID: N/A           Interface: GigabitEthernet1/0/1
     TableID: 0x2         BkInterface: GigabitEthernet1/0/2
        Flag: 0x82d01        BfdSrcIp: N/A
     DbIndex: 0xd          BfdIfIndex: 0x0
        Type: Normal       BfdVrfIndex: 0
  TrackIndex: 0xffffffff        Label: NULL
  Preference: 60          vrfIndexDst: 0
     BfdMode: N/A          vrfIndexNH: 0
   Permanent: 0                 Tag: 0

 Destination: 0.0.0.0/0
      NibID: 0x1100000b       NextHop: 2.2.2.11
   MainNibID: N/A           BkNextHop: N/A
```

```
   BkNibID: N/A            Interface: GigabitEthernet1/0/3
   TableID: 0x2          BkInterface: GigabitEthernet1/0/4
      Flag: 0x82d01         BfdSrcIp: N/A
   DbIndex: 0xd           BfdIfIndex: 0x0
      Type: Normal        BfdVrfIndex: 0
 TrackIndex: 0xffffffff         Label: NULL
 Preference: 60           vrfIndexDst: 0
   BfdMode: N/A           vrfIndexNH: 0
  Permanent: 0                  Tag: 0
```

...

Table 3 Command output

Field	Description
destination	Destination address/prefix.
NibID	ID of the NIB.
MainNibID	ID of the primary next hop for static route FRR.
BkNibID	ID of the backup next hop for static route FRR.
NextHop	Next hop address.
BkNextHop	Backup next hop address.
Interface	Output interface of the route.
BkInterface	Backup output interface.
TableID	ID of the table to which the route belongs.
Flag	Flag of the route.
DbIndex	Index of the database to which the route belongs.
Type	Route type: • Normal. • DHCP. • NAT. • IPsec.
BfdSrcIp	Source IP address of the indirect BFD session.
BfdIfIndex	Index of the interface where BFD is enabled.
BfdVrfIndex	Index of the VPN instance where BFD is enabled. This field displays **0** if BFD is enabled for the public network.
BfdMode	BFD session mode: • **N/A**—No BFD session is configured. • **Ctrl**—Control packet mode • **Echo**—Echo packet mode.
TrackIndex	NQA Track index.
Label	This field is not supported in the current software version. Label.
vrfIndexDst	Index of VPN instance that the destination belongs to. For the public network, this field displays **0**.

Field	Description
vrfIndexNH	Index of the VPN instance that the next hop belongs to. For the public network, this field displays **0**.
Permanent	Permanent static route flag. 1 indicates a permanent static route.

ip route-static

Use **ip route-static** to configure a static route.

Use **undo ip route-static** to delete a static route.

Syntax

ip route-static { *dest-address* { *mask-length* | *mask* } | **group** *group-name* } *interface-type interface-number* [**dhcp** | *next-hop-address*] [**backup-interface** *interface-type interface-number* [**backup-nexthop** *backup-nexthop-address*] [**permanent**] | **bfd** { **control-packet** | **echo-packet** | **static** *session-name* } | **permanent** | **track** *track-entry-number*] [**preference** *preference*] [**tag** *tag-value*] [**description** *text*]

ip route-static { *dest-address* { *mask-length* | *mask* } | **group** *group-name* } *next-hop-address* [**bfd control-packet bfd-source** *ip-address* | **permanent** | **track** *track-entry-number*] [**preference** *preference*] [**tag** *tag-value*] [**description** *text*]

ip route-static { *dest-address* { *mask-length* | *mask* } | **group** *group-name* } **vpn-instance** *d-vpn-instance-name next-hop-address* [**bfd control-packet bfd-source** *ip-address* | **permanent** | **track** *track-entry-number*] [**preference** *preference*] [**tag** *tag-value*] [**description** *text*]

undo ip route-static { *dest-address* { *mask-length* | *mask* } | **group** *group-name* } [*interface-type interface-number* [**dhcp** | *next-hop-address*] | *next-hop-address* | **vpn-instance** *d-vpn-instance-name next-hop-address*] [**preference** *preference*]

Default

No static route is configured.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

dest-address: Specifies the destination IP address of the static route, in dotted decimal notation.

mask-length: Specifies the mask length, an integer in the range of 0 to 32.

mask: Specifies the subnet mask in dotted decimal notation.

group *group-name*: Specifies a static route group by its name, a case-sensitive string of 1 to 31 characters.

vpn-instance *d-vpn-instance-name*: Specifies a destination MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If a destination VPN instance is specified, packets will search for the output interface in the destination VPN instance based on the configured next hop address.

interface-type interface-number: Specifies an output interface by its type and number. For more information, see *Layer 3—IP Routing Configuration Guide*.

dhcp: Specifies the default router designated by the DHCP server for the output interface as the next hop of the static route.

next-hop-address: Specifies the IP address of the next hop, in dotted decimal notation. For more information, see *Layer 3—IP Routing Configuration Guide*.

backup-interface *interface-type interface-number*: Specifies a backup output interface by its type and number. If the backup output interface is a broadcast interface, you must specify the backup next hop address.

backup-nexthop *backup-nexthop-address*: Specifies a backup next hop address.

bfd: Enables BFD to detect reachability of the static route's next hop. When the next hop is unreachable, the system immediately switches to the backup route.

control-packet: Specifies the BFD control mode.

bfd-source *ip-address*: Specifies the source IP address of BFD packets. As a best practice, specify the loopback interface address.

echo-packet: Specifies the BFD echo mode.

static *session-name*: Specifies a static BFD session by its name, a case-sensitive string of 1 to 64 characters. You can specify a nonexistent static BFD session. For the configuration to take effect, you must create the static BFD session.

permanent: Specifies the route as a permanent static route. If the output interface is down, the permanent static route is still active.

track *track-entry-number*: Associates the static route with a track entry specified by its number in the range of 1 to 1024. For more information about Track, see *Network Management and Monitoring Configuration Guide*.

preference *preference*: Specifies a preference for the static route, in the range of 1 to 255. The default is 60.

tag *tag-value*: Sets a tag value for marking the static route, in the range of 1 to 4294967295. The default is 0. Tags of routes are used for route control in routing policies. For more information about routing policies, see *Layer 3—IP Routing Configuration Guide*.

description *text*: Configures a description of 1 to 60 characters for the static route. The description can include special characters, such as the space, except the question mark (?).

Usage guidelines

If the destination IP address and the mask are both 0.0.0.0 (or 0), the configured route is a default route. The default route is used for forwarding a packet matching no entry in the routing table.

Implement different routing policies to configure different route preferences. For example, to enable load sharing for multiple routes to the same destination, assign the same preference to the routes. To enable the routes to back up one another, assign different preferences to them.

Follow these guidelines when you specify the output interface or the next hop address of the static route:

- If the output interface is a Null 0 interface, no next hop address is required.
- If the output interface is a point-to-point interface, you can specify only the output interface. You do not need to change the configuration of the route even if the peer address is changed.

- Multiple next hops might exist if the output interface is a broadcast interface (for example, an Ethernet interface or VLAN interface). You must specify both the output interface and next hop IP address for the static route.

Follow these guidelines when you configure a static route:

- Enabling BFD for a flapping route could worsen the route flapping situation. Therefore, use it with caution. For more information about BFD, see *Network Management and Monitoring Configuration Guide*.
- For static routing-Track-NQA collaboration, you must configure the same VPN instance ID for the next hop to be detected and the NQA operation.
- If a static route needs route recursion, the associated track entry must monitor the next hop of the recursive route instead of that of the static route. Otherwise, a valid route might be mistakenly considered invalid.

If you specify a static route group, all prefixes in the static route group will be assigned the next hop and output interface specified by using this command.

After an interface obtains an IP address and gateway address through DHCP, the device automatically generates a static route with the interface as the output interface. The destination address of the static route is 0.0.0.0/0 and the next hop of the static route is the default router (the gateway address designated by the DHCP server). This static route cannot form ECMP routes with manually configured static routes. The device uses this static route to guide traffic forwarding only after the manually configured static routes become invalid.

Specify the **dhcp** keyword to use both the automatically generated static route and the manually configured static routes to guide traffic forwarding. This keyword is applicable when the device has dual egress WAN links.

The **dhcp** keyword enables the device to automatically generate a static route destined for the specified network with the DHCP-designated default router of the output interface as the next hop. This static route takes effect only after the output interface obtains an IP address and gateway address through DHCP, and becomes invalid upon the DHCP lease expiration. The next hop of this static route changes as the gateway address of the output interface changes. In addition, this static route can form ECMP routes with manually configured static routes.

To specify the **dhcp** keyword, make sure the output interface of the static route is a broadcast interface.

Examples

Configure a static route, whose destination address is 1.1.1.1/24, next hop address is 2.2.2.2, tag value is 45, and description information is **for internet**.

```
<Sysname> system-view
[Sysname] ip route-static 1.1.1.1 24 2.2.2.2 tag 45 description for internet
```

Related commands

display ip routing-table protocol

ip route-static-group

prefix

ip route-static default-preference

Use **ip route-static default-preference** to configure a default preference for static routes.

Use **undo ip route-static default-preference** to restore the default.

Syntax

ip route-static default-preference *default-preference*

undo ip route-static default-preference

Default

The default preference of static routes is 60.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

default-preference: Specifies a default preference for static routes, in the range of 1 to 255.

Usage guidelines

If no preference is specified for a static route, the default preference applies.

When the default preference is reconfigured, it applies only to newly added static routes.

Examples

Set a default preference of 120 for static routes.

```
<Sysname> system-view
[Sysname] ip route-static default-preference 120
```

Related commands

display ip routing-table protocol

ip route-static fast-reroute auto

Use **ip route-static fast-reroute auto** to configure static route FRR to automatically select a backup next hop.

Use **undo ip route-static fast-reroute auto** to disable static route FRR from automatically selecting a backup next hop.

Syntax

ip route-static fast-reroute auto

undo ip route-static fast-reroute auto

Default

Static route FRR is disabled from automatically selecting a backup next hop.

Views

System view

Predefined user roles

network-admin

context-admin

Examples

Configure static route FRR to automatically select a backup next hop.

```
<Sysname> system-view
[Sysname] ip route-static fast-reroute auto
```

ip route-static primary-path-detect bfd echo

Use **ip route-static primary-path-detect bfd echo** to enable BFD echo packet mode for static route FRR.

Use **undo ip route-static primary-path-detect bfd** to disable BFD echo packet mode for static route FRR.

Syntax

ip route-static primary-path-detect bfd echo

undo ip route-static primary-path-detect bfd

Default

BFD echo packet mode for static route FRR is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command enables static route FRR to use BFD echo packet mode for fast failure detection on the primary link.

Examples

Enable BFD echo packet mode for static route FRR.

```
<Sysname> system-view
[Sysname] ip route-static 1.1.1.1 32 gigabitethernet 1/0/1 2.2.2.2 backup-interface
gigabitethernet 1/0/2 backup-nexthop 3.3.3.3
[Sysname] ip route-static primary-path-detect bfd echo
```

ip route-static vpn-instance

Use **ip route-static vpn-instance** to configure a static route in a VPN instance.

Use **undo ip route-static vpn-instance** to delete a static route from a VPN instance.

Syntax

ip route-static vpn-instance *s-vpn-instance-name dest-address* { *mask-length* | *mask* } *interface-type interface-number* [**dhcp** | *next-hop-address*] [**backup-interface** *interface-type interface-number* [**backup-nexthop** *backup-nexthop-address*] [**permanent**] | **bfd** { **control-packet** | **echo-packet** | **static** *session-name* } | **permanent** | **track** *track-entry-number*] [**preference** *preference*] [**tag** *tag-value*] [**description** *text*]

ip route-static vpn-instance *s-vpn-instance-name dest-address* { *mask-length* | *mask* } **vpn-instance** *d-vpn-instance-name next-hop-address* [**bfd control-packet bfd-source** *ip-address* | **permanent** | **track** *track-entry-number*] [**preference** *preference*] [**tag** *tag-value*] [**description** *text*]

ip route-static vpn-instance *s-vpn-instance-name dest-address* { *mask-length* | *mask* } *next-hop-address* [**public**] [**bfd control-packet**

bfd-source *ip-address* | **permanent** | **track** *track-entry-number*] [**preference** *preference*] [**tag** *tag-value*] [**description** *text*]

ip route-static vpn-instance *s-vpn-instance-name dest-address* { *mask-length* | *mask* } **vpn-instance** *d-vpn-instance-name* [**track** *track-entry-number*] [**preference** *preference*] [**tag** *tag-value*] [**description** *text*]

ip route-static vpn-instance *s-vpn-instance-name* **group** *group-name interface-type interface-number* [**dhcp** | *next-hop-address*] [**bfd** { **control-packet** | **echo-packet** | **static** *session-name* } | **backup-interface** *interface-type interface-number* [**backup-nexthop** *backup-nexthop-address*] [**permanent**]] [**preference** *preference*] [**tag** *tag-value*] [**description** *text*]

ip route-static vpn-instance *s-vpn-instance-name* **group** *group-name next-hop-address* [**public**] [**bfd control-packet bfd-source** *ip-address* | **permanent** | **track** *track-entry-number*] [**preference** *preference*] [**tag** *tag-value*] [**description** *text*]

undo ip route-static vpn-instance *s-vpn-instance-name* { *dest-address* { *mask-length* | *mask* } | **group** *group-name* } [*interface-type interface-number* [**dhcp** | *next-hop-address*] | *next-hop-address* [**public**] | **vpn-instance** *d-vpn-instance-name next-hop-address*] [**preference** *preference*]

Default

No static route is configured in a VPN instance.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

s-vpn-instance-name: Specifies a source MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. Each VPN instance has its own routing table, and the configured static route is installed in the routing tables of the specified VPN instances.

dest-address: Specifies the destination IP address of the static route, in dotted decimal notation.

mask-length: Specifies the mask length, an integer in the range of 0 to 32.

mask: Specifies the subnet mask in dotted decimal notation.

group *group-name*: Specifies a static route group by its name, a case-sensitive string of 1 to 31 characters.

vpn-instance *d-vpn-instance-name*: Specifies a destination MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If a destination VPN instance is specified, packets will search for the output interface in the destination VPN instance based on the configured next hop address.

interface-type interface-number: Specifies an output interface by its type and number. For more information, see *Layer 3—IP Routing Configuration Guide*.

dhcp: Specifies the default router designated by the DHCP server for the output interface as the next hop of the static route.

next-hop-address: Specifies the IP address of the next hop, in dotted decimal notation. For more information, see *Layer 3—IP Routing Configuration Guide*.

backup-interface *interface-type interface-number*: Specifies a backup output interface by its type and number. If the backup output interface is a non-P2P interface (an NBMA interface or broadcast interface), you must specify the backup next hop address.

backup-nexthop *backup-nexthop-address*: Specifies a backup next hop address.

bfd: Enables BFD to detect reachability of the static route's next hop. When the next hop is unreachable, the system immediately switches to the backup route.

control-packet: Specifies the BFD control mode.

bfd-source *ip-address*: Specifies the source IP address of BFD packets. As a best practice, specify the loopback interface address.

echo-packet: Specifies the BFD echo mode.

static *session-name*: Specifies a static BFD session by its name, a case-sensitive string of 1 to 64 characters. You can specify a nonexistent static BFD session. For the configuration to take effect, you must create the static BFD session.

permanent: Specifies the route as a permanent static route. If the output interface is down, the permanent static route is still active.

track *track-entry-number*: Associates the static route with a track entry specified by its number in the range of 1 to 1024. For more information about Track, see *Network Management and Monitoring Configuration Guide*.

public: Specifies the public network, which indicates that the specified next hop address is on the public network. The device searches for the output interface in the public network based on the next hop address for packets matching the static route. If you do not specify this keyword or the destination VPN instance, the specified next hop address is in the source VPN instance. The device searches for the output interface in the source VPN instance based on the next hop address for packets matching the static route.

preference *preference*: Specifies a preference for the static route, in the range of 1 to 255. The default is 60.

tag *tag-value*: Sets a tag value for marking the static route, in the range of 1 to 4294967295. The default is 0. Tags of routes are used for route control in routing policies. For more information about routing policies, see *Layer 3—IP Routing Configuration Guide*.

description *text*: Configures a description of 1 to 60 characters for the static route. The description can include special characters, such as the space, except the question mark (?).

Usage guidelines

If the destination IP address and the mask are both 0.0.0.0 (or 0), the configured route is a default route. The default route is used for forwarding a packet matching no entry in the routing table.

Implement different routing policies to configure different route preferences. For example, to enable load sharing for multiple routes to the same destination, assign the same preference to the routes. To enable the routes to back up one another, assign different preferences to them.

Follow these guidelines when you specify the output interface or the next hop address of the static route:

- If the output interface is a Null 0 interface, no next hop address is required.
- If the output interface is a point-to-point interface, you can specify only the output interface. You do not need to change the configuration of the route even if the peer address is changed.
- If the output interface is a broadcast interface (for example, an Ethernet interface or VLAN interface), the device uses the next hop IP address to obtain the MAC address of the next hop. Therefore, you must specify both the output interface and next hop IP address.

Follow these guidelines when you configure a static route:

- Enabling BFD for a flapping route could worsen the route flapping situation. Therefore, use it with caution. For more information about BFD, see *Network Management and Monitoring Configuration Guide*.
- For static routing-Track-NQA collaboration, you must configure the same VPN instance ID for the next hop to be detected and the NQA operation.
- If a static route needs route recursion, the associated track entry must monitor the next hop of the related route instead of that of the recursive static route. Otherwise, a valid route might be mistakenly considered invalid.

If you specify a static route group, all prefixes in the static route group will be assigned the next hop and output interface specified by using this command.

After an interface obtains an IP address and gateway address through DHCP, the device automatically generates a static route with the interface as the output interface. The destination address of the static route is 0.0.0.0/0 and the next hop of the static route is the default router (the gateway address designated by the DHCP server). This static route cannot form ECMP routes with manually configured static routes. The device uses this static route to guide traffic forwarding only after the manually configured static routes become invalid.

Specify the **dhcp** keyword to use both the automatically generated static route and the manually configured static routes to guide traffic forwarding. This keyword is applicable when the device has dual egress WAN links.

The **dhcp** keyword enables the device to automatically generate a static route destined for the specified network with the DHCP-designated default router of the output interface as the next hop. This static route takes effect only after the output interface obtains an IP address and gateway address through DHCP, and becomes invalid upon the DHCP lease expiration. The next hop of this static route changes as the gateway address of the output interface changes. In addition, this static route can form ECMP routes with manually configured static routes.

To specify the **dhcp** keyword, make sure the output interface of the static route is a broadcast interface.

Examples

Configure a static route in VPN instance **vpn1**, whose destination address is 1.1.1.1/24, next hop address is 2.2.2.2 in VPN instance **vpn2**, tag value is 45, and description information is **for internet**.

```
<Sysname> system-view
[Sysname] ip route-static vpn-instance vpn1 1.1.1.1 24 vpn-instance vpn2 2.2.2.2 tag 45
description for internet
```

Related commands

display ip routing-table protocol

ip route-static-group

prefix

ip route-static-group

Use **ip route-static-group** to create a static route group and enter its view, or enter the view of an existing static route group.

Use **undo ip route-static-group** to delete a static route group.

Syntax

ip route-static-group *group-name*

undo ip route-static-group *group-name*

Default

No static route groups exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies the static route group name, a case-sensitive string of 1 to 31 characters.

Examples

Create static route group **test** and enter its view.

```
<Sysname> system-view
[Sysname] ip route-static-group test
[Sysname-route-static-group-test]
```

Related commands

ip route-static

prefix

prefix

Use **prefix** to add a static route prefix to a static route group.

Use **undo prefix** to delete a static route prefix from a static route group.

Syntax

prefix *dest-address* { *mask-length* | *mask* }

undo prefix *dest-address* { *mask-length* | *mask* }

Default

No static route prefix is added to a static route group.

Views

Static route group view

Predefined user roles

network-admin

context-admin

Parameters

dest-address: Specifies the destination IP address of the static route, in dotted decimal notation.

mask-length: Specifies the mask length, an integer in the range of 0 to 32.

mask: Specifies the subnet mask in dotted decimal notation.

Usage guidelines

Execute this command repeatedly to add multiple static route prefixes to a static route group.

After you add static route prefixes to a static route group, you can specify that group in the **ip route-static group** command to configure static routes with the prefixes. To configure more static routes, you only need to add new static route prefixes to the group.

Examples

Add static route prefix 1.1.1.1/32 to static route group **test**.

```
<Sysname> system-view
[Sysname] ip route-static-group test
[Sysname-route-static-group-test] prefix 1.1.1.1 32
```

Related commands

ip route-static

ip route-static-group

Contents

IPv6 static routing commands

delete ipv6 static-routes all

Use **delete ipv6 static-routes all** to delete all IPv6 static routes.

Syntax

delete ipv6 [**vpn-instance** *vpn-instance-name*] **static-routes all**

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command deletes all IPv6 static routes for the public network.

Usage guidelines

CAUTION:

This command might interrupt network communication and cause packet forwarding failure. Before executing the command, make sure you fully understand the potential impact on the network.

When you use this command, the system will prompt you to confirm the operation before deleting all the IPv6 static routes.

Examples

Delete all IPv6 static routes.

```
<Sysname> system-view
[Sysname] delete ipv6 static-routes all
This will erase all IPv6 static routes and their configurations, you must reconfigure all static routes.
Are you sure?[Y/N]:y
```

Related commands

ipv6 route-static

display ipv6 route-static nib

Use **display ipv6 route-static nib** to display IPv6 static route next hop information.

Syntax

display ipv6 route-static nib [*nib-id*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

nib-id: Specifies a NIB by its ID, a hexadecimal string in the range of 1 to ffffffff.

verbose: Displays detailed IPv6 static route next hop information. If you do not specify this keyword, the command displays brief IPv6 static route next hop information.

Examples

Display brief IPv6 static route next hop information.

```
<Sysname> display ipv6 route-static nib
Total number of nexthop(s): 35

      NibID: 0x21000000        Sequence: 0
       Type: 0x41               Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: 2::3
    IFIndex: 0x0              LocalAddr: ::
   TopoNthp: Invalid

      NibID: 0x21000001        Sequence: 1
       Type: 0x41               Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: 3::4
    IFIndex: 0x0              LocalAddr: ::
   TopoNthp: Invalid

...
```

Table 1 Command output

Field	Description
NibID	ID of the NIB.
Sequence	Sequence number of the NIB.
Type	Type of the NIB.
Flushed	Indicates whether the route with the NIB has been flushed to the FIB.
UserKey0	Reserved data 1.
UserKey1	Reserved data 2.
VrfNthp	Index of the VPN instance to which the next hop belongs. This field displays **0** if the next hop is on the public network.
Nexthop	Next hop address.
IFIndex	Interface index
LocalAddr	Local interface address.

Field	Description
TopoNthp	This field is not supported in the current software version. Index of the topology that contains the next hop. This field displays **Invalid** if the next hop is on an IPv6 network, because the router does not support multiple topologies.

Display detailed IPv6 static route next hop information.

```
<Sysname> display ipv6 route-static nib verbose
Total number of nexthop(s): 35

      NibID: 0x21000000        Sequence: 0
       Type: 0x41               Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: 2::3
    IFIndex: 0x0              LocalAddr: ::
   TopoNthp: Invalid
     RefCnt: 1              FlushRefCnt: 0
       Flag: 0x12               Version: 1
 1 nexthop(s):
PrefixIndex: 0              OrigNexthop: 2::3
  RelyDepth: 2              RealNexthop: ::
  Interface: NULL0            LocalAddr: ::
  TunnelCnt: 0                      Vrf: default-vrf
   TunnelID: N/A               Topology:
     Weight: 0

      NibID: 0x21000001        Sequence: 1
       Type: 0x41               Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: 3::4
    IFIndex: 0x0              LocalAddr: ::
   TopoNthp: Invalid
     RefCnt: 1              FlushRefCnt: 0
       Flag: 0x12               Version: 1
 1 nexthop(s):
PrefixIndex: 0              OrigNexthop: 3::4
  RelyDepth: 1              RealNexthop: ::
  Interface: GE1/0/1          LocalAddr: ::
  TunnelCnt: 0                      Vrf: default-vrf
   TunnelID: N/A               Topology:
     Weight: 0

...
```

Table 2 Command output

Field	Description
x nexthop(s)	Number of next hops.

Field	Description
PrefixIndex	Prefix index of the next hop for an ECMP route.
Vrf	VPN instance name. For the public network, this field displays **default-vrf**.
OrigNexthop	Original next hop.
RealNexthop	Real next hop.
Interface	Output interface.
localAddr	Local interface address.
RelyDepth	Recursion depth.
TunnelCnt	Number of tunnels after route recursion.
TunnelID	ID of the tunnel after route recursion.
Topology	This field is not supported in the current software version. Topology name. This field is blank for IPv6, because IPv6 does not support multiple topologies.
Weight	ECMP route weight. This field displays 0 for non-ECMP routes.
RefCnt	Reference count of the next hop.
FlushRefCnt	Reference count of the next hop that is flushed to the FIB.
Flag	Flag of the next hop.
Version	Version of the next hop.

display ipv6 route-static routing-table

Use **display ipv6 route-static routing-table** to display IPv6 static routing table information.

Syntax

display ipv6 route-static routing-table [**vpn-instance** *vpn-instance-name*] [*ipv6-address prefix-length*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the command displays IPv6 static routing table information for the public network.

ipv6-address: Specifies the destination IPv6 address.

prefix-length: Specifies the prefix length in the range of 0 to 128.

Examples

Display IPv6 static routing table information.

```
<Sysname> display ipv6 route-static routing-table
Total number of routes: 5

Status: * - valid

*Destination: 1::1/128
       NibID: 0x21000000        NextHop: 2::2
   MainNibID: N/A             BkNextHop: N/A
     BkNibID: N/A             Interface: GigabitEthernet1/0/1
     TableID: 0xa           BkInterface: N/A
        Flag: 0x80d0a          BfdSrcIp: N/A
     DbIndex: 0x3            BfdIfIndex: 0x0
        Type: Normal        BfdVrfIndex: 0
  TrackIndex: 0xffffffff          Label: NULL
  Preference: 60            vrfIndexDst: 0
     BfdMode: N/A            vrfIndexNH: 0
   Permanent: 0                     Tag: 0

*Destination: 1::1234/128
      NibID: 0x21000000        NextHop: 2::2
   MainNibID: N/A             BkNextHop: N/A
     BkNibID: N/A             Interface: NULL0
     TableID: 0xa           BkInterface: N/A
        Flag: 0x80d0a          BfdSrcIp: N/A
     DbIndex: 0x1            BfdIfIndex: 0x0
        Type: Normal        BfdVrfIndex: 0
  TrackIndex: 0xffffffff          Label: NULL
  Preference: 60            vrfIndexDst: 0
     BfdMode: N/A            vrfIndexNH: 0
   Permanent: 0                     Tag: 0

...
```

Table 3 Command output

Field	Description
Destination	Destination address/prefix.
NibID	ID of the NIB.
MainNibID	ID of the primary next hop for static route FRR.
BkNibID	ID of the backup next hop for static route FRR.
NextHop	Next hop address.
BkNextHop	Backup next hop address.
Interface	Output interface of the route.
BkInterface	Backup output interface.

Field	Description
TableID	ID of the table to which the route belongs.
DbIndex	Index of the database to which the route belongs.
Type	Route type: • Normal. • DHCP. • NAT.
BfdSrcIp	Source IPv6 address of the indirect BFD session.
BfdIfIndex	Index of the interface where BFD is enabled.
BfdVrfIndex	Index of the VPN instance where BFD is enabled. This field displays **0** if BFD is enabled for the public network.
BfdMode	BFD session mode: • **N/A**—No BFD session is configured. • **Ctrl**—Control packet mode. • **Echo**—Echo packet mode.
TrackIndex	NQA Track index.
Label	This field is not supported in the current software version. Label.
vrfIndexDst	Index of the VPN instance to which the destination belongs. For the public network, this field displays **0**.
vrfIndexNH	Index of the VPN instance to which the next hop belongs. For the public network, this field displays **0**.
Permanent	Permanent static route flag. 1 indicates a permanent static route.

ipv6 route-static

Use **ipv6 route-static** to configure an IPv6 static route.

Use **undo ipv6 route-static** to remove an IPv6 static route.

Syntax

ipv6 route-static *ipv6-address prefix-length* { *interface-type interface-number* [*next-hop-address*] [**bfd** { **control-packet** | **echo-packet** } [**bfd-source** *ipv6-address*] | **permanent** | **track** *track-entry-number*] | [**vpn-instance** *d-vpn-instance-name*] *next-hop-address* [**bfd control-packet bfd-source** *ipv6-address* | **permanent** | **track** *track-entry-number*] } [**preference** *preference*] [**tag** *tag-value*] [**description** *text*]

undo ipv6 route-static *ipv6-address prefix-length* [*interface-type interface-number* [*next-hop-address*] | [**vpn-instance** *d-vpn-instance-name*] *next-hop-address*] [**preference** *preference*]

ipv6 route-static vpn-instance *s-vpn-instance-name ipv6-address prefix-length* { *interface-type interface-number* [*next-hop-address*] [**bfd** { **control-packet** | **echo-packet** } [**bfd-source** *ipv6-address*] | **permanent** | **track** *track-entry-number*] | *next-hop-address* [**public**] [**bfd control-packet bfd-source** *ipv6-address* | **permanent**] | **vpn-instance** *d-vpn-instance-name next-hop-address* [**bfd control-packet bfd-source**

ipv6-address | **permanent** | **track** *track-entry-number*] } [**preference** *preference*] [**tag** *tag-value*] [**description** *text*]

undo ipv6 route-static vpn-instance *s-vpn-instance-name ipv6-address prefix-length* [*interface-type interface-number* [*next-hop-address*] | *next-hop-address* [**public**] | **vpn-instance** *d-vpn-instance-name next-hop-address*] [**preference** *preference*]

Default

No IPv6 static route is configured.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address prefix-length: Specifies the IPv6 address and prefix length.

interface-type interface-number: Specifies an output interface by its type and number. If the output interface is an NBMA interface or broadcast interface and not a point-to-point (P2P) interface, the next hop address must be specified.

next-hop-address: Specifies the next hop IPv6 address.

bfd: Enables BFD to detect reachability of the static route's next hop.

control-packet: Specifies the BFD control packet mode.

bfd-source *ipv6-address*: Specifies the source IPv6 address of BFD packets.

echo-packet: Specifies the BFD echo packet mode.

permanent: Specifies the IPv6 route as a permanent IPv6 static route. If the output interface is down, the permanent IPv6 static route is still active.

track *track-entry-number*: Associates the IPv6 static route with a track entry specified by its number in the range of 1 to 1024. For more information about Track, see *Network Management and Monitoring Configuration Guide*.

public: Indicates the next hop is on the public network.

- With this keyword specified, the system searches for an output interface for the IPv6 static route from the public network IPv6 routing table based on the specified next hop.
- Without this keyword and the destination VPN instance specified, the next hop of the IPv6 static route belongs to the source VPN instance. In this case, the system searches for an output interface for the IPv6 static route from the routing table of the source VPN instance based on the specified next hop.

vpn-instance *d-vpn-instance-name*: Specifies a destination MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If a destination VPN is specified, packets will search for the output interface based on the specified next hop (IPv6 address) for the static route.

preference *preference*: Specifies a preference for IPv6 static routes, in the range of 1 to 255. The default is 60.

tag *tag-value*: Sets a tag for marking the static route, in the range of 1 to 4294967295. The default is 0. Tags of routes are used for route control in routing policies. For more information about routing policies, see *Layer 3—IP Routing Configuration Guide*.

description *text*: Configures a description for the IPv6 static route, which consists of 1 to 60 characters, including special characters such as the space, but excluding the question mark (?).

vpn-instance *s-vpn-instance-name*: Specifies a source MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. Each VPN has its own routing table, and the configured static route is installed in the routing tables of the specified VPNs.

Usage guidelines

An IPv6 static route that has the destination address configured as **::/0** (a prefix length of 0) is the default IPv6 route. If the destination address of an IPv6 packet does not match any entry in the routing table, this default route is used to forward the packet.

Follow these guidelines to configure the output interface, next hop address, or both for a static route:

- If the output interface is a broadcast interface or an NBMA interface, the next hop address must be specified.
- If the output interface is a P2P interface, you can specify only the output interface. You do not need to change the configuration of the route even if the peer address is changed.

Follow these guidelines when you configure BFD for IPv6 static routes:

- If you specify the source IPv6 address of BFD packets, you must specify the IPv6 address as the next hop IPv6 address on the peer device.
- If you specify a non-P2P output interface and a direct next hop, specify the **bfd-source** *ipv6-address* option as a best practice. Make sure the source IPv6 address of BFD packets meets the following requirements:
  - The address is the same as the IPv6 address of the output interface.
  - The address is on the same network segment as the next hop IPv6 address of the same type.

    For example, if the next hop IPv6 address is a link-local address, the source IPv6 address of BFD packets must also be a link-local address.

Follow these guidelines when you configure a static route:

- Enabling BFD for a flapping route could worsen the route flapping situation. Therefore, use it with caution. For more information about BFD, see *Network Management and Monitoring Configuration Guide*.
- The next hop IPv6 address of echo packets must be a global unicast address.

For IPv6 static routing-Track-NQA collaboration, you must configure the same VPN instance ID for the next hop to be detected and the NQA operation.

Examples

Configure an IPv6 static route, with the destination address 1:1:2::/64 and next hop 1:1:3::1.

```
<Sysname> system-view
[Sysname] ipv6 route-static 1:1:2:: 64 1:1:3::1
```

Related commands

display ipv6 routing-table protocol

ipv6 route-static default-preference

Use **ipv6 route-static default-preference** to set a default preference for IPv6 static routes.

Use **undo ipv6 route-static default-preference** to restore the default.

Syntax

ipv6 route-static default-preference *default-preference*

undo ipv6 route-static default-preference

Default

The default preference of IPv6 static routes is 60.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

default-preference: Specifies a default preference for IPv6 static routes, in the range of 1 to 255.

Usage guidelines

If no preference is specified for an IPv6 static route, the default preference applies.

When the default preference is reconfigured, it applies only to newly added IPv6 static routes.

Examples

Set a default preference of 120 for IPv6 static routes.

```
<Sysname> system-view
[Sysname] ipv6 route-static default-preference 120
```

Related commands

display ipv6 routing-table protocol

Contents

RIP commands

bfd all-interfaces enable

Use **bfd all-interfaces enable** to enable BFD on all interfaces of a RIP process.

Use **undo bfd all-interfaces enable** to restore the default.

Syntax

bfd all-interfaces enable [**ctrl**]

undo bfd all-interfaces enable

Default

BFD is disabled on the interfaces of a RIP process.

Views

RIP view

Predefined user roles

network-admin

context-admin

Parameters

ctrl: Enables BFD bidirectional control detection for both directly and indirectly connected neighbors. If you do not specify this keyword, RIP uses BFD single-hop echo detection for directly connected neighbors and uses BFD bidirectional control detection for indirectly connected neighbors.

Usage guidelines

RIP supports the following BFD detection modes:

- **Single-hop echo detection**—Detection mode for a directly connected neighbor. In this mode, a BFD session is established only when the directly connected neighbor has route information to send.
- **Single-hop echo detection for a specific destination**—Detection mode for a directly connected neighbor. In this mode, a BFD session is established to the specified RIP neighbor when RIP is enabled on the local interface.
- **Bidirectional control detection**—Detection mode for both directly and indirectly connected neighbors. In this mode, a BFD session is established only when both ends have routes to send and BFD is enabled on the receiving interface.

You must configure bidirectional control detection on both ends of a link for it to take effect.

The BFD session to a neighbor does not come down when you execute the **undo peer** command to delete its address. This is because the RIP neighbor relationship is not immediately deleted when you execute the **undo peer** command.

The BFD setting configured in interface view takes precedence over the BFD setting configured in RIP view.

Examples

Enable BFD on all interfaces of RIP process 1.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] bfd all-interfaces enable
```

Related commands

rip bfd

checkzero

Use **checkzero** to enable zero field check on RIPv1 messages.

Use **undo checkzero** to disable zero field check.

Syntax

checkzero

undo checkzero

Default

The zero field check function is enabled.

Views

RIP view

Predefined user roles

network-admin

context-admin

Usage guidelines

When the zero field check is enabled, the router discards RIPv1 messages in which zero fields contain non-zero values. If all messages are trustworthy, disable this feature to reduce the workload of the CPU.

Examples

Disable zero field check on RIPv1 messages for RIP process 1.

```
<Sysname> system-view
[Sysname] rip
[Sysname-rip-1] undo checkzero
```

default cost

Use **default cost** to configure a default metric for redistributed routes.

Use **undo default cost** to restore the default.

Syntax

default cost *cost-value*

undo default cost

Default

The default metric of redistributed routes is 0.

Views

RIP view

Predefined user roles

network-admin

context-admin

Parameters

cost-value: Specifies a default metric for redistributed routes, in the range of 0 to 16.

Usage guidelines

When you use the **import-route** command to redistribute routes from another routing protocol without specifying a metric, the metric specified by the **default cost** command applies.

Examples

Configure a default metric of 3 for redistributed routes.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] default cost 3
```

Related commands

import-route

default-route

Use **default-route** to configure all interfaces running a RIP process to advertise a default route with a specified metric to RIP neighbors.

Use **undo default-route** to restore the default.

Syntax

default-route { **only** | **originate** } [**cost** *cost-value* | **route-policy** *route-policy-name*]*

undo default-route

Default

No default route is sent to RIP neighbors.

Views

RIP view

Predefined user roles

network-admin

context-admin

Parameters

only: Advertises only a default route.

originate: Advertises both a default route and other routes.

cost-value: Specifies a cost for the default route, in the range of 1 to 15. The default is 1.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case sensitive string of 1 to 63 characters. If you specify this option, the command advertises a default route only when a route in the routing table matches the routing policy.

Usage guidelines

A RIP router configured with this feature does not receive any default route from RIP neighbors.

Examples

Configure all interfaces running RIP process 100 to send only a default route with a metric of 2 to RIP neighbors.

```
<Sysname> system-view
```

```
[Sysname] rip 100
[Sysname-rip-100] default-route only cost 2
```

Related commands

rip default-route

display rip

Use **display rip** to display state and configuration information for a RIP process.

Syntax

display rip [*process-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies a RIP process by its ID in the range of 1 to 65535. If no process is specified, the command displays state and configuration information for all RIP processes.

Examples

Display current state and configuration information for all RIP processes.

```
<Sysname> display rip
  Public VPN-instance name:
    RIP process: 1
       RIP version: 1
       Preference: 100
           Routing policy: abc
       Fast-reroute:
           Routing policy: frr
       Checkzero: Enabled
       Default cost: 0
       Summary: Enabled
       Host routes: Enabled
       Maximum number of load balanced routes: 8
       Update time   :   30 secs  Timeout time         :  180 secs
       Suppress time :  120 secs  Garbage-collect time :  120 secs
       Update output delay:   20(ms)  Output count:    3
       Graceful-restart interval:   60 secs
       Triggered Interval : 5 50 200
       BFD: Enabled (ctrl)
       Silent interfaces: None
       Default routes: Originate  Default routes cost: 3
       Verify-source: Enabled
```

```
Networks:
    1.0.0.0
Configured peers:
    197.168.6.2
Triggered updates sent: 0
Number of routes changes: 1
Number of replies to queries: 0
```

Table 1 Command output

Field	Description
Public VPN-instance name	The RIP process runs on the public network.
Private VPN-instance name	VPN instance where the RIP process runs.
RIP process	RIP process ID.
RIP version	RIP version 1 or 2.
Preference	RIP preference.
Fast-reroute	RIP FRR.
Checkzero	Indicates whether the zero field check is enabled for RIPv1 messages: **Enabled** or **Disabled**.
Default cost	Default cost of redistributed routes.
Summary	Indicates whether route summarization is enabled: **Enabled** or **Disabled**.
Host routes	Indicates whether to receive host routes: **Enabled** or **Disabled**.
Maximum number of load balanced routes	Maximum number of ECMP routes for load balancing.
Update time	RIP update interval, in seconds.
Timeout time	RIP timeout time, in seconds.
Suppress time	RIP suppress interval, in seconds.
Garbage-collect time	RIP garbage-collect interval, in seconds.
Update output delay	RIP packet sending interval, in seconds.
Output count	Maximum number of RIP packets sent at each interval.
Graceful-restart interval	GR interval, in seconds.
Triggered Interval	Triggered update sending interval.
BFD	Whether BFD is enabled: • **Disabled**—Disabled in RIP view. • **Enabled**—Enabled in RIP view. RIP uses BFD single-hop echo detection for a directly connected neighbor and uses BFD bidirectional control detection for an indirectly connected neighbor. • **Enabled (ctrl)**—Enabled in RIP view. RIP uses BFD bidirectional control detection for both directly and indirectly connected neighbors.
Silent interfaces	Silent interfaces, which do not periodically send updates.

Field	Description
Default routes	Indicates whether a default route is sent to RIP neighbors. • **only**—Only a default route is advertised. • **originate**—A default route is advertised along with other routes. • **disable**—No default route is advertised.
Default routes cost	Metric for a default route.
Verify-source	Indicates whether the source IP address is checked for received RIP routing updates: **Enabled** or **Disabled**.
Networks	Networks enabled with RIP.
Configured peers	Configured neighbors.
Triggered updates sent	Number of triggered updates sent.
Number of routes changes	Number of route changes.
Number of replies to queries	Number of RIP responses.

display rip database

Use **display rip database** to display active routes for a RIP process.

Syntax

display rip *process-id* **database** [*ip-address* { *mask-length* | *mask* }]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies a RIP process by its ID in the range of 1 to 65535.

ip-address { *mask-length* | *mask* }: Displays active routes for the specified IP address. If you do not specify this argument, the command displays all actives routes for a RIP process.

Examples

Display active routes for RIP process 100.

```
<Sysname> display rip 100 database
   1.0.0.0/8, auto-summary
       1.1.1.0/24, cost 16, interface summary
       1.1.1.0/24, cost 0, nexthop 1.1.1.1, RIP-interface
       1.1.2.0/24, cost 0, imported
   2.0.0.0/8, auto-summary
   2.0.0.0/8, cost 1, nexthop 1.1.1.2
```

Display active routes with destination IP address 1.1.1.0 and mask length 24 for RIP process 100.

```
<Sysname> display rip 100 database 1.1.1.0 24
   1.1.1.0/24, cost 16, interface summary
   1.1.1.0/24, cost 0, nexthop 1.1.1.1, RIP-interface
```

Table 2 Command output

Field	Description
cost	Cost of the route.
auto-summary	Indicates that the route is a RIP automatic summary route.
interface summary	Indicates that the route is a RIP interface summary route.
nexthop	Address of the next hop.
RIP-interface	Direct route on a RIP-enabled interface.
imported	Indicates that the route is redistributed from another routing protocol.

display rip graceful-restart

Use **display rip graceful-restart** to display the GR status for a RIP process.

Syntax

display rip [*process-id*] **graceful-restart**

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies a RIP process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays the GR status for all RIP processes.

Examples

Display the GR status for RIP process 1.

```
<Sysname> display rip 1 graceful-restart
 RIP process: 1
 Graceful Restart capability     : Enabled
 Current GR state                : Normal
 Graceful Restart period         : 60  seconds
 Graceful Restart remaining time : 0   seconds
```

Table 3 Command output

Field	Description
Graceful Restart capability	Indicates whether GR is enabled: **Enabled** or **Disabled**.
Current GR state	GR state: • **Under GR**—GR is in progress.

Field	Description
	• **Normal**—No GR is in progress or GR has completed.
Graceful Restart period	GR interval.

display rip interface

Use **display rip interface** to display RIP interface information for a RIP process.

Syntax

display rip *process-id* **interface** [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies a RIP process by its ID in the range of 1 to 65535.

interface-type interface-number: Specifies an interface by its type and number. If no interface is specified, the command displays information about all RIP interfaces for the RIP process.

Examples

Display information about all interfaces for RIP process 1.

```
<Sysname> display rip 1 interface
Total: 1

 Interface: GigabitEthernet1/0/2
    Address/Mask: 1.1.1.1/24          Version: RIPv1
    MetricIn: 0                       MetricIn route policy: Not designated
    MetricOut: 1                      MetricOut route policy: Not designated
    Split-horizon/Poison-reverse: On/Off  Input/Output: On/On
    Default route: Off
    Update output delay:  20(ms)      Output count: 3
    BFD: Enabled (ctrl), inherited
    Current number of packets/Maximum number of packets: 0/2000
```

Table 4 Command output

Field	Description
Total	Number of interfaces running RIP.
Interface	Name of an interface running RIP.
Address/Mask	IP address and mask of the interface.
Version	RIP version running on the interface.
MetricIn	Additional metric added to incoming routes.

Field	Description
MetricIn route policy	Name of the routing policy used to add an additional metric for incoming routes. If no routing policy is used, the field displays **Not designated**.
MetricOut	Additional metric added to outgoing routes.
MetricOut route policy	Name of the routing policy used to add an additional routing metric for outgoing routes. If no routing policy is used, the field displays **Not designated**.
Split-horizon	Indicates whether split horizon is enabled: • **on**—Enabled. • **off**—Disabled.
Poison-reverse	Indicates whether poison reverse is enabled: • **on**—Enabled. • **off**—Disabled.
Input/Output	Indicates whether the interface is enabled to receive and send RIP messages: • **on**—Enabled. • **off**—Disabled.
Default route	Indicates whether to send a default route to RIP neighbors: • **Only**—Advertises only a default route. • **Originate**—Advertises both a default route and other routes. • **No-originate**—Advertises only non-default routes. • **Off**—Advertises no default route.
Default route cost	Metric for a default route.
Update output delay	RIP packet sending interval.
Output count	Maximum number of RIP packets that can be sent at each interval.
BFD	Whether BFD for RIP is enabled: • **Disabled**—Disabled in interface view and RIP view. • **Enabled**—Enabled on the RIP interface. The interface uses BFD single-hop echo detection for a directly connected neighbor and uses BFD bidirectional control detection for an indirectly connected neighbor. • **Enabled (ctrl)**—Enabled on the RIP interface. The interface uses BFD bidirectional control detection for both directly and indirectly connected neighbors. • **Enabled, inherited**—Enabled in RIP view. RIP uses BFD single-hop echo detection for a directly connected neighbor and uses BFD bidirectional control detection for an indirectly connected neighbor. The RIP interface uses the BFD setting configured in RIP view. • **Enabled (ctrl), inherited**—Enabled in RIP view. RIP uses BFD bidirectional control detection for both directly and indirectly connected neighbors. The RIP interface uses the BFD setting configured in RIP view. • **Enabled (destination)**—Enabled on the RIP interface. The interface uses BFD single-hop echo detection for a specific destination.
Current number of packets /Maximum number of packets	Number of RIP packets to be sent/maximum number of RIP packets that can be sent within a certain interval.

display rip neighbor

Use **display rip neighbor** to display neighbor information for a RIP process.

Syntax

display rip *process-id* **neighbor** [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies a RIP process by its ID in the range of 1 to 65535.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify this argument, the command displays all neighbor information for the RIP process.

Examples

Display neighbor information for RIP process 1.

```
<Sysname> display rip 1 neighbor
 Neighbor address: 197.168.2.3
     Interface  : GigabitEthernet1/0/2
     Version    : RIPv2     Last update: 00h00m02s
     Relay nbr  : N/A       BFD session: N/A
     Bad packets: 0         Bad routes : 0
```

Table 5 Command output

Field	Description
Interface	Output interface that is connected to the neighbor.
Version	Version of RIP that the neighbor runs.
Last update	Time elapsed since the most recent update.
Relay nbr	Relay neighbor type.
BFD session	BFD session type.
Bad packets	Number of received bad packets.
Bad routes	Number of received bad routes.

display rip non-stop-routing

Use **display rip non-stop-routing** to display the NSR status for a RIP process.

Syntax

display rip [*process-id*] **non-stop-routing**

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies a RIP process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays the NSR status for all RIP processes.

Examples

Display the NSR status for RIP process 1.

```
<Sysname> display rip 1 non-stop-routing
RIP process: 1
 Nonstop Routing capability: Enabled
 Current NSR state         : Finish
```

Table 6 Command output

Field	Description
Nonstop Routing capability	Indicates whether NSR is enabled: **Enabled** or **Disabled**.
Current NSR state	NSR state: • Initialization. • **Smooth**—Upgrading data. • **Advertising**—Advertising routes. • **Redistribution**—Redistributing routes. • Finish.

display rip route

Use **display rip route** to display routing information for a RIP process.

Syntax

display rip *process-id* **route** [*ip-address* { *mask-length* | *mask* } [**verbose**] | **peer** *ip-address* | **statistics**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies a RIP process by its ID in the range of 1 to 65535.

ip-address { *mask-length* | *mask* }: Displays route information for the specified IP address.

verbose: Displays all routing information for the specified destination IP address. If you do not specify this keyword, the command displays only information about optimal routes with the specified destination IP address.

peer *ip-address*: Displays route information learned from the specified neighbor.

statistics: Displays route statistics, including the total number of routes and number of routes from each neighbor.

Usage guidelines

If no optional parameters are specified, the **display rip** *process-id* **route** command displays all routing information for a RIP process.

Examples

Display all routing information for RIP process 1.

```
<Sysname> display rip 1 route
 Route Flags: R - RIP
              P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
              D - Direct, O - Optimal, F - Flush to RIB
 ------------------------------------------------------------------------------
 Peer 1.1.1.1 on GigabitEthernet1/0/2
      Destination/Mask        Nexthop           Cost    Tag     Flags   Sec
      3.0.0.0/8               1.1.1.1           1       0       RAOF    24
 Local route
      Destination/Mask        Nexthop           Cost    Tag     Flags   Sec
      4.4.4.4/32              0.0.0.0           0       0       RDOF    -
      1.1.1.0/24              0.0.0.0           0       0       RDOF    -
```

Display specified routing information for RIP process 1.

```
<Sysname> display rip 1 route 3.0.0.0 8 verbose
 Route Flags: R - RIP
              P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
              D - Direct, O - Optimal, F - Flush to RIB
 ------------------------------------------------------------------------------
 Peer 1.1.1.1 on GigabitEthernet1/0/2
  Destination/Mask    OrigNexthop/RealNexthop          Cost  Tag   Flags Sec
  3.0.0.0/8           1.1.1.1/1.1.1.1                  1     0     RAOF  16
```

Table 7 Command output

Field	Description
Route Flags	• **R**—RIP route. • **P**—The route never ages out. • **A**—The route is aging. • **S**—The route is suppressed. • **G**—The route is in Garbage-collect state. • **D**—The route is a direct route. • **O**—The route is an optimal route. • **F**—The route has been flushed to the RIB.
Peer *X.X.X.X* on *interface-type interface-number*	Routing information learned from a neighbor on a RIP interface.
Local route	Locally generated direct routes.

Field	Description
Destination/Mask	Destination IP address and subnet mask.
Nexthop	Next hop of the route.
OrigNexthop/RealNexthop	If the route is from a directly connected neighbor, the original next hop is the real next hop. If the route is from an indirectly connected neighbor, the **RealNexthop** field displays the recursive next hop for the route. Otherwise, the field is blank.
Cost	Cost of the route.
Tag	Route tag.
Flags	Route state.
Sec	Remaining time of the timer corresponding to the route state.

Display routing statistics for RIP process 1.

```
<Sysname> display rip 1 route statistics
 Peer                    Optimal/Aging       Optimal/Permanent       Garbage
 1.1.1.1                 1/1                 0/0                     0
 Local                   2/0                 0/0                     0
 Total                   3/1                 0/0                     0
```

Table 8 Command output

Field	Description
Peer	IP address of a neighbor.
Optimal	Total number of optimal routes.
Aging	Total number of aging routes.
Permanent	Total number of routes that never age out.
Garbage	Total number of routes in the Garbage-collection state.
Local	Total number of locally generated direct routes.
Total	Total number of routes learned from all RIP neighbors.

fast-reroute

Use **fast-reroute** to configure RIP FRR.

Use **undo fast-reroute** to disable RIP FRR.

Syntax

fast-reroute route-policy *route-policy-name*

undo fast-reroute

Default

RIP FRR is disabled.

Views

RIP view

Predefined user roles

network-admin

context-admin

Parameters

route-policy *route-policy-name*: Specifies a routing policy by its name, a case sensitive string of 1 to 63 characters. If you specify this option, the command designates a backup next hop for the routes that match the routing policy.

Usage guidelines

RIP FRR is available only when the state of primary link (with Layer 3 interfaces staying up) changes from bidirectional to unidirectional or down. A unidirectional link refers to the link through which packets are forwarded only from one end to the other.

RIP FRR is only effective for RIP routes that are learned from directly connected neighbors.

Equal-cost routes do not support RIP FRR.

Examples

Enable RIP FRR and use routing policy **frr** to specify a backup next hop.

```
<Sysname> system-view
[Sysname] ip prefix-list abc index 10 permit 100.1.1.0 24
[Sysname] route-policy frr permit node 10
[Sysname-route-policy-frr-10] if-match ip address prefix-list abc
[Sysname-route-policy-frr-10] apply fast-reroute backup-interface gigabitethernet 1/0/1
backup-nexthop 193.1.1.8
[Sysname-route-policy-frr-10] quit
[Sysname] rip 100
[Sysname-rip-100] fast-reroute route-policy frr
```

filter-policy export

Use **filter-policy export** to configure RIP to filter redistributed routes.

Use **undo filter-policy export** to remove the filtering.

Syntax

filter-policy { *ipv4-acl-number* | **prefix-list** *prefix-list-name* } **export** [*interface-type interface-number* | **bgp** | **direct** | { **isis** | **ospf** | **rip** } [*process-id*] | **static**]

undo filter-policy export [*interface-type interface-number* | **bgp** | **direct** | { **isis** | **ospf** | **rip** } [*process-id*] | **static**]

Default

RIP does not filter redistributed routes.

Views

RIP view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-acl-number: Specifies an IPv4 ACL by its number in the range of 2000 to 3999 to filter redistributed routes.

prefix-list *prefix-list-name*: Specifies an IP prefix list by its name, a case-sensitive string of 1 to 63 characters, to filter redistributed routes.

interface-type interface-number: Specifies an interface by its type and number.

bgp: Filters routes redistributed from BGP.

direct: Filters direct routes.

isis: Filters routes redistributed from IS-IS.

ospf: Filters routes redistributed from OSPF.

rip: Filters routes redistributed from RIP.

process-id: Specifies a process ID of OSPF, IS-IS, or RIP, in the range of 1 to 65535. The default value is 1.

Usage guidelines

You can configure only one filtering policy to filter routes redistributed from a routing protocol or an interface. Without any protocol or interface specified, the filtering policy applies globally. If you execute this command multiple times, the most recent configuration takes effect.

To remove the filtering policy configured for a protocol or an interface, use the **undo filter-policy export** command with the protocol or interface specified.

To reference an advanced ACL (with a number from 3000 to 3999) in the command, configure the ACL using one of the following methods:

- To deny/permit a route with the specified destination, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* command.
- To deny/permit a route with the specified destination and mask, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* **destination** *dest-addr dest-wildcard* command.

The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the subnet mask of the route. For the mask configuration to take effect, specify a contiguous subnet mask.

Examples

Use basic ACL 2000 to filter redistributed routes.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule deny source 192.168.10.0 0.0.0.255
[Sysname-acl-ipv4-basic-2000] quit
[Sysname] rip 1
[Sysname-rip-1] filter-policy 2000 export
```

Use IP prefix list **abc** to filter redistributed routes.

```
<Sysname> system-view
[Sysname] ip prefix-list abc index 10 permit 11.0.0.0 8
[Sysname] rip 1
[Sysname-rip-1] filter-policy prefix-list abc export
```

Configure advanced ACL 3000 to permit only route 113.0.0.0/16 to pass. Use ACL 3000 to filter redistributed routes.

```
<Sysname> system-view
```

```
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule 10 permit ip source 113.0.0.0 0 destination 255.255.0.0
0
[Sysname-acl-ipv4-adv-3000] rule 100 deny ip
[Sysname-acl-ipv4-adv-3000] quit
[Sysname] rip 1
[Sysname-rip-1] filter-policy 3000 export
```

Related commands

acl (*ACL and QoS Command Reference*)

import-route

ip prefix-list

filter-policy import

Use **filter-policy import** to configure RIP to filter received routes.

Use **undo filter-policy import** to remove the filtering.

Syntax

filter-policy { *ipv4-acl-number* | **gateway** *prefix-list-name* | **prefix-list** *prefix-list-name* [**gateway** *prefix-list-name*] } **import** [*interface-type interface-number*]

undo filter-policy import [*interface-type interface-number*]

Default

RIP does not filter received routes.

Views

RIP view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-acl-number: Specifies an IPv4 ACL by its number in the range of 2000 to 3999 to filter received routes.

prefix-list *prefix-list-name*: Specifies an IP prefix list by its name, a case-sensitive string of 1 to 63 characters, to filter received routes.

gateway *prefix-list-name*: Specifies an IP prefix list by its name, a case-sensitive string of 1 to 63 characters, to filter routes based on their next hops.

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

You can configure only one filtering policy to filter routes received on an interface. Without any interface specified, the filtering policy applies globally. If you execute this command multiple times, the most recent configuration takes effect.

To remove the filtering policy configured for an interface, use the **undo filter-policy import** command with the interface specified.

To reference an advanced ACL (with a number from 3000 to 3999) in the command, configure the ACL using one of the following methods:

- To deny/permit a route with the specified destination, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* command
- To deny/permit a route with the specified destination and mask, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* **destination** *dest-addr dest-wildcard* command.

The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the subnet mask of the route. For the mask configuration to take effect, specify a contiguous subnet mask.

Examples

Use basic ACL 2000 to filter received RIP routes.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule deny source 192.168.10.0 0.0.0.255
[Sysname-acl-ipv4-basic-2000] quit
[Sysname] rip 1
[Sysname-rip-1] filter-policy 2000 import
```

Use IP prefix list **abc** to filter received RIP routes.

```
<Sysname> system-view
[Sysname] ip prefix-list abc index 10 permit 11.0.0.0 8
[Sysname] rip 1
[Sysname-rip-1] filter-policy prefix-list abc import
```

Configure advanced ACL 3000 to permit only route 113.0.0.0/16 to pass. Use ACL 3000 to filter received routes.

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule 10 permit ip source 113.0.0.0 0 destination 255.255.0.0
0
[Sysname-acl-ipv4-adv-3000] rule 100 deny ip
[Sysname-acl-ipv4-adv-3000] quit
[Sysname] rip 1
[Sysname-rip-1] filter-policy 3000 import
```

Related commands

acl (*ACL and QoS Command Reference*)

ip prefix-list

graceful-restart

Use **graceful-restart** to enable RIP GR.

Use **undo graceful-restart** to disable RIP GR.

Syntax

graceful-restart

undo graceful-restart

Default

RIP GR is disabled.

Views

RIP view

Predefined user roles

network-admin

context-admin

Usage guidelines

The **graceful-restart** command and the **non-stop-routing** command are mutually exclusive.

Examples

Enable GR for RIP process 1.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] graceful-restart
```

graceful-restart interval

Use **graceful-restart interval** to set the GR interval.

Use **undo graceful-restart interval** to restore the default.

Syntax

graceful-restart interval *interval*

undo graceful-restart interval

Default

The GR interval is 60 seconds.

Views

RIP view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies the GR interval in the range of 5 to 360 seconds.

Examples

Set the GR interval to 200 seconds for RIP process 1.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] graceful-restart interval 200
```

host-route

Use **host-route** to enable host route reception.

Use **undo host-route** to disable host route reception.

Syntax

host-route

undo host-route

Default

RIP receives host routes.

Views

RIP view

Predefined user roles

network-admin

context-admin

Usage guidelines

A router might receive many host routes from the same subnet. These routes are not helpful for routing and occupy a large number of resources. To solve this problem, use the **undo host-route** command to disable RIP from receiving host routes.

This command takes effect only for RIPv2 routes.

Examples

Disable RIP from receiving host routes.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] undo host-route
```

import-route

Use **import-route** to enable route redistribution.

Use **undo import-route** to disable route redistribution.

Syntax

import-route bgp [*as-number*] [**allow-ibgp**] [**cost** *cost-value* | **route-policy** *route-policy-name* | **tag** *tag*] *

import-route { **direct** | **static** } [**cost** *cost-value* | **route-policy** *route-policy-name* | **tag** *tag*] *

import-route { **isis** | **ospf** | **rip** } [*process-id* | **all-processes**] [**allow-direct** | **cost** *cost-value* | **route-policy** *route-policy-name* | **tag** *tag*] *

undo import-route { **bgp** | **direct** | { **isis** | **ospf** | **rip** } [*process-id* | **all-processes**] | **static** }

Default

RIP does not redistribute routes.

Views

RIP view

Predefined user roles

network-admin

context-admin

Parameters

bgp: Redistributes BGP routes.

direct: Redistributes direct routes.

isis: Redistributes IS-IS routes.

ospf: Redistributes OSPF routes.

rip: Redistributes RIP routes.

static: Redistributes static routes.

as-number: Specifies an AS by its number in the range of 1 to 4294967295. This argument applies only to the BGP protocol. If you do not specify the *as-number* argument, this command redistributes all IPv4 EBGP routes. As a best practice, specify the AS number to avoid redistributing excessive IPv4 EBGP routes.

process-id: Specifies a RIP, IS-IS, or OSPF process by its ID in the range of 1 to 65535. The default is 1.

all-processes: Enables route redistribution from all IS-IS, OSPF or RIP processes.

allow-ibgp: Allows redistribution of IBGP routes. The **import-route bgp** command redistributes only EBGP routes. The **import-route bgp allow-ibgp** command additionally redistributes IBGP routes and might cause routing loops. Therefore, use it with caution.

allow-direct: Redistributes the networks of the local interfaces enabled with the specified routing protocol. If you do not specify the **allow-direct** keyword, the networks of the local interfaces are not redistributed. If you specify both the **allow-direct** keyword and the **route-policy** *route-policy-name* option, make sure the **if-match** rule defined in the routing policy does not conflict with the **allow-direct** keyword. For example, if you specify the **allow-direct** keyword, do not configure the **if-match route-type** rule for the routing policy. Otherwise, the **allow-direct** keyword does not take effect.

cost *cost-value*: Specifies a cost for redistributed routes, in the range of 0 to 16. The default cost is 0.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters.

tag *tag*: Specifies a tag for marking redistributed routes, in the range of 0 to 65535. The default is 0.

Usage guidelines

This command redistributes only active routes. To view route state information, use the **display ip routing-table protocol** command.

When you execute the **undo** form of the command, per-process setting has higher priority than the all-processes setting.

- The **undo import-route** { **isis** | **ospf** | **rip** } **all-processes** command cannot remove the setting configured for a process by using the **import-route** { **isis** | **ospf** | **rip** } *process-id* command. To remove the setting for that process, you must specify the process ID in the **undo** form of the command.

Examples

Redistribute static routes into RIP, and set the cost for redistributed routes to 4.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] import-route static cost 4
```

Related commands

default cost

maximum load-balancing

Use **maximum load-balancing** to set the maximum number of RIP equal-cost multi-path (ECMP) routes for load balancing.

Use **undo maximum load-balancing** to restore the default.

Syntax

maximum load-balancing *number*

undo maximum load-balancing

Default

The maximum number of RIP ECMP routes equals the maximum number of ECMP routes, which is configurable by using the **max-ecmp-num** command.

Views

RIP view

Predefined user roles

network-admin

context-admin

Parameters

number: Specifies the maximum number of RIP ECMP routes. Load balancing is not implemented when the value is 1.

The following compatibility matrixes show the value ranges for the maximum number of RIP ECMP routes:

Models	Value range
NFNX5-HD6480	1 to 16
NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	1 to 32

Usage guidelines

You can set a smaller value for the **max-ecmp-num** command than the current value for the **maximum load-balancing** command. After a reboot, the value for the **maximum load-balancing** command automatically changes to be the same as the value for the **max-ecmp-num** command.

Examples

Set the maximum number of RIP ECMP routes to 2.

```
<Sysname> system-view
[Sysname] rip
[Sysname-rip-1] maximum load-balancing 2
```

Related commands

max-ecmp-num

network

Use **network** to enable RIP on an interface attached to a specified network.

Use **undo network** to disable RIP on an interface attached to a specified network.

Syntax

network *network-address* [*wildcard-mask*]

undo network *network-address*

Default

RIP is disabled on an interface.

Views

RIP view

Predefined user roles

network-admin

context-admin

Parameters

network-address: Specifies a subnet address where an interface resides.

wildcard-mask: Specifies an IP address wildcard mask. A wildcard mask can be thought of as a subnet mask, with 1s and 0s inverted. For example, a wildcard mask of 255.255.255.0 corresponds to a subnet mask of 0.0.0.255. If you do not specify this argument, the command uses the natural mask.

Usage guidelines

RIP runs only on an interface attached to the specified network, which can be configured with a wildcard mask. An interface not on the specified network does not receive or send RIP routes, or advertise its direct routes.

For a single RIP process, the **network** 0.0.0.0 command can enable RIP on all interfaces. If multiple RIP processes exist, the command is not applicable.

If a physical interface is attached to multiple networks, you cannot advertise these networks in different RIP processes.

Examples

Enable RIP process 100 on the interface attached to the network 129.102.0.0.

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] network 129.102.0.0
```

Related commands

rip enable

non-stop-routing

Use **non-stop-routing** to enable RIP NSR.

Use **undo non-stop-routing** to disable RIP NSR.

Syntax

non-stop-routing

undo non-stop-routing

Default

RIP NSR is disabled.

Views

RIP view

Predefined user roles

network-admin

context-admin

Usage guidelines

RIP NSR enabled for a RIP process takes effect only on that process. As a best practice, enable RIP NSR for each process if multiple RIP processes exist.

The **non-stop-routing** command and the **graceful-restart** command are mutually exclusive.

Examples

Enable NSR for RIP process 1.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] non-stop-routing
```

output-delay

Use **output-delay** to set the rate at which an interface sends RIP packets.

Use **undo output-delay** to restore the default.

Syntax

output-delay *time* **count** *count*

undo output-delay

Default

An interface sends up to three RIP packets every 20 milliseconds.

Views

RIP view

Predefined user roles

network-admin

context-admin

Parameters

time: Specifies the sending interval in the range of 10 to 100 milliseconds.

count: Specifies the maximum number of RIP packets sent at each interval, in the range of 1 to 30.

Examples

Configure all interfaces running RIP process 1 to send up to 10 RIP packets every 60 milliseconds.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] output-delay 60 count 10
```

peer

Use **peer** to specify a RIP neighbor in the NBMA network, where routing updates destined for the neighbor are only unicasts and not multicast or broadcast.

Use **undo peer** to remove a RIP neighbor.

Syntax

peer *ip-address*

undo peer *ip-address*

Default

RIP does not unicast updates to any neighbor.

Views

RIP view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the IP address of a RIP neighbor, in dotted decimal notation.

Usage guidelines

Do not use the **peer** *ip-address* command when the neighbor is directly connected. Otherwise, the neighbor might receive both unicast and multicast (or broadcast) messages with the same routing information.

This command must be executed together with the **undo validate-source-address** command, which disables source IP address check on inbound RIP routing updates.

Examples

Configure RIP to unicast updates to peer 202.38.165.1.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] peer 202.38.165.1
```

Related commands

validate-source-address

preference

Use **preference** to specify a preference for RIP routes.

Use **undo preference** to restore the default.

Syntax

preference { *preference* | **route-policy** *route-policy-name* } *

undo preference

Default

The preference of RIP routes is 100.

Views

RIP view

Predefined user roles

network-admin

context-admin

Parameters

preference: Specifies a preference for RIP routes, in the range of 1 to 255. The smaller the value, the higher the preference.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

You can specify a routing policy by using the keyword **route-policy** to set a preference for matching RIP routes.

- The preference set by the routing policy applies to all matching RIP routes. The preference of other routes is set by the **preference** command.
- If no preference is set by the routing policy, the preference of all RIP routes is set by the **preference** command.

Examples

Set a preference of 120 for RIP routes.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] preference 120
```

reset rip process

Use **reset rip process** to reset a RIP process.

Syntax

reset rip *process-id* **process**

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

process-id: Specifies a RIP process by its ID in the range of 1 to 65535.

Usage guidelines

After executing the command, you are prompted to confirm the operation.

Examples

Reset RIP process 100.

```
<Sysname> reset rip 100 process
Reset RIP process? [Y/N]:y
```

reset rip statistics

Use **reset rip statistics** to clear statistics for a RIP process.

Syntax

reset rip *process-id* **statistics**

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

process-id: Specifies a RIP process by its ID in the range of 1 to 65535.

Examples

Clear statistics for RIP process 100.

```
<Sysname> reset rip 100 statistics
```

rip

Use **rip** to enable RIP and enter RIP view.

Use **undo rip** to disable RIP.

Syntax

rip [*process-id*] [**vpn-instance** *vpn-instance-name*]

undo rip [*process-id*]

Default

RIP is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

process-id: Specifies a RIP process by its ID in the range of 1 to 65535. The default is 1.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the RIP process runs on the public network.

Usage guidelines

You must enable a RIP process before configuring global parameters for it. This restriction does not apply to configuring interface parameters.

If you disable a RIP process, the configured interface parameters become invalid.

Examples

Enable RIP process 1 and enter RIP view.

```
<Sysname> system-view
[Sysname] rip
[Sysname-rip-1]
```

rip authentication-mode

Use **rip authentication-mode** to configure RIPv2 authentication.

Use **undo rip authentication-mode** to restore the default.

Syntax

rip authentication-mode { **keychain** *keychain-name* { **rfc2453** | **rfc4822** } | **md5** { **rfc2082** { **cipher** | **plain** } *string key-id* | **rfc2453** { **cipher** | **plain** } *string* } | **simple** { **cipher** | **plain** } *string* }

undo rip authentication-mode

Default

RIPv2 authentication is not configured.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

keychain: Specifies keychain authentication.

keychain-name: Specifies a keychain by its name, a case-sensitive string of 1 to 63 characters.

rfc2453: Uses the message format defined in RFC 2453 (IETF standard).

rfc4822: Uses the message format defined in RFC 4822.

md5: Specifies MD5 authentication.

rfc2082: Uses the message format defined in RFC 2082.

cipher: Specifies a password in encrypted form.

plain: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 16 characters. Its encrypted form is a case-sensitive string of 33 to 53 characters.

key-id: Specifies the key ID in the range of 1 to 255.

rfc2453: Uses the message format defined in RFC 2453 (IETF standard).

simple: Specifies the simple authentication mode.

Usage guidelines

A newly configured key overwrites the old one, if any.

Although you can specify an authentication mode for RIPv1 in interface view, the configuration does not take effect because RIPv1 does not support authentication.

RIPv2 sends and receives packets on an interface configured with keychain authentication as follows:

- Before sending a packet, RIPv2 must obtain a valid send key from the keychain to authenticate the packet.

  RIPv2 does not send the packet if no valid send key is available.
- After receiving a packet, RIPv2 performs the following operations:
  - If the **rfc2453** keyword is specified, RIPv2 uses valid accept keys in the keychain to authenticate the packet.
    - RIPv2 accepts the packet if it is successfully authenticated by an accept key.
    - RIPv2 discards the packet if the packet authentication fails.
  - If the **rfc4822** keyword is specified, RIPv2 performs the following operations:
    - Searches the keychain for a valid accept key using the key ID carried in the packet.
    - Uses the authentication algorithm and key string of the key to authenticate the packet.

      RIPv2 accepts the packet if the authentication succeeds. If the packet authentication fails or no valid accept key is available, RIPv2 discards the packet.

Follow these guidelines when you configure keychain authentication for an interface enabled with RIPv2:

- If the **rfc2453** keyword is specified, RIPv2 supports only the MD5 authentication algorithm of the keychain and a key string length of up to 16 characters. If RIPv2 obtains a key string containing more than 16 characters, it uses the first 16 characters of the key string for authentication.
- If the **rfc4822** keyword is specified, RIPv2 supports only the key IDs with a value range of 0 to 255. Any packets carrying a key ID not in the range will be discarded. RIPv2 supports the MD5, HMAC-SHA-1, HMAC-SM3, and HMAC-SHA-256 authentication algorithms of the keychain. The MD5 authentication algorithm can use the message format defined in RFC 2082.

Examples

Configure MD5 authentication on GigabitEthernet 1/0/1, and specify a plaintext key **rose** in the format defined in RFC 2453.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rip version 2
[Sysname-GigabitEthernet1/0/1] rip authentication-mode md5 rfc2453 plain rose
```

Related commands

rip version

rip bfd

Use **rip bfd** to configure BFD for RIP on an interface.

Use **undo rip bfd enable** to restore the default.

Syntax

rip bfd { **disable** | **enable** [**ctrl** | **destination** *ip-address*] }

undo rip bfd enable

Default

BFD for RIP is disabled on an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

`disable`: Disables BFD for RIP on the interface. You can do this to avoid network instability when link flapping occurs on the interface.

`enable`: Enables BFD for RIP on the interface.

`ctrl`: Enables BFD bidirectional control detection for both directly and indirectly connected neighbors. If you do not specify this keyword, the interface uses BFD single-hop echo detection for a directly connected neighbor and BFD bidirectional control detection for an indirectly connected neighbor.

`destination` *`ip-address`*: Specifies a destination to which the interface establishes a BFD session. If you do not specify this option, the interface establishes a BFD session to its RIP neighbor.

Usage guidelines

RIP supports the following BFD detection modes:

- **Single-hop echo detection**—Detection mode for a directly connected neighbor. In this mode, a BFD session is established only when the directly connected neighbor has route information to send.
- **Single-hop echo detection for a specific destination**—Detection mode for a directly connected neighbor. In this mode, a BFD session is established to the specified RIP neighbor when RIP is enabled on the local interface.
- **Bidirectional control detection**—Detection mode for both directly and indirectly connected neighbors. In this mode, a BFD session is established only when both ends have routes to send and BFD is enabled on the receiving interface.

If you specify the **`destination`** *`ip-address`* option, the interface uses BFD single-hop echo detection to detect link failure on the link to the specified destination. If a failure is detected on the link, the interface does not send or receive RIP packets anymore.

The **`bfd all-interfaces enable`** command in RIP view enables BFD for RIP on all interfaces of the RIP process. To disable BFD on one of those interfaces, you must use the **`rip bfd disable`** command instead of the **`undo rip bfd enable`** command in interface view.

You must configure bidirectional control detection on both ends of a link for it to take effect.

The BFD session to a neighbor does not come down when you execute the **`undo peer`** command to delete its address. This is because the RIP neighbor relationship is not immediately deleted when you execute the **`undo peer`** command.

Examples

Enable BFD for RIP on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rip bfd enable
```

rip default-route

Use **`rip default-route`** to configure a RIP interface to advertise a default route with a specified metric.

Use **undo rip default-route** to disable a RIP interface from sending a default route.

Syntax

rip default-route { { **only** | **originate** } [**cost** *cost-value* | **route-policy** *route-policy-name*] * | **no-originate** }

undo rip default-route

Default

A RIP interface advertises a default route if the RIP process that the interface runs is enabled to advertise a default route.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

only: Advertises only a default route.

originate: Advertises both a default route and other routes.

cost-value: Specifies a cost for the default route, in the range of 1 to 15. The default is 1.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case sensitive string of 1 to 63 characters. If you specify this option, the command advertises a default route only when a route in the routing table matches the routing policy.

no-originate: Advertises only non-default routes.

Usage guidelines

An interface that is enabled to advertise a default route does not receive any default route from RIP neighbors.

Examples

Configure GigabitEthernet 1/0/1 to advertise only a default route with a metric of 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rip default-route only cost 2
```

Configure GigabitEthernet 1/0/1 to advertise a default route with a metric of 4 and other routes.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rip default-route originate cost 4
```

Related commands

default-route

rip enable

Use **rip enable** to enable RIP on an interface.

Use **undo rip enable** to disable RIP on an interface.

Syntax

rip *process-id* **enable** [**exclude-subip**]

undo rip enable

Default

RIP is disabled on an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

process-id: Specifies a RIP process by its ID in the range of 1 to 65535.

exclude-subip: Excludes secondary IP addresses from being enabled with RIP. If you do not specify this keyword, RIP is also enabled on secondary IP addresses of a RIP-enabled interface.

Usage guidelines

The **rip enable** command has a higher priority than the **network** command.

Examples

Enable RIP process 100 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rip 100 enable
```

Related commands

network

rip input

Use **rip input** to enable an interface to receive RIP messages.

Use **undo rip input** to disable an interface from receiving RIP messages.

Syntax

rip input

undo rip input

Default

An interface is enabled to receive RIP messages.

Views

Interface view

Predefined user roles

network-admin

context-admin

Examples

Disable GigabitEthernet 1/0/1 from receiving RIP messages.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] undo rip input
```

rip max-packet-length

Use **rip max-packet-length** to set the maximum length of RIP packets.

Use **undo rip max-packet-length** to restore the default.

Syntax

rip max-packet-length *value*

undo rip max-packet-length

Default

The maximum length of RIP packets is 512 bytes.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

value: Specifies the maximum length of RIP packets, in the range of 32 to 65535 bytes.

Usage guidelines

The supported maximum length of RIP packets varies by vendor. Use this feature with caution to avoid compatibility issues.

When authentication is enabled, follow these guidelines to ensure packet forwarding:

- For simple authentication, the maximum length of RIP packets must be no less than 52 bytes.
- For MD5 authentication (with packet format defined in RFC 2453), the maximum length of RIP packets must be no less than 56 bytes.
- For MD5 authentication (with packet format defined in RFC 2082), the maximum length of RIP packets must be no less than 72 bytes.

If the configured value in the **rip max-packet-length** command is greater than the MTU of an interface, the interface MTU value is used as the maximum length of RIP packets.

Examples

Set the maximum length of RIP packets on GigabitEthernet 1/0/1 to 1024 bytes.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rip max-packet-length 1024
```

rip metricin

Use **rip metricin** to configure an interface to add a metric to inbound routes.

Use **undo rip metricin** to restore the default.

Syntax

rip metricin [**route-policy** *route-policy-name*] *value*

undo rip metricin

Default

The additional metric of an inbound route is 0.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

route-policy *route-policy-name*: Specifies a routing policy by its name, a case sensitive string of 1 to 63 characters. If you specify this option, the command adds an additional metric for the routes that match the routing policy.

value: Adds an additional metric to inbound routes, in the range of 0 to 16.

Usage guidelines

When a valid RIP route is received, the system adds a metric to it and then installs it into the routing table. The metric of the route received on the configured interface is then increased. If the sum of the additional metric and the original metric is greater than 16, the metric of the route will be 16.

If a routing policy is referenced with the **route-policy** keyword, the following operations can be performed:

- Routes matching the policy are added with the metric specified in the **apply cost** command configured in the policy. Routes not matching it are added with the metric specified in the **rip metricin** command. The **rip metricin** command does not support specifying the **+** or **–** keyword in the **apply cost** command to add or reduce a metric.
- If the **apply cost** command is not configured in the policy, all the inbound routes are added with the metric specified in the **rip metricin** command.

Examples

Configure GigabitEthernet 1/0/1 to add a metric of 6 to the inbound route 1.0.0.0/8 and to add a metric of 2 to other inbound routes.

```
<Sysname> system-view
[Sysname] ip prefix-list 123 permit 1.0.0.0 8
[Sysname] route-policy abc permit node 10
[Sysname-route-policy-abc-10] if-match ip address prefix-list 123
[Sysname-route-policy-abc-10] apply cost 6
[Sysname-route-policy-abc-10] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rip metricin route-policy abc 2
```

Related commands

apply cost

rip metricout

Use **rip metricout** to configure an interface to add a metric to outbound routes.

Use **undo rip metricout** to restore the default.

Syntax

rip metricout [**route-policy** *route-policy-name*] *value*

undo rip metricout

Default

The additional metric for outbound routes is 1.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

route-policy *route-policy-name*: Specifies a routing policy by its name, a case sensitive string of 1 to 63 characters. If you specify this option, the command adds an additional metric for the routes that match the routing policy.

value: Adds an additional metric to outbound routes, in the range of 1 to 16.

Usage guidelines

With the command configured on an interface, the metric of RIP routes sent on the interface will be increased.

If a routing policy is referenced with the **route-policy** keyword, the following operations can be performed:

- Routes matching the policy is added with the metric specified in the **apply cost** command configured in the policy. Routes not matching it are added with the metric specified in the **rip metricout** command. The **rip metricout** command does not support specifying the **+** or **–** keyword in the **apply cost** command to add or reduce a metric.
- If the **apply cost** command is not configured in the policy, all the outbound routes are added with the metric specified in the **rip metricout** command.

Examples

Configure GigabitEthernet 1/0/1 to add a metric of 6 to the outbound route 1.0.0.0/8 and to add a metric of 2 to other outbound routes.

```
<Sysname> system-view
[Sysname] ip prefix-list 123 permit 1.0.0.0 8
[Sysname] route-policy abc permit node 10
[Sysname-route-policy-abc-10] if-match ip address prefix-list 123
[Sysname-route-policy-abc-10] apply cost 6
[Sysname-route-policy-abc-10] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rip metricout route-policy abc 2
```

Related commands

apply cost

rip mib-binding

Use **rip mib-binding** to bind a RIP process to MIB.

Use **undo rip mib-binding** to restore the default.

Syntax

rip mib-binding *process-id*

undo rip mib-binding

Default

MIB operation is bound to the RIP process with the smallest process ID.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

process-id: Specifies a RIP process by its ID in the range of 1 to 65535.

Usage guidelines

If the specified process ID does not exist, the MIB binding configuration does not take effect.

Deleting a RIP process bound to MIB operation deletes the MIB binding configuration. After the RIP process is deleted, MIB operation is bound to the RIP process with the smallest process ID.

Examples

Bind RIP process 100 to MIB.

```
<Sysname> system-view
[Sysname] rip mib-binding 100
```

rip output

Use **rip output** to enable an interface to send RIP messages.

Use **undo rip output** to disable an interface from sending RIP messages.

Syntax

rip output

undo rip output

Default

An interface sends RIP messages.

Views

Interface view

Predefined user roles

network-admin

context-admin

Examples

Disable GigabitEthernet 1/0/1 from sending RIP messages.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo rip output
```

rip output-delay

Use **rip output-delay** to set the RIP packet sending interval for an interface and the maximum number of RIP packets that can be sent at each interval.

Use **undo rip output-delay** to restore the default.

Syntax

rip output-delay *time* **count** *count*

undo rip output-delay

Default

An interface uses the RIP packet sending rate set for the RIP process that the interface runs.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

Time: Specifies the RIP packet sending interval in the range of 10 to 100 milliseconds.

count: Specifies the maximum number of RIP packets sent at each interval, in the range of 1 to 30.

Examples

Configure GigabitEthernet 1/0/1 to send a maximum of six RIP packets every 30 milliseconds.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rip output-delay 30 count 6
```

Related commands

output-delay

rip poison-reverse

Use **rip poison-reverse** to enable the poison reverse feature.

Use **undo rip poison-reverse** to disable the poison reverse feature.

Syntax

rip poison-reverse

undo rip poison-reverse

Default

The poison reverse feature is disabled.

Views

Interface view

Predefined user roles

network-admin

context-admin

Examples

Enable the poison reverse feature on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rip poison-reverse
```

rip primary-path-detect bfd

Use **rip primary-path-detect bfd** to enable BFD for RIP FRR.

Use **undo rip primary-path-detect bfd** to disable BFD for RIP FRR.

Syntax

rip primary-path-detect bfd { **ctrl** | **echo** }

undo rip primary-path-detect bfd

Default

BFD for RIP FRR is disabled.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ctrl: Enables BFD bidirectional control detection for RIP FRR to detect primary link failures.

echo: Enables BFD single-hop echo detection for RIP FRR to detect primary link failures.

Usage guidelines

For quicker RIP FRR, use BFD on the primary link of redundant links to detect link failure.

You must configure bidirectional control detection on both ends of a link for it to take effect.

Examples

Enable BFD single-hop echo detection for RIP FRR on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] fast-reroute route-policy frr
[Sysname-rip-1] quit
[Sysname] bfd echo-source-ip 1.1.1.1
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rip primary-path-detect bfd echo
```

rip split-horizon

Use **rip split-horizon** to enable the split horizon feature.

Use **undo rip split-horizon** to disable the split horizon feature.

Syntax

rip split-horizon

undo rip split-horizon

Default

The split horizon feature is enabled.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

The split horizon feature prevents routing loops. If you want to disable the feature, make sure the operation is necessary.

If both split horizon and poison reverse are enabled, only the poison reverse feature takes effect.

Examples

Enable the split horizon feature on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rip split-horizon
```

rip summary-address

Use **rip summary-address** to configure a summary route on an interface.

Use **undo rip summary-address** to remove a summary route on an interface.

Syntax

rip summary-address *ip-address* { *mask-length* | *mask* }

undo rip summary-address *ip-address* { *mask-length* | *mask* }

Default

No summary route is configured on an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the destination IP address of the summary route.

mask-length: Specifies the subnet mask length of the summary route, in the range of 0 to 32.

mask: Specifies the subnet mask of the summary route, in dotted decimal notation.

Usage guidelines

This command takes effect only when automatic route summarization is disabled.

Examples

Configure a summary route on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rip summary-address 10.0.0.0 255.255.255.0
```

Related commands

summary

rip version

Use **rip version** to specify a RIP version on an interface.

Use **undo rip version** to restore the default.

Syntax

rip version { **1** | **2** [**broadcast** | **multicast**] }

undo rip version

Default

No RIP version is configured on an interface. The interface can send RIPv1 broadcasts, and receive RIPv1 broadcasts and unicasts, and RIPv2 broadcasts, multicasts, and unicasts.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

1: Specifies the RIP version as RIPv1.

2: Specifies the RIP version as RIPv2.

[**broadcast** | **multicast**]: Sends RIPv2 messages in broadcast mode or multicast mode (default).

Usage guidelines

If an interface has no RIP version configured, it uses the global RIP version. Otherwise, it uses the RIP version configured on it.

An interface running RIPv1 can perform the following operations:

- Sends RIPv1 broadcast messages.
- Receives RIPv1 broadcast and unicast messages.

An interface running RIPv2 in broadcast mode can perform the following operations:

- Sends RIPv2 broadcast messages.
- Receives RIPv1 broadcast and unicast messages, and RIPv2 broadcast, multicast, and unicast messages.

An interface running RIPv2 in multicast mode can perform the following operations:

- Sends RIPv2 multicast messages.
- Receives RIPv2 broadcast, multicast, and unicast messages.

Examples

Configure RIPv2 in broadcast mode on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rip version 2 broadcast
```

Related commands

version

silent-interface

Use **silent-interface** to disable interfaces from sending RIP messages. The interfaces can still receive RIP messages.

Use **undo silent-interface** to enable interfaces to send RIP messages.

Syntax

silent-interface { *interface-type interface-number* | **all** }

undo silent-interface { *interface-type interface-number* | **all** }

Default

All RIP interfaces can send RIP messages.

Views

RIP view

Predefined user roles

network-admin

context-admin

Parameters

interface-type interface-number: Disables a specified interface from sending RIP messages.

all: Disables all interfaces from sending RIP messages.

Examples

Disable all interfaces from sending RIP messages except GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] silent-interface all
[Sysname-rip-100] undo silent-interface gigabitethernet 1/0/1
[Sysname-rip-100] network 131.108.0.0
```

summary

Use **summary** to enable automatic RIPv2 route summarization. Natural masks are used to advertise summary routes to reduce the size of routing tables.

Use **undo summary** to disable automatic RIPv2 route summarization to advertise all subnet routes.

Syntax

summary

undo summary

Default

Automatic RIPv2 route summarization is enabled.

Views

RIP view

Predefined user roles

network-admin

context-admin

Usage guidelines

Automatic RIPv2 route summarization can reduce the routing table size to enhance the scalability and efficiency for large networks.

Examples

Disable automatic RIPv2 route summarization.

```
<Sysname> system-view
[Sysname] rip
[Sysname-rip-1] undo summary
```

Related commands

rip summary-address

rip version

timer triggered

Use **timer triggered** to set the interval for sending triggered updates.

Use **undo timer triggered** to restore the default.

Syntax

timer triggered *maximum-interval* [*minimum-interval* [*incremental-interval*]]

undo timer triggered

Default

The maximum interval is 5 seconds, the minimum interval is 50 milliseconds, and the incremental interval is 200 milliseconds.

Views

RIP view

Predefined user roles

network-admin

context-admin

Parameters

maximum-interval: Specifies the maximum interval in the range of 1 to 5 seconds.

minimum-interval: Specifies the minimum interval in the range of 10 to 5000 milliseconds.

incremental-interval: Specifies the incremental interval in the range of 100 to 1000 milliseconds.

Usage guidelines

The *minimum-interval* and *incremental-interval* cannot be greater than the *maximum-interval*.

For a stable network, the *minimum-interval* setting is used. If network changes become frequent, the incremental interval *incremental-interval* is used to extend the triggered update sending interval until the *maximum-interval* is reached.

Examples

For RIP process 1, set the maximum interval, minimum interval, and incremental interval to 2 seconds, 100 milliseconds, and 100 milliseconds, respectively.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] timer triggered 2 100 100
```

timers

Use **timers** to set RIP timers.

Use **undo timers** to restore the default.

Syntax

timers { **garbage-collect** *garbage-collect-value* | **suppress** *suppress-value* | **timeout** *timeout-value* | **update** *update-value* } *

undo timers { **garbage-collect** | **suppress** | **timeout** | **update** } *

Default

The garbage-collect timer is 120 seconds, the suppress timer is 120 seconds, the timeout timer is 180 seconds, and the update timer is 30 seconds.

Views

RIP view

Predefined user roles

network-admin

context-admin

Parameters

garbage-collect-value: Specifies the garbage-collect timer in the range of 1 to 3600 seconds.

suppress-value: Specifies the suppress timer in the range of 0 to 3600 seconds.

timeout-value: Specifies the timeout timer in the range of 1 to 3600 seconds.

update-value: Specifies the update timer in the range of 1 to 3600 seconds.

Usage guidelines

RIP uses the following timers:

- **Update timer**—Specifies the interval between routing updates.
- **Timeout timer**—Specifies the route aging time. If no update for a route is received before the timer expires, RIP sets the metric of the route to 16.
- **Suppress timer**—Specifies how long a RIP route stays in suppressed state. When the metric of a route becomes 16, the route enters the suppressed state. If RIP receives an update for the

route with a metric less than 16 from the same neighbor, RIP uses this route to replace the suppressed route.

- **Garbage-collect timer**—Specifies the interval from when the metric of a route becomes 16 to when it is deleted from the routing table. During the garbage-collect timer length, RIP advertises the route with a metric of 16. If no update is announced for that route before the garbage-collect timer expires, RIP deletes the route from the routing table.

As a best practice, do not change the default values of these timers.

The timer lengths must be consistent on all routers on the network.

The timeout timer must be greater than the update timer.

Examples

Set the update, timeout, suppress, and garbage-collect timers to 5, 15, 15, and 30 seconds.

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] timers update 5 timeout 15 suppress 15 garbage-collect 30
```

validate-source-address

Use **validate-source-address** to enable source IP address check on inbound RIP routing updates.

Use **undo validate-source-address** to disable source IP address check on inbound RIP routing updates.

Syntax

validate-source-address

undo validate-source-address

Default

Source IP address check on inbound RIP routing updates is enabled.

Views

RIP view

Predefined user roles

network-admin

context-admin

Examples

Disable source IP address check on inbound RIP routing updates.

```
<Sysname> system-view
[Sysname-rip] rip 100
[Sysname-rip-100] undo validate-source-address
```

version

Use **version** to specify a global RIP version.

Use **undo version** to restore the default.

Syntax

version { **1** | **2** }

undo version

Default

No global RIP version is configured. An RIP interface can send RIPv1 broadcasts and receive RIPv1 broadcasts and unicasts, and RIPv2 broadcasts, multicasts, and unicasts.

Views

RIP view

Predefined user roles

network-admin

context-admin

Parameters

1: Specifies the RIP version as RIPv1.

2: Specifies the RIP version as RIPv2. RIPv2 messages are multicast.

Usage guidelines

An interface prefers the RIP version configured on it over the global RIP version.

If no RIP version is specified for the interface and the global version is RIPv1, the interface uses RIPv1 and can perform the following operations:

- Send RIPv1 broadcasts.
- Receive RIPv1 broadcasts and unicasts.

If no RIP version is specified for the interface and the global version is RIPv2, the interface uses RIPv2 multicast mode and can perform the following operations:

- Send RIPv2 multicasts.
- Receive RIPv2 broadcasts, multicasts, and unicasts.

Examples

Specify the global RIP version as RIPv2.

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] version 2
```

Related commands

rip version

Contents

RIPng commands

checkzero

Use **checkzero** to enable zero field check on RIPng packets.

Use **undo checkzero** to disable zero field check.

Syntax

checkzero

undo checkzero

Default

Zero field check is enabled.

Views

RIPng view

Predefined user roles

network-admin

context-admin

Usage guidelines

Some fields in RIPng packet headers must be zero. These fields are called zero fields. You can enable zero field check on incoming RIPng packets. If a zero field of a packet contains a non-zero value, RIPng discards the packet.

Examples

Disable zero field check on RIPng packets for RIPng 100.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] undo checkzero
```

default cost

Use **default cost** to configure a default metric for redistributed routes.

Use **undo default cost** to restore the default.

Syntax

default cost *cost-value*

undo default cost

Default

The default metric of redistributed routes is 0.

Views

RIPng view

Predefined user roles

network-admin

context-admin

Parameters

cost-value: Specifies a default metric for redistributed routes, in the range of 0 to 16.

Usage guidelines

When you use the **import-route** command to redistribute routes from another routing protocol without specifying a metric, the metric specified by the **default cost** command applies.

Examples

Configure a default metric of 2 for redistributed routes.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] default cost 2
```

Related commands

import-route

display ripng

Use **display ripng** to display state and configuration information for a RIPng process.

Syntax

display ripng [*process-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies a RIPng process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays information about all RIPng processes.

Examples

Display state and configuration information for all configured RIPng processes.

```
<Sysname> display ripng
  Public VPN-instance name:

RIPng process: 1
       Preference: 100
           Routing policy: abc
       Fast-reroute:
           Routing policy: abc
       Checkzero: Enabled
       Default cost: 0
       Maximum number of load balanced routes: 6
       Update time   :   30 secs  Timeout time         :  180 secs
       Suppress time :  120 secs  Garbage-collect time :  120 secs
```

```
Update output delay:   20(ms)  Output count:    3
Graceful-restart interval:   60 secs
Triggered Interval : 5 50 200
Number of periodic updates sent: 256
Number of triggered updates sent: 0
```

Table 1 Command output

Field	Description
Public VPN-instance name	Public network where the RIPng process runs.
Private VPN-instance name	VPN where the RIPng process runs.
RIPng process	RIPng process ID.
Preference	RIPng preference.
Checkzero	Indicates whether zero field check for RIPng packet headers is enabled: **Enabled** or **Disabled**.
Default Cost	Default metric of redistributed routes.
Fast-reroute	RIPng FRR.
Maximum number of balanced paths	Maximum number of load-balanced routes.
Update time	RIPng update interval, in seconds.
Timeout time	RIPng timeout interval, in seconds.
Suppress time	RIPng suppress interval, in seconds.
Garbage-collect time	RIPng garbage collection interval, in seconds.
Update output delay	RIPng packet sending interval, in milliseconds.
Output count	Maximum number of RIPng packets that can be sent at each interval.
Graceful-restart interval	GR interval in seconds.
Triggered Interval	Triggered update sending interval.

display ripng database

Use **display ripng database** to display all active routes in the advertising database for a RIPng process.

Syntax

display ripng *process-id* **database** [*ipv6-address prefix-length*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies a RIPng process by its ID in the range of 1 to 65535.

ipv6-address prefix-length: Specifies an IPv6 address. The *ipv6-address* argument specifies an IPv6 address. The *prefix-length* argument specifies a prefix length in the range of 0 to 128.

Examples

Display active routes for RIPng process 1.

```
<Sysname> display ripng 1 database
   1::/64,
        cost 0, RIPng-interface
   10::/32,
        cost 0, imported
   2::2/128,
       via FE80::20C:29FF:FE7A:E3E4, cost 1
```

Table 2 Command output

Field	Description
cost	Route metric value.
imported	Indicates the route is redistributed from another routing protocol.
RIPng-interface	Route learned from the interface.
via	Next hop IPv6 address.

display ripng graceful-restart

Use **display ripng graceful-restart** to display GR information.

Syntax

display ripng [*process-id*] **graceful-restart**

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies a RIPng process by its ID in the range of 1 to 65535.

Examples

Display GR information for RIPng process 1.

```
<Sysname> display ripng 1 graceful-restart
RIPng process: 1
 Graceful Restart capability    : Enabled
 Current GR state               : Normal
```

```
Graceful Restart period        : 60  seconds
Graceful Restart remaining time: 0   seconds
```

Table 3 Command output

Field	Description
Graceful Restart capability	Indicates whether GR is enabled: **Enabled** or **Disabled**.
Current GR state	GR state: • **Under GR**—GR is in process. • **Normal**—GR is not in progress or has completed.

display ripng interface

Use **display ripng interface** to display interface information for a RIPng process.

Syntax

display ripng *process-id* **interface** [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies a RIPng process by its ID in the range of 1 to 65535.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify this argument, the command displays information about all interfaces for the RIPng process.

Examples

Display interface information for RIPng process 1.

```
<Sysname> display ripng 1 interface
Total: 1

 Interface: GigabitEthernet1/0/2
        Link-local address: FE80::20C:29FF:FEC8:B4DD
        Split-horizon: On               Poison-reverse: Off
        MetricIn: 0                     MetricOut: 1
        Default route: Off
        Update output delay: 20 (ms)    Output count: 3
        Primary path detection mode: BFD echo
        Summary address:
               1::/16
```

Table 4 Command output

Field	Description
Total	Number of interfaces running RIPng.
Interface	Name of an interface running RIPng.
Link Local Address	Link-local address of an interface running RIPng.
Split-horizon	Indicates whether split horizon is enabled: • **On**—Enabled. • **Off**—Disabled.
Poison-reverse	Indicates whether poison reverse is enabled: • **On**—Enabled. • **Off**—Disabled.
MetricIn/MetricOut	Additional metric to incoming and outgoing routes.
Default route	• **Only**—The interface advertises only a default route. • **Originate**—The interface advertises a default route and other RIPng routes. • **Off**—In this state, the interface does not advertise a default route. • **In garbage-collection status**—In this state, the interface advertises a default route with a metric of 16.
Update output delay	RIPng packet sending interval, in milliseconds.
Output count	Maximum number of RIPng packets that can be sent at each interval.
Default route cost	Cost of the default route.
Primary path detection mode	**BFD echo** indicates that BFD single-hop echo detection is used to detect primary link failures.

display ripng neighbor

Use **`display ripng neighbor`** to display neighbor information for a RIPng process.

Syntax

`display ripng` *`process-id`* **`neighbor`** [*`interface-type interface-number`*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

`process-id`: Specifies a RIPng process by its ID in the range of 1 to 65535.

`interface-type interface-number`: Specifies an interface by its type and number. If you do not specify this argument, the command displays information about all neighbors for the RIPng process.

Examples

Display neighbor information for RIPng process 1.

```
<Sysname> display ripng 1 neighbor
Neighbor Address: FE80::230:FF:FE00:0
     Interface  : GigabitEthernet1/0/1
     Version    : RIPng version 1     Last update: 00h00m27s
     Bad packets: 0                   Bad routes : 0
```

Table 5 Command output

Field	Description
Neighbor Address	Link-local address of a neighbor interface.
Interface	Name of a neighbor interface.
Version	Version of RIPng that a neighbor runs.
Last update	Time elapsed since the most recent update.

display ripng non-stop-routing

Use **display ripng non-stop-routing** to display RIPng NSR information.

Syntax

display ripng [*process-id*] **non-stop-routing**

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies a RIPng process by its ID in the range of 1 to 65535.

Examples

Display NSR information for RIPng process 1.

```
<Sysname> display ripng 1 non-stop-routing
RIPng process: 1
 Nonstop Routing capability: Enabled
 Current NSR state         : Finish
```

Table 6 Command output

Field	Description
Nonstop Routing capability	Indicates whether NSR is enabled: **Enabled** or **Disabled**.

Field	Description
Current NSR state	NSR state: • **Initialization**—Initialization state. • **Smooth**—Upgrading data. • **Advertising**—Advertising routes. • **Redistribution**—Redistributing routes. • **Finish**—Finished.

display ripng route

Use **display ripng route** to display all RIPng routes for a RIPng process.

Syntax

display ripng *process-id* **route** [*ipv6-address prefix-length* [**verbose**] | **peer** *ipv6-address* | **statistics**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies a RIPng process by its ID in the range of 1 to 65535.

ipv6-address prefix-length: Specifies an IPv6 address. The *ipv6-address* argument specifies an IPv6 address. The *prefix-length* argument specifies a prefix length in the range of 0 to 128.

verbose: Displays all routing information for the specified destination IPv6 address. If you do not specify this keyword, the command displays only optimal RIPng routes with the specified destination IPv6 address.

peer *ipv6-address*: Specifies a neighbor by its IPv6 address.

statistics: Displays routing information statistics, including total number of routes and the number of routes learned from each neighbor.

Examples

Display routing information for RIPng process 1.

```
<Sysname> display ripng 1 route
   Route Flags: A - Aging, S - Suppressed, G - Garbage-collect, D – Direct
                O - Optimal, F - Flush to RIB
 ------------------------------------------------------------------

 Peer FE80::20C:29FF:FED4:7171 on GigabitEthernet1/0/2
 Destination 4::4/128,
     via FE80::20C:29FF:FED4:7171, cost 1, tag 0, AOF, 5 secs
 Local route
 Destination 3::3/128,
```

```
     via ::, cost 0, tag 0, DOF
 Destination 6::/64,
     via ::, cost 0, tag 0, DOF
```

Display information about routes with the specified prefix for RIPng process 1.

```
<Sysname> display ripng 1 route 3::3 128 verbose
   Route Flags: A - Aging, S - Suppressed, G - Garbage-collect, D – Direct
                O - Optimal, F - Flush to RIB
 ----------------------------------------------------------------
 Peer FE80::4283:59FF:FE97:205 on GigabitEthernet1/0/2
 Destination 3::3/128,
     via FE80::4283:59FF:FE97:205, cost 1, tag 0, AOF, 28 secs
```

Table 7 Command output

Field	Description
A–Aging	The route is in aging state.
S–Suppressed	The route is in suppressed state.
G–Garbage-collect	The route is in Garbage-collect state.
D–Direct	The route is a direct route.
Local route	The route is a locally generated direct route.
O - Optimal	The route is an optimal route.
F - Flush to RIB	The route has been flushed to the RIB.
Peer	Neighbor connected to the interface.
Destination	IPv6 destination address.
via	Next hop IPv6 address.
cost	Routing metric value.
tag	Route tag.
secs	Time a route entry has stayed in the current state.

Display routing information statistics for RIPng process 1.

```
<Sysname> display ripng 1 route statistics
Peer                                          Optimal/Aging    Garbage
 FE80::20C:29FF:FED4:7171                      1/2              0
 Local                                         2/0              0
 total                                         3/2              0
```

Table 8 Command output

Field	Description
Peer	IPv6 address of the neighbor.
Optimal	Number of optimal routes.
Aging	Number of routes in aging state.
Garbage	Number of routes in Garbage-collection state.
Local	Total number of locally generated direct route.
total	Total number of routes learned from RIPng neighbors.

enable ipsec-profile

Use **enable ipsec-profile** to apply an IPsec profile to a RIPng process.

Use **undo enable ipsec-profile** to remove the IPsec profile from the RIPng process.

Syntax

enable ipsec-profile *profile-name*

undo enable ipsec-profile

Default

No IPsec profile is applied to a RIPng process.

Views

RIPng view

Predefined user roles

network-admin

context-admin

Parameters

profile-name: Specifies an IPsec profile by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

To configure an IPsec profile, see IPsec in *Security Configuration Guide*.

Examples

Apply IPsec profile **profile001** to RIPng process 1.

```
<Sysname> system-view
[Sysname] ripng 1
[Sysname-ripng-1] enable ipsec-profile profile001
```

fast-reroute

Use **fast-reroute** to configure RIPng FRR.

Use **undo fast-reroute** to disable RIPng FRR.

Syntax

fast-reroute route-policy *route-policy-name*

undo fast-reroute

Default

RIPng FRR is disabled.

Views

RIPng view

Predefined user roles

network-admin

context-admin

Parameters

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

RIPng FRR is available only when the state of primary link (with Layer 3 interfaces in up state) changes from bidirectional to unidirectional or down.

RIPng FRR is effective only for RIPng routes that are learned from directly connected neighbors.

Equal-cost routes do not support RIPng FRR.

Examples

Enable RIPng FRR and use routing policy **frr** to specify a backup next hop.

```
<Sysname> system-view
[Sysname] ipv6 prefix-list abc index 10 permit 100:: 64
[Sysname] route-policy frr permit node 10
[Sysname-route-policy-frr-10] if-match ipv6 address prefix-list abc
[Sysname-route-policy-frr-10] apply ipv6 fast-reroute backup-interface gigabitethernet
1/0/1 backup-nexthop FE80::8
[Sysname-route-policy-frr-10] quit
[Sysname] ripng 100
[Sysname-ripng-100] fast-reroute route-policy frr
```

filter-policy export

Use **filter-policy export** to configure RIPng to filter redistributed routes.

Use **undo filter-policy export** to remove the filtering.

Syntax

filter-policy { *ipv6-acl-number* | **prefix-list** *prefix-list-name* } **export** [*protocol* [*process-id*]]

undo filter-policy export [*protocol* [*process-id*]]

Default

RIPng does not filter redistributed routes.

Views

RIPng view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-acl-number: Specifies an IPv6 ACL by its number in the range of 2000 to 3999 to filter redistributed routes.

prefix-list *prefix-list-name*: Specifies an IPv6 prefix list by its name, a string of 1 to 63 characters, to filter redistributed routes.

protocol: Filters routes redistributed from a routing protocol.

process-id: Specifies the process ID of the specified routing protocol, in the range of 1 to 65535. This argument is available only when the routing protocol is **ripng**, **ospfv3**, or **isisv6**. The default is 1.

Usage guidelines

If the *protocol* argument is specified, RIPng filters only routes redistributed from the specified routing protocol. Otherwise, RIPng filters all redistributed routes.

To use an advanced ACL (with a number from 3000 to 3999) in the command, configure the ACL in one of the following ways:

- To deny/permit a route with the specified destination, use the **rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix* command.
- To deny/permit a route with the specified destination and prefix, use the **rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix* **destination** *dest dest-prefix* command.

The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the prefix of the route. For the prefix configuration to take effect, specify a contiguous prefix.

Examples

Use IPv6 prefix list to filter redistributed RIPng updates.

```
<Sysname> system-view
[Sysname] ipv6 prefix-list abc index 10 permit 100:1:: 32
[Sysname] ripng 100
[Sysname-ripng-100] filter-policy prefix-list abc export
```

Configure advanced IPv6 ACL 3000 to permit only route 2001::1/128 to pass. Use advanced IPv6 ACL 3000 to filter redistributed routes.

```
<Sysname> system-view
[Sysname] acl ipv6 advanced 3000
[Sysname-acl-ipv6-adv-3000] rule 10 permit ipv6 source 2001::1 128 destination
ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff 128
[Sysname-acl-ipv6-adv-3000] rule 100 deny ipv6
[Sysname-acl-ipv6-adv-3000] quit
[Sysname] ripng 100
[Sysname-ripng-100] filter-policy 3000 export
```

filter-policy import

Use **filter-policy import** to configure RIPng to filter received routes.

Use **undo filter-policy import** to restore the default.

Syntax

filter-policy { *ipv6-acl-number* | **prefix-list** *prefix-list-name* } **import**

undo filter-policy import

Default

RIPng does not filter received routes.

Views

RIPng view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-acl-number: Specifies an IPv6 ACL by its number in the range of 2000 to 3999 to filter received routes.

prefix-list *prefix-list-name*: Specifies an IPv6 prefix list by its name, a string of 1 to 63 characters, to filter received routes.

Usage guidelines

To use an advanced ACL (with a number from 3000 to 3999) in the command, configure the ACL in one of the following ways:

- To deny/permit a route with the specified destination, use the **rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix* command.
- To deny/permit a route with the specified destination and prefix, use the **rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix* **destination** *dest dest-prefix* command.

The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the prefix of the route. For the configuration to take effect, specify a contiguous prefix.

Examples

Use the IPv6 prefix list **abc** to filter received RIPng updates.

```
<Sysname> system-view
[Sysname] ipv6 prefix-list abc index 10 permit 100:1:: 32
[Sysname] ripng 100
[Sysname-ripng-100] filter-policy prefix-list abc import
```

Configure advanced IPv6 ACL 3000 to permit only route 2001::1/128 to pass. Use advanced IPv6 ACL 3000 to filter received routes.

```
<Sysname> system-view
[Sysname] acl ipv6 advanced 3000
[Sysname-acl-ipv6-adv-3000] rule 10 permit ipv6 source 2001::1 128 destination
ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff 128
[Sysname-acl-ipv6-adv-3000] rule 100 deny ipv6
[Sysname-acl-ipv6-adv-3000] quit
[Sysname] ripng 100
[Sysname-ripng-100] filter-policy 3000 import
```

graceful-restart

Use **graceful-restart** to enable Graceful Restart (GR) for RIPng.

Use **undo graceful-restart** to disable RIPng GR.

Syntax

graceful-restart

undo graceful-restart

Default

RIPng GR is disabled.

Views

RIPng view

Predefined user roles

network-admin

context-admin

Usage guidelines

RIPng GR and RIPng NSR are mutually exclusive. Do not configure the **graceful-restart** command and the **non-stop-routing** command at the same time.

Examples

Enable GR for RIPng process 1.

```
<Sysname> system-view
[Sysname] ripng 1
[Sysname-ripng-1] graceful-restart
```

graceful-restart interval

Use **graceful-restart interval** to set the GR interval.

Use **undo graceful-restart interval** to restore the default.

Syntax

graceful-restart interval *interval*

undo graceful-restart interval

Default

The GR interval is 60 seconds.

Views

RIPng view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies the GR interval in the range of 5 to 360 seconds.

Examples

Set the GR interval to 200 seconds for RIPng process 1.

```
<Sysname> system-view
[Sysname] ripng 1
[Sysname-ripng-1] graceful-restart interval 200
```

import-route

Use **import-route** to enable route redistribution.

Use **undo import-route** to disable route redistribution.

Syntax

import-route bgp4+ [*as-number*] [**allow-ibgp**] [**cost** *cost-value* | **route-policy** *route-policy-name*] *

undo import-route bgp4+

import-route { **direct** | **static** } [**cost** *cost-value* | **route-policy** *route-policy-name*] *

undo import-route { **direct** | **static** }

import-route { **isisv6** | **ospfv3** | **ripng** } [*process-id*] [**allow-direct** | **cost** *cost-value* | **route-policy** *route-policy-name*] *

undo import-route { **isisv6** | **ospfv3** | **ripng** } [*process-id*]

Default

RIPng does not redistribute routes.

Views

RIPng view

Predefined user roles

network-admin

context-admin

Parameters

bgp4+: Redistributes BGP4+ routes.

direct: Redistributes direct routes.

isisv6: Redistributes IPv6 IS-IS routes.

ospfv3: Redistributes OSPFv3 routes.

ripng: Redistributes RIPng routes.

static: Redistributes static routes.

as-number: Specifies an AS by its number in the range of 1 to 4294967295. If you do not specify the *as-number* argument, this command redistributes all IPv6 EBGP routes. As a best practice, specify the AS number to avoid redistributing excessive IPv6 EBGP routes.

process-id: Specifies an OSPFv3, IPv6 IS-IS, or RIPng process by its ID in the range of 1 to 65535. The default is 1.

allow-ibgp: Allows redistribution of IBGP routes. The **import-route bgp4+** command redistributes only EBGP routes. The **import-route bgp4+ allow-ibgp** command additionally redistributes IBGP routes and might cause routing loops. Therefore, use it with caution.

allow-direct: Redistributes the networks of the local interfaces enabled with the specified routing protocol. If you do not specify this keyword, the networks of the local interfaces are not redistributed. If you specify both the **allow-direct** keyword and the **route-policy** *route-policy-name* option, make sure the **if-match** rule defined in the routing policy does not conflict with the **allow-direct** keyword. For example, if you specify the **allow-direct** keyword, do not configure the **if-match route-type** rule for the routing policy. Otherwise, the **allow-direct** keyword does not take effect.

cost *cost-value*: Specifies a metric for redistributed routes, in the range of 0 to 16. The default metric is 0.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

This command redistributes only active routes. To view route state information, use the **display ipv6 routing-table protocol** command.

Examples

Redistribute routes from IPv6 IS-IS process 7 into RIPng and set the metric for redistributed routes to 7.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] import-route isisv6 7 cost 7
```

maximum load-balancing

Use **maximum load-balancing** to set the maximum number of equal-cost multi-path (ECMP) routes for load balancing.

Use **undo maximum load-balancing** to restore the default.

Syntax

maximum load-balancing *number*

undo maximum load-balancing

Default

The maximum number of RIPng ECMP routes equals the maximum number of ECMP routes, which is configurable by using the **max-ecmp-num** command.

Views

RIPng view

Predefined user roles

network-admin

context-admin

Parameters

number: Specifies the maximum number of ECMP routes. When this argument takes a value of 1, RIPng does not perform load balancing.

The following compatibility matrixes show the value ranges for the maximum number of RIPng ECMP routes:

Models	Value range
NFNX5-HD6480	1 to 16
NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	1 to 32

Usage guidelines

You can set a smaller value for the **max-ecmp-num** command than the current value for the **maximum load-balancing** command. After a reboot, the value for the **maximum load-balancing** command automatically changes to be the same as the value for the **max-ecmp-num** command.

Examples

Set the maximum number of ECMP routes to 2.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] maximum load-balancing 2
```

Related commands

max-ecmp-num

non-stop-routing

Use **non-stop-routing** to enable RIPng NSR.

Use **undo non-stop-routing** to disable RIPng NSR.

Syntax

non-stop-routing

undo non-stop-routing

Default

RIPng NSR is disabled.

Views

RIPng view

Predefined user roles

network-admin

context-admin

Usage guidelines

RIPng NSR enabled for a RIPng process takes effect only on that process. If multiple RIPng processes exist, enable RIPng NSR for each process as a best practice.

RIPng NSR and RIPng GR are mutually exclusive. Do not configure the **non-stop-routing** command and the **graceful-restart** command at the same time.

Examples

Enable NSR for RIPng process 1.

```
<Sysname> system-view
[Sysname] ripng 1
[Sysname-ripng-1] non-stop-routing
```

output-delay

Use **output-delay** to set the RIPng packet sending interval and the maximum number of RIPng packets that can be sent at each interval.

Use **undo output-delay** to restore the default.

Syntax

output-delay *time* **count** *count*

undo output-delay

Default

A RIPng process sends a maximum of three RIPng packets every 20 milliseconds.

Views

RIPng view

Predefined user roles

network-admin

context-admin

Parameters

time: Specifies the RIPng packet sending interval in the range of 10 to 100 milliseconds.

count: Specifies the maximum number of RIPng packets sent by a RIPng process at each interval, in the range of 1 to 30.

Usage guidelines

If you configure the RIPng packet sending rate for both a RIPng process and an interface running the RIPng process, the configuration on the interface takes effect.

Examples

Configure RIPng process 1 to send a maximum of 10 RIPng packets every 60 milliseconds.

```
<Sysname> system-view
[Sysname] ripng 1
[Sysname-ripng-1] output-delay 60 count 10
```

Related commands

ripng output-delay

preference

Use **preference** to set the preference for RIPng routes.

Use **undo preference** to restore the default.

Syntax

preference { *preference* | **route-policy** *route-policy-name* } *

undo preference

Default

The preference of RIPng routes is 100.

Views

RIPng view

Predefined user roles

network-admin

context-admin

Parameters

preference: Specifies the preference for RIPng routes, in the range of 1 to 255. The smaller the value, the higher the preference.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

You can specify a routing policy to set a preference for the matching RIPng routes.

- The preference set by the routing policy applies to all matching RIPng routes. The preference of other routes is set by the **preference** command.

- If no preference is set by the routing policy, the preference of all RIPng routes is set by the **preference** command.

Examples

Set the preference for RIPng routes to 120.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] preference 120
```

reset ripng process

Use **reset ripng process** to restart a RIPng process.

Syntax

reset ripng *process-id* **process**

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

process-id: Specifies a RIPng process by its ID in the range of 1 to 65535.

Usage guidelines

After executing the command, you are prompted to confirm the operation.

Examples

Restart RIPng process 100.

```
<Sysname> reset ripng 100 process
Reset RIPng process? [Y/N]:y
```

reset ripng statistics

Use **reset ripng statistics** to clear statistics for a RIPng process.

Syntax

reset ripng *process-id* **statistics**

Views

User view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies a RIPng process by its ID in the range of 1 to 65535.

Examples

Clear statistics for RIPng process 100.

```
<Sysname> reset ripng 100 statistics
```

ripng

Use **ripng** to enable RIPng and enter RIPng view.

Use **undo ripng** to disable RIPng.

Syntax

ripng [*process-id*] [**vpn-instance** *vpn-instance-name*]

undo ripng [*process-id*]

Default

RIPng is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

process-id: Specifies a RIPng process by its ID in the range of 1 to 65535. The default value is 1.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the RIPng process runs on the public network.

Usage guidelines

Before you configure global RIPng parameters, you must create a RIPng process. This restriction does not apply to configuring interface RIPng parameters.

If you disable a RIPng process, the configured RIPng parameters become invalid.

Examples

Create RIPng process 100 and enter its view.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100]
```

ripng default-route

Use **ripng default-route** to configure a RIPng interface to advertise a default route with a specified metric.

Use **undo ripng default-route** to disable a RIPng interface from sending a default route.

Syntax

ripng default-route { **only** | **originate** } [**cost** *cost-value* | **route-policy** *route-policy-name*] *

undo ripng default-route

Default

A RIPng process does not advertise a default route.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

only: Advertises only an IPv6 default route (::/0).

originate: Advertises an IPv6 default route (::/0) and other routes.

cost-value: Specifies a cost for the default route, in the range of 1 to 15. The default is 1.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters. The command advertises a default route only when a route in the routing table matches the routing policy.

Usage guidelines

This command enables the interface to advertise a RIPng default route in a route update regardless of whether the default route exists in the local IPv6 routing table.

A RIPng interface configured to advertise a default route does not receive any default routes from its neighbors.

Examples

Configure RIPng on GigabitEthernet 1/0/1 to advertise only a default route.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ripng default-route only
```

Configure RIPng on GigabitEthernet 1/0/1 to advertise a default route and other routes.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ripng default-route originate
```

ripng enable

Use **ripng enable** to enable RIPng on an interface.

Use **undo ripng enable** to disable RIPng on an interface.

Syntax

ripng *process-id* **enable**

undo ripng enable

Default

RIPng is disabled on an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

process-id: Specifies a RIPng process by its ID in the range of 1 to 65535.

Examples

Enable RIPng 100 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ripng 100 enable
```

ripng ipsec-profile

Use **ripng ipsec-profile** to apply an IPsec profile to a RIPng interface.

Use **undo ripng ipsec-profile** to remove the IPsec profile from the RIPng interface.

Syntax

ripng ipsec-profile *profile-name*

undo ripng ipsec-profile

Default

No IPsec profile is applied to a RIPng interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

profile-name: Specifies an IPsec profile by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

To configure an IPsec profile, see IPsec in *Security Configuration Guide*.

Examples

Apply IPsec profile **profile001** to GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ripng ipsec-profile profile001
```

ripng metricin

Use **ripng metricin** to configure an interface to add a metric to inbound RIPng routes.

Use **undo ripng metricin** to restore the default.

Syntax

ripng metricin *value*

undo ripng metricin

Default

The additional metric of an inbound route is 0.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

value: Adds an additional metric to inbound routes, in the range of 0 to 16.

Examples

Configure GigabitEthernet 1/0/1 to add a metric of 12 to inbound RIPng routes.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ripng metricin 12
```

ripng metricout

Use **ripng metricout** to configure an interface to add a metric to outbound RIPng routes.

Use **undo ripng metricout** to restore the default.

Syntax

ripng metricout *value*

undo ripng metricout

Default

The additional metric of outbound routes is 1.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

value: Adds an additional metric to outbound routes, in the range of 1 to 16.

Examples

Configure RIPng on GigabitEthernet 1/0/1 to add a metric of 12 to outbound RIPng routes.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ripng metricout 12
```

ripng output-delay

Use **ripng output-delay** to set the RIPng packet sending interval and the maximum number of RIPng packets that can be sent by an interface at each interval.

Use **undo ripng output-delay** to restore the default.

Syntax

ripng output-delay *time* **count** *count*

undo ripng output-delay

Default

An interface uses the RIPng packet sending rate set for the RIPng process that the interface runs.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

time: Specifies the RIPng packet sending interval in the range of 10 to 100 milliseconds.

count: Specifies the maximum number of RIPng packets sent at each interval, in the range of 1 to 30.

Usage guidelines

If you set the RIPng packet sending rate for both a RIPng process and an interface running the RIPng process, the configuration on the interface takes effect.

Examples

Configure GigabitEthernet 1/0/1 to send a maximum of six RIPng packets every 30 milliseconds.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ripng output-delay 30 count 6
```

Related commands

output-delay

ripng poison-reverse

Use **ripng poison-reverse** to enable poison reverse.

Use **undo ripng poison-reverse** to disable poison reverse.

Syntax

ripng poison-reverse

undo ripng poison-reverse

Default

Poison reverse is disabled.

Views

Interface view

Predefined user roles

network-admin

context-admin

Examples

Enable poison reverse for RIPng update messages on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ripng poison-reverse
```

ripng primary-path-detect bfd echo

Use **ripng primary-path-detect bfd echo** to enable BFD single-hop echo detection for RIPng FRR.

Use **undo ripng primary-path-detect bfd** to disable BFD single-hop echo detection for RIPng FRR.

Syntax

ripng primary-path-detect bfd echo

undo ripng primary-path-detect bfd

Default

BFD single-hop echo detection is disabled for RIPng FRR.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

For quicker RIPng FRR, use BFD single-hop echo detection on the primary link of redundant links to detect link failure.

For correct operation of BFD, make sure the interface is configured with an IPv6 global unicast address before you execute this command. For more information about IPv6 global unicast addresses, see IPv6 basics configuration in *Layer 3—IP Services Configuration Guide*.

Examples

Enable BFD single-hop echo detection for RIPng FRR on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] ripng 1
[Sysname-ripng-1] fast-reroute route-policy frr
[Sysname-ripng-1] quit
[Sysname] bfd echo-source-ipv6 1::1
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ripng primary-path-detect bfd echo
```

ripng split-horizon

Use **ripng split-horizon** to enable split horizon.

Use **undo ripng split-horizon** to disable split horizon.

Syntax

ripng split-horizon

undo ripng split-horizon

Default

Split horizon is enabled.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

Split horizon prevents routing loops. If you want to disable this feature, make sure the operation is indispensable.

If both poison reverse and split horizon are enabled, only poison reverse takes effect.

Examples

Enable split horizon on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ripng split-horizon
```

ripng summary-address

Use **ripng summary-address** to configure a summary network to be advertised through an interface.

Use **undo ripng summary-address** to remove a summary network.

Syntax

ripng summary-address *ipv6-address prefix-length*

undo ripng summary-address *ipv6-address prefix-length*

Default

No summary network is configured to be advertised through an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address: Specifies the destination IPv6 address of the summary route.

prefix-length: Specifies the prefix length of the destination IPv6 address of the summary route, in the range of 0 to 128. It indicates the number of consecutive 1s of the prefix, which defines the network ID.

Usage guidelines

Networks on the summary network will not be advertised. The cost of the summary route is the lowest cost among summarized routes.

Examples

Assign an IPv6 address with the 64-bit prefix to GigabitEthernet 1/0/1 and configure a summary with the 35-bit prefix.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 address 2001:200::3EFF:FE11:6770/64
[Sysname-GigabitEthernet1/0/1] ripng summary-address 2001:200:: 35
```

timer triggered

Use **timer triggered** to set the interval for sending triggered updates.

Use **undo timer triggered** to restore the default.

Syntax

timer triggered *maximum-interval* [*minimum-interval* [*incremental-interval*]]

undo timer triggered

Default

The maximum, minimum, and incremental intervals for sending triggered updates are 5 seconds, 50 milliseconds, and 200 milliseconds, respectively.

Views

RIPng view

Predefines user roles

network-admin

context-admin

Parameters

maximum-interval: Specifies the maximum interval for sending triggered updates, in the range of 1 to 5 seconds.

minimum-interval: Specifies the minimum interval for sending triggered updates, in the range of 10 to 5000 milliseconds.

incremental-interval: Specifies the incremental interval for sending triggered updates, in the range of 100 to 1000 milliseconds.

Usage guidelines

The minimum interval and the incremental interval cannot be greater than the maximum interval.

For a stable network, the minimum interval is used. If network changes become frequent, the incremental interval *incremental-interval* is used to increase the triggered update sending interval until the *maximum-interval* is reached.

Examples

Set the maximum, minimum, and incremental intervals for sending triggered updates to 2 seconds, 100 milliseconds, and 100 milliseconds, respectively.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] timer triggered 2 100 100
```

timers

Use **timers** to set RIPng timers.

Use **undo timers** to restore the default.

Syntax

timers { **garbage-collect** *garbage-collect-value* | **suppress** *suppress-value* | **timeout** *timeout-value* | **update** *update-value* } *

undo timers { **garbage-collect** | **suppress** | **timeout** | **update** } *

Default

The garbage-collect timer is 120 seconds, the suppress timer is 120 seconds, the timeout timer is 180 seconds, and the update timer is 30 seconds.

Views

RIPng view

Predefines user roles

network-admin

context-admin

Parameters

garbage-collect-value: Sets the garbage-collect timer in the range of 1 to 86400 seconds.

suppress-value: Sets the suppress timer in the range of 0 to 86400 seconds.

timeout-value: Sets the timeout timer in the range of 1 to 86400 seconds.

update-value: Sets the update timer in the range of 1 to 86400 seconds.

Usage guidelines

RIPng has the following timers:

- **Update timer**—Interval between update messages.
- **Timeout timer**—Route aging time. If no update for a route is received before the timer expires, RIPng sets the metric of the route to 16.
- **Suppress timer**—How long a RIPng route stays in suppressed state. When the metric of a route becomes 16, the route enters the suppressed state. If RIPng receives an update for the route from the same neighbor and the route in the update has a metric less than 16, RIPng uses the route to replace the suppressed route.
- **Garbage-collect timer**—Interval from when the metric of a route becomes 16 to when it is deleted from the routing table. During the garbage-collect timer length, RIPng advertises the route with a metric of 16. If no update is announced for that route before the garbage-collect timer expires, RIPng deletes the route from the routing table.

As a best practice, do not change the default values of these timers.

The timer lengths must be kept consistent on all routers in the network.

Examples

Set the update, timeout, suppress, and garbage-collect timers to 5 seconds, 15 seconds, 15 seconds, and 30 seconds.

```
<Sysname> system-view
[Sysname] ripng 1
[Sysname-ripng-1] timers update 5 timeout 15 suppress 15 garbage-collect 30
```

Contents

OSPF commands

abr-summary

Use **abr-summary** to configure route summarization on an ABR.

Use **undo abr-summary** to remove the configuration.

Syntax

abr-summary *ip-address* { *mask-length* | *mask* } [**advertise** | **not-advertise**] [**cost** *cost-value*]

undo abr-summary *ip-address* { *mask-length* | *mask* }

Default

Route summarization is not configured on an ABR.

Views

OSPF area view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the destination IP address of the summary route in dotted decimal notation.

mask-length: Specifies the mask length in the range of 0 to 32.

mask: Specifies the mask of the IP address, in dotted decimal notation.

advertise | **not-advertise**: Advertises the summary route or not. By default, the command advertises the summary route.

cost *cost-value*: Specifies the cost of the summary route, in the range of 1 to 16777215. The default cost is the largest cost value among routes that are summarized.

Usage guidelines

This command applies only to an ABR to summarize multiple contiguous networks into one network.

To enable ABR to advertise specific routes that have been summarized, use the **undo abr-summary** command.

Examples

Summarize networks 36.42.10.0/24 and 36.42.110.0/24 in Area 1 into 36.42.0.0/16.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] network 36.42.10.0 0.0.0.255
[Sysname-ospf-100-area-0.0.0.1] network 36.42.110.0 0.0.0.255
[Sysname-ospf-100-area-0.0.0.1] abr-summary 36.42.0.0 255.255.0.0
```

area

Use **area** to create an OSPF area and enter OSPF area view.

Use **undo area** to remove an OSPF area.

Syntax

area *area-id*

undo area *area-id*

Default

No OSPF areas exist.

Views

OSPF view

Predefined user roles

network-admin

context-admin

Parameters

area-id: Specifies an area by its ID, an IP address or a decimal integer in the range of 0 to 4294967295 that is translated into the IP address format.

Examples

Create Area 0 and enter Area 0 view.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 0
[Sysname-ospf-100-area-0.0.0.0]
```

asbr-summary

Use **asbr-summary** to configure route summarization on an ASBR.

Use **undo asbr-summary** to remove the configuration.

Syntax

asbr-summary *ip-address* { *mask-length* | *mask* } [**cost** *cost-value* | **not-advertise** | **nssa-only** | **tag** *tag*] *

undo asbr-summary *ip-address* { *mask-length* | *mask* }

Default

Route summarization is not configured on an ASBR.

Views

OSPF view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the destination IP address of the summary route.

mask-length: Specifies the mask length in the range of 0 to 32.

mask: Specifies the mask in dotted decimal notation.

cost *cost-value*: Specifies the cost of the summary route, in the range of 1 to 16777214. If you do not specify this option, the largest cost among the summarized routes applies. If the routes in Type-5 LSAs translated from Type-7 LSAs are Type-2 external routes, the largest cost among the summarized routes plus 1 applies.

not-advertise: Disables advertising the summary route. If you do not specify this keyword, the command advertises the route.

nssa-only: Limits the route advertisement to the NSSA area by setting the P-bit of Type-7 LSAs to 0. By default, the P-bit of Type-7 LSAs is set to 1. If the ASBR is also an ABR and **FULL** state neighbors exist in the backbone area, the P-bit of Type-7 LSAs originated by the ASBR is set to 0. This keyword applies to the NSSA ASBR.

tag *tag*: Specifies a tag for the summary route, in the range of 0 to 4294967295. The default is 1. The tag can be used by a routing policy to control summary route advertisement.

Usage guidelines

An ASBR can summarize routes in the following LSAs:

- Type-5 LSAs.
- Type-7 LSAs in an NSSA area.
- Type-5 LSAs translated by the ASBR (also an ABR) from Type-7 LSAs in an NSSA area.

  If the ASBR (ABR) is not a translator, it cannot summarize routes in Type-5 LSAs translated from Type-7 LSAs.

To enable ASBR to advertise specific routes that have been summarized, use the **undo asbr-summary** command.

Examples

Summarize redistributed static routes into a single route, and specify a tag value of 2 and a cost of 100 for the summary route.

```
<Sysname> system-view
[Sysname] ip route-static 10.2.1.0 24 null 0
[Sysname] ip route-static 10.2.2.0 24 null 0
[Sysname] ospf 100
[Sysname-ospf-100] import-route static
[Sysname-ospf-100] asbr-summary 10.2.0.0 255.255.0.0 tag 2 cost 100
```

authentication-mode

Use **authentication-mode** to specify an authentication mode for an OSPF area.

Use **undo authentication-mode** to remove the configuration.

Syntax

For MD5/HMAC-MD5/HMAC-SHA-256 authentication:

authentication-mode { **hmac-md5** | **hmac-sha-256** | **md5** } *key-id* { **cipher** | **plain** } *string*

undo authentication-mode [{ **hmac-md5** | **hmac-sha-256** | **md5** } *key-id*]

For simple authentication:

authentication-mode simple { **cipher** | **plain** } *string*

undo authentication-mode

For keychain authentication:

authentication-mode keychain *keychain-name*

undo authentication-mode

Default

No authentication is performed for an area.

Views

OSPF area view

Predefined user roles

network-admin

context-admin

Parameters

hmac-md5: Specifies the HMAC-MD5 authentication mode.

hmac-sha-256: Specifies the HMAC-SHA-256 authentication mode.

md5: Specifies the MD5 authentication mode.

simple: Specifies the simple authentication mode.

key-id: Specifies a key by its ID in the range of 0 to 255.

cipher: Specifies a key in encrypted form.

plain: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. This argument is case sensitive.

- In simple authentication mode, the plaintext form of the key is a string of 1 to 8 characters. The encrypted form of the key is a string of 33 to 41 characters.
- In MD5/HMAC-MD5/HMAC-SHA-256 authentication mode, the plaintext form of the key is a string of 1 to 255 characters. The encrypted form of the key is a string of 33 to 373 characters.

keychain: Specifies the keychain authentication mode.

keychain-name: Specifies a keychain by its name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

To establish or maintain adjacencies, routers in the same area must have the same authentication mode and key.

If MD5, HMAC-MD5, or HMAC-SHA-256 authentication is configured, you can configure multiple keys, each having a unique key ID and key string. As a best practice to minimize the risk of key compromise, use only one key for an area and delete the old key after key replacement.

To replace the key used for MD5, HMAC-MD5, or HMAC-SHA-256 authentication in an area, you must configure the new key before removing the old key from each router. OSPF uses the key rollover mechanism to ensure that the routers can pass authentication before the replacement is complete across the area. After you configure a new key on a router, the router sends copies of the same packet, each authenticated by a different key, including the new key and the keys in use. This practice continues until the router detects that all its neighbors have the new key.

When keychain authentication is configured for an OSPF area, OSPF performs the following operations before sending a packet:

1. Obtains a valid send key from the keychain.

   OSPF does not send the packet if it fails to obtain a valid send key.
2. Uses the key ID, authentication algorithm, and key string to authenticate the packet.

   If the key ID is greater than 255, OSPF does not send the packet.

When keychain authentication is configured for an OSPF area, OSPF performs the following operations after receiving a packet:

1. Uses the key ID carried in the packet to obtain a valid accept key from the keychain.

   OSPF discards the packet if it fails to obtain a valid accept key.

2. Uses the authentication algorithm and key string for the valid accept key to authenticate the packet.

   If the authentication fails, OSPF discards the packet.

OSPF supports only the MD5, HMAC-SM3, HMAC-MD5, and HMAC-SHA-256 authentication algorithms for keychain authentication.

The ID of keys used for keychain authentication can only be in the range of 0 to 255.

Examples

Configure OSPF Area 0 to use the MD5 authentication mode, and set the key ID to 15 and the key to **abc** in plaintext form.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 0
[Sysname-ospf-100-area-0.0.0.0] authentication-mode md5 15 plain abc
```

Related commands

ospf authentication-mode

bandwidth-reference

Use **bandwidth-reference** to set a reference bandwidth value for link cost calculation.

Use **undo bandwidth-reference** to restore the default value.

Syntax

bandwidth-reference *value*

undo bandwidth-reference

Default

The reference bandwidth value is 100 Mbps for link cost calculation.

Views

OSPF view

Predefined user roles

network-admin

context-admin

Parameters

value: Specifies the reference bandwidth value for link cost calculation, in the range of 1 to 4294967 Mbps.

Usage guidelines

If no cost values are configured for links, OSPF calculates their cost values by using the following formula: Cost = Reference bandwidth value / Expected interface bandwidth. The expected bandwidth of an interface is configured with the **bandwidth** command (see *Interface Command Reference*). If the calculated cost is greater than 65535, the value of 65535 is used. If the calculated cost is less than 1, the value of 1 is used.

Examples

Set the reference bandwidth value to 1000 Mbps.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] bandwidth-reference 1000
```

Related commands

ospf cost

database-filter peer

Use **database-filter peer** to filter LSAs for the specified P2MP neighbor.

Use **undo database-filter peer** to restore the default.

Syntax

database-filter peer *ip-address* { **all** | { **ase** [**acl** *ipv4-acl-number*] | **nssa** [**acl** *ipv4-acl-number*] | **summary** [**acl** *ipv4-acl-number*] } * }

undo database-filter peer *ip-address*

Default

The LSAs for the specified P2MP neighbor are not filtered.

Views

OSPF view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies a P2MP neighbor by its IP address.

all: Filters all LSAs except the Grace LSAs.

ase: Filters Type-5 LSAs.

nssa: Filters Type-7 LSAs.

summary: Filters Type-3 LSAs.

acl *ipv4-acl-number*: Specifies an IPv4 ACL by its number in the range of 2000 to 3999.

Usage guidelines

On an P2MP network, a router might have multiple OSPF neighbors with the P2MP type. Use this command to prevent the router from sending LSAs to the specified neighbor.

When you specify an ACL, follow these guidelines:

- If the ACL does not exist or has no rules, OSPF does not filter the LSAs sent to the specified neighbor.
- If a rule in the ACL is applied to a VPN instance, the rule will deny all of the LSAs sent to the specified neighbor.

To use an advanced ACL (with a number from 3000 to 3999) in the command, configure the ACL using one of the following methods:

- To deny/permit LSAs with the specified link state ID, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* command.

- To deny/permit LSAs with the specified link state ID and mask, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* **destination** *dest-addr dest-wildcard* command.

The **source** keyword specifies the link state ID of an LSA and the **destination** keyword specifies the subnet mask of the LSA. For the mask configuration to take effect, specify a contiguous subnet mask.

If the specified neighbor has already received an LSA, the LSA still exists in the LSDB of the neighbor after you execute the command.

Examples

Filter all LSAs (except the Grace LSAs) for the P2MP neighbor with the IP address 121.20.20.121.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] database-filter peer 121.20.20.121 all
```

Configure advanced ACL 3000 to filter Type-3 LSAs for the P2MP neighbor with the IP address 121.20.20.121.

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000]rule 10 deny ip source 121.20.0.0 0 destination 255.255.0.0
0
[Sysname-acl-ipv4-adv-3000] rule 100 permit ip
[Sysname-acl-ipv4-adv-3000] quit
[Sysname] ospf 1
[Sysname-ospf-1] database-filter peer 121.20.20.121 summary acl 3000
```

Related commands

ospf database-filter

default

Use **default** to configure default parameters for redistributed routes.

Use **undo default** to remove the configuration.

Syntax

default { **cost** *cost-value* | **tag** *tag* | **type** *type* } *

undo default { **cost** | **tag** | **type** } *

Default

The cost is 1, the tag is 1, and the route type is 2.

Views

OSPF view

Predefined user roles

network-admin

context-admin

Parameters

cost *cost-value*: Specifies a default cost for redistributed routes, in the range of 0 to 16777214.

tag *tag*: Specifies a tag for redistributed routes, in the range of 0 to 4294967295.

type *type*: Specifies a type for redistributed routes: 1 or 2.

Examples

Set the default cost, tag, and type to 10, 100, and 2 for redistributed external routes.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] default cost 10 tag 100 type 2
```

Related commands

import-route

default-cost

Use **default-cost** to set a cost for the default route advertised to the stub or NSSA area.

Use **undo default-cost** to restore the default value.

Syntax

default-cost *cost-value*

undo default-cost

Default

The cost is 1.

Views

OSPF area view

Predefined user roles

network-admin

context-admin

Parameters

cost-value: Specifies a cost for the default route advertised to the Stub or NSSA area, in the range of 0 to 16777214.

Usage guidelines

This command takes effect only on the ABR of a stub area or the ABR or ASBR of an NSSA area.

Examples

Configure Area 1 as a stub area, and set the cost of the default route advertised to the stub area to 20.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] stub
[Sysname-ospf-100-area-0.0.0.1] default-cost 20
```

Related commands

nssa

stub

default-route-advertise

Use **default-route-advertise** to redistribute a default route into the OSPF routing domain.

Use **undo default-route-advertise** to restore the default.

Syntax

default-route-advertise [[**always** | **permit-calculate-other**] | **cost** *cost-value* | **route-policy** *route-policy-name* | **type** *type*] *

default-route-advertise [**summary cost** *cost-value*]

undo default-route-advertise

Default

No default route is redistributed into the OSPF routing domain.

Views

OSPF view

Predefined user roles

network-admin

context-admin

Parameters

always: Redistributes a default route in a Type-5 LSA into the OSPF routing domain regardless of whether a default route exists in the routing table. If you do not specify this keyword, the router redistributes a default route only when an active default route that does not belong to the current OSPF process exists in the IP routing table.

permit-calculate-other: Enables OSPF to calculate default routes received from other routers. If you do not specify this keyword, OSPF does not calculate default routes from other routers. If the router does not redistribute any default route in a Type-5 LSA into the OSPF routing domain, the router calculates default routes from other routers. It calculates these routes regardless of whether this keyword is specified.

cost *cost-value*: Specifies a cost for the default route, in the range of 0 to 16777214. If you do not specify this option, the default cost specified by the **default-cost** command applies.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters. When the routing policy is matched and one of the following conditions is met, the command redistributes a default route in a Type-5 LSA into the OSPF routing domain:

- A default route exists in the routing table.
- The **always** keyword is specified.

The routing policy modifies values in the Type-5 LSA.

type *type*: Specifies a type for the Type-5 LSA: 1 or 2. If you do not specify this option, the default type for the Type-5 LSA specified by the **default type** command applies.

summary: Advertises the specified default route in a Type-3 LSA. This keyword is available only for VPNs.

Usage guidelines

This command redistributes a default route in a Type-5 LSA, which cannot be redistributed with the **import-route** command. If the local routing table has no default route, you must specify the **always** keyword for the command.

The **default-route-advertise summary cost** command is applicable only to VPNs. It enables a PE router to redistribute a default external route in a Type-3 LSA to CE routers.

Examples

Redistribute a default route into the OSPF routing domain, regardless of whether the default route exists in the local routing table.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] default-route-advertise always
```

Related commands

default

import-route

description

Use **description** to configure a description for an OSPF process or area.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

No description is configured for an OSPF process or area.

Views

OSPF view

OSPF area view

Predefined user roles

network-admin

context-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 80 characters.

Usage guidelines

The description specified by this command is used to identify an OSPF process or area.

Examples

Describe OSPF process 100 as **abc**.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] description abc
```

Describe OSPF Area 0 as **bone area**.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 0
[Sysname-ospf-100-area-0.0.0.0] description bone area
```

discard-route

Use **discard-route** to configure discard routes for summary networks.

Use **undo discard-route** to restore the default.

Syntax

discard-route { **external** { *preference* | **suppression** } | **internal** { *preference* | **suppression** } } *

undo discard-route [**external** | **internal**] *

Default

A device generates discard routes with preference 255 for summary networks.

Views

OSPF view

Predefined user roles

network-admin

context-admin

Parameters

external: Specifies discard routes for redistributed summary networks on the ASBR. These discard routes are external discard routes.

preference: Specifies a preference for external discard routes, in the range of 1 to 255.

suppression: Disables the ASBR from generating external discard routes for summary networks.

internal: Specifies discard routes for summary networks on the ABR. These discard routes are internal discard routes.

preference: Specifies a preference for internal discard routes, in the range of 1 to 255.

suppression: Disables the ABR from generating internal discard routes for summary networks.

Examples

Generate external and internal discard routes with preference 100 and 200, respectively.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] discard-route external 100 internal 200
```

display ospf

Use **display ospf** to display OSPF process information.

Syntax

display ospf [*process-id*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays information about all OSPF processes.

verbose: Displays detailed OSPF process information. If you do not specify this keyword, the command displays brief OSPF process information.

Examples

Display detailed OSPF process information.

```
<Sysname> display ospf verbose

          OSPF Process 1 with Router ID 192.168.1.2
                  OSPF Protocol Information

 RouterID: 192.168.1.2      Router type:  NSSA
 Route tag: 0
 Multi-VPN-Instance is not enabled
 Ext-community type: Domain ID 0x105, Route Type 0x8000, Router ID 0x8001
 Domain ID: 0.0.0.0:23
 Opaque capable
 Originating router-LSAs with maximum metric
    Condition: On startup for 600 seconds, State: Inactive
    Advertise stub links with maximum metric in router-LSAs
    Advertise summary-LSAs with metric 16711680
    Advertise external-LSAs with metric 16711680
 Originating LSAs with metric 65500 controlled by RBM
 ECMP group is enabled
 ISPF is enabled
 SPF-schedule-interval: 5 50 200
 LSA generation interval: 5
 LSA arrival interval: 1000
 Transmit pacing: Interval: 20 Count: 3
 Default ASE parameters: Metric: 1 Tag: 1 Type: 2
 Route preference: 10
 ASE route preference: 150
 SPF computation count: 22
 RFC 1583 compatible
 Fast-reroute: Lfa Enabled
 Node-Protecing Preference: 40
 Lowest-cost Preference: 20
 Graceful restart interval: 120
 SNMP trap rate limit interval: 2  Count: 300
 This process is currently bound to MIB
 Area count: 1   NSSA area count: 1
 Normal areas with up interfaces: 0
 NSSA areas with up interfaces: 1
 Up interfaces: 1
 ExChange/Loading neighbors: 0
```

```
Full neighbors:3
Calculation trigger type: Full
Current calculation type: SPF calculation
Current calculation phase: Calculation area topology
Process reset state: N/A
Current reset type: N/A
Next reset type: N/A
Reset prepare message replied: -/-/-/-
Reset process message replied: -/-/-/-
Reset phase of module:
  M-N/A, P-N/A, L-N/A, C-N/A, R-N/A

Area: 0.0.0.1          (MPLS TE  not enabled)
Authtype: None    Area flag: NSSA
7/5 translator state: Disabled
7/5 translate stability timer interval: 0
SPF scheduled count: 5
ExChange/Loading neighbors: 0
Up interfaces: 1

Interface: 192.168.1.2 (GigabitEthernet1/0/1)
Cost: 1       State: DR        Type: Broadcast    MTU: 1500
Priority: 1
Designated router: 192.168.1.2
Backup designated router: 192.168.1.1
Timers: Hello 10 , Dead 40 , Poll  40 , Retransmit 5 , Transmit Delay 1
FRR backup: Enabled
Enabled by network configuration
Prefix-SID type: Index
  Value: 101
  Process ID: ospf 1
  Prefix-SID validity: Invalid
```

Table 1 Command output

Field	Description
OSPF Process 1 with Router ID 192.168.1.2	OSPF process ID and OSPF router ID.
RouterID	Router ID.
Router type	Router type: • ABR. • ASBR. • NSSA. • Null.
Route tag	Tag of redistributed routes.
Multi-VPN-Instance is not enabled	The OSPF process does not support multi-VPN-instance.
Ext-community type	OSPF extended community attribute type codes: • **Domain ID**—Domain ID code.

	• **Route Type**—Route type code. • **Router ID**—Router ID code.
Domain ID	OSPF domain ID (primary ID).
Opaque capable	Opaque LSA advertisement and reception capability is enabled.
Originating router-LSAs with maximum metric	The maximum cost value for router LSAs (excluding stub links) is used.
Condition	Status of the stub router: • Always. • On startup while BGP is converging. • On startup while BGP is converging for *xxx* seconds, where *xxx* is specified by the user. • On startup for *xxx* seconds, where *xxx* is specified by the user.
State	Whether the stub router is active.
Originating LSAs with metric *xxx* controlled by RBM	The device is the backup device in Remote Backup Management (RBM). • **Originating LSAs with metric +*n* controlled by RBM**—When OSPF generates an LSA, the cost is the sum of the original cost and *n.* • **Originating LSAs with metric *n* controlled by RBM**—When OSPF generates an LSA, the cost is *n.* This field is displayed only when RBM has adjusted the OSPF cost.
ECMP group is enabled	ECMP route grouping is enabled. This field is displayed only when ECMP route grouping is enabled.
SPF-schedule-interval	Interval for SPF calculations. If the SPF calculation interval is fixed, this field also displays **in milliseconds** enclosed with brackets.
LSA generation interval	LSA generation interval.
LSA arrival interval	LSA arrival interval.
Transmit pacing	LSU packet transmit rate of the interface: • **Interval**—LSU transmit interval of the interface. • **Count**—Maximum number of LSU packets sent at each interval.
Default ASE parameters	Default ASE parameters: **Metric**, **Tag**, and **Type**.
Route preference	Internal route preference.
ASE route preference	External route preference.
SPF computation count	SPF computation count of the OSPF process.
RFC1583 compatible	Compatible with RFC 1583.
Fast-reroute	FRR type: **LFA**—LFA is enabled.
Node-Protecing Preference	Preference for node protection policy.
Lowest-cost Preference	Preference for lowest-cost policy.
Graceful restart interval	GR interval.
SNMP trap rate limit interval	SNMP notification sending interval.

Count	Number of sent SNMP notifications.
ExChange/Loading neighbors	Neighbors in ExChange/Loading state.
Full neighbors	Neighbors in Full state.
Calculation trigger type	Route calculation trigger type: • **Full**—Calculation of all routes is triggered. • **Area topology change**—Topology change in an area. • **Intra router change**—Incremental intra-area route change. • **ASBR change**—Incremental ASBR route change. • **7to5 translator**—Type-7-to-Type-5 LSA translator role change. • **Full IP prefix**—Calculation of all IP prefixes is triggered. • **Full intra AS**—Calculation of all intra-AS prefixes is triggered. • **Inc intra AS**—Calculation of incremental intra-AS prefixes is triggered. • **Full inter AS**—Calculation of all AS-external prefixes is triggered. • **Inc inter AS**—Calculation of incremental AS-external prefixes is triggered. • **N/A**—Route calculation is not triggered.
Current calculation type	Current route calculation type: • SPF calculation. • **Intra router calculation**—Intra-area route calculation. • **ASBR calculation**—Inter-area ASBR route calculation. • **Inc intra router**—Incremental intra-area route calculation. • **Inc ASBR calculation**—Incremental inter-area ASBR route calculation. • **7to5 translator**—Type-7-to-Type-5 LSA calculation. • **Full intra AS**—Calculation of all intra-AS prefixes. • **Inc intra AS**—Calculation of incremental intra-AS prefixes. • **Full inter AS**—Calculation of all AS-external prefixes. • **Inc inter AS**—Calculation of incremental AS-external prefixes. • **Forward address**—Forwarding address calculation. • **N/A**—Route calculation is not triggered.
Current calculation phase	Current route calculation phase: • **Calculation area topology**—Calculating area topology. • **Calculation router**—Calculating routes on routers. • **Calculation intra AS**—Calculating intra-AS routes. • **7to5 translator**—Calculating Type-7-to-Type-5 LSAs. • **Forward address**—Calculating forwarding addresses. • **Calculation inter AS**—Calculating AS-external routes. • **Calculation end**—Ending phase of calculation. • **N/A**—Route calculation is not triggered.
Process reset state	Process reset state: • **N/A**—The process is not reset. • **Under reset**—The process is in the reset progress. • **Under RIB smooth**—The process is synchronizing the RIB.

Current reset type	Current process reset type: • **N/A**—The process is not reset. • **Normal**—Normal reset. • **GR quit**—Normal reset when GR quits abnormally. • **Delete**—Delete OSPF process. • **VPN delete**—Delete VPN.
Next reset type	Next process reset type: • **N/A**—The process is not reset. • **Normal**—Normal reset. • **GR quit**—Normal reset when GR quits abnormally. • **Delete**—Delete OSPF process. • **VPN delete**—Delete VPN.
Reset prepare message replied	Modules that reply reset prepare messages: • **P**—Neighbor maintenance module. • **L**—LSDB synchronization module. • **C**—Route calculation module. • **R**—Route redistribution module.
Reset process message replied	Modules that reply reset process messages: • **P**—Neighbor maintenance module. • **L**—LSDB synchronization module. • **C**—Route calculation module. • **R**—Route redistribution module.

Reset phase of module	Reset phase of each module:
	• Main control module:
	  ○ **N/A**—Not reset.
	  ○ Delete area.
	  ○ Delete process.
	• Neighbor maintenance (P) module:
	  ○ **N/A**—Not reset.
	  ○ Delete neighbor.
	  ○ Delete interface.
	  ○ **Delete vlink**—Delete virtual link.
	• LSDB synchronization (L) module:
	  ○ **N/A**—Not reset.
	  ○ Stop timer.
	  ○ **Delete ASE**—Delete all ASE LSAs.
	  ○ **Delete ASE maps**—Delete ASE LSA maps.
	  ○ Clear process data.
	  ○ **Delete area LSA**—Delete LSAs and maps from an area.
	  ○ **Delete area interface**—Delete interfaces from an area.
	  ○ **Delete process**—Delete process-related resources.
	  ○ **Restart**—Restart process-related resources.
	• Route calculation (C) module:
	  ○ **N/A**—Not reset.
	  ○ **Delete topology**—Delete area topology.
	  ○ **Delete router**—Delete routes of routers.
	  ○ **Delete intra AS**—Delete intra-AS routes
	  ○ **Delete inter AS**—Delete AS-external routes.
	  ○ **Delete forward address**—Delete forwarding address list.

	○ **Delete advertise**—Delete advertising router list. • Route redistribution (R) module: ○ **N/A**—Not reset. ○ **Delete ABR summary**—Delete summary routes of the ABR. ○ **Delete ASBR summary**—Delete summary routes of the ASBR. ○ **Delete import**—Delete redistributed routes.
Area	Area ID in the IP address format.
Authentication type	Authentication type of the area: • **None**—No authentication. • **Simple**—Simple authentication. • **Cryptographic**—Encrypted authentication. Options include MD5, HMAC-MD5, and HMAC-SHA-256. • **Keychain**—Keychain authentication.
Area flag	Type of the area: • Normal. • Stub. • StubNoSummary (totally stub area). • NSSA. • NSSANoSummary (totally NSSA area).
7/5 translator state	State of the translator that translates Type-7 LSAs to Type-5 LSAs: • **Enabled**—The translator is specified through commands. • **Elected**—The translator is designated through election. • **Disabled**—The device is not a translator.
7/5 translate stability timer interval	Stability interval for Type-7 LSA-to-Type-5 LSA translation.
SPF scheduled Count	SPF calculation count in the OSPF area.
Interface	Interface in the area.
Cost	Interface cost.
State	Interface state.
Type	Interface network type.
MTU	Interface MTU.
Priority	Router priority.
Timers	OSPF timers: • **Hello**—Interval for sending hello packets. • **Dead**—Interval within which the neighbor is down. • **Poll**—Interval for sending hello packets. • **Retransmit**—Interval for retransmitting LSAs.
FRR backup	Whether Loop Free Alternate (LFA) calculation is enabled on an interface.
Enabled by interface configuration (including secondary IP addresses)	OSPF is enabled on the interface. **including secondary IP addresses** indicates that OSPF advertises the direct routes to the primary and secondary addresses of the interface.
Keychain authentication: Enabled (*xx*), inherited	Keychain authentication is enabled. The name of the keychain is *xx*. If the interface uses the authentication mode of its area, this field displays **inherited** after the

	authentication mode.
Cryptographic authentication: Enabled, inherited	Authentication mode used by the interface. If the interface uses the authentication mode of its area, this field displays **inherited** after the authentication mode. Optional authentication modes include: • **Simple**—Simple authentication. • **Cryptographic**—Encrypted authentication. Options include MD5, HMAC-MD5, and HMAC-SHA-256.
The last key is *xx*	The most recent MD5/HMAC-MD5/HMAC-SHA-256 authentication key ID is *xx*.
The rollover is in progress, *xx* neighbor(s) left	Key rollover for MD5/HMAC-MD5/HMAC-SHA-256 authentication is in progress. The number of neighbors that have not completed rollover is *xx*.

display ospf abr-asbr

Use **display ospf abr-asbr** to display routes to the ABR or ASBR.

Syntax

display ospf [*process-id*] **abr-asbr** [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays routes to the ABR and ASBR for all OSPF processes.

verbose: Displays detailed information. If you do not specify this keyword, the command displays brief information.

Usage guidelines

If you use this command on routers in a stub area, the commands displays no ASBR information.

Examples

Display brief information about routes to the ABR or ASBR.

```
<Sysname> display ospf abr-asbr

          OSPF Process 1 with Router ID 192.168.1.2
                 Routing Table to ABR and ASBR

 Type        Destination       Area       Cost  Nexthop         RtType
 Inter       3.3.3.3           0.0.0.0    3124  10.1.1.2        ASBR
 Intra       2.2.2.2           0.0.0.0    1562  10.1.1.2        ABR
```

Display detailed information about routes to the ABR or ASBR.

```
<Sysname> display ospf abr-asbr verbose
```

```
          OSPF Process 10 with Router ID 101.1.1.11
                  Routing Table to ABR and ASBR

Destination: 1.1.1.1            RtType     : ASBR
Area       : 0.0.0.1            Type       : Intra
Nexthop    : 150.0.1.12         BkNexthop  : 0.0.0.0
Interface  : GE1/0/1            BkInterface: N/A
Cost       : 1000
```

Table 2 Command output

Field	Description
Type	Type of the route to the ABR or ASBR: • **Inter**—Inter-area route. • **Intra**—Intra-area route.
Destination	Router ID of an ABR or ASBR.
Area	ID of the area of the next hop.
Cost	Cost from the router to the ABR or ASBR.
Nexthop	Next hop address.
BkNexthop	Backup next hop address.
RtType	Router type: ABR or ASBR.
Interface	Output interface.
BkInterface	Backup output interface.

display ospf abr-summary

Use **display ospf abr-summary** to display ABR summary route information.

Syntax

display ospf [*process-id*] [**area** *area-id*] **abr-summary** [*ip-address* { *mask-length* | *mask* }] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays information about ABR summary routes for all OSPF processes.

area *area-id*: Specifies an OSPF area by its ID. The area ID is an IP address or a decimal integer in the range of 0 to 4294967295 that is translated into the IP address format. If you do not specify this option, the command displays information about ABR summary routes for all OSPF areas.

ip-address: Specifies a summary route by its IP address.

mask-length: Specifies the mask length in the range of 0 to 32.

mask: Specifies the mask in dotted decimal notation.

verbose: Displays detailed ABR summary route information. If you do not specify this keyword, the command displays brief ABR summary route information.

Usage guidelines

If you do not specify an IP address, this command displays information about all summary routes on the ABR.

Examples

Display brief information about summary routes on the ABR.

```
<Sysname> display ospf abr-summary

          OSPF Process 1 with Router ID 2.2.2.2
                  ABR Summary Addresses

                        Area: 0.0.0.1
 Total summary addresses: 1
 Net             Mask            Status        Count      Cost
 100.0.0.0       255.0.0.0       Advertise     1          (Not Configured)
```

Table 3 Command output

Field	Description
Area	Area to which the summary routes belong.
Total summary addresses	Total number of summary routes.
Net	Address of the summary route.
Mask	Mask of the summary route address.
Status	Advertisement status of the summary route: **Advertise** or **Non-Advertise**.
Count	Number of summarized routes.
Cost	Cost of the summary route.

Display detailed information about summary routes on the ABR.

```
<Sysname> display ospf abr-summary verbose

          OSPF Process 1 with Router ID 2.2.2.2
                  ABR Summary Addresses

                        Area: 0.0.0.1
 Total summary addresses: 1

 Net         : 100.0.0.0
 Mask        : 255.0.0.0
```

```
Status      : Advertise
Cost        : (Not Configured)
Routes count: 1
  Destination            NetMask                Metric
  100.1.1.0              255.255.255.0          1000
```

Table 4 Command output

Field	Description
Destination	Destination address of a summarized route.
NetMask	Network mask of a summarized route.
Metric	Metric of a summarized route.

display ospf asbr-summary

Use **display ospf asbr-summary** to display ASBR summary route information.

Syntax

display ospf [*process-id*] **asbr-summary** [*ip-address* { *mask-length* | *mask* }]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays information about ASBR summary routes for all OSPF processes.

ip-address: Specifies an IP address in dotted decimal notation.

mask-length: Specifies the mask length in the range of 0 to 32.

mask: Specifies the mask in dotted decimal notation.

Usage guidelines

If you do not specify an IP address, this command displays information about all ASBR summary routes.

Examples

Display ASBR summary route information in OSPF process 1.

```
<Sysname> display ospf 1 asbr-summary

          OSPF Process 1 with Router ID 2.2.2.2
                  Summary Addresses
```

```
Total Summary Address Count: 1

                  Summary Address

 Net         : 30.1.0.0
 Mask        : 255.255.0.0
 Tag         : 20
 Status      : Advertise
 Cost        : 10 (Configured)
 The Count of Route is : 2

 Destination     Net Mask        Proto      Process   Type     Metric

 30.1.2.0        255.255.255.0   OSPF       2         2        1
 30.1.1.0        255.255.255.0   OSPF       2         2        1
```

Table 5 Command output

Field	Description
Total Summary Address Count	Total number of summary routes.
Net	Address of the summary route.
Mask	Mask of the summary route address.
Tag	Tag of the summary route.
Status	Advertisement status of the summary route.
Cost	Cost of the summary route.
The Count of Route is	Number of summarized routes.
Destination	Destination address of a summarized route.
Net Mask	Network mask of a summarized route.
Proto	Routing protocol from which the route was redistributed.
Process	Process ID of the routing protocol from which the route was redistributed.
Type	Type of a summarized route.
Metric	Metric of a summarized route.

display ospf event-log

Use **display ospf event-log** to display OSPF log information.

Syntax

display ospf [*process-id*] **event-log** { **lsa-flush** | **peer** [*neighbor-id*] [**slot** *slot-number*] | **spf** }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays OSPF log information for all processes.

lsa-flush: Specifies LSA aging log information.

peer: Specifies neighbor state change log information.

neighbor-id: Specifies a neighbor by its router ID. If you do not specify this argument, the command displays state change log information for all neighbors.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays neighbor state change information on the member device where the active process resides.

spf: Specifies route calculation log information.

Usage guidelines

Route calculation logs show the number of routes newly installed in the IP routing table.

Neighbor logs include information about the following events:

- The OSPF neighbor state goes down.
- The OSPF neighbor state goes backward because the local end receives BadLSReq, SeqNumberMismatch, and 1-Way events.

Examples

Display OSPF LSA aging log information for all processes.

```
<Sysname> display ospf event-log lsa-flush

          OSPF Process 1 with Router ID 1.1.1.1
                  LSA Flush Log

 Date: 2013-09-22 Time: 14:47:33 Received MaxAge LSA from 10.1.1.1
 Type: 1   LS ID: 2.2.2.2         AdvRtr: 2.2.2.2           Seq#: 80000001

 Date: 2013-09-22 Time: 14:47:33 Flushed MaxAge LSA by the self
 Type: 1   LS ID: 1.1.1.1         AdvRtr: 1.1.1.1           Seq#: 80000001

 Date: 2013-09-22 Time: 14:47:33 Received MaxAge LSA from 10.1.2.2
 Type: 1   LS ID: 2.2.2.2         AdvRtr: 2.2.2.2           Seq#: 80000001

 Date: 2013-09-22 Time: 14:47:33 Flushed MaxAge LSA by the self
 Type: 1   LS ID: 1.1.1.1         AdvRtr: 1.1.1.1           Seq#: 80000001
```

Table 6 Command output

Field	Description
Date/Time	Time when the device receives an LSA that has reached the maximum age.
Received MaxAge LSA from *X.X.X.X*	The device received an LSA that has reached the maximum age from *X.X.X.X*.

Flushed MaxAge LSA by the self	The device flushed the LSA that has reached the maximum age.
Type	LSA type.
LS ID	LSA link state ID.
AdvRtr	Advertising router.
Seq#	LSA sequence number.

Display OSPF route calculation log information for all processes.

```
<Sysname> display ospf event-log spf

          OSPF Process 1 with Router ID 1.1.1.2
                  SPF Log

Date       Time     Duration   Intra Inter External Reason
2012-06-27 15:28:26 0.95       1     1     10000    Intra-area LSA
2012-06-27 15:28:23 0.2        0     0     0        Area 0 full neighbor
2012-06-27 15:28:19 0          0     0     0        Intra-area LSA
2012-06-27 15:28:19 0          0     0     0        external LSA
2012-06-27 15:28:19 0.3        0     0     0        Intra-area LSA
2012-06-27 15:28:12 0          1     0     0        Intra-area LSA
2012-06-27 15:28:11 0          0     0     0        Routing policy
2012-06-27 15:28:11 0          0     0     0        Intra-area LSA
```

Table 7 Command output

Field	Description
Date/Time	Time when the route calculation starts.
Duration	Duration of the route calculation, in seconds.
Intra	Number of intra-area routes newly installed in the IP routing table.
Inter	Number of inter-area routes newly installed in the IP routing table.
External	Number of external routes newly installed in the IP routing table.
Reason	Reasons why the route calculation is performed: • **Intra-area LSA**—Intra-area LSA changes. • **Inter-area LSA**—Inter-area LSA changes. • **External LSA**—External LSA changes. • **Configuration**—Configuration changes. • **Area 0 full neighbor**—Number of **FULL**-state neighbors in Area 0 changes. • **Area 0 up interface**—Number of interfaces in up state in Area 0 changes. • **LSDB overflow state**—Overflow status changes. • **AS number**—AS number changes. • **ABR summarization**—ABR summarization changes. • **GR end**—GR ends. • **Routing policy**—Routing policy changes. • **Intra-area tunnel**—Intra-area tunnel changes. • **Others**—Other reasons.

Display OSPF neighbor log information for OSPF process 1.

```
<Sysname> display ospf 1 event-log peer

          OSPF Process 1 with Router ID 1.1.1.1
                  Neighbors Log

Date       Time     Local Address   Remote Address  Router ID       Reason
2012-12-31 12:35:45 197.168.1.1     197.168.1.2     2.2.2.2         IntPhyChange
2012-12-31 12:35:19 197.168.1.1     197.168.1.2     2.2.2.2         ConfNssaArea
2012-12-31 12:34:59 197.168.1.1     197.168.1.2     2.2.2.2         SilentInt
```

Table 8 Command output

Field	Description
Date/Time	Time when the neighbor state changes.
Local Address	Local address of the neighbor relationship.
Remote Address	Peer address of the neighbor relationship.
Router ID	Neighbor router ID.
Reason	Reasons for neighbor state changes: • **ResetConnect**—The connection is lost due to insufficient memory. • **IntChange**—The interface parameter has changed. • **VlinkChange**—The virtual link parameter has changed. • **ResetOspf**—The OSPF process is reset. • **UndoOspf**—The OSPF process is deleted. • **UndoArea**—The OSPF area is deleted. • **UndoNetwork**—The interface is disabled. • **SilentInt**—The interface is configured as a silent interface. • **IntLogChange**—The logical attribute of the interface has changed. • **IntPhyChange**—The physical attribute of the interface has changed. • **IntVliChange**—The virtual link attribute of the interface has changed. • **VlinkDown**—The virtual link goes down. • **DeadExpired**—The dead timer expires. • **ConfStubArea**—The interface is configured with stub area parameters. • **ConfNssaArea**—The interface is configured with NSSA area parameters. • **AuthChange**—The authentication type has changed. • **OpaqueChange**—The Opaque capability has changed. • **Retrans**—Excessive retransmissions. • **LLSChange**—The LLS capability has changed. • **OOBChange**—The OOB capability has changed. • **GRChange**—The GR capability has changed. • **BFDDown**—The interface is shut down by BFD. • **BadLSReq**—The interface receives BadLSReq events. • **SeqMismatch**—The interface receives SeqNumberMismatch events. • **1-Way**—The interface receives 1-Way events.

Related commands

reset ospf event-log

display ospf event-log hello

Use **display ospf event-log hello** to display OSPF log information about received or sent hello packets.

Syntax

display ospf [*process-id*] **event-log hello** { **received** [**abnormal** | **dropped**] | **sent** } [*neighbor-id*] [**slot** *slot-number*]

display ospf [*process-id*] **event-log hello sent** { **abnormal** | **failed** } [*neighbor-address*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays OSPF log information for all processes.

received: Specifies log information for received hello packets.

sent: Specifies log information for sent hello packets.

abnormal: Specifies log information for abnormal hello packets received or sent at intervals greater than or equal to 1.5 times the hello interval.

dropped: Specifies log information for received hello packets that were dropped.

failed: Specifies log information for hello packets that failed to be sent.

neighbor-address: Specifies a neighbor by its IP address. If you do not specify this argument, the command displays received or sent hello packet log information for all neighbors.

neighbor-id: Specifies a neighbor by its router ID. If you do not specify this argument, the command displays received or sent hello packet log information for all neighbors.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays received or sent hello packet log information on the member device where the active process resides.

Examples

Display log information for sent hello packets.

```
<Sysname> display ospf event-log hello sent

         OSPF Process 1 with Router ID 5.5.5.5
                 Hello Log

Interface: GE1/0/1
Neighbor address: 10.1.1.2, NbrID: 1.0.0.2
First 4 hello packets sent:
  2018-08-05 20:10:10:121, failed, errno: 132
```

```
  2018-08-05 20:10:30:121, succeeded
  2018-08-05 20:10:20:121, succeeded
  2018-08-05 20:10:40:121, succeeded
Last 4 hello packets sent before Full->Down at 2018-08-06 14:52:10:121
  2018-08-06 14:51:40:021, succeeded
  2018-08-06 14:51:50:021, succeeded
  2018-08-06 14:52:00:021, failed, errno: 132
  2018-08-06 14:52:10:010, failed, errno: 132

Interface: GE1/0/1
Neighbor address: 10.1.1.2, NbrID: 1.0.0.2
First 4 hello packets sent:
  2018-08-05 20:10:10:121, failed, errno: 132
  2018-08-05 20:10:30:121, succeeded
  2018-08-05 20:10:20:121, succeeded
  2018-08-05 20:10:40:121, succeeded
Last 4 hello packets sent before Full->Init at 2018-08-06 11:16:20:171
  2018-08-06 11:15:20:121, succeeded
  2018-08-06 11:15:30:121, succeeded
  2018-08-06 11:15:40:121, succeeded
  2018-08-06 11:15:50:121, succeeded
```

Table 9 Command output

Field	Description
Interface	Interface that sends the hello packets.
Neighbor address	IP address of the neighbor.
NbrID	Router ID of the neighbor.
First 4 hello packets sent	Time and result (**succeeded** or **failed**) for sending the first four hello packets. For a packet failed to be sent, an error code is displayed in the **errno** field.
Last 4 hello packets sent before Full->Down at 2018-01-06 14:52:10:121	Time and result (**succeeded** or **failed**) for sending the last four hello packets before neighbor state change. For a packet failed to be sent, an error code is displayed in the **errno** field.

Display log information for hello packets that failed to be sent.

```
<Sysname> display ospf event-log hello sent failed

         OSPF Process 1 with Router ID 5.5.5.5
                 Hello Log

Date: 2018-08-06 Time: 14:51:20:121 Interface: GE1/0/1
Destination address: 224.0.0.5, sent failed, errno: 132

Date: 2018-08-06 Time: 11:20:20:116 Interface: GE1/0/2
Destination address: 10.1.1.2, sent failed, errno: 132
```

Table 10 Command output

Field	Description
Date	Date for the hello packet sending failure, in the format of YYYY-MM-DD. YYYY represents the year, MM represents the month, and DD represents the day.
Time	Time for the hello packet sending failure, in the format of hh:mm:ss:xxx. hh represents the hours, mm represents the minutes, and ss represents the seconds, and xxx represents the milliseconds.
Interface	Interface that sends the hello packet.
Destination address	Destination IP address of the hello packet.
error	Error code for the hello packet sending failure.

Display log information for abnormal hello packets sent.

```
<Sysname> display ospf event-log hello sent abnormal

         OSPF Process 1 with Router ID 5.5.5.5
                 Hello Log

Date: 2018-08-06 Time: 11:21:12:121 Interface: GE1/0/2
Destination address: 224.0.0.5, last one sent: 2018-08-06 11:20:51:916

Date: 2018-08-06 Time: 11:56:21:312 Interface: GE1/0/2
Destination address: 10.1.1.2, last one sent: 2018-08-06 11:56:02:691
```

Table 11 Command output

Field	Description
Date	Date for sending the abnormal hello packet, in the format of YYYY-MM-DD. YYYY represents the year, MM represents the month, and DD represents the day.
Time	Time for sending the abnormal hello packet, in the format of hh:mm:ss:xxx. hh represents the hours, mm represents the minutes, and ss represents the seconds, and xxx represents the milliseconds.
Interface	Interface that sends the abnormal hello packet.
Destination address	Destination IP address of the abnormal hello packet.
last one sent	Time for sending the last hello packet before sending the abnormal hello packet.

Display log information for received hello packets.

```
<Sysname> display ospf event-log hello received

         OSPF Process 1 with Router ID 5.5.5.5
                 Hello Log

Interface: GE1/0/1
Neighbor address: 10.1.1.2, NbrID: 1.0.0.2
First 4 hello packets received:
  2018-08-05 20:11:10:121
```

```
  2018-08-05 20:11:30:121
  2018-08-05 20:11:20:121
  2018-08-05 20:11:40:121
Last 4 hello packets received before Exchange->Down at 2018-08-06 14:52:10:121
  2018-08-06 14:51:10:121
  2018-08-06 14:51:30:121
  2018-08-06 14:51:20:121
  2018-08-06 14:51:40:121

Interface: GE1/0/1
Neighbor address: 10.1.1.1, NbrID: 1.0.0.1
First 4 hello packets received:
  2018-08-06 19:11:15:121
  2018-08-06 19:11:35:121
  2018-08-06 19:11:25:121
  2018-08-06 19:11:45:121
Last 4 hello packets received before Full->Init at 2018-08-06 21:16:20:171
  2018-08-06 21:15:45:121
  2018-08-06 21:15:55:121
  2018-08-06 21:16:05:121
  2018-08-06 21:16:15:121
```

Table 12 Command output

Field	Description
Interface	Interface that receives the hello packets.
Neighbor address	IP address of the neighbor.
NbrID	Router ID of the neighbor.
First 4 hello packets received	Time for receiving the first four hello packets.
Last 4 hello packets received before Full->Init at 2018-01-06 21:16:20:171	Time for receiving the last four hello packets before neighbor state change, in the format of YYYY-MM-DD hh:mm:ss:xxx. YYYY represents the year, MM represents the month, and DD represents the day. hh represents the hours, mm represents the minutes, and ss represents the seconds, and xxx represents the milliseconds.

Display log information for received hello packets that were dropped.

```
<Sysname> display ospf event-log hello received dropped

         OSPF Process 1 with Router ID 5.5.5.5
                 Hello Log

Date: 2018-08-06 Time: 14:51:22:791 Interface: GE1/0/1
Source address: 10.1.1.1, NbrID: 1.0.0.1, area: 0.0.0.1
Drop reason: Hello-time mismatch

Date: 2018-08-06 Time: 14:51:20:121 Interface: GE1/0/1
Source address: 10.1.1.2, NbrID: 1.0.0.2, area: 0.0.0.1
Drop reason: NP-bit mismatch
```

Table 13 Command output

Field	Description
Date	Date for dropping the received hello packet, in the format of YYYY-MM-DD. YYYY represents the year, MM represents the month, and DD represents the day.
Time	Time for dropping the received hello packet, in the format of hh:mm:ss:xxx. hh represents the hours, mm represents the minutes, and ss represents the seconds, and xxx represents the milliseconds.
Interface	Interface that receives the hello packet.
Source address	Source IP address of the received hello packet.
NbrID	Router ID of the neighbor.
area	Area to which the neighbor interface belongs.
Drop reason	Reason for dropping the hello packet: • **Area under reset**—The area is in the reset progress. • **Router ID conflict**—Route ID conflict. • **Area mismatch**—Area ID mismatch. • **Unknown virtual link**—The hello packet is from an unknown virtual link. • **Authentication failure**—Authentication check failure. • **Peer address check failure**—Neighbor address check failure. • **Not DR or BDR**—The destination IP address of the hello packet is 224.0.0.6, but the interface is not a DR or BDR. • **Unknown unicast peer**—The hello packet is from an unknown unicast neighbor. • **Option mismatch**—Option mismatch. • **Subnet mask mismatch**—Subnet mask mismatch. • **Address mismatch**—Address range mismatch. • **Hello timer mismatch**—Hello timer mismatch. • **Dead timer mismatch**—Dead timer mismatch. • **Peer change**—The source IP address or router ID has changed.

Display log information for abnormal hello packets received.

```
<Sysname> display ospf event-log hello received abnormal

         OSPF Process 1 with Router ID 5.5.5.5
                 Hello Log

Date: 2018-08-06 Time: 10:12:22:121 Interface: GE1/0/1
Source address: 10.1.1.2, NbrID: 1.0.0.2, area: 0.0.0.1
Last one received: 2018-08-06 10:12:04:212

Date: 2018-08-06 Time: 14:51:20:121 Interface: GE1/0/1
Source address: 10.1.1.2, NbrID: 1.0.0.2, area: 0.0.0.1
Last one received: 2018-08-06 14:51:05:113
```

Table 14 Command output

Field	Description
Date	Date for receiving the abnormal hello packet, in the format of YYYY-MM-DD.

	YYYY represents the year, MM represents the month, and DD represents the day.
Time	Time for receiving the abnormal hello packet, in the format of hh:mm:ss:xxx. hh represents the hours, mm represents the minutes, and ss represents the seconds, and xxx represents the milliseconds.
Interface	Interface that receives the abnormal hello packet.
Source address	Source IP address of the received abnormal hello packet.
NbrID	Router ID of the neighbor.
area	Area to which the neighbor interface belongs.
last one sent	Time for receiving the last hello packet before receiving the abnormal hello packet.

Related commands

reset ospf event-log hello

display ospf fast-reroute lfa-candidate

Use **display ospf fast-reroute lfa-candidate** to display OSPF FRR backup next hop information.

Syntax

display ospf [*process-id*] [**area** *area-id*] **fast-reroute lfa-candidate**

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays FRR backup next hop information for all processes.

area *area-id*: Specifies an OSPF area by its ID. The area ID is an IP address or a decimal integer in the range of 0 to 4294967295 that is translated into the IP address format. If you do not specify this option, the command displays FRR backup next hop information for all OSPF areas.

Examples

Display OSPF FRR backup next hop information.

```
<Sysname> display ospf 1 area 0 fast-reroute lfa-candidate

          OSPF Process 1 with Router ID 2.2.2.2
                  LFA Candidate List

Area: 0.0.0.0
 Candidate nexthop count: 2
 NextHop          IntIP            Interface
```

```
10.0.1.1          10.0.1.2          GE1/0/2
10.0.11.1         10.0.11.2         GE1/0/3
```

Table 15 Command output

Field	Description
Area	Area to which the backup next hops belong.
Candidate nexthop count	Number of backup next hops.
NextHop	Backup next hop address.
IntIP	IP address of the output interface.
Interface	Output interface.

display ospf graceful-restart

Use **display ospf graceful-restart** to display GR information.

Syntax

display ospf [*process-id*] **graceful-restart** [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays GR information for all processes.

verbose: Displays detailed GR information. If you do not specify this keyword, the command displays brief GR information.

Examples

Display detailed GR information.

```
<Sysname> display ospf graceful-restart verbose

          OSPF Process 1 with Router ID 1.1.1.1
              Graceful Restart information

Graceful Restart capability     : Enable(IETF)
Graceful Restart support        : Planned and un-planned,Partial
Helper capability               : Enable(IETF)
Helper support                  : Planned and un-planned (IETF),Strict LSA check
Current GR state                : Normal
Graceful Restart period         : 40 seconds
Number of neighbors under Helper: 0
Number of restarting neighbors  : 0
```

```
Last exit reason:
  Restarter  : None
  Helper     : None

Area: 0.0.0.0
Authtype: None Area flag: Normal
Area up Interface count: 2

Interface: 40.4.0.1 (GigabitEthernet1/0/2)
Restarter state: Normal  State: P-2-P     Type: PTP
Last exit reason:
  Restarter  : None
  Helper     : None
Neighbor count of this interface: 1
Number of neighbors under Helper: 0
Neighbor        IP address      GR state     Last Helper exit reason
3.3.3.3         40.4.0.3        Normal       None

Virtual-link Neighbor-ID  -> 4.4.4.4, Neighbor-State: Full
Restarter state: Normal
Interface: 20.2.0.1 (Vlink)
Transit Area: 0.0.0.1
Last exit reason:
  Restarter  : None
  Helper     : None
Neighbor        IP address      GR state     Last Helper exit reason
4.4.4.4         20.2.0.4        Normal       Reset neighbor
```

Table 16 Command output

Field	Description
OSPF Process 1 with Router ID 1.1.1.1 Graceful Restart information	GR information for OSPF process 1 with router ID 1.1.1.1.
Graceful Restart capability	Whether GR is enabled: • **Enable(IETF)**—IETF GR is enabled. • **Enable(Nonstandard)**—Non-IETF GR is enabled. • **Disable**—GR is disabled.
Graceful Restart support	GR modes that the process supports (displayed only when GR is enabled): • **Planned and un-planned**—Supports both planned and unplanned GR. • **Planned only**—Supports only planned GR. • **Partial**—Supports partial GR. • **Global**—Supports global GR.

Field	Description
Helper capability	Helper capability that the process supports: • **Enable(IETF)**—Supports IETF GR helper capability. • **Enable(Nonstandard)**—Supports non-IETF GR helper capability. • **Enable(IETF and nonstandard)**—Supports both IETF GR helper capability and non-IETF GR helper capability. • **Disable**—Does not support GR helper capability.
Helper support	Policies that the helper supports (displayed only when GR helper is enabled): • **Strict lsa check**—The helper supports strict LSA checking. • **Planned and un-planned**—The helper supports planned and unplanned GR. • **Planned only**—The helper supports only planned GR.
Current GR state	GR state: • **Normal**—GR is not in progress or has completed. • **Under GR**—GR is in process. • **Under Helper**—The process is acting as GR helper.
Last exit reason	Last exit reason: • **Restarter**—Reason that the restarter exited most recently. • **Helper**—Reason that the helper exited most recently.
Area	Area ID in IP address format.
Authtype	Authentication type of the area: • **None**—No authentication. • **Simple**—Simple authentication. • **MD5**—MD5 authentication.
Area flag	Type of the area: • Normal. • Stub. • StubNoSummary (totally stub area). • NSSA. • NSSANoSummary (totally NSSA area).
Area up Interface count	Number of up interfaces in the area.
Interface	Interface in the area.
Restarter state	Restarter state on the interface.
State	Interface state.
Type	Interface network type.
Neighbor count of this interface	Neighbors of an interface.
Neighbor	Neighbor router ID.
IP address	Neighbor IP address.
GR state	Neighbor GR state: • **Normal**—GR is not in progress or has completed. • **Under GR**—GR is in process. • **Under Helper**—The process is acting as GR helper.

Field	Description
Last Helper exit reason	Reason that the helper exited most recently.
Virtual-link Neighbor-ID	Router ID of the virtual link's neighbor.
Neighbor-State	Neighbor state: Down, Init, 2-Way, ExStart, Exchange, Loading, and Full.
Interface	Output interface of the virtual link.

display ospf hostname-table

Use **display ospf hostname-table** to display the router ID-to-host name mapping table.

Syntax

display ospf [*process-id*] **hostname-table**

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify an OSPF process, this command displays the router ID-to-host name mapping tables for all OSPF processes.

Examples

Display the router ID-to-host name mapping tables for all OSPF processes.

```
<Sysname> display ospf hostname-table

        OSPF Process 1 with Router ID 192.168.56.21
               Hostname Table Information

                       Area: 0.0.0.1
Router ID           Hostname
192.168.56.21       RouterA
```

display ospf interface

Use **display ospf interface** to display OSPF interface information.

Syntax

display ospf [*process-id*] **interface** [*interface-type interface-number* | **verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies an OSPF process ID in the range of 1 to 65535. If you do not specify this argument, the command displays the OSPF interface information for all OSPF processes.

interface-type interface-number: Specifies an interface by its type and number.

verbose: Displays detailed OSPF information for all interfaces.

Usage guidelines

If you do not specify the *interface-type interface-number* argument or the **verbose** keyword, this command displays OSPF brief information for all interfaces.

Examples

Display all OSPF interface brief information.

```
<Sysname> display ospf interface

          OSPF Process 1 with Router ID 192.168.1.1
                  Interfaces

 Area: 0.0.0.0
 IP Address      Type         State    Cost  Pri   DR              BDR
 192.168.1.1     PTP          P-2-P    1562  1     0.0.0.0         0.0.0.0

 Area: 0.0.0.1
 IP Address      Type         State    Cost  Pri   DR              BDR
 172.16.0.1      Broadcast    DR       1     1     172.16.0.1      0.0.0.0
```

Table 17 Command output

Field	Description
Area	Area ID of the interface.
IP Address	Interface IP address (regardless of whether TE is enabled or not).
Type	Interface network type: PTP (P2P), PTMP (P2MP), Broadcast, or NBMA.
State	Interface state: • **Down**—No protocol traffic can be sent or received on the interface. • **Loopback**—The interface is in loopback state and it cannot forward traffic. • **Waiting**—The interface starts sending and receiving Hello packets. The router is trying to determine the identity of the (Backup) designated router for the network. • **P-2-P**—The interface will send Hello packets at the hello interval, and try to establish an adjacency with the neighbor. • **DR**—The router is the designated router on the network. • **BDR**—The router is the backup designated router on the network. • **DROther**—The router is a DR Other router on the attached network.
Cost	Interface cost.

Field	Description
Pri	Router priority.
DR	DR on the interface's network segment.
BDR	BDR on the interface's network segment.

Display detailed information about GigabitEthernet 1/0/1.

```
<Sysname> display ospf interface gigabitethernet 1/0/1


          OSPF Process 1 with Router ID 192.168.1.1
                  Interfaces

 Area: 0.0.0.0

 Interface: 172.16.0.1 (GigabitEthernet1/0/1)
 Cost: 1       State: DR        Type: Broadcast    MTU: 1500
 Priority: 1
 Designated router: 172.16.0.1
 Backup designated router: 0.0.0.0
 Timers: Hello 10, Dead 40, Poll  40, Retransmit 5, Transmit Delay 1
 FRR backup: Enabled
 Primary path detection mode: BFD ctrl
 Enabled by interface configuration (including secondary IP addresses)
 BFD: echo
 Cryptographic authentication: Enabled, inherited
    The last key is 1.
```

Table 18 Command output

Field	Description
Interface	Information about the interface, such as the IP address.
Timers	OSPF timers (in seconds): **Hello**, **Dead**, **Poll**, and **Retransmit**.
Transmit Delay	LSA transmission delay on the interface, in seconds.
FRR backup	Whether LFA calculation is enabled on an interface.
Primary path detection mode	Primary link detection mode: • **BFD ctrl**—BFD control packet mode. • **BFD echo**—BFD echo packet mode.
Enabled by interface configuration (including secondary IP addresses)	OSPF is enabled on the interface (including secondary IP addresses).
BFD	BFD session mode enabled on the interface: • **ctrl**—BFD control packet mode. • **echo**—BFD echo packet mode.
Keychain authentication: Enabled (*xx*), inherited	Keychain authentication is enabled. The name of the keychain is *xx*. If the interface uses the authentication mode of its area, this field displays **inherited** after the authentication mode.

Field	Description
Cryptographic authentication: Enabled, inherited	Authentication mode used by the interface. If the interface uses the authentication mode of its area, this field displays **inherited** after the authentication mode. Optional authentication modes include: • **Simple**—Simple authentication. • **Cryptographic**—Encrypted authentication. Options include MD5, HMAC-MD5, or HMAC-SHA-256.
The last key is *xx*	The most recent MD5/HMAC-MD5/HMAC-SHA-256 authentication key ID is *xx*.
The rollover is in progress, *xx* neighbor(s) left.	Key rollover for MD5/HMAC-MD5/HMAC-SHA-256 authentication is in progress. The number of neighbors that have not completed rollover is *xx*.
Nexthop	Next hop address. This field displays 0.0.0.0 for a P2P network.

display ospf interface hello

Use **display ospf interface hello** to display information about hello packets sent by OSPF interfaces.

Syntax

display ospf [*process-id*] **interface** [*interface-type interface-number*] **hello**

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies an OSPF process ID in the range of 1 to 65535. If you do not specify this argument, the command displays hello packet information for all OSPF processes.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify this argument, the command displays information about the hello packets sent by all OSPF interfaces.

Usage guidelines

This command displays information for only the hello packets sent in multicast.

Examples

Display information about hello packets sent by all OSPF interfaces.

```
<Sysname> display ospf interface hello


          OSPF Process 1 with Router ID 192.168.1.1
                  Interfaces

 Area: 0.0.0.0
```

```
Interface: 172.16.0.1 (GigabitEthernet1/0/1)
First 4 hello packets sent:
  2018-08-05 11:05:10:121, succeeded
  2018-08-05 11:05:20:121, succeeded
  2018-08-05 11:05:30:121, succeeded
  2018-08-05 11:05:40:121, succeeded
Last 4 hello packets sent:
  2018-08-06 11:15:10:121, succeeded
  2018-08-06 11:15:20:121, succeeded
  2018-08-06 11:15:30:121, succeeded
  2018-08-06 11:15:40:121, succeeded
```

Table 19 Command output

Field	Description
Area	Area to which the interface belongs.
Interface	IP address of the interface.
First 4 hello packets sent	Time and result (**succeeded** or **failed**) for sending the first four hello packets.
Last 4 hello packets sent	Time and result (**succeeded** or **failed**) for sending the last four hello packets when the command is executed.

display ospf lsdb

Use **display ospf lsdb** to display OSPF LSDB information.

Syntax

display ospf [*process-id*] **lsdb** [**brief** | **originate-router** *advertising-router-id* | **self-originate**] [**age** { **max-value** *max-age-value* | **min-value** *min-age-value* } *] [**resolve-hostname**]

display ospf [*process-id*] **lsdb hostname** *host-name* [**age** { **max-value** *max-age-value* | **min-value** *min-age-value* } *]

display ospf [*process-id*] **lsdb** { **ase** | **opaque-as** } [*link-state-id*] [**originate-router** *advertising-router-id* | **self-originate**] [**age** { **max-value** *max-age-value* | **min-value** *min-age-value* } *] [**resolve-hostname**]

display ospf [*process-id*] **lsdb** { **ase** | **opaque-as** } [*link-state-id*] **hostname** *host-name* [**age** { **max-value** *max-age-value* | **min-value** *min-age-value* } *] | **opaque-area**

display ospf [*process-id*] [**area** *area-id*] **lsdb** { **asbr** | **network** | **nssa** | **opaque-link** | **router** | **summary** } [*link-state-id*] [**originate-router** *advertising-router-id* | **self-originate**] [**age** { **max-value** *max-age-value* | **min-value** *min-age-value* } *] [**resolve-hostname**]

display ospf [*process-id*] [**area** *area-id*] **lsdb** { **asbr** | **network** | **nssa** | **opaque-link** | **router** | **summary** } [*link-state-id*] **hostname** *host-name* [**age** { **max-value** *max-age-value* | **min-value** *min-age-value* } *]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays LSDB information for all OSPF processes.

age: Displays LSAs whose ages are in the specified range. If you do not specify this keyword, the command displays all LSAs in the LSDB.

max-value *max-age-value*: Specifies the maximum age of LSAs, in the range of 0 to 3600 seconds. The default value is 3600.

min-value *min-age-value*: Specifies the minimum age of LSAs, in the range of 0 to 3600 seconds. The default value is 0. The *min-age-value* cannot be greater than the *max-age-value*.

area *area-id*: Specifies an OSPF area by its ID. The area ID is an IP address or a decimal integer in the range of 0 to 4294967295 that is translated into the IP address format. If you do not specify this option, the command displays LSDB information for all OSPF areas.

brief: Displays brief LSDB information.

asbr: Displays Type-4 LSA (ASBR Summary LSA) information in the LSDB.

ase: Displays Type-5 LSA (AS External LSA) information in the LSDB.

network: Displays Type-2 LSA (Network LSA) information in the LSDB.

nssa: Displays Type-7 LSA (NSSA External LSA) information in the LSDB.

opaque-as: Displays Type-11 LSA (Opaque-AS LSA) information in the LSDB.

opaque-link: Displays Type-9 LSA (Opaque-link LSA) information in the LSDB.

router: Displays Type-1 LSA (Router LSA) information in the LSDB.

summary: Displays Type-3 LSA (Network Summary LSA) information in the LSDB.

link-state-id: Specifies a link state ID in the IP address format.

originate-router *advertising-router-id*: Specifies an advertising router by its ID.

self-originate: Displays information about self-originated LSAs.

hostname *host-name*: Displays LSAs advertised by the router with the specified host name. If you do not specify this option, the command displays all LSAs in the OSPF LSDB.

resolve-hostname: Displays host names in OSPF LSDB information. If you do not specify this keyword, the OSPF LSDB information does not include host names.

Examples

Display OSPF LSDB information.

```
<Sysname> display ospf lsdb
         OSPF Process 1 with Router ID 192.168.0.1
                 Link State Database
```

```
                        Area: 0.0.0.0
 Type      LinkState ID    AdvRouter          Age  Len   Sequence   Metric
 Router    192.168.0.2     192.168.0.2        474  36    80000004   0
 Router    192.168.0.1     192.168.0.1        21   36    80000009   0
 Network   192.168.0.1     192.168.0.1        321  32    80000003   0
 Sum-Net   192.168.1.0     192.168.0.1        321  28    80000002   1
 Sum-Net   192.168.2.0     192.168.0.2        474  28    80000002   1
                        Area: 0.0.0.1
 Type      LinkState ID    AdvRouter          Age  Len   Sequence   Metric
 Router    192.168.0.1     192.168.0.1        21   36    80000005   0
 Sum-Net   192.168.2.0     192.168.0.1        321  28    80000002   2
 Sum-Net   192.168.0.0     192.168.0.1        321  28    80000002   1
                        Type 9 Opaque (Link-Local Scope) Database
 Flags: * -Vlink interface LSA
 Type      LinkState ID    AdvRouter          Age  Len   Sequence   Interfaces
*Opq-Link  3.0.0.0         7.2.2.1            8    14    80000001   10.1.1.2
*Opq-Link  3.0.0.0         7.2.2.2            8    14    80000001   20.1.1.2
```

Display OSPF LSDB information, including the host names of the advertising routers.

```
<Sysname> display ospf lsdb resolve-hostname

         OSPF Process 1 with Router ID 2.2.2.2
                 Link State Database

                        Area: 0.0.0.0
 Type      LinkState ID    AdvRouter       Age  Len   Sequence  Metric
 Router    1.1.1.1         1.1.1.1         1419 36    80000004  0
 Router    2.2.2.2         RouterB         1420 36    80000004  0
 Network   192.168.12.2    RouterB         1420 32    80000001  0
 Sum-Net   192.168.13.0    1.1.1.1         1456 28    80000001  1

                        Area: 0.0.0.1
 Type      LinkState ID    AdvRouter       Age  Len   Sequence  Metric
 Router    3.3.3.3         3.3.3.3         1416 36    80000003  0
 Router    1.1.1.1         1.1.1.1         1415 36    80000003  0
 Network   192.168.13.2    3.3.3.3         1416 32    80000001  0
 Sum-Net   192.168.12.0    1.1.1.1         1456 28    80000001  1

                 Type 10 Opaque (Area-Local Scope) Database
 Type      LinkState ID    AdvRouter       Age  Len   Sequence  Area
 Opq-Area  4.0.0.0         RouterB         470  32    80000001  0.0.0.0
```

Table 20 Command output

Field	Description
Area	LSDB information for the area.
Type	LSA type.
LinkState ID	Link state ID.
AdvRouter	Advertising router.

Field	Description
Age	Age of the LSA.
Len	Length of the LSA.
Sequence	Sequence number of the LSA.
Metric	Cost of the LSA.
*Opq-Link	Opaque LSA generated by a virtual link.

Display Type-2 LSA (Network LSA) information in the LSDB.

```
<Sysname> display ospf 1 lsdb network

          OSPF Process 1 with Router ID 192.168.1.1
                  Link State Database

                          Area: 0.0.0.0

    Type      : Network
    LS ID     : 192.168.0.2
    Adv Rtr   : 192.168.2.1
    LS age    : 922
    Len       : 32
    Options   :  E
    Seq#      : 80000003
    Checksum    : 0x8d1b
    Net Mask  : 255.255.255.0
       Attached Router    192.168.1.1
       Attached Router    192.168.2.1

                          Area: 0.0.0.1

    Type      : Network
    LS ID     : 192.168.1.2
    Adv Rtr   : 192.168.1.2
    LS age    : 782
    Len       : 32
    Options   :  NP
    Seq#      : 80000003
    Checksum    : 0x2a77
    Net Mask  : 255.255.255.0
       Attached Router    192.168.1.1
       Attached Router    192.168.1.2
```

Display Type-2 LSA (Network LSA) information in the LSDB, including the host names of the advertising routers.

```
<Sysname> display ospf 1 lsdb network resolve-hostname

         OSPF Process 1 with Router ID 2.2.2.2
                 Link State Database
```

```
                    Area: 0.0.0.0

  Type      : Network
  LS ID     : 192.168.12.2
  Adv Rtr   : 2.2.2.2
  Hostname  : RouterB
  LS age    : 1552
  Len       : 32
  Options   : O E
  Seq#      : 80000001
  Checksum  : 0xbdd0
  Net Mask  : 255.255.255.0
     Attached Router    1.1.1.1
     Attached Router    2.2.2.2

                    Area: 0.0.0.1

  Type      : Network
  LS ID     : 192.168.13.2
  Adv Rtr   : 3.3.3.3
  LS age    : 1548
  Len       : 32
  Options   : O E
  Seq#      : 80000001
  Checksum  : 0xc6be
  Net Mask  : 255.255.255.0
     Attached Router    1.1.1.1
     Attached Router    3.3.3.3
```

Table 21 Command output

Field	Description
Type	LSA type.
LS ID	DR IP address.
Adv Rtr	Router that advertised the LSA.
Hostname	Host name of the advertising router.
LS age	LSA age time.
Len	LSA length.
Options	LSA options: • **O**—Opaque LSA advertisement capability. • **E**—AS External LSA reception capability. • **EA**—External extended LSA reception capability. • **DC**—On-demand link support. • **N**—NSSA external LSA support. • **P**—Capability of an NSSA ABR to translate Type-7 LSAs into Type-5 LSAs.
Seq#	LSA sequence number.

Field	Description
Checksum	LSA checksum.
Net Mask	Network mask.
Attached Router	ID of the router that established adjacency with the DR, and ID of the DR itself.

Display Type-9 LSA information in the LSDB of OSPF process 1.

```
<Sysname> display ospf 1 lsdb opaque-link

         OSPF Process 1 with Router ID 1.1.1.1
                 Link State Database

                          Area: 0.0.0.0

    Type      : Opq-Link
    LS ID     : 3.0.0.0
    Adv Rtr   : 1.1.1.1
    LS age    : 2
    Len       : 44
    Options   : O E
    Seq#      : 80000001
    Checksum  : 0x31cf
      Opaque type: 3(Grace LSA)
      Opaque ID: 0
      IETF Graceful Restart Period: 120
      Restart Reason:    1 - software restart
      Neighbor Interface Address  : 192.168.12.1
```

display ospf nexthop

Use **display ospf nexthop** to display OSPF next hop information.

Syntax

display ospf [*process-id*] **nexthop**

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays next hop information for all OSPF processes.

Examples

Display OSPF next hop information.

```
<Sysname> display ospf nexthop

          OSPF Process 1 with Router ID 1.1.1.2
                  Neighbor Nexthop Information

 NbrID           Nexthop         Interface               RefCount   Status
 192.168.12.1    0.0.0.0         GE1/0/2                 4          Valid
 192.168.12.2    192.168.12.2    GE1/0/2                 3          Valid
 192.168.12.1    0.0.0.0         Loop100                 1          Valid
```

Table 22 Command output

Field	Description
NbrID	Neighbor router ID.
Nexthop	Next hop address.
Interface	Output interface.
RefCount	Reference count (routes that use the next hop).
Status	Next hop status: • **Valid**. • **Invalid**.

display ospf non-stop-routing status

Use **display ospf non-stop-routing status** to display OSPF NSR information.

Syntax

display ospf [*process-id*] **non-stop-routing status**

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays OSPF NSR information for all OSPF processes.

Examples

Display OSPF NSR information.

```
<Sysname> display ospf non-stop-routing status

                OSPF Process 1 with Router ID 192.168.33.12
                      Non Stop Routing information
```

```
Non Stop Routing capability : Enabled
Upgrade phase : Normal
```

Table 23 Command output

Field	Description
Non Stop Routing capability	NSR status: enabled or disabled.
Upgrade phase	Upgrade phase: • **Prepare**—Upgrade preparation phase. • **Restore Smooth**—Upgrade phase. • **Preroute**—Route pre-calculation phase. • **Calculating**—Route calculation phase. • **Redisting**—Route redistribution phase. • **Original and age**—LSA generation and aging phase. • **Normal**—Normal status.

display ospf peer

Use **`display ospf peer`** to display information about OSPF neighbors.

Syntax

`display ospf` [*`process-id`*] **`peer`** [**`hello`** | **`verbose`**] [*`interface-type interface-number`*] [[*`neighbor-id`*] [**`resolve-hostname`**] | **`hostname`** *`host-name`*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

`process-id`: Specifies an OSPF process by ID in the range of 1 to 65535. If you do not specify this argument, the command displays OSPF neighbor information for all OSPF processes.

`hello`: Displays information about the hello packets sent to and received from neighbor routers. In scenarios where hello packets are sent in multicast, the command displays information for only the hello packets received from neighbor routers.

`verbose`: Displays detailed neighbor information. If you do not specify this keyword, the command displays brief OSPF neighbor information.

`interface-type interface-number`: Specifies an interface by its type and number. If you do not specify this argument, the command displays neighbor information for all interfaces.

`neighbor-id`: Specifies a neighbor router ID. If you do not specify this argument, the command displays all neighbor information.

`resolve-hostname`: Resolves the host names of the neighbor routers. If you do not specify this keyword, the command cannot resolve the host names of the neighbor routers.

hostname *host-name*: Specifies a neighbor router by its host name, a case-sensitive string of 1 to 255 characters. If you do not specify this option, the command displays information for all neighbors.

Examples

Display detailed OSPF neighbor information.

```
<Sysname> display ospf peer verbose

          OSPF Process 1 with Router ID 1.1.1.1
                  Neighbors

 Area 0.0.0.0 interface 1.1.1.1(GigabitEthernet1/0/1)'s neighbors
 Router ID: 1.1.1.2          Address: 1.1.1.2          GR State: Normal
   State: Full  Mode: Nbr is master  Priority: 1
   DR: 1.1.1.2  BDR: 1.1.1.1  MTU: 0
   Options is 0x02 (-|-|-|-|-|-|E|-)
   Dead timer due in 33  sec
   Neighbor is up for 02:03:35
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 6
   BFD status: Disabled
 Last Neighbor Down Event:
 Router ID: 22.22.22.22
 Local Address: 11.11.11.11
 Remote Address: 22.22.22.22
 Time: Apr  9 03:18:19 2014
 Reason: Ospf_ifachange
```

Table 24 Command output

Field	Description
Area *areaID* interface *IPAddress*(*InterfaceName*)'s neighbors	Neighbor information for the interface in the specified area: • **areaID**—Area to which the neighbor belongs. • **IPAddress**—Interface IP address. • **InterfaceName**—Interface name.
Router ID	Neighbor router ID.
Address	Neighbor router address.
GR State	This field is not supported in the current software version. GR state: • Normal. • Restarter. • Complete. • Helper.
Hostname	Host name of the neighbor router.

Field	Description
State	Neighbor state: • **Down**—Initial state of a neighbor conversation. • **Init**—The router has received a Hello packet from the neighbor. However, the router has not established bidirectional communication with the neighbor. The router did not appear in the neighbor's hello packet. • **Attempt**—Available only in an NBMA network. In this state, the OSPF router has not received any information from a neighbor for a period. The router can send Hello packets at a longer interval to keep the neighbor relationship. • **2-Way**—Communication between the two routers is bidirectional. The local router appears in the neighbor's Hello packet. • **Exstart**—The goal of this state is to decide which router is the master, and to decide upon the initial Database Description (DD) sequence number. • **Exchange**—The router is sending DD packets to the neighbor, describing its entire link-state database. • **Loading**—The router sends LSRs packets to the neighbor, requesting more recent LSAs. • **Full**—The neighboring routers are fully adjacent.
Mode	Neighbor mode for LSDB synchronization.
Priority	Neighboring router priority.
DR	DR on the interface's network segment.
BDR	BDR on the interface's network segment.
MTU	Interface MTU.
Options	LSA options: • **O**—Opaque LSA advertisement capability. • **E**—AS External LSA reception capability. • **EA**—External extended LSA reception capability. • **DC**—On-demand link support. • **N**—NSSA external LSA support. • **P**—Capability of an NSSA ABR to translate Type-7 LSAs into Type-5 LSAs.
Dead timer due in 33 sec	This dead timer will expire in 33 seconds.
Neighbor is up for 02:03:35	The neighbor has been up for 02:03:35.
Authentication Sequence	Authentication sequence number.
Neighbor state change count	Count of neighbor state changes.
BFD status	This field is not supported in the current software version. BFD status: • Disabled. • Enabled (Control mode). • Enabled (Echo mode).
Last Neighbor Down Event	The most recent neighbor down event.
Time	Time when the neighbor went down.
Reason	Reason for the neighbor down event.

Display brief OSPF neighbor information.

```
<Sysname> display ospf peer

          OSPF Process 1 with Router ID 1.1.1.1
               Neighbor Brief Information

 Area: 0.0.0.0
 Router ID       Address         Pri Dead-Time  State             Interface
 1.1.1.2         1.1.1.2         1   40         Full/DR           GE1/0/1
```

Display brief OSPF neighbor information and resolve the host names of the neighbor routers.

```
<Sysname> display ospf peer resolve-hostname
         OSPF Process 1 with Router ID 1.1.1.1
               Neighbor Brief Information
 Area: 0.0.0.0
 Router ID       Address         Pri Dead-Time  State             Interface
 RouterA         1.1.1.2         1   34         Full/DR           GE1/0/1
```

Table 25 Command output

Field	Description
Area	Neighbor area.
Router ID	ID or host name of the neighbor router.
Address	Neighbor interface address.
Pri	Neighboring router priority.
Dead-Time	Dead interval remained.
Interface	Interface connected to the neighbor.
State	Neighbor state: Down, Init, Attempt, 2-Way, Exstart, Exchange, Loading, or Full.

Display information about the hello packets sent to and received from neighbor routers.

```
<Sysname> display ospf peer hello

          OSPF Process 1 with Router ID 1.1.1.1
                  Neighbors

 Area 0.0.0.0 interface 1.1.1.1(GigabitEthernet1/0/1)'s neighbors
 Router ID: 1.1.1.2          Address: 1.1.1.2
 First 4 hello packets received:
   2018-01-06 09:12:10:121
   2018-01-06 09:12:20:121
   2018-01-06 09:12:30:121
   2018-01-06 09:12:40:121
 Last 4 hello packets received:
   2018-01-06 11:15:10:121
   2018-01-06 11:15:20:121
   2018-01-06 11:15:30:121
   2018-01-06 11:15:40:121
 First 4 hello packets sent:
```

```
  2018-01-06 09:12:12:121, failed, errno:132
  2018-01-06 09:12:22:121, succeeded
  2018-01-06 09:12:32:121, succeeded
  2018-01-06 09:12:42:121, succeeded
Last 4 hello packets sent:
  2018-01-06 11:15:12:121, succeeded
  2018-01-06 11:15:22:121, succeeded
  2018-01-06 11:15:32:121, failed, errno:132
  2018-01-06 11:15:42:121, failed, errno:132
```

Table 26 Command output

Field	Description
Router ID	Router ID of the neighbor.
Address	IP address of the neighbor interface.
First 4 hello packets received	Time for receiving the first four hello packets from neighbors.
Last 4 hello packets received	Time for receiving the last four hello packets from neighbors.
First 4 hello packets sent	Time and result (**succeeded** or **failed**) for sending the first four hello packets to neighbors. For a packet failed to be sent, an error code is displayed in the **errno** field. This field is not displayed in scenarios where hello packets are sent in multicast.
Last 4 hello packets sent	Time and result (**succeeded** or **failed**) for sending the last four hello packets to neighbors when the command is executed. For a packet failed to be sent, an error code is displayed in the **errno** field. This field is not displayed in scenarios where hello packets are sent in multicast.

display ospf peer statistics

Use **display ospf peer statistics** to display OSPF neighbor statistics.

Syntax

display ospf [*process-id*] **peer statistics**

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays OSPF neighbor statistics for all OSPF processes.

Examples

Display OSPF neighbor statistics.

```
<Sysname> display ospf peer statistics
          OSPF Process 1 with Router ID 10.3.1.1
                    Neighbor Statistics
  Area ID         Down Attempt Init 2-Way ExStart Exchange Loading Full Total
  0.0.0.0         0    0       0    0     0       0        0       1    1
  0.0.0.2         0    0       0    0     0       0        0       1    1
  Total           0    0       0    0     0       0        0       2    2
```

Table 27 Command output

Field	Description
Area ID	The state statistics for all the routers in the area to which the router belongs is displayed.
Down	Number of neighboring routers in Down state in the same area.
Attempt	Number of neighboring routers in Attempt state in the same area.
Init	Number of neighboring routers in Init state in the same area.
2-Way	Number of neighboring routers in 2-Way state in the same area.
ExStart	Number of neighboring routers in ExStart state in the same area.
Exchange	Number of neighboring routers in Exchange state in the same area.
Loading	Number of neighboring routers in Loading state in the same area.
Full	Number of neighboring routers in Full state in the same area.
Total	Total number of neighbors in the same state: Down, Attempt, Init, 2-Way, ExStart, Exchange, Loading, or Full.

display ospf request-queue

Use **display ospf request-queue** to display OSPF request queue information.

Syntax

display ospf [*process-id*] **request-queue** [*interface-type interface-number*] [*neighbor-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays the OSPF request queue information for all OSPF processes.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify this argument, the command displays the OSPF request queue information for all interfaces.

neighbor-id: Specifies a neighbor's router ID. If you do not specify this argument, the command displays the OSPF request queue information for all OSPF neighbors.

Examples

Display OSPF request queue information.

```
<Sysname> display ospf request-queue

         OSPF Process 100 with Router ID 192.168.1.59
                 Link State Request List

  The Router's Neighbor is Router ID 2.2.2.2         Address 10.1.1.2
  Interface 10.1.1.1         Area 0.0.0.0
  Request list:
       Type       LinkState ID      AdvRouter         Sequence   Age
       Router     2.2.2.2           1.1.1.1           80000004   1
       Network    192.168.0.1       1.1.1.1           80000003   1
       Sum-Net    192.168.1.0       1.1.1.1           80000002   2
```

Table 28 Command output

Field	Description
The Router's Neighbor is Router ID	Neighbor router ID.
Address	Neighbor interface IP address.
Interface	Local interface IP address.
Area	Area ID.
Retransmit list	Request list information.
Type	LSA type.
LinkState ID	Link state ID.
AdvRouter	Advertising router.
Sequence	LSA sequence number.
Age	LSA age.

display ospf retrans-queue

Use **display ospf retrans-queue** to display retransmission queue information.

Syntax

display ospf [*process-id*] **retrans-queue** [*interface-type interface-number*] [*neighbor-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays retransmission queue information for all OSPF processes.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify this argument, the command displays retransmission queue information for all interfaces.

neighbor-id: Specifies a neighbor's router ID. If you do not specify this argument, the command displays retransmission queue information for all neighbors.

Examples

Display OSPF retransmission queue information.

```
<Sysname> display ospf retrans-queue

          OSPF Process 100 with Router ID 192.168.1.59
                  Link State Retransmission List

  The Router's Neighbor is Router ID 2.2.2.2         Address 10.1.1.2
  Interface 10.1.1.1         Area 0.0.0.0
  Retransmit list:
       Type       LinkState ID      AdvRouter         Sequence   Age
       Router     2.2.2.2           2.2.2.2           80000004   1
       Network    12.18.0.1         2.2.2.2           80000003   1
       Sum-Net    12.18.1.0         2.2.2.2           80000002   2
```

Table 29 Command output

Field	Description
The Router's Neighbor is Router ID	Neighbor router ID.
Address	Neighbor interface IP address.
Interface	Interface address of the router.
Area	Area ID.
Retrans List	Retransmission list.
Type	LSA type.
LinkState ID	Link state ID.
AdvRouter	Advertising router.
Sequence	LSA sequence number.
Age	LSA age.

display ospf routing

Use **display ospf routing** to display OSPF routing information.

Syntax

display ospf [*process-id*] **routing** [*ip-address* { *mask-length* | *mask* }] [**interface** *interface-type interface-number*] [**nexthop** *nexthop-address*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays the routing information for all OSPF processes.

ip-address: Specifies a destination IP address.

mask-length: Specifies mask length in the range of 0 to 32.

mask: Specifies the mask in dotted decimal notation.

interface *interface-type interface-number*: Displays routes passing the specified output interface. If you do not specify this option, the command displays OSPF routing information for all interfaces.

nexthop *nexthop-address*: Displays routes passing the specified next hop. If you do not specify this option, the command displays all OSPF routing information.

verbose: Displays detailed OSPF routing information. If you do not specify this keyword, the command displays brief OSPF routing information.

Examples

Display OSPF routing information.

```
<Sysname> display ospf routing

          OSPF Process 1 with Router ID 192.168.1.2
                   Routing Table

Routing for network
 Destination        Cost  Type       NextHop         AdvRouter     Area
 192.168.1.0/24     1562  Stub       192.168.1.2     192.168.1.2   0.0.0.0
 172.16.0.0/16      1563  Inter      192.168.1.1     192.168.1.1   0.0.0.0

 Total nets: 2
 Intra area: 1  Inter area: 1  ASE: 0  NSSA: 0
```

Table 30 Command output

Field	Description
Destination	Destination network.
Cost	Cost to destination.
Type	Route type: transit, stub, inter, Type-1, and Type-2.
NextHop	Next hop address.
AdvRouter	Advertising router.
Area	Area ID.

Field	Description
Total nets	Total networks.
Intra area	Total intra-area routes.
Inter area	Total inter-area routes.
ASE	Total ASE routes.
NSSA	Total NSSA routes.

Display detailed OSPF routing information.

```
<Sysname> display ospf routing verbose

          OSPF Process 2 with Router ID 192.168.1.112
                   Routing Table

Routing for network

 Destination: 192.168.1.0/24
    Priority: Low                    Type: Stub
   AdvRouter: 192.168.1.2            Area: 0.0.0.0
  SubProtoID: 0x1               Preference: 10
     NextHop: 192.168.1.2        BkNextHop: N/A
      IfType: Broadcast           BkIfType: N/A
   Interface: GE1/0/2          BkInterface: N/A
       NibID: 0x1300000c            Status: Normal
        Cost: 1562
     InLabel: 4294967295       Tunnel type: -
    OutLabel: 4294967295     OutLabel flag: -
  BkOutLabel: 4294967295   BkOutLabel flag: -

 Destination: 172.16.0.0/16
    Priority: Low                    Type: Inter
   AdvRouter: 192.168.1.1            Area: 0.0.0.0
  SubProtoID: 0x1               Preference: 10
     NextHop: 192.168.1.1        BkNextHop: N/A
      IfType: Broadcast           BkIfType: N/A
   Interface: GE1/0/3          BkInterface: N/A
       NibID: 0x1300000c            Status: Normal
        Cost: 1563
     InLabel: 4294967295       Tunnel type: -
    OutLabel: 4294967295     OutLabel flag: -
  BkOutLabel: 4294967295   BkOutLabel flag: -
 Destination: 91.1.0.0/16
    Priority: Low                    Type: Type2
   AdvRouter: 2.2.2.2                 Tag: 0
  SubProtoID: 0x8               Preference: 150
     NextHop: 21.41.0.2          BkNextHop: N/A
      IfType: PTP                 BkIfType: N/A
   Interface: GE1/0/4          BkInterface: N/A
```

```
      NibID: 0x13000003            Status: Normal
       Cost: 1                ECMP group: 0x1300001a
    InLabel: 4294967295       Tunnel type: -
   OutLabel: 4294967295     OutLabel flag: -
 BkOutLabel: 4294967295   BkOutLabel flag: -

Destination: 91.1.0.0/16
   Priority: Low                    Type: Type2
  AdvRouter: 3.3.3.3                 Tag: 0
 SubProtoID: 0x8               Preference: 150
    NextHop: 31.41.0.3          BkNextHop: N/A
     IfType: PTP                 BkIfType: N/A
  Interface: GE1/0/3          BkInterface: N/A
      NibID: 0x13000005            Status: Normal
       Cost: 1                ECMP group: 0x1300001a
    InLabel: 4294967295       Tunnel type: -
   OutLabel: 4294967295     OutLabel flag: -
 BkOutLabel: 4294967295   BkOutLabel flag: -

Total nets: 4
Intra area: 2  Inter area: 0  ASE: 2  NSSA: 0
```

Table 31 Command output

Field	Description
Priority	Prefix priority: critical, high, medium, and low.
Type	Route type: Transit, Stub, Inter, Type1, or Type2.
AdvRouter	Advertising router.
Area	Area ID.
SubProtoID	Sub protocol ID.
Preference	OSPF route preference.
NextHop	Primary next hop IP address.
BkNextHop	Backup next hop IP address.
IfType	Type of the network to which the primary next hop belongs.
BkIfType	Type of the network to which the backup next hop belongs.
Interface	Output interface.
BkInterface	Backup output interface.
NibID	Next hop ID.

Field	Description
Status	Route status: • **Local**—The route is on the local end and is not sent to the route management module. • **Invalid**—The next hop is invalid. • **Stale**—The next hop is stale. • **Normal**—The route is available. • **Delete**—The route is deleted. • **Host-Adv**—The route is a host route. • **Rely**—The route is a recursive route.
Cost	Cost to destination.
ECMP group	ECMP route group ID. This field is displayed only when ECMP route groups exist.
InLabel	This field is not supported in the current software version. Incoming label. A value of 4294967295 indicates that the incoming label is invalid.
Tunnel type	This field is not supported in the current software version. Tunnel type. Only **SR** (which means SR tunnel) is supported in the current software version.
OutLabel	This field is not supported in the current software version. Outgoing label. A value of 4294967295 indicates that the outgoing label is invalid.
OutLabel flag	This field is not supported in the current software version. Outgoing label flag: • **E**—Explicit null flag. The upstream neighbor must replace the SID with an explicit null flag before forwarding the packets. • **I**—Implicit null flag. The upstream neighbor must replace the SID with an implicit null flag before forwarding the packets. This flag is not supported in the current software version. • **N**—Normal flag. • **P**—SR label preferred flag.
BkOutLabel	This field is not supported in the current software version. Backup outgoing label. A value of 4294967295 indicates that the backup outgoing label is invalid.
BkOutLabel flag	This field is not supported in the current software version. Backup outgoing label flag: • **E**—Explicit null flag. The upstream neighbor must replace the SID with an explicit null flag before forwarding the packets. • **I**—Implicit null flag. The upstream neighbor must replace the SID with an implicit null flag before forwarding the packets. • **N**—Normal flag. • **P**—SR label preferred flag.

display ospf spf-tree

Use **display ospf spf-tree** to display SPF tree information.

Syntax

display ospf [*process-id*] [**area** *area-id*] **spf-tree** [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify a process, this command displays SPF tree information for all OSPF processes.

area *area-id*: Specifies an OSPF area by its ID. The area ID is an IP address or a decimal integer in the range of 0 to 4294967295 that is translated into the IP address format. If you do not specify an area, this command displays SPF tree information for all OSPF areas.

verbose: Displays detailed SPF tree information. If you do not specify this keyword, the command displays brief SPF tree information.

Examples

Display brief SPF tree information for Area 0 in OSPF process 1.

```
<Sysname> display ospf 1 area 0 spf-tree

          OSPF Process 1 with Router ID 100.0.0.4

        Flags: S-Node is on SPF tree       R-Node is directly reachable
               I-Node or Link is init      D-Node or Link is to be deleted
               P-Neighbor is parent        A-Node is in candidate list
               C-Neighbor is child         T-Node is tunnel destination
               H-Nexthop changed           N-Link is a new path
               V-Link is involved          G-Link is in change list

                  Area: 0.0.0.0  Shortest Path Tree

 SpfNode         Type    Flag      SpfLink         Type   Cost  Flag
>192.168.119.130 Network S R
                                 -->114.114.114.111 NET2RT 0     C
                                 -->100.0.0.4       NET2RT 0     P
>114.114.114.111 Router  S
                                 -->192.168.119.130 RT2NET 65535 P
>100.0.0.4       Router  S
                                 -->192.168.119.130 RT2NET 10    C
```

Table 32 Command output

Field	Description
SpfNode	SPF node, represented by a router ID when the node type is **Router**, or the IP address of the DR when the node type is **Network**. Node flag: • **I**—The node is in initialization state. • **A**—The node is on the candidate list. • **S**—The node is on the SPF tree. • **R**—The node is directly connected to the root node. • **D**—The node is to be deleted. • **T**—The node is the tunnel destination.
SpfLink	SPF link, representing the peer node. Link type: • **RT2RT**—Router to router. • **NET2RT**—Network to router. • **RT2NET**—Router to network. Link flag: • **I**—The link is in initialization state. • **P**—The peer is the parent node. • **C**—The peer is the child node. • **D**—The link is to be deleted. • **H**—The next hop is changed. • **V**—When the peer node is deleted or added, the peer node is not on the SPF tree or is deleted. • **N**—The link is newly added, and both end nodes are on the SPF tree. • **G**—The link is on the area change list.

Display detailed SPF tree information for Area 0 in OSPF process 1.

```
<Sysname> display ospf 1 area 0 spf-tree verbose

          OSPF Process 1 with Router ID 100.0.0.4

        Flags: S-Node is on SPF tree       R-Node is directly reachable
               I-Node or Link is init      D-Node or Link is to be deleted
               P-Neighbor is parent        A-Node is in candidate list
               C-Neighbor is child         T-Node is tunnel destination
               H-Nexthop changed           N-Link is a new path
               V-Link is involved          G-Link is in change list

                  Area: 0.0.0.0  Shortest Path Tree

>LsId(192.168.119.130)
 AdvId    : 100.0.0.4       NodeType     : Network
 Mask     : 255.255.255.0   SPFLinkCnt   : 2
 Distance : 10
 VlinkData: 0.0.0.0         ParentLinkCnt: 1          NodeFlag: S R
 NextHop  : 1
```

```
  192.168.119.130    Interface: GE1/0/2           Flag: -
BkNextHop: 1
  0.0.0.0            Interface: GE1/0/2           Flag: -
-->LinkId(114.114.114.111)
   AdvId   : 100.0.0.4       LinkType   : NET2RT
   LsId    : 192.168.119.130 LinkCost   : 0           NextHopCnt: 1
   LinkData: 0.0.0.0         LinkNewCost: 0           LinkFlag  : C
-->LinkId(100.0.0.4)
   AdvId   : 100.0.0.4       LinkType   : NET2RT
   LsId    : 192.168.119.130 LinkCost   : 0           NextHopCnt: 1
   LinkData: 0.0.0.0         LinkNewCost: 0           LinkFlag  : P
```

Table 33 Command output

Field	Description
LsId	Link state ID.
AdvId	ID of the advertising router.
NodeType	Node type: • **Network**—Network node. • **Router**—Router node.
Mask	Network mask. Its value is 0 for a router node.
SPFLinkCnt	Number of SPF links.
Distance	Cost to the root node.
VlinkData	Destination address of virtual link packets.
ParentLinkCnt	Number of parent links.
NodeFlag	Node flag: • **I**—The node is in initialization state. • **A**—The node is on the candidate list. • **S**—The node is on the SPF tree. • **R**—The node is directly connected to the root node. • **D**—The node is to be deleted. • **T**—The node is the tunnel destination.
NextHop	Next hop.
Interface	Output interface.
Flag	This field is not supported in the current software version. Identifies the type of the next hop. **SR** means SR tunnel. For other types, this field displays a hyphen (**-**).
Protect	Traffic protection type: **Link** or **Node**.
BkNextHop	Backup next hop.
LinkId	Link ID.
LinkType	Link type: • **RT2RT**—Router to router. • **NET2RT**—Network to router. • **RT2NET**—Router to network.
LinkCost	Link cost.

Field	Description
NextHopCnt	Number of next hops.
LinkData	Link data.
LinkNewCost	New link cost.
LinkFlag	Link flag: • **I**—The link is in initialization state. • **P**—The peer is the parent node. • **C**—The peer is the child node. • **D**—The link is to be deleted. • **H**—The next hop is changed. • **V**—When the peer node is deleted or added, the peer node is not on the SPF tree or is deleted. • **N**—The link is newly added, and both end nodes are on the SPF tree. • **G**—The link is on the area change list.

display ospf statistics

Use **display ospf statistics** to display OSPF statistics.

Syntax

display ospf [*process-id*] **statistics** [**error** | **packet** [**hello** | *interface-type interface-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays OSPF statistics for all OSPF processes.

error: Displays error statistics. If you do not specify this keyword, the command displays OSPF packet, LSA, and route statistics.

packet: Displays OSPF packet statistics.

hello: Displays statistics of the sent and received hello packets. If you do not specify this keyword, the command displays statistics of all types of sent and received packets.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify this argument, the command displays statistics for all interfaces.

Examples

Display OSPF statistics.

```
<Sysname> display ospf statistics
```

```
         OSPF Process 1 with Router ID 2.2.2.2
                 Statistics

I/O statistics
 Type                    Input     Output
 Hello                   61        122
 DB Description          2          3
 Link-State Req          1          1
 Link-State Update       3          3
 Link-State Ack          3          2

LSAs originated by this router
 Router  : 4
 Network : 0
 Sum-Net : 0
 Sum-Asbr: 0
 External: 0
 NSSA    : 0
 Opq-Link: 0
 Opq-Area: 0
 Opq-As  : 0

LSAs originated: 4  LSAs received: 7

Routing table:
  Intra area: 2  Inter area: 3  ASE/NSSA: 0
```

Table 34 Command output

Field	Description
I/O statistics	Statistics about input/output packets and LSAs.
Type	OSPF packet type.
Input	Packets received.
Output	Packets sent.
Hello	Hell packet.
DB Description	Database Description packet.
Link-State Req	Link-State Request packet.
Link-State Update	Link-State Update packet.
Link-State Ack	Link-State Acknowledge packet.
LSAs originated by this router	LSAs originated by this router.
Router	Number of Type-1 LSAs originated.
Network	Number of Type-2 LSAs originated.
Sum-Net	Number of Type-3 LSAs originated.
Sum-Asbr	Number of Type-4 LSAs originated.
External	Number of Type-5 LSAs originated.

Field	Description
NSSA	Number of Type-7 LSAs originated.
Opq-Link	Number of Type-9 LSAs originated.
Opq-As	Number of Type-11 LSAs originated.
LSA originated	Number of LSAs originated.
LSA received	Number of LSAs received.
Routing table	Routing table information.
Intra area	Number of intra-area routes.
Inter area	Number of inter-area routes.
ASE/NSSA	Number of ASE/NSSA routes.

Display OSPF error statistics.

```
<Sysname> display ospf statistics error

          OSPF Process 1 with Router ID 192.168.1.112
                  OSPF Packet Error Statistics

 0          : Router ID confusion        0          : Bad packet
 0          : Bad version                0          : Bad checksum
 0          : Bad area ID                0          : Drop on unnumbered link
 0          : Bad virtual link           0          : Bad authentication type
 0          : Bad authentication key     0          : Packet too small
 0          : Neighbor state low         0          : Transmit error
 0          : Interface down             0          : Unknown neighbor
 0          : HELLO: Netmask mismatch    0          : HELLO: Hello-time mismatch
 0          : HELLO: Dead-time mismatch  0          : HELLO: Ebit option mismatch
 0          : DD: MTU option mismatch    0          : DD: Unknown LSA type
 0          : DD: Ebit option mismatch   0          : ACK: Bad ack
 0          : ACK: Unknown LSA type      0          : REQ: Empty request
 0          : REQ: Bad request           0          : UPD: LSA checksum bad
 0          : UPD: Unknown LSA type      0          : UPD: Less recent LSA
```

Table 35 Command output

Field	Description
Router ID confusion	Packets with duplicate router ID.
Bad packet	Packets illegal.
Bad version	Packets with wrong version.
Bad checksum	Packets with wrong checksum.
Bad area ID	Packets with invalid area ID.
Drop on unnumbered link	Packets dropped on the unnumbered interface.
Bad virtual link	Packets on wrong virtual links.
Bad authentication type	Packets with invalid authentication type.
Bad authentication key	Packets with invalid authentication key.

Field	Description
Packet too small	Packets too small in length.
Neighbor state low	Packets received in low neighbor state.
Transmit error	Packets with error when being transmitted.
Interface down	Shutdown times of the interface.
Unknown neighbor	Packets received from unknown neighbors.
HELLO: Netmask mismatch	Hello packets with mismatched mask.
HELLO: Hello-time mismatch	Hello packets with mismatched hello timer.
HELLO: Dead-time mismatch	Hello packets with mismatched dead timer.
HELLO: Ebit option mismatch	Hello packets with mismatched E-bit in the option field.
DD: MTU option mismatch	DD packets with mismatched MTU.
DD: Unknown LSA type	DD packets with unknown LSA type.
DD: Ebit option mismatch	DD packets with mismatched E-bit in the option field.
ACK: Bad ack	Bad LSAck packets for LSU packets.
ACK: Unknown LSA type	LSAck packets with unknown LSA type.
REQ: Empty request	LSR packets with no request information.
REQ: Bad request	Bad LSR packets.
UPD: LSA checksum bad	LSU packets with wrong LSA checksum.
UPD: Unknown LSA type	LSU packets with unknown LSA type.
UPD: Less recent LSA	LSU packets without the most recent LSA.

Display OSPF packet statistics for all processes and interfaces.

```
<Sysname> display ospf statistics packet

          OSPF Process 100 with Router ID 192.168.1.59
                  Packet Statistics

 Waiting to send packet count: 0
         Hello      DD         LSR        LSU        ACK        Total
 Input : 489        6          2          44         40         581
 Output: 492        8          2          45         40         587

 Area: 0.0.0.1
 Interface: 20.1.1.1 (GigabitEthernet1/0/1)
         DD         LSR        LSU        ACK        Total
 Input : 0          0          0          0          0
 Output: 0          0          0          0          0

 Interface: 100.1.1.1 (GigabitEthernet1/0/2)
         DD         LSR        LSU        ACK        Total
 Input : 3          1          22         16         42
 Output: 2          1          19         20         42
```

Table 36 Command output

Field	Description
Waiting to send packet count	Number of packets waiting to be sent.
Total	Total number of packets.
Input	Number of received packets.
Output	Number of sent packets.
Area	Area ID.
Interface	Interface address and interface name.

Display statistics of the sent and received hello packets.

```
<Sysname> display ospf statistics packet hello

          OSPF Process 1 with Router ID 1.1.1.1
                  Hello statistics
   Total sent                            : 201
   Total sent failed                     : 0
   Sent after one and a half intervals   : 0
   Total received                        : 221
   Total received dropped                : 0
   Received after one and a half intervals: 0
```

Table 37 Command output

Field	Description
Total sent	Total number of hello packets sent.
Total sent failed	Total number of hello packets that failed to be sent.
Sent after one and a half intervals	Total number of hello packets sent at intervals greater than 1.5 times the hello interval.
Total received	Total number of hello packets received.
Total received dropped	Total number of received hello packets that were dropped.
Received after one and a half intervals	Total number of hello packets received at intervals greater than 1.5 times the hello interval.

Related commands

`reset ospf statistics`

display ospf vlink

Use **`display ospf vlink`** to display OSPF virtual link information.

Syntax

`display ospf` [*`process-id`*] **`vlink`**

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays the OSPF virtual link information for all OSPF processes.

Examples

Display OSPF virtual link information.

```
<Sysname> display ospf vlink
          OSPF Process 1 with Router ID 3.3.3.3
                  Virtual Links

 Virtual-link Neighbor-ID  -> 2.2.2.2, Neighbor-State: Full
 Interface: 10.1.2.1 (GigabitEthernet1/0/1)
 Cost: 1562  State: P-2-P  Type: Virtual
 Transit Area: 0.0.0.1
 Timers: Hello 10 , Dead 40 , Retransmit 5 , Transmit Delay 1
 Cryptographic authentication: Enabled
    The last key is 1.
```

Table 38 Command output

Field	Description
Virtual-link Neighbor-ID	ID of the neighbor on the virtual link.
Neighbor-State	Neighbor state: Down, Init, 2-Way, ExStart, Exchange, Loading, Full.
Interface	IP address and name of the local interface on the virtual link.
Cost	Interface route cost.
State	Interface state.
Type	Virtual link.
Transit Area	Transit area ID.
Timers	Values of timers (in seconds): **Hello**, **Dead**, and **Retransmit**.
Transmit Delay	LSA transmission delay on the interface, in seconds.
Keychain authentication: Enabled (*xx*), inherited	Keychain authentication is enabled. **xx** represents the name of the keychain. If the virtual link uses the authentication mode of the backbone area, this field displays **inherited** after the authentication mode.
Cryptographic authentication: Enabled, inherited	Authentication mode used by the virtual link. If the virtual link uses the authentication mode of the backbone area, this field displays **inherited** after the authentication mode. Optional authentication modes include: • **Simple**—Simple authentication. • **Cryptographic**—Encrypted authentication. Options include MD5, HMAC-MD5, or HMAC-SHA-256.
The last key is *xx*	The most recent MD5/HMAC-MD5/HMAC-SHA-256 authentication key ID is *xx*.

Field	Description
The rollover is in progress, *xx* neighbor(s) left	Key rollover for MD5/HMAC-MD5/HMAC-SHA-256 authentication is in progress. The number of neighbors that have not completed rollover is *xx*.

display router id

Use **display router id** to display the global router ID.

Syntax

display router id

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display the global router ID.

```
<Sysname> display router id
         Configured router ID is 1.1.1.1
```

distribute bgp-ls

Use **distribute bgp-ls** to enable the device to advertise OSPF link state information to BGP.

Use **undo distribute bgp-ls** to restore the default.

Syntax

distribute bgp-ls [**instance-id** *id*] [**strict-link-checking**]

undo distribute bgp-ls

Default

The device does not advertise OSPF link state information to BGP.

Views

OSPF view

Predefined user roles

network-admin

context-admin

Parameters

instance-id *id*: Specifies an instance by its ID in the range of 0 to 65535. If you do not specify an instance, this command advertises OSPF link state information of instance 0 to BGP.

strict-link-checking: Enables strict checking on link state information advertised to BGP. If you specify this keyword, the local and remote ends of a link must be in the same subnet so that the

link state information can be advertised to BGP. If you do not specify this keyword, the link state information is advertised to BGP even if the local and remote ends of the link are in different subnets. This keyword applies only to P2P links.

Usage guidelines

After the device advertises OSPF link state information to BGP, BGP can advertise the information for intended applications.

If multiple OSPF processes have the same link state information and instance ID, only the link state information of the OSPF process with the smallest process ID is advertised.

To advertise the same link state information of different OSPF processes to BGP, specify a different instance ID for each OSPF process.

As a best practice, enable strict link state information checking when the following conditions exist:

- The link state information advertised to BGP contains multiple equal-cost links.
- The local and remote ends of each equal-cost link are in the same subnet.

This prevents the device from advertising error link state information to BGP when the equal-cost links flap.

Strict link state information checking and prefix suppression are mutually exclusive. Before you enable strict link state information checking, make sure prefix suppression is disabled.

Examples

Enable the device to advertise link state information for OSPF process 1 to BGP.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] distribute bgp-ls
```

dscp

Use **dscp** to set the DSCP value for outgoing OSPF packets.

Use **undo dscp** to restore the default.

Syntax

dscp *dscp-value*

undo dscp

Default

The DSCP value for outgoing OSPF packets is 48.

Views

OSPF view

Predefined user roles

network-admin

context-admin

Parameters

dscp-value: Specifies the DSCP value in the range of 0 to 63 for outgoing OSPF packets.

Examples

Set the DSCP value for outgoing OSPF packets to 63 in OSPF process 1.

```
<Sysname> system-view
[Sysname] ospf 1
```

```
[Sysname-ospf-1] dscp 63
```

ecmp-group enable

Use **ecmp-group enable** to enable OSPF to group ECMP routes.

Use **undo ecmp-group enable** to restore the default.

Syntax

ecmp-group enable

undo ecmp-group enable

Default

OSPF does not group ECMP routes.

Views

OSPF view

Predefined user roles

network-admin

context-admin

Usage guidelines

Configure this command to enable OSPF to group ECMP routes by prefix to speed up route convergence.

This command is applicable to a network when the network has a large number of ECMP routes and different route prefixes in the network have the same next hops. For example, OSPF learns 10000 route prefixes and all route prefixes have the same 16 next hops (1.1.1.1 to 1.1.1.16). If you do not configure this command, OSPF has to send all ECMP routes of every route prefix (10000 × 16 routes) to the route management module. After you configure this command, OSPF groups the ECMP routes by prefix and sends the route groups (10000 route groups) to the route management module.

If the output interfaces to the next hops of ECMP routes are TE tunnel interfaces, OSPF groups the ECMP routes regardless of whether you enable this feature or not.

Examples

Enable OSPF process 1 to group ECMP routes.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] ecmp-group enable
```

enable link-local-signaling

Use **enable link-local-signaling** to enable the OSPF link-local signaling (LLS) capability.

Use **undo enable link-local-signaling** to disable the OSPF LLS capability.

Syntax

enable link-local-signaling

undo enable link-local-signaling

Default

OSPF link-local signaling capability is disabled.

Views

OSPF view

Predefined user roles

network-admin

context-admin

Examples

Enable link-local signaling for OSPF process 1.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] enable link-local-signaling
```

enable out-of-band-resynchronization

Use **enable out-of-band-resynchronization** to enable the OSPF out-of-band resynchronization (OOB-Resynch) capability.

Use **undo enable out-of-band-resynchronization** to disable the OSPF out-of-band resynchronization capability.

Syntax

enable out-of-band-resynchronization

undo enable out-of-band-resynchronization

Default

The OSPF out-of-band resynchronization capability is disabled.

Views

OSPF view

Predefined user roles

network-admin

context-admin

Usage guidelines

Before you configure this command, enable the link-local signaling capability.

Examples

Enable the out-of-band resynchronization capability for OSPF process 1.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] enable link-local-signaling
[Sysname-ospf-1] enable out-of-band-resynchronization
```

Related commands

enable link-local-signaling

event-log

Use **event-log** to set the number of OSPF logs.

Use **undo event-log** to remove the configuration.

Syntax

event-log { **hello** { **received** [**abnormal** | **dropped**] | **sent** [**abnormal** | **failed**] } | **lsa-flush** | **peer** | **spf** } **size** *count*

undo event-log { **hello** { **received** [**abnormal** | **dropped**] | **sent** [**abnormal** | **failed**] } | **lsa-flush** | **peer** | **spf** } **size**

Default

The device can generate a maximum of 100 logs for each type.

Views

OSPF view

Predefined user roles

network-admin

context-admin

Parameters

hello: Specifies the number of logs for received or sent hello packets.

received: Specifies the number of logs for received hello packets.

sent: Specifies the number of logs for sent hello packets.

abnormal: Specifies the number of logs for abnormal hello packets received or sent at intervals greater than or equal to 1.5 times the hello interval.

dropped: Specifies the number of logs for received hello packets that were dropped.

failed: Specifies the number of logs for hello packets that failed to be sent.

lsa-flush: Specifies the number of LSA aging logs.

peer: Specifies the number of neighbor state change logs.

spf: Specifies the number of route calculation logs.

size *count*: Specifies the number of OSPF logs, in the range of 0 to 65535.

Examples

Set the number of route calculation logs to 50 in OSPF process 100.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] event-log spf size 50
```

fast-reroute

Use **fast-reroute** to configure OSPF FRR.

Use **undo fast-reroute** to restore the default.

Syntax

fast-reroute { **lfa** [**abr-only**] | **route-policy** *route-policy-name* }

undo fast-reroute

Default

OSPF FRR is disabled.

Views

OSPF view

Predefined user roles

network-admin

context-admin

Parameters

lfa: Uses the LFA algorithm to calculate a backup next hop for all routes.

abr-only: Uses the next hop of the route to the ABR as the backup next hop.

route-policy *route-policy-name*: Uses a routing policy to designate a backup next hop. The *route-policy-name* argument is a case-sensitive string of 1 to 63 characters.

Usage guidelines

When both OSPF FRR and PIC are configured, OSPF FRR takes effect.

Do not use the **fast-reroute lfa** command together with the **vlink-peer** command.

Examples

Enable FRR to calculate a backup next hop for all routes by using LFA algorithm in OSPF process 1.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] fast-reroute lfa
```

fast-reroute tiebreaker

Use **fast-reroute tiebreaker** to set the priority for the node-protection or lowest-cost backup path selection policy.

Use **undo fast-reroute tiebreaker** to restore the default.

Syntax

fast-reroute tiebreaker { **lowest-cost** | **node-protecting** } **preference** *preference*

undo fast-reroute tiebreaker { **lowest-cost** | **node-protecting** }

Default

The priority values of the node-protection and lowest-cost backup path selection policies are 40 and 20, respectively.

Views

OSPF view

Predefined user roles

network-admin

context-admin

Parameters

lowest-cost: Sets a priority value for the lowest-cost backup path selection policy.

node-protecting: Sets a priority value for the node-protection backup path selection policy.

preference *preference*: Specifies a priority value in the range of 1 to 255. A higher value indicates a higher priority.

Usage guidelines

If you execute this command multiple times for a backup path selection policy, the most recent configuration takes effect.

If the node-protection policy has the higher priority but the backup path calculation still fails, OSPF uses the lowest-cost policy for further calculation.

If the lowest-cost policy has the higher priority but the backup path calculation still fails, OSPF does not perform further backup path calculation.

Examples

Set the priority value of the node-protection backup path selection policy to 100.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] fast-reroute tiebreaker node-protecting preference 100
```

Related commands

fast-reroute

filter

Use **filter** to configure OSPF to filter inbound/outbound Type-3 LSAs on an ABR.

Use **undo filter** to disable Type-3 LSA filtering.

Syntax

filter { *ipv4-acl-number* | **prefix-list** *prefix-list-name* | **route-policy** *route-policy-name* } { **export** | **import** }

undo filter { **export** | **import** }

Default

Type-3 LSAs are not filtered.

Views

OSPF area view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-acl-number: Specifies an IPv4 ACL by its number in the range of 2000 to 3999 to filter inbound/outbound Type-3 LSAs.

prefix-list-name: Specifies an IP prefix list by its name, a case-sensitive string of 1 to 63 characters, to filter inbound/outbound Type-3 LSAs.

route-policy-name: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to filter inbound/outbound Type-3 LSAs.

export: Filters Type-3 LSAs advertised to other areas.

import: Filters Type-3 LSAs advertised into the local area.

Usage guidelines

This command applies only to an ABR.

When you specify an ACL, follow these guidelines:

- If the ACL does not exist or has no rules, the ABR does not filter Type-3 LSAs.
- If a rule in the ACL is applied to a VPN instance, the rule will deny all Type-3 LSAs.

To use an advanced ACL (with a number from 3000 to 3999) in the command, configure the ACL using one of the following methods:

- To deny/permit Type-3 LSAs with the specified link state ID, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* command.
- To deny/permit Type-3 LSAs with the specified link state ID and mask, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* **destination** *dest-addr dest-wildcard* command.

The **source** keyword specifies the link state ID of a Type-3 LSA and the **destination** keyword specifies the subnet mask of the LSA. For the mask configuration to take effect, specify a contiguous subnet mask.

Examples

Use IP prefix list **my-prefix-list** to filter inbound Type-3 LSAs. Use basic ACL 2000 to filter outbound Type-3 LSAs in OSPF Area 1.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] filter prefix-list my-prefix-list import
[Sysname-ospf-100-area-0.0.0.1] filter 2000 export
```

filter-policy export

Use **filter-policy export** to configure OSPF to filter redistributed routes.

Use **undo filter-policy export** to remove the configuration.

Syntax

filter-policy { *ipv4-acl-number* | **prefix-list** *prefix-list-name* } **export** [**bgp** | **direct** | { **isis** | **ospf** | **rip** } [*process-id*] | **static**]

undo filter-policy export [**bgp** | **direct** | { **isis** | **ospf** | **rip** } [*process-id*] | **static**]

Default

OSPF does not filter redistributed routes.

Views

OSPF view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-acl-number: Specifies an IPv4 ACL by its number in the range of 2000 to 3999 to filter redistributed routes by destination address.

prefix-list-name: Specifies an IP prefix list by its name, a case-sensitive string of 1 to 63 characters, to filter redistributed routes by destination address.

bgp: Filters routes redistributed from BGP.

direct: Filters direct routes.

isis: Filters routes redistributed from IS-IS.

ospf: Filters routes redistributed from OSPF.

rip: Filters routes redistributed from RIP.

process-id: Specifies a process by its ID in the range of 1 to 65535. The default value is 1.

Usage guidelines

If you do not specify any parameters, the command filters all redistributed routes.

When you specify an ACL, follow these guidelines:

- If the ACL does not exist or has no rules, OSPF does not filter redistributed routes.
- If a rule in the ACL is applied to a VPN instance, the rule will deny all redistributed routes.

To use an advanced ACL (with a number from 3000 to 3999) in the command, configure the ACL using one of the following methods:

- To deny/permit a route with the specified destination, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* command.
- To deny/permit a route with the specified destination and mask, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* **destination** *dest-addr dest-wildcard* command.

The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the subnet mask of the destination address. For the mask configuration to take effect, specify a contiguous subnet mask.

Examples

Configure OSPF process 100 to filter redistributed routes by using basic ACL 2000.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule deny source 192.168.10.0 0.0.0.255
[Sysname-acl-ipv4-basic-2000] quit
[Sysname] ospf 100
[Sysname-ospf-100] filter-policy 2000 export
```

Configure advanced ACL 3000 to permit only route 113.0.0.0/16. Configure OSPF process 100 to filter redistributed routes by using advanced ACL 3000.

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule 10 permit ip source 113.0.0.0 0 destination 255.255.0.0
0
[Sysname-acl-ipv4-adv-3000] rule 100 deny ip
[Sysname-acl-ipv4-adv-3000] quit
[Sysname] ospf 100
[Sysname-ospf-100] filter-policy 3000 export
```

Related commands

import-route

filter-policy import

Use **filter-policy import** to configure OSPF to filter routes calculated using received LSAs.

Use **undo filter-policy import** to restore the default.

Syntax

filter-policy { *ipv4-acl-number* [**gateway** *prefix-list-name*] | **gateway** *prefix-list-name* | **prefix-list** *prefix-list-name* [**gateway** *prefix-list-name*] | **route-policy** *route-policy-name* } **import**

undo filter-policy import

Default

OSPF does not filter routes calculated using received LSAs.

Views

OSPF view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-acl-number: Specifies an IPv4 ACL by its number in the range of 2000 to 3999 to filter received routes by destination.

gateway *prefix-list-name*: Specifies an IP prefix list by its name, a case-sensitive string of 1 to 63 characters, to filter received routes by next hop.

prefix-list *prefix-list-name*: Specifies an IP prefix list by its name, a case-sensitive string of 1 to 63 characters, to filter received routes by destination.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to filter received routes.

Usage guidelines

When you specify an ACL, follow these guidelines:

- If the ACL does not exist or has no rules, OSPF does not filter calculated routes.
- If a rule in the ACL is applied to a VPN instance, the rule will deny all calculated routes.

To use an advanced ACL (with a number from 3000 to 3999) in the command or in the specified routing policy, configure the ACL in one of the following ways:

- To deny/permit a route with the specified destination, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* command.
- To deny/permit a route with the specified destination and mask, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* **destination** *dest-addr dest-wildcard* command.

The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the subnet mask of the destination address. For the mask configuration to take effect, specify a contiguous subnet mask.

Examples

Use basic ACL 2000 to filter received routes.

```
<Sysname> system-view
[Sysname] acl basic 2000
```

```
[Sysname-acl-ipv4-basic-2000] rule deny source 192.168.10.0 0.0.0.255
[Sysname-acl-ipv4-basic-2000] quit
[Sysname] ospf 100
[Sysname-ospf-100] filter-policy 2000 import
```

Configure advanced ACL 3000 to permit only route 113.0.0.0/16. Use ACL 3000 to filter received routes.

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule 10 permit ip source 113.0.0.0 0 destination 255.255.0.0
0
[Sysname-acl-ipv4-adv-3000] rule 100 deny ip
[Sysname-acl-ipv4-adv-3000] quit
[Sysname] ospf 100
[Sysname-ospf-100] filter-policy 3000 import
```

graceful-restart

Use **graceful-restart** to enable OSPF GR.

Use **undo graceful-restart** to disable OSPF GR.

Syntax

graceful-restart [**ietf** | **nonstandard**] [**global** | **planned-only**] *

undo graceful-restart

Default

OSPF GR is disabled.

Views

OSPF view

Predefined user roles

network-admin

context-admin

Parameters

ietf: Enables IETF GR.

nonstandard: Enables non-IETF GR.

global: Enables global GR. In global GR mode, a GR process can be completed only when all GR helpers exist. A GR process fails if a GR helper fails (for example, the interface connected to the GR helper goes down). If you do not specify this keyword, the command enables partial GR. In partial GR mode, a GR process can be completed if a GR helper exists.

planned-only: Enables only planned GR. If you do not specify this keyword, the command enables both planned GR and unplanned GR.

Usage guidelines

GR includes planned GR and unplanned GR.

- **Planned GR**—Manually restarts OSPF by using the **reset ospf process** command or performs an active/standby process switchover by using the **placement reoptimize** command. Before OSPF restart or active/standby switchover, the GR restarter sends Grace-LSAs to GR helpers.

- **Unplanned GR**—OSPF restarts or an active/standby switchover occurs because of device failure. Before OSPF restart or active/standby switchover, the GR restarter does not send Grace-LSAs to GR helpers.

Before enabling IETF GR for OSPF, enable Opaque LSA advertisement and reception with the **opaque-capability enable** command.

Before enabling non-IETF GR for OSPF, enable OSPF LLS with the **enable link-local-signaling** command and OOB-Resynch with the **enable out-of-band-resynchronization** command.

If you do not specify the **nonstandard** or **ietf** keyword, this command enables non-IETF GR for OSPF.

OSPF GR and OSPF NSR are mutually exclusive. Do not configure the **graceful-restart** command and the **non-stop-routing** command at the same time.

Examples

Enable IETF GR for OSPF process 1.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] opaque-capability enable
[Sysname-ospf-1] graceful-restart ietf
```

Enable non-IETF GR for OSPF process 1.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] enable link-local-signaling
[Sysname-ospf-1] enable out-of-band-resynchronization
[Sysname-ospf-1] graceful-restart nonstandard
```

Related commands

enable link-local-signaling

enable out-of-band-resynchronization

opaque-capability enable

graceful-restart helper enable

Use **graceful-restart helper enable** to enable OSPF GR helper capability.

Use **undo graceful-restart helper enable** to disable OSPF GR helper capability.

Syntax

graceful-restart helper enable [**planned-only**]

undo graceful-restart helper enable

Default

OSPF GR helper capability is enabled.

Views

OSPF view

Predefined user roles

network-admin

context-admin

Parameters

planned-only: Enables only planned GR for the GR helper. If you do not specify this keyword, the command enables both planned GR and unplanned GR for the GR helper.

Usage guidelines

The **planned-only** keyword is available only for the IETF GR helper.

Examples

Enable GR helper capability for OSPF process 1.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] graceful-restart helper enable
```

graceful-restart helper strict-lsa-checking

Use **graceful-restart helper strict-lsa-checking** to enable strict LSA checking capability for GR helper.

Use **undo graceful-restart helper strict-lsa-checking** to disable strict LSA checking capability for GR helper.

Syntax

graceful-restart helper strict-lsa-checking

undo graceful-restart helper strict-lsa-checking

Default

Strict LSA checking capability for GR helper is disabled.

Views

OSPF view

Predefined user roles

network-admin

context-admin

Usage guidelines

When an LSA change on the GR helper is detected, the GR helper device exits the GR helper mode.

Examples

Enable strict LSA checking capability for GR helper in OSPF process 1.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] graceful-restart helper strict-lsa-checking
```

graceful-restart interval

Use **graceful-restart interval** to set the GR interval.

Use **undo graceful-restart interval** to restore the default.

Syntax

graceful-restart interval *interval*

undo graceful-restart interval

Default

The GR interval is 120 seconds.

Views

OSPF view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies the GR interval in the range of 40 to 1800 seconds.

Usage guidelines

For GR restart to succeed, the value of the GR restart interval cannot be smaller than the maximum OSPF neighbor dead time of all the OSPF interfaces.

Examples

Set the GR interval for OSPF process 1 to 100 seconds.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] graceful-restart interval 100
```

Related commands

ospf timer dead

host-advertise

Use **host-advertise** to advertise a host route.

Use **undo host-advertise** to remove a host route.

Syntax

host-advertise *ip-address cost-value*

undo host-advertise *ip-address*

Default

No host route is advertised.

Views

OSPF area view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the IP address of a host.

cost-value: Specifies a cost for the route, in the range of 1 to 65535.

Examples

Advertise host route 1.1.1.1 with a cost of 100.

```
<Sysname> system-view
```

```
[Sysname] ospf 100
[Sysname-ospf-100] area 0
[Sysname-ospf-100-area-0.0.0.0] host-advertise 1.1.1.1 100
```

hostname

Use **hostname** to enable the OSPF dynamic host name mapping feature.

Use **undo hostname** to disable the OSPF dynamic host name mapping feature.

Syntax

hostname [*host-name*]

undo hostname

Default

The OSPF dynamic host name mapping feature is disabled.

Views

OSPF view

Predefined user roles

network-admin

context-admin

Parameters

host-name: Specifies the host name mapped to the router ID of the OSPF process, a case-sensitive string of 1 to 255 characters. If you do not specify this argument, the device name is mapped to the router ID of the OSPF process.

Usage guidelines

OSPF uses Type-11 LSAs to carry information about the dynamic host name attribute. Therefore, make sure the opaque LSA reception and advertisement capability is enabled.

Examples

Enable the dynamic host name mapping feature for OSPF process 1, and specify the host name mapped to the router ID as **red**.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] hostname red
```

Related commands

display ospf hostname-table

opaque-capability enable

import-route

Use **import-route** to enable route redistribution.

Use **undo import-route** to disable route redistribution.

Syntax

import-route bgp [*as-number*] [**allow-ibgp**] [**cost** *cost-value* | **nssa-only** | **route-policy** *route-policy-name* | **tag** *tag* | **type** *type*] *

import-route { **direct** | **guard** | **static** } [**cost** *cost-value* | **nssa-only** | **route-policy** *route-policy-name* | **tag** *tag* | **type** *type*] *

import-route { **isis** | **ospf** | **rip** } [*process-id* | **all-processes**] [**allow-direct** | **cost** *cost-value* | **nssa-only** | **route-policy** *route-policy-name* | **tag** *tag* | **type** *type*] *

undo import-route { **bgp** | **direct** | **guard** | { **isis** | **ospf** | **rip** } [*process-id* | **all-processes**] | **static** }

Default

OSPF does not redistribute routes.

Views

OSPF view

Predefined user roles

network-admin

context-admin

Parameters

bgp: Redistributes BGP routes.

direct: Redistributes direct routes.

guard: Redistributes guard routes.

isis: Redistributes IS-IS routes.

ospf: Redistributes OSPF routes.

rip: Redistributes RIP routes.

static: Redistributes static routes.

as-number: Redistributes routes in an AS specified by its number in the range of 1 to 4294967295. If you do not specify this argument, this command redistributes all IPv4 EBGP routes. As a best practice, specify an AS number to prevent the system from redistributing excessive IPv4 EBGP routes.

process-id: Specifies a process by its ID in the range of 1 to 65535. The default is 1.

all-processes: Redistributes routes from all the processes of the specified routing protocol.

allow-ibgp: Redistributes IBGP routes. The **import-route bgp** command redistributes only EBGP routes. Because the **import-route bgp allow-ibgp** command redistributes both EBGP and IBGP routes and might cause routing loops, use it with caution.

allow-direct: Redistributes the networks of the local interfaces enabled with the specified routing protocol. If you do not specify this keyword, the networks of the local interfaces are not redistributed. If you specify both the **allow-direct** keyword and the **route-policy** *route-policy-name* option, make sure the **if-match** rule defined in the routing policy does not conflict with the **allow-direct** keyword. For example, if you specify the **allow-direct** keyword, do not configure the **if-match route-type** rule for the routing policy. Otherwise, the **allow-direct** keyword does not take effect.

cost *cost-value*: Specifies a route cost in the range of 0 to 16777214. The default is 1.

nssa-only: Limits the route advertisement to the NSSA area by setting the P-bit of Type-7 LSAs to 0. If you do not specify this keyword, the P-bit of Type-7 LSAs is set to 1. If the router acts as both an ASBR and an ABR and **FULL** state neighbors exist in the backbone area, the P-bit is set to 0. This keyword applies to NSSA routers.

route-policy *route-policy-name*: Specifies a routing policy to filter redistributed routes. The *route-policy-name* argument is a case-sensitive string of 1 to 63 characters.

tag *tag*: Specifies a tag for external LSAs, in the range of 0 to 4294967295. The default is 1.

type *type*: Specifies a cost type, 1 or 2. The default is 2.

Usage guidelines

This command redistributes routes destined for other ASs from another protocol. AS external routes include the following types:

- **Type-1 external routes**—Have high credibility. The cost of Type-1 external routes is comparable with the cost of OSPF internal routes. The cost of a Type-1 external route equals the cost from the router to the ASBR plus the cost from the ASBR to the external route's destination.
- **Type-2 external routes**—Have low credibility. OSPF considers the cost from the ASBR to the destination of a Type-2 external route is much bigger than the cost from the ASBR to an OSPF internal router. The cost of a Type-2 external route equals the cost from the ASBR to the Type-2 external route's destination.

The **import-route** command redistributes only active routes. To display information about active routes, use the **display ip routing-table protocol** command. The **import-route** command cannot redistribute default external routes.

The **import-route nssa-only** command redistributes AS-external routes in Type-7 LSAs only into the NSSA area.

The **undo import-route** { **isis** | **ospf** | **rip** } **all-processes** command removes only the configuration made by the **import-route** { **isis** | **ospf** | **rip** } **all-processes** command, instead of the configuration made by the **import-route** { **isis** | **ospf** | **rip** } *process-id* command.

Examples

Redistribute routes from RIP process 40 and specify the type, tag, and cost as 2, 33, and 50 for redistributed routes.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] import-route rip 40 type 2 tag 33 cost 50
```

Related commands

default-route-advertise

ispf enable

Use **ispf enable** to enable OSPF incremental SPF (ISPF).

Use **undo ispf enable** to disable OSPF ISPF.

Syntax

ispf enable

undo ispf enable

Default

OSPF ISPF is enabled.

Views

OSPF view

Predefined user roles

network-admin

context-admin

Usage guidelines

Upon topology changes, ISPF recomputes only the affected part of the SPT, instead of the entire SPT.

Examples

Disable ISPF for OSPF process 100.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] undo ispf enable
```

log-peer-change

Use **log-peer-change** to enable logging for OSPF neighbor state changes.

Use **undo log-peer-change** to disable logging for OSPF neighbor state changes.

Syntax

log-peer-change

undo log-peer-change

Default

Logging for OSPF neighbor state changes is enabled.

Views

OSPF view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command enables output of OSPF neighbor state changes to the information center. The information center processes the logs according to user-defined output rules (whether and where to output logs). For more information about the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Disable logging for neighbor state changes for OSPF process 100.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] undo log-peer-change
```

lsa-arrival-interval

Use **lsa-arrival-interval** to set the LSA arrival interval.

Use **undo lsa-arrival-interval** to restore the default.

Syntax

lsa-arrival-interval *interval*

undo lsa-arrival-interval

Default

The LSA arrival interval is 1000 milliseconds.

Views

OSPF view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies the LSA arrival interval in the range of 0 to 60000 milliseconds.

Usage guidelines

If an LSA that has the same LSA type, LS ID, and originating router ID as the previous LSA is received within the interval, OSPF discards the LSA. This feature helps avoid overuse of system resources due to frequent network changes.

As a best practice, set the interval with the **lsa-arrival-interval** command to be smaller than or equal to the minimum interval set with the **lsa-generation-interval** command.

Examples

Set the LSA arrival interval to 200 milliseconds.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] lsa-arrival-interval 200
```

Related commands

lsa-generation-interval

lsa-generation-interval

Use **lsa-generation-interval** to set the OSPF LSA generation interval.

Use **undo lsa-generation-interval** to restore the default.

Syntax

lsa-generation-interval *maximum-interval* [*minimum-interval* [*incremental-interval*]]

undo lsa-generation-interval

Default

The maximum interval is 5 seconds, the minimum interval is 50 milliseconds, and the incremental interval is 200 milliseconds.

Views

OSPF view

Predefined user roles

network-admin

context-admin

Parameters

maximum-interval: Specifies the maximum LSA generation interval in the range of 1 to 60 seconds.

minimum-interval: Specifies the minimum LSA generation interval in the range of 10 to 60000 milliseconds.

incremental-interval: Specifies the LSA generation incremental interval in the range of 10 to 60000 milliseconds.

Usage guidelines

When network changes are infrequent, LSAs are generated at the minimum interval. If network changes become frequent, the LSA generation interval increases by the incremental interval × 2^{n-2} for each generation until the maximum interval is reached. The value *n* is the number of generation times.

The minimum interval and the incremental interval cannot be greater than the maximum interval.

Examples

Set the maximum LSA generation interval to 2 seconds, minimum interval to 100 milliseconds, and incremental interval to 100 milliseconds.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] lsa-generation-interval 2 100 100
```

Related commands

lsa-arrival-interval

lsdb-overflow-interval

Use **lsdb-overflow-interval** to set the interval that OSPF exits overflow state.

Use **undo lsdb-overflow-interval** to restore the default.

Syntax

lsdb-overflow-interval *interval*

undo lsdb-overflow-interval

Default

The OSPF exit overflow interval is 300 seconds.

Views

OSPF view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies the interval that OSPF exits overflow state, in the range of 0 to 2147483647 seconds.

Usage guidelines

When the number of LSAs in the LSDB exceeds the upper limit, the LSDB is in an overflow state. In this state, OSPF does not receive any external LSAs and deletes the external LSAs generated by itself to save system resources.

You can configure the interval that OSPF exits overflow state. An interval of 0 indicates that the timer is not started and OSPF does not exit overflow state.

Examples

Set the OSPF exit overflow interval to 10 seconds.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] lsdb-overflow-interval 10
```

lsdb-overflow-limit

Use **lsdb-overflow-limit** to set the upper limit of external LSAs in the LSDB.

Use **undo lsdb-overflow-limit** to restore the default.

Syntax

lsdb-overflow-limit *number*

undo lsdb-overflow-limit

Default

The number of external LSAs is not limited.

Views

OSPF view

Predefined user roles

network-admin

context-admin

Parameters

number: Specifies the upper limit of external LSAs in the LSDB, in the range of 1 to 1000000.

Examples

Set the upper limit of external LSAs to 400000.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] lsdb-overflow-limit 400000
```

maximum load-balancing

Use **maximum load-balancing** to set the maximum number of equal-cost multi-path (ECMP) routes for load balancing.

Use **undo maximum load-balancing** to restore the default.

Syntax

maximum load-balancing *number*

undo maximum load-balancing

Default

The maximum number of OSPF ECMP routes is 32.

Views

OSPF view

Predefined user roles

network-admin

context-admin

Parameters

number: Specifies the maximum number of ECMP routes. No ECMP load balancing is available when the number is set to 1.

Usage guidelines

The value range for the *number* argument of the **maximum load-balancing** command depends on the maximum number of ECMP routes supported by the system. You can use the **max-ecmp-num** command to set the maximum number of ECMP routes supported by the system to *m*. After a reboot, the value range for the *number* argument is 1 to *m*.

Examples

Set the maximum number of ECMP routes to 2.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] maximum load-balancing 2
```

network

Use **network** to enable OSPF on the interface attached to the specified network in the area.

Use **undo network** to disable OSPF for the interface attached to the specified network in the area.

Syntax

network *ip-address wildcard-mask*

undo network *ip-address wildcard-mask*

Default

OSPF is not enabled for any interface.

Views

OSPF area view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the IP address of a network.

wildcard-mask: Specifies the wildcard mask of the IP address. For example, the wildcard mask of mask 255.0.0.0 is 0.255.255.255.

Usage guidelines

This command enables OSPF on the interface attached to the specified network. The interface's primary IP address must be in the specified network. If only the interface's secondary IP address is on the network, the interface cannot run OSPF.

Examples

Specify the interface whose primary IP address is on network 131.108.20.0/24 to run OSPF in Area 2.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 2
[Sysname-ospf-100-area-0.0.0.2] network 131.108.20.0 0.0.0.255
```

Related commands

ospf

non-stop-routing

Use **non-stop-routing** to enable OSPF NSR.

Use **undo non-stop-routing** to disable OSPF NSR.

Syntax

non-stop-routing

undo non-stop-routing

Default

OSPF NSR is disabled.

Views

OSPF view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command takes effect only for the current process. As a best practice, enable OSPF NSR for each process if multiple OSPF processes exist.

OSPF NSR and OSPF GR are mutually exclusive. Do not configure the **non-stop-routing** command and the **graceful-restart** command at the same time.

Examples

Enable NSR for OSPF process 100.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] non-stop-routing
```

nssa

Use **nssa** to configure an area as an NSSA area.

Use **undo nssa** to restore the default.

Syntax

nssa [**default-route-advertise** [**cost** *cost-value* | **nssa-only** | **route-policy** *route-policy-name* | **type** *type*] * | **no-import-route** | **no-summary** | **suppress-fa** | [[[**translate-always**] [**translate-ignore-checking-backbone**]] | **translate-never**] | **translator-stability-interval** *value*] *

undo nssa

Default

No area is configured as an NSSA area.

Views

OSPF area view

Predefined user roles

network-admin

context-admin

Parameters

default-route-advertise: Used on an NSSA ABR or an ASBR only. With this keyword, an NSSA ABR redistributes a default route in a Type-7 LSA into the NSSA area. The ABR redistributes a default route regardless of whether a default route exists in the routing table. With this keyword, an ASBR redistributes a default route in a Type-7 LSA only when the default route exists in the routing table.

cost *cost-value*: Specifies a cost for the default route, in the range of 0 to 16777214. If you do not specify this option, the default cost specified by the **default-cost** command applies.

nssa-only: Limits the default route advertisement to the NSSA area by setting the P-bit of Type-7 LSAs to 0. By default, the P-bit of Type-7 LSAs is set to 1. If the router acts as both an ASBR and an ABR and **FULL** state neighbors exist in the backbone area, the P-bit is set to 0.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters. When a default route exists in the routing table and the routing policy is matched, the command redistributes a default route in a Type-7 LSA into the OSPF routing domain. The routing policy modifies values in the Type-7 LSA.

type *type*: Specifies a type for the Type-7 LSA, 1 or 2. If you do not specify this option, the default type specified by the **default type** command applies.

no-import-route: Used on an NSSA ABR to control the **import-route** command to not redistribute routes into the NSSA area.

no-summary: Used only on an ABR to advertise a default route in a Type-3 summary LSA into the NSSA area and to not advertise other summary LSAs into the area. The area is a totally NSSA area.

suppress-fa: Suppresses the forwarding address in the Type-7 LSAs from being placed in the Type-5 LSAs.

translate-always: Always translates Type-7 LSAs to Type-5 LSAs. This keyword takes effect only on an NSSA ABR.

translate-ignore-checking-backbone: Ignores checking for FULL state neighbors in the backbone area during the translator election in the NSSA area.

translate-never: Never translates Type-7 LSAs to Type-5 LSAs. This keyword takes effect only on an NSSA ABR.

translator-stability-interval *value*: Specifies the stability interval of the translator. During the interval, the translator can maintain its translating capability after another device becomes the new translator. The *value* argument is the stability interval in the range of 0 to 900 seconds and

defaults to 0. A value of 0 means the translator does not maintain its translating capability when a new translator arises.

Usage guidelines

All routers attached to an NSSA area must be configured with the **nssa** command in area view.

If you specify the **translate-ignore-checking-backbone** keyword for an ABR, you must also specify the keyword for other ABRs in the NSSA area. This ensures that a translator can be elected among the ABRs.

Examples

Configure Area 1 as an NSSA area.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] nssa
```

Related commands

default-cost

opaque-capability enable

Use **opaque-capability enable** to enable opaque LSA advertisement and reception.

Use **undo opaque-capability** to disable opaque LSA advertisement and reception.

Syntax

opaque-capability enable

undo opaque-capability

Default

The feature is enabled.

Views

OSPF view

Predefined user roles

network-admin

context-admin

Usage guidelines

After the opaque LSA advertisement and reception capability is enabled, OSPF can receive and advertise Type-9 and Type-11 opaque LSAs.

Examples

Disable opaque LSA advertisement and reception.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] undo opaque-capability
```

ospf

Use **ospf** to enable OSPF and enter OSPF view.

Use **undo ospf** to disable OSPF.

Syntax

ospf [*process-id* | **router-id** { **auto-select** | *router-id* } | **vpn-instance** *vpn-instance-name*] *

undo ospf [*process-id*] [**router-id**]

Default

OSPF is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535.

router-id: Specifies an OSPF router ID. If you do not specify an OSPF router ID, the global router ID is used.

auto-select: Automatically obtains an OSPF router ID.

router-id: Manually specifies an OSPF router ID in dotted decimal notation. The value range is from 0.0.0.1 to 255.255.255.255.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the OSPF process runs on the public network.

Usage guidelines

Enable an OSPF process before performing other tasks.

You can enable multiple OSPF processes on a router and specify different router IDs for them.

If you specify the **auto-select** keyword, the OSPF process obtains a router ID in the following ways:

- During the startup of the OSPF process, the primary IPv4 address of the first interface that runs the process is specified as the router ID.
- During the reboot of the router, the primary IPv4 address of the first interface that runs the process is specified as the router ID.
- During the restart of the OSPF process, the highest primary IPv4 address of the loopback interface that runs the process is specified as the router ID. If no loopback address is available, the highest primary IPv4 address of the interface that runs the process is used, regardless of the interface state (up or down).

If you do not specify the **router-id** keyword, the **undo ospf** command shuts down an OSPF process. If you specify the **router-id** keyword, the **undo ospf** command specifies the global router ID as the router ID. The setting takes effect after the OSPF process restarts.

Examples

Enable OSPF process 100 and specify router ID 10.10.10.1.

```
<Sysname> system-view
[Sysname] ospf 100 router-id 10.10.10.1
[Sysname-ospf-100]
```

ospf area

Use **ospf area** to enable OSPF on an interface.

Use **undo ospf area** to disable OSPF on an interface.

Syntax

ospf *process-id* **area** *area-id* [**exclude-subip**]

undo ospf *process-id* **area** [**exclude-subip**]

Default

OSPF is not enabled on an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535.

area-id: Specifies an area by its ID, an IP address or a decimal integer in the range of 0 to 4294967295 that is translated into the IP address format.

exclude-subip: Excludes secondary IP addresses. If you do not specify this keyword, the command enables OSPF also on secondary IP addresses.

Usage guidelines

The **ospf area** command has a higher priority than the **network** command.

If the specified process and area do not exist, the command creates the process and area. Disabling an OSPF process on an interface does not delete the OSPF process or the area.

Examples

Enable OSPF process 1 on GigabitEthernet 1/0/2 that is in Area 2 and exclude secondary IP addresses.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] ospf 1 area 2 exclude-subip
```

Related commands

network

ospf authentication-mode

Use **ospf authentication-mode** to set the authentication mode and key on an interface.

Use **undo ospf authentication-mode** to remove specified configuration.

Syntax

For MD5/HMAC-MD5 authentication:

ospf authentication-mode { **hmac-md5** | **hmac-sha-256** | **md5** } *key-id* { **cipher** | **plain** } *string*

undo ospf authentication-mode { **hmac-md5** | **hmac-sha-256** | **md5** } *key-id*

For simple authentication:

ospf authentication-mode simple { **cipher** | **plain** } *string*

undo ospf authentication-mode simple

For keychain authentication:

ospf authentication-mode keychain *keychain-name*

undo ospf authentication-mode keychain

Default

No authentication is performed for an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

hmac-md5: Specifies HMAC-MD5 authentication.

hmac-sha-256: Specifies HMAC-SHA-256 authentication.

md5: Specifies MD5 authentication.

simple: Specifies simple authentication.

key-id: Specifies a key by its ID in the range of 1 to 255.

cipher: Specifies a key in encrypted form.

plain: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. This argument is case sensitive.

- In simple authentication mode, the plaintext form of the key is a string of 1 to 8 characters. The encrypted form of the key is a string of 33 to 41 characters.
- In MD5/HMAC-MD5/HMAC-SHA-256 authentication mode, the plaintext form of the key is a string of 1 to 255 characters. The encrypted form of the key is a string of 33 to 373 characters.

keychain: Specifies keychain authentication.

keychain-name: Specifies a keychain by its name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

To establish or maintain adjacencies, interfaces attached to the same network segment must have the same authentication mode and key.

If MD5, HMAC-MD5, or HMAC-SHA-256 authentication is configured, you can configure multiple keys, each having a unique key ID and key string. To minimize the risk of key compromise, use only one key for an interface and delete the old key after key replacement.

To replace the key used for MD5, HMAC-MD5, or HMAC-SHA-256 authentication on an interface, you must configure the new key before removing the old key from each router. OSPF uses the key rollover mechanism to ensure that the routers can pass authentication before the replacement is complete on the interface. After you configure a new key on a router, the router sends copies of the same packet, each authenticated by a different key, including the new key and the keys in use. This practice continues until the router detects that all its neighbors have the new key.

When keychain authentication is configured for an OSPF interface, OSPF performs the following operations before sending a packet:

1. Obtains a valid send key from the keychain.

   OSPF does not send the packet if it fails to obtain a valid send key.

2. Uses the key ID, authentication algorithm, and key string to authenticate the packet.

   If the key ID is greater than 255, OSPF does not send the packet.

When keychain authentication is configured for an OSPF interface, OSPF performs the following operations after receiving a packet:

1. Uses the key ID carried in the packet to obtain a valid accept key from the keychain.

   OSPF discards the packet if it fails to obtain a valid accept key.

2. Uses the authentication algorithm and key string for the valid accept key to authenticate the packet.

   If the authentication fails, OSPF discards the packet.

The authentication algorithm can only be MD5, HMAC-SM3, HMAC-MD5, or HMAC-SHA-256 and the ID of keys used for keychain authentication can only be in the range of 0 to 255.

Examples

On GigabitEthernet 1/0/1, enable MD5 authentication, and set the interface key ID to 15 and the key to **123456** in plaintext form.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospf authentication-mode md5 15 plain 123456
```

On GigabitEthernet 1/0/1, enable simple authentication, and set the key to **123456** in plaintext form.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospf authentication-mode simple plain 123456
```

Related commands

authentication-mode

ospf bfd enable

Use **ospf bfd enable** to enable BFD on an OSPF interface.

Use **undo ospf bfd enable** to disable BFD on an OSPF interface.

Syntax

ospf bfd enable [**echo**]

undo ospf bfd enable

Default

BFD for OSPF is disabled.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

echo: Enables BFD single-hop echo detection. If you do not specify this keyword, the command enables BFD bidirectional control detection.

Examples

Enable BFD for OSPF on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] ospf
[Sysname-ospf-1] area 0
[Sysname-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.255.255
[Sysname-ospf-1-area-0.0.0.0] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospf bfd enable
```

ospf cost (interface view)

Use **ospf cost** to set an OSPF cost for an interface.

Use **undo ospf cost** to restore the default.

Syntax

ospf cost *cost-value*

undo ospf cost

Default

An interface computes its OSPF cost according to the interface bandwidth. For a loopback interface, the cost is 0.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

cost-value: Specifies an OSPF cost in the range of 0 to 65535 for a loopback interface, and in the range of 1 to 65535 for other interfaces.

Usage guidelines

If you do not execute this command, the interface automatically computes its OSPF cost.

Examples

Set the OSPF cost on GigabitEthernet 1/0/1 to 65.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospf cost 65
```

Related commands

bandwidth-reference

ospf database-filter

Use **ospf database-filter** to filter outbound LSAs on an interface.

Use **undo ospf database-filter** to restore the default.

Syntax

ospf database-filter { **all** | { **ase** [**acl** *ipv4-acl-number*] | **nssa** [**acl** *ipv4-acl-number*] | **summary** [**acl** *ipv4-acl-number*] } * }

undo ospf database-filter

Default

The outbound LSAs are not filtered on the interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

all: Filters all outbound LSAs except the Grace LSAs.

ase: Filters outbound Type-5 LSAs.

nssa: Filters outbound Type-7 LSAs.

summary: Filters outbound Type-3 LSAs.

acl *ipv4-acl-number*: Specifies an IPv4 ACL by its number in the range of 2000 to 3999.

Usage guidelines

When you specify an ACL, follow these guidelines:

- If the ACL does not exist or has no rules, OSPF does not filter outbound LSAs.
- If a rule in the ACL is applied to a VPN instance, the rule will deny all outbound LSAs.

To use an advanced ACL (with a number from 3000 to 3999) in the command, configure the ACL using one of the following methods:

- To deny/permit LSAs with the specified link state ID, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* command.
- To deny/permit LSAs with the specified link state ID and mask, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* **destination** *dest-addr dest-wildcard* command.

The **source** keyword specifies the link state ID of an LSA and the **destination** keyword specifies the subnet mask of the LSA. For the mask configuration to take effect, specify a contiguous subnet mask.

If the neighbor has already received an LSA to be filtered, the LSA still exists in the LSDB of the neighbor after you execute the command.

Examples

Filter all outbound LSAs (except the Grace LSAs) on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospf database-filter all
```

On GigabitEthernet 1/0/2, configure ACL 2000, 2100, and 2200 to filter outbound Type-5, Type-7, and Type-3 LSAs, respectively.

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] ospf database-filter ase acl 2000 nssa acl 2100 summary
acl 2200
```

Related commands

database-filter peer

ospf dr-priority

Use **ospf dr-priority** to set the router priority for DR/BDR election on an interface.

Use **undo ospf dr-priority** to restore the default value.

Syntax

ospf dr-priority *priority*

undo ospf dr-priority

Default

The router priority is 1.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

priority: Specifies the router priority for the interface, in the range of 0 to 255.

Usage guidelines

The greater the value, the higher the priority for DR/BDR election. If a device has a priority of 0, it will not be elected as a DR or BDR.

Examples

Set the router priority on GigabitEthernet 1/0/1 to 8.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospf dr-priority 8
```

ospf fast-reroute lfa-backup

Use **ospf fast-reroute lfa-backup** to enable LFA on an interface.

Use **undo ospf fast-reroute lfa-backup** to disable LFA on an interface.

Syntax

ospf fast-reroute lfa-backup

undo ospf fast-reroute lfa-backup

Default

LFA is enabled on an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

An interface enabled with LFA can be selected as a backup interface. After you disable LFA on the interface, it cannot be selected as a backup interface.

Examples

Disable GigabitEthernet 1/0/1 from calculating a backup next hop by using the LFA algorithm.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo ospf fast-reroute lfa-backup
```

ospf mib-binding

Use **ospf mib-binding** to bind an OSPF process to the public MIB.

Use **undo ospf mib-binding** to restore the default.

Syntax

ospf mib-binding *process-id*

undo ospf mib-binding

Default

The public MIB is bound to the OSPF process with the smallest process ID.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535.

Usage guidelines

To access information or data about an OSPF process in **RFC4750-OSPF.MIB**, use this command. To access information or data about an OSPF process in a private MIB for the device, you do not need to use this command. You can access information or data about all OSPF processes in the private MIBs.

If the specified process ID does not exist, a notification is displayed to report that the MIB binding configuration has failed.

Deleting an OSPF process that has been bound to the public MIB unbinds the OSPF process from the MIB, and re-binds the MIB to the OSPF process with the smallest process ID.

Examples

Bind OSPF process 100 to the public MIB.

```
<Sysname> system-view
```

```
[Sysname] ospf mib-binding 100
```

ospf mtu-enable

Use **ospf mtu-enable** to enable an interface to add the interface MTU into DD packets.

Use **undo ospf mtu-enable** to restore the default.

Syntax

ospf mtu-enable

undo ospf mtu-enable

Default

The MTU in DD packets is 0.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

After a virtual link is established through a Virtual-Template or Tunnel, two devices on the link from different vendors might have different MTU values. To make them consistent, restore the interfaces' MTU to the default value 0.

After you configure this command, the interface checks whether the MTU in a received DD packet is greater than its own MTU. If yes, the interface discards the packet.

Examples

Enable GigabitEthernet 1/0/1 to add the interface MTU value into DD packets.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospf mtu-enable
```

ospf network-type

Use **ospf network-type** to specify the network type for an interface.

Use **undo ospf network-type** to restore the default.

Syntax

ospf network-type { **broadcast** | **nbma** | **p2mp** [**unicast**] | **p2p** [**peer-address-check**] }

undo ospf network-type

Default

The network type of an interface is broadcast.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

broadcast: Specifies the network type as broadcast.

nbma: Specifies the network type as NBMA.

p2mp: Specifies the network type as P2MP.

unicast: Specifies the P2MP interface to unicast OSPF packets. By default, a P2MP interface multicasts OSPF packets.

p2p: Specifies the network type as P2P.

peer-address-check: Checks whether the peer interface and the local interface are on the same network segment. Two P2P interfaces can establish a neighbor relationship only when they are on the same network segment.

Usage guidelines

If a router on a broadcast network does not support multicast, configure the network type for the connected interfaces as NBMA.

If any two routers on an NBMA network are directly connected through a virtual link, the network is fully meshed. You can configure the network type for the connected interfaces as NBMA. If two routers are not directly connected, configure the P2MP network type so that the two routers can exchange routing information through another router.

When the network type of an interface is NBMA or P2MP unicast, you must use the **peer** command to specify the neighbor.

If only two routers run OSPF on a network, you can configure the network type for the connected interfaces as P2P.

When the network type of an interface is P2MP unicast, all OSPF packets are unicast by the interface.

Examples

Specify the OSPF network type for GigabitEthernet 1/0/1 as NBMA.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospf network-type nbma
```

Related commands

ospf dr-priority

ospf prefix-suppression

Use **ospf prefix-suppression** to disable an OSPF interface from advertising all its IP prefixes, except for the prefixes of secondary IP addresses.

Use **undo ospf prefix-suppression** to restore the default.

Syntax

ospf prefix-suppression [**disable**]

undo ospf prefix-suppression

Default

Prefix suppression is disabled.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

disable: Disables prefix suppression for an interface.

Usage guidelines

To disable prefix suppression for an interface associated with an OSPF process that has been enabled with prefix suppression, use the **ospf prefix-suppression disable** command on that interface.

Examples

Enable prefix suppression for GigabitEthernet 1/0/2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] ospf prefix-suppression
```

Related commands

prefix-suppression

ospf primary-path-detect bfd

Use **ospf primary-path-detect bfd** to enable BFD for primary link failure detection for OSPF.

Use **undo ospf primary-path-detect bfd** to disable BFD for primary link failure detection for OSPF.

Syntax

ospf primary-path-detect bfd { **ctrl** | **echo** }

undo ospf primary-path-detect bfd

Default

BFD is disabled for primary link failure detection for OSPF.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ctrl: Enables BFD control packet mode.

echo: Enables BFD echo packet mode.

Usage guidelines

This command enables OSPF PIC or OSPF FRR to use BFD to detect primary link failures.

Examples

On GigabitEthernet 1/0/1, enable BFD control packet mode for OSPF FRR.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] fast-reroute lfa
[Sysname-ospf-1] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospf primary-path-detect bfd ctrl
```

On GigabitEthernet 1/0/2, enable BFD echo packet mode for OSPF PIC.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] pic additional-path-always
[Sysname-ospf-1] quit
[Sysname] bfd echo-source-ip 1.1.1.1
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] ospf primary-path-detect bfd echo
```

ospf timer dead

Use **ospf timer dead** to set the neighbor dead interval.

Use **undo ospf timer dead** to restore the default.

Syntax

ospf timer dead *seconds*

undo ospf timer dead

Default

The dead interval is 40 seconds for broadcast and P2P interfaces. The dead interval is 120 seconds for P2MP and NBMA interfaces.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies the dead interval in the range of 1 to 2147483647 seconds.

Usage guidelines

If an interface receives no hello packet from a neighbor within the dead interval, the interface considers the neighbor down. The dead interval on an interface is a minimum of four times longer than the hello interval. Devices attached to the same network segment must have the same dead interval.

By default, the neighbor dead interval is four times longer than the hello interval. If you specify a hello interval and do not specify a dead interval, the default dead interval is four times longer than the specified hello interval. To specify a hello interval, use the **ospf timer hello** command.

When you use the **ospf timer dead** command on an interface, following these guidelines:

- The specified neighbor dead interval can be issued to and can take effect on the interface only when it is not shorter than the hello interval.
- To avoid neighbor flapping, do not set a short dead interval.

Examples

Set the dead interval for GigabitEthernet 1/0/1 to 60 seconds.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospf timer dead 60
```

Related commands

ospf timer hello

ospf timer hello

Use **ospf timer hello** to set the hello interval on an interface.

Use **undo ospf timer hello** to restore the default.

Syntax

ospf timer hello *seconds*

undo ospf timer hello

Default

The hello interval is 10 seconds for P2P and broadcast interfaces, and is 30 seconds for P2MP and NBMA interfaces.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies the hello interval in the range of 1 to 65535 seconds.

Usage guidelines

The shorter the hello interval, the faster the topology converges, and the more resources are consumed. Make sure the hello interval on two neighboring interfaces is the same.

Examples

Set the hello interval on GigabitEthernet 1/0/1 to 20 seconds.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospf timer hello 20
```

Related commands

ospf timer dead

ospf timer poll

Use **ospf timer poll** to set the poll interval on an NBMA interface.

Use **undo ospf timer poll** to restore the default.

Syntax

ospf timer poll *seconds*

undo ospf timer poll

Default

The poll interval is 120 seconds on an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies the poll interval in the range of 1 to 2147483647 seconds.

Usage guidelines

When an NBMA interface finds its neighbor is down, it sends hello packets at the poll interval.

The poll interval must be a minimum of four times the hello interval.

Examples

Set the poll timer interval on GigabitEthernet 1/0/1 to 130 seconds.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospf timer poll 130
```

Related commands

ospf timer hello

ospf timer retransmit

Use **ospf timer retransmit** to set the LSA retransmission interval on an interface.

Use **undo ospf timer retransmit** to restore the default.

Syntax

ospf timer retransmit *seconds*

undo ospf timer retransmit

Default

The LSA retransmission interval is 5 seconds on an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies the LSA retransmission interval in the range of 1 to 3600 seconds.

Usage guidelines

After sending an LSA, an interface waits for an acknowledgment packet. If the interface receives no acknowledgment within the retransmission interval, it retransmits the LSA.

To avoid unnecessary retransmissions, set an appropriate retransmission interval. For example, you can set a large retransmission interval value on a low-speed link.

Examples

Set the LSA retransmission interval to 8 seconds on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospf timer retransmit 8
```

ospf trans-delay

Use **ospf trans-delay** to set the LSA transmission delay on an interface.

Use **undo ospf trans-delay** to restore the default.

Syntax

ospf trans-delay *seconds*

undo ospf trans-delay

Default

The LSA transmission delay is 1 second.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies the LSA transmission delay in the range of 1 to 3600 seconds.

Usage guidelines

Each LSA in the LSDB has an age that increases by 1 every second, but the age does not change during transmission. Adding a transmission delay into the age time is important in low speed networks.

Examples

Set the LSA transmission delay to 3 seconds on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospf trans-delay 3
```

ospf ttl-security

Use **ospf ttl-security** to enable OSPF GTSM for an interface.

Use **ospf ttl-security disable** to disable OSPF GTSM for an interface.

Use **undo ospf ttl-security** to restore the default.

Syntax

ospf ttl-security [**hops** *hop-count* | **disable**]

undo ospf ttl-security

Default

An interface uses the GTSM configuration of the area to which the interface belongs.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

hops *hop-count*: Specifies the hop limit for checking OSPF packets, in the range of 1 to 254. The default hop limit is 1 for packets from common neighbors, and is 255 for packets from virtual link neighbors.

disable: Disables OSPF GTSM for the interface.

Usage guidelines

GTSM checks OSPF packets from common neighbors and virtual link neighbors.

GTSM protects the device by comparing the TTL value in the IP header of incoming OSPF packets against a valid TTL range. If the TTL value is within the valid TTL range, the packet is accepted. If not, the packet is discarded.

The valid TTL range is from 255 – the configured hop count + 1 to 255.

When GTSM is configured, the OSPF packets sent by the device have a TTL of 255. To use GTSM, you must configure GTSM on both the local and peer devices. You can specify different *hop-count* values for them.

The GTSM configuration in OSPF area view applies to all OSPF interfaces in the area. The GTSM configuration in interface view takes precedence over the configuration in OSPF area view.

If a virtual link exists in an area, you can enable GTSM for the interfaces on the virtual link. If you do not know the interfaces on the virtual link, enable GTSM in area view to prevent packet loss.

Examples

Enable OSPF GTSM for GigabitEthernet 1/0/1 and set the hop limit to 254.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospf ttl-security hops 254
```

Enable GTSM in OSPF area view and disable OSPF GTSM for GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] ttl-security
[Sysname-ospf-100-area-0.0.0.1] quit
[Sysname-ospf-100] quit
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ospf ttl-security disable
```

Related commands

ttl-security

peer

Use **peer** to specify a neighbor in an NBMA or P2MP network.

Use **undo peer** to remove a neighbor in an NBMA or P2MP network.

Syntax

peer *ip-address* [**cost** *cost-value* | **dr-priority** *priority*]

undo peer *ip-address*

Default

No neighbor is specified.

Views

OSPF view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies a neighbor by its IP address.

cost *cost-value*: Specifies the cost to reach the neighbor, in the range of 1 to 65535.

dr-priority *priority*: Specifies the DR priority for the neighbor, in the range of 0 to 255. The default neighbor DR priority is 1.

Usage guidelines

On an NBMA or P2MP network, OSPF packets are sent in unicast, so you must use this command to specify neighbors.

The cost set with the **peer** command applies only to P2MP neighbors. If no cost is specified, the cost to the neighbor equals the local interface's cost.

A router uses the priority set with the **peer** command to determine whether to send a hello packet to the neighbor rather than for DR election. The DR priority set with the **ospf dr-priority** command is used for DR election.

Examples

Specify the neighbor 1.1.1.1.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] peer 1.1.1.1
```

Related commands

ospf dr-priority

pic

Use **pic** to enable OSPF PIC.

Use **undo pic** to disable OSPF PIC.

Syntax

pic [**additional-path-always**]

undo pic

Default

OSPF PIC is enabled.

Views

OSPF view

Predefined user roles

network-admin

context-admin

Parameters

additional-path-always: Allows the indirect suboptimal route as the backup route.

Usage guidelines

Prefix Independent Convergence (PIC) enables the device to speed up network convergence by ignoring the number of prefixes. PIC applies only to inter-area routes and external routes.

When both OSPF PIC and OSPF FRR are configured, OSPF FRR takes effect.

Examples

Configure OSPF PIC to support the suboptimal route as the backup route.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] pic additional-path-always
```

preference

Use **preference** to set a preference for OSPF.

Use **undo preference** to remove the configuration.

Syntax

preference [**ase**] { *preference* | **route-policy** *route-policy-name* } *

undo preference [**ase**]

Default

The preference is 10 for OSPF internal routes and 150 for OSPF external routes (ASE routes).

Views

OSPF view

Predefined user roles

network-admin

context-admin

Parameters

ase: Specifies a preference for OSPF external routes. If you do not specify this keyword, the command sets a preference for OSPF internal routes.

preference: Specifies the preference value in the range of 1 to 255. A smaller value represents a higher preference.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to set a preference for the specified routes.

Usage guidelines

If multiple routing protocols find routes to the same destination, the router uses the route found by the protocol with the highest preference.

When the **route-policy** *route-policy-name* option is specified, the following preferences take effect:

- For routes matching the routing policy, the preference set in the routing policy takes effect.
- For other routes, the preference set with the **preference** command takes effect.

Examples

Set a preference of 200 for OSPF external routes.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] preference ase 200
```

Set a preference of 100 for OSPF internal routes matching the specified routing policy, and set a preference of 150 for other routes.

```
<Sysname> system-view
[Sysname] ip prefix-list test index 10 permit 100.1.1.0 24
[Sysname] route-policy pre permit node 10
[Sysname-route-policy-pre-10] if-match ip address prefix-list test
[Sysname-route-policy-pre-10] apply preference 100
[Sysname-route-policy-pre-10] quit
[Sysname] ospf 100
[Sysname-ospf-100] preference route-policy pre 150
```

prefix-priority

Use **prefix-priority** to enable prefix prioritization.

Use **undo prefix-priority** to disable prefix prioritization.

Syntax

prefix-priority route-policy *route-policy-name*

undo prefix-priority

Default

Prefix prioritization is disabled.

Views

OSPF view

Predefined user roles

network-admin

context-admin

Parameters

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to set a priority for the specified route prefixes.

Usage guidelines

Prefix prioritization enables the device to install prefixes in descending priority order: critical, high, medium, and low. The prefix priorities are assigned through routing policies. When a route is assigned multiple prefix priorities, it uses the highest priority.

By default, the 32-bit OSPF host routes have a medium priority and other routes have a low priority.

Examples

Use a routing policy to assign the medium priority to the specified route prefixes.

```
<Sysname> system-view
[Sysname] ip prefix-list test index 10 permit 100.1.1.0 24
[Sysname] route-policy pre permit node 10
[Sysname-route-policy-pre-10] if-match ip address prefix-list test
[Sysname-route-policy-pre-10] apply prefix-priority medium
[Sysname-route-policy-pre-10] quit
[Sysname] ospf 100
[Sysname-ospf-100] prefix-priority route-policy pre
```

prefix-suppression

Use **prefix-suppression** to disable an OSPF process from advertising all IP prefixes except for the prefixes of loopback interfaces, secondary IP addresses, and passive interfaces.

Use **undo prefix-suppression** to restore the default.

Syntax

prefix-suppression

undo prefix-suppression

Default

An OSPF process advertises all prefixes.

Views

OSPF view

Predefined user roles

network-admin

context-admin

Usage guidelines

By default, an OSPF interface advertises all of its prefixes in LSAs. To speed up OSPF convergence, you can suppress interfaces from advertising all their prefixes. This feature helps improve network security by preventing IP routing to the suppressed networks.

As a best practice, configure prefix suppression on all OSPF routers if you want to use prefix suppression.

To disable an OSPF process from advertising the prefixes of loopback and passive interfaces, configure prefix suppression on the interfaces by using the **ospf prefix-suppression** command.

When prefix suppression is enabled:

- On P2P and P2MP networks, OSPF does not advertise Type-3 links in Type-1 LSAs. Other routing information can still be advertised to ensure traffic forwarding.
- On broadcast and NBMA networks, the DR generates Type-2 LSAs with a mask length of 32 to suppress network routes. Other routing information can still be advertised to ensure traffic forwarding. If no neighbors exist, the DR also does not advertise the primary IP addresses of interfaces in Type-1 LSAs.

Examples

Enable prefix suppression for OSPF process 1.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] prefix-suppression
```

Related commands

ospf prefix-suppression

reset ospf event-log

Use **reset ospf event-log** to clear OSPF log information.

Syntax

reset ospf [*process-id*] **event-log** [**lsa-flush** | **peer** [**slot** *slot-number*] | **spf**]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command clears OSPF log information for all OSPF processes.

lsa-flush: Clears LSA aging log information.

peer: Clears neighbor state change log information.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears neighbor state change information on the member device where the active process resides.

spf: Clears route calculation log information.

Usage guidelines

If you do not specify a log type, this command clears all log information.

Examples

Clear OSPF route calculation log information for all OSPF processes.

```
<Sysname> reset ospf event-log spf
```

Related commands

display ospf event-log

reset ospf event-log hello

Use **reset ospf event-log hello** to clear OSPF log information about received or sent hello packets.

Syntax

reset ospf [*process-id*] **event-log hello** { **received** [**abnormal** | **dropped**] | **sent** [**abnormal** | **failed**] } [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command clears OSPF log information for all processes.

received: Specifies log information for received hello packets.

sent: Specifies log information for sent hello packets.

abnormal: Specifies log information for abnormal hello packets received or sent at intervals greater than or equal to 1.5 times the hello interval.

dropped: Specifies log information for received hello packets that were dropped.

failed: Specifies log information for hello packets that failed to be sent.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears received or sent hello packet log information on the member device where the active process resides.

Examples

Clear sent hello packet log information for all OSPF processes.

```
<Sysname> reset ospf event-log hello sent
```

Related commands

display ospf event-log hello

reset ospf process

Use **reset ospf process** to restart all OSPF processes or a specified process.

Syntax

reset ospf [*process-id*] **process** [**graceful-restart**]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify a process, this command restarts all OSPF processes.

graceful-restart: Resets the OSPF process by using GR.

Usage guidelines

The **reset ospf process** command performs the following actions:

- Clears all invalid LSAs without waiting for their timeouts.
- Makes a newly configured router ID take effect.
- Starts a new DR/BDR election.
- Keeps previous OSPF configurations.

The system prompts you to select whether to restart OSPF process upon execution of this command.

Examples

Restart all OSPF processes.

```
<Sysname> reset ospf process
Reset OSPF process? [Y/N]:y
```

reset ospf redistribution

Use **reset ospf redistribution** to restart route redistribution.

Syntax

reset ospf [*process-id*] **redistribution**

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify a process, this command restarts route redistribution for all OSPF processes.

Examples

Restart route redistribution.

```
<Sysname> reset ospf redistribution
```

reset ospf statistics

Use **reset ospf statistics** to clear OSPF statistics.

Syntax

reset ospf [*process-id*] **statistics**

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

process-id: Clears the statistics for an OSPF process specified by its ID in the range of 1 to 65535.

Examples

Clear OSPF statistics for all processes.

```
<Sysname> reset ospf statistics
```

Related commands

display ospf statistics

rfc1583 compatible

Use **rfc1583 compatible** to enable compatibility with RFC 1583.

Use **undo rfc1583 compatible** to disable compatibility with RFC 1583.

Syntax

rfc1583 compatible

undo rfc1583 compatible

Default

Compatibility with RFC 1583 is enabled.

Views

OSPF view

Predefined user roles

network-admin

context-admin

Usage guidelines

RFC 1583 specifies a different method than RFC 2328 for selecting the optimal route to a destination in another AS. When multiple routes are available to the ASBR, OSPF selects the optimal route by using the following procedure:

1. Selects the route with the highest preference.
   - If RFC 2328 is compatible with RFC 1583, all these routes have equal preference.
   - If RFC 2328 is not compatible with RFC 1583, the intra-area route in a non-backbone area is preferred to reduce the burden of the backbone area. The inter-area route and intra-area route in the backbone area have equal preference.
2. Selects the route with lower cost if two routes have equal preference.
3. Selects the route with larger originating area ID if two routes have equal cost.

To avoid routing loops, set identical RFC 1583-compatibility on all routers in a routing domain.

Examples

Disable compatibility with RFC 1583.

```
<Sysname> system-view
[Sysname] ospf 100
```

```
[Sysname-ospf-100] undo rfc1583 compatible
```

router id

Use **router id** to configure a global router ID.

Use **undo router id** to restore the default.

Syntax

router id *router-id*

undo router id

Default

No global router ID is configured.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

router-id: Specifies the router ID, in the format of an IPv4 address.

Usage guidelines

OSPF uses a router ID to identify a device. If no router ID is specified, the global router ID is used.

If no global router ID is configured, the highest loopback interface IP address is used as the router ID. If no loopback interface IP address is available, the highest physical interface IP address is used, regardless of the interface status (up or down).

During an active/standby process switchover, the new active process checks whether the previously backed up router ID is valid. If not, the process selects a new router ID.

A new router ID is selected only when the interface IP address used as the router ID is removed or changed. Other events will not trigger a router ID re-selection. For example, router ID re-selection is not triggered in the following situations:

- The interface goes down.
- You change the router ID to the address of a loopback interface after a physical interface address is selected as the router ID.
- A higher interface IP address is configured as the router ID.

After a router ID is changed, you must use the **reset** command to enable it.

Examples

Configure a global router ID as 1.1.1.1.

```
<Sysname> system-view
[Sysname] router id 1.1.1.1
```

silent-interface

Use **silent-interface** to disable an interface or all interfaces from receiving and sending OSPF packets.

Use **undo silent-interface** to remove the configuration.

Syntax

silent-interface { *interface-type interface-number* | **all** }

undo silent-interface { *interface-type interface-number* | **all** }

Default

An interface can receive and send OSPF packets.

Views

OSPF view

Predefined user roles

network-admin

context-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

all: Specifies all interfaces.

Usage guidelines

To disable a network from receiving and sending OSPF routes, use the command on the interface connected to the network.

Examples

Disable GigabitEthernet 1/0/1 from receiving and sending OSPF packets.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] silent-interface gigabitethernet 1/0/1
```

snmp trap rate-limit

Use **snmp trap rate-limit** to set the SNMP notification output interval and the maximum number of SNMP notifications that can be output at each interval.

Use **undo snmp trap rate-limit** to restore the default.

Syntax

snmp trap rate-limit interval *trap-interval* **count** *trap-number*

undo snmp trap rate-limit

Default

OSPF outputs a maximum of seven SNMP notifications within 10 seconds.

Views

OSPF view

Predefined user roles

network-admin

context-admin

Parameters

interval *trap-interval*: Specifies the SNMP notification output interval in the range of 2 to 60 seconds.

count *trap-number*: Specifies the number of SNMP notifications output by OSPF at each interval, in the range of 0 to 300. The value of 0 indicates that OSPF does not output SNMP notifications.

Examples

Configure OSPF to output a maximum of 10 SNMP notifications within 5 seconds.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] snmp trap rate-limit interval 5 count 10
```

snmp-agent trap enable ospf

Use **snmp-agent trap enable ospf** to enable SNMP notifications for OSPF.

Use **undo snmp-agent trap enable ospf** to disable SNMP notifications for OSPF.

Syntax

snmp-agent trap enable ospf [**authentication-failure** | **bad-packet** | **config-error** | **grhelper-status-change** | **grrestarter-status-change** | **if-state-change** | **lsa-maxage** | **lsa-originate** | **lsdb-approaching-overflow** | **lsdb-overflow** | **neighbor-state-change** | **nssatranslator-status-change** | **retransmit** | **virt-authentication-failure** | **virt-bad-packet** | **virt-config-error** | **virt-retransmit** | **virtgrhelper-status-change** | **virtif-state-change** | **virtneighbor-state-change**] *

undo snmp-agent trap enable ospf [**authentication-failure** | **bad-packet** | **config-error** | **grhelper-status-change** | **grrestarter-status-change** | **if-state-change** | **lsa-maxage** | **lsa-originate** | **lsdb-approaching-overflow** | **lsdb-overflow** | **neighbor-state-change** | **nssatranslator-status-change** | **retransmit** | **virt-authentication-failure** | **virt-bad-packet** | **virt-config-error** | **virt-retransmit** | **virtgrhelper-status-change** | **virtif-state-change** | **virtneighbor-state-change**] *

Default

SNMP notifications for OSPF are enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

authentication-failure: Specifies notifications about authentication failures on an interface.

bad-packet: Specifies notifications about error messages received on an interface.

config-error: Specifies notifications about error configuration of an interface.

grhelper-status-change: Specifies notifications about GR helper state change.

grrestarter-status-change: Specifies notifications about GR restarter state change.

if-state-change: Specifies notifications about interface state change.

lsa-maxage: Specifies LSA max age notifications.

lsa-originate: Specifies notifications about locally generated LSAs.

lsdb-approaching-overflow: Specifies notifications about approaching LSDB overflows.

lsdb-overflow: Specifies LSDB overflow notifications.

neighbor-state-change: Specifies notifications about neighbor state change.

nssatranslator-status-change: Specifies notifications about NSSA translator state change.

retransmit: Specifies notifications about packets that are received and forwarded on an interface.

virt-authentication-failure: Specifies notifications about authentication failures on a virtual interface.

virt-bad-packet: Specifies notifications about error messages received on a virtual interface.

virt-config-error: Specifies notifications about error configuration of a virtual interface.

virt-retransmit: Specifies notifications about packets that are received and forwarded on a virtual interface.

virtgrhelper-status-change: Specifies notifications about neighbor GR helper state changes of a virtual interface.

virtif-state-change: Specifies notifications about virtual interface state change.

virtneighbor-state-change: Specifies notifications about the neighbor state change of a virtual interface.

Examples

Disable SNMP notifications for OSPF.

```
<Sysname> system-view
[Sysname] undo snmp-agent trap enable ospf
```

spf-schedule-interval

Use **spf-schedule-interval** to set the OSPF SPF calculation interval.

Use **undo spf-schedule-interval** to restore the default.

Syntax

spf-schedule-interval { *maximum-interval* [*minimum-interval* [*incremental-interval*]] | **millisecond** *interval* }

undo spf-schedule-interval

Default

The maximum calculation interval is 5 seconds, the minimum interval is 50 milliseconds, and the incremental interval is 200 milliseconds.

Views

OSPF view

Predefined user roles

network-admin

context-admin

Parameters

maximum-interval: Specifies the maximum OSPF SPF calculation interval in the range of 1 to 60 seconds.

minimum-interval: Specifies the minimum OSPF SPF calculation interval in the range of 10 to 60000 milliseconds.

incremental-interval: Specifies the incremental OSPF SPF calculation interval in the range of 10 to 60000 milliseconds.

millisecond *interval*: Specifies the fixed OSPF SPF calculation interval in the range of 0 to 10000 milliseconds.

Usage guidelines

Based on the LSDB, an OSPF router uses SPF to calculate a shortest path tree with itself as the root. OSPF uses the shortest path tree to determine the next hop to a destination. By adjusting the SPF calculation interval, you can prevent overconsumption of bandwidth and router resources due to frequent topology changes.

After you execute the **spf-schedule-interval** *maximum-interval* [*minimum-interval* [*incremental-interval*]] command, the minimum interval is used for a stable network. If network changes become frequent, the SPF calculation interval increases by the incremental interval × 2^{n-2} for each calculation until the maximum interval is reached. The value *n* is the number of calculation times.

The minimum interval and the incremental interval cannot be greater than the maximum interval.

For a network that requires fast route convergence, use the **spf-schedule-interval millisecond** *interval* command to set a short SPF calculation interval.

Examples

Set the maximum SPF calculation interval to 10 seconds, minimum interval to 500 milliseconds, and incremental interval to 300 milliseconds.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] spf-schedule-interval 10 500 300
```

stub

Use **stub** to configure an area as a stub area.

Use **undo stub** to restore the default.

Syntax

stub [**default-route-advertise-always** | **no-summary**] *

undo stub

Default

No area is a stub area.

Views

OSPF area view

Predefined user roles

network-admin

context-admin

Parameters

default-route-advertise-always: Enables the ABR to advertise a default route in a Type-3 LSA into the stub area regardless of whether **FULL**-state neighbors exist in the backbone area. If you do not specify this keyword, the ABR advertises a default route in a Type-3 LSA into the stub area only when a minimum of one **FULL**-state neighbor exists in the backbone area.

no-summary: Enables the ABR to advertise only a default route in a Type-3 LSA into the stub area without advertising any other Type-3 LSAs. The area is a totally stub area.

Usage guidelines

To configure an area as a stub area, use the **stub** command on all routers attached to the area.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure Area 1 as a stub area.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] stub
```

Related commands

default-cost

stub-router

Use **stub-router** to configure a router as a stub router.

Use **undo stub-router** to restore the default.

Syntax

stub-router [**external-lsa** [*max-metric-value*] | **include-stub** | **on-startup** { *seconds* | **wait-for-bgp** [*seconds*] } | **summary-lsa** [*max-metric-value*]] *

undo stub-router

Default

The router is not configured as a stub router.

Views

OSPF view

Predefined user roles

network-admin

context-admin

Parameters

external-lsa *max-metric-value*: Specifies a cost for the external LSAs, in the range of 1 to 16777215. The default is 16711680.

include-stub: Specifies the cost of the stub links (link type 3) in Router LSAs to the maximum value 65535.

on-startup *seconds*: Specifies the router as a stub router during reboot, and specifies the timeout time in the range of 5 to 86400 seconds.

wait-for-bgp *seconds*: Specifies the router as a stub router during BGP route convergence after reboot, and specifies the timeout time in the range of 5 to 86400 seconds. The default timeout time is 600 seconds.

summary-lsa *max-metric-value*: Specifies a cost for the Type-3 LSAs, in the range of 1 to 16777215. The default cost value is 16711680.

Usage guidelines

The router LSAs sent by the stub router over different links contain different link type values. A value of 3 represents a link to a stub network, and the cost of the link is not changed. A value of 1, 2, or 4 represents a point-to-point link, a link to a transit network, or a virtual link. The cost of these links is set to 65535. Neighbors on such links will not send packets to the stub router as long as they have a route with a smaller cost.

Examples

Configure a stub router.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] stub-router
```

transmit-pacing

Use **transmit-pacing** to set the LSU transmission interval and the maximum number of LSU packets that can be sent at each interval.

Use **undo transmit-pacing** to restore the default.

Syntax

transmit-pacing interval *interval* **count** *count*

undo transmit-pacing

Default

An OSPF interface sends a maximum of three LSU packets every 20 milliseconds.

Views

OSPF view

Predefined user roles

network-admin

context-admin

Parameters

interval *interval*: Specifies an interval at which an interface sends LSU packets, in the range of 0 to 1000 milliseconds. If the router has multiple OSPF interfaces, increase this interval to reduce the total number of LSU packets sent by the router every second. As a best practice to maintain network stability, do not set the interval to 0 milliseconds when the OSPF LSDB is large or network changes are frequent.

count *count*: Specifies the maximum number of LSU packets sent by an interface at each interval, in the range of 1 to 200. If the router has multiple OSPF interfaces, decrease the maximum number to reduce the total number of LSU packets sent by the router every second.

Examples

Configure all the interfaces running OSPF process 1 to send a maximum of 10 LSU packets every 30 milliseconds.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] transmit-pacing interval 30 count 10
```

ttl-security

Use **ttl-security** to enable OSPF GTSM for an area.

Use **undo ttl-security** to disable OSPF GTSM for an area.

Syntax

ttl-security [**hops** *hop-count*]

undo ttl-security

Default

OSPF GTSM is disabled for an OSPF area.

Views

OSPF area view

Predefined user roles

network-admin

context-admin

Parameters

hops *hop-count*: Specifies the hop limit for checking OSPF packets, in the range of 1 to 254. The default hop limit is 1 for packets from common neighbors, and is 255 for packets from virtual link neighbors.

Usage guidelines

After you enable GTSM in area view, GTSM checks OSPF packets from common neighbors and virtual link neighbors.

GTSM protects the device by comparing the TTL value in the IP header of incoming OSPF packets against a valid TTL range. If the TTL value is within the valid TTL range, the packet is accepted. If not, the packet is discarded.

The valid TTL range is from 255 – the configured hop count + 1 to 255.

When GTSM is configured, the OSPF packets sent by the device have a TTL of 255. To use GTSM, you must configure GTSM on both the local and peer devices. You can specify different *hop-count* values for them.

The GTSM configuration in OSPF area view applies to all OSPF interfaces in the area. The GTSM configuration in interface view takes precedence over the configuration in OSPF area view.

As a best practice, set the hop limit if a virtual link exists in an area. You can enable GTSM for the interfaces on the virtual link. If you do not know the interfaces on the virtual link, enable GTSM in area view to prevent packet loss.

Examples

Enable OSPF GTSM for OSPF area 1.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] ttl-security
```

Related commands

ospf ttl-security

vlink-peer

Use **vlink-peer** to configure a virtual link.

Use **undo vlink-peer** to remove a virtual link.

Syntax

vlink-peer *router-id* [**dead** *seconds* | **hello** *seconds* | { { **hmac-md5** | **hmac-sha-256** | **md5** } *key-id* { **cipher** | **plain** } *string* | **keychain** *keychain-name* | **simple** { **cipher** | **plain** } *string* } | **retransmit** *seconds* | **trans-delay** *seconds*] *

undo vlink-peer *router-id* [**dead** | **hello** | { **hmac-md5** | **hmac-sha-256** | **md5** } *key-id* | **keychain** | **retransmit** | **simple** | **trans-delay**] *

Default

No virtual links exist.

Views

OSPF area view

Predefined user roles

network-admin

context-admin

Parameters

router-id: Specifies the router ID of the neighbor on the virtual link.

dead *seconds*: Specifies the dead interval in the range of 1 to 32768 seconds. The default is 40. The dead interval must be identical with that on the virtual link neighbor, and a minimum of four times the hello interval.

hello *seconds*: Specifies the hello interval in the range of 1 to 8192 seconds. The default is 10. It must be identical with the hello interval on the virtual link neighbor.

hmac-md5: Specifies the HMAC-MD5 authentication mode.

hmac-sha-256: Specifies the HMAC-SHA-256 authentication mode.

md5: Specifies the MD5 authentication mode.

simple: Specifies the simple authentication mode.

key-id: Specifies the key ID for MD5 or HMAC-MD5 authentication, in the range of 1 to 255.

cipher: Specifies a key in encrypted form.

plain: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. This argument is case sensitive.

- In simple authentication mode, the plaintext form of the key is a string of 1 to 8 characters. The encrypted form of the key is a string of 33 to 41 characters.
- In MD5/HMAC-MD5/HMAC-SHA-256 authentication mode, the plaintext form of the key is a string of 1 to 255 characters. The encrypted form of the key is a string of 33 to 373 characters.

keychain: Specifies the keychain authentication mode.

keychain-name: Specifies a keychain by its name, a case-sensitive string of 1 to 63 characters.

retransmit *seconds*: Specifies the retransmission interval in the range of 1 to 3600 seconds. The default is 5.

trans-delay *seconds*: Specifies the transmission delay interval in the range of 1 to 3600 seconds. The default is 1.

Usage guidelines

As defined in RFC 2328, all non-backbone areas must maintain connectivity to the backbone. You can use the **vlink-peer** command to configure a virtual link to connect an area to the backbone.

When you configure this command, follow these guidelines:

- The smaller the hello interval is, the faster the network converges, and the more network resources are consumed.
- A retransmission interval that is too small can cause unnecessary retransmissions. A large value is appropriate for a low speed link.
- Specify an appropriate transmission delay with the **trans-delay** keyword.

You can specify either MD5/HMAC-MD5/HMAC-SHA-256 authentication or simple authentication for a virtual link. For MD5/HMAC-MD5/HMAC-SHA-256 authentication, you can configure multiple keys by executing this command multiple times, and each command must have a unique key ID and key string.

To modify the key of a virtual link, perform the following key rollover configurations:

1. Configure a new MD5/HMAC-MD5/HMAC-SHA-256 authentication key for the virtual link on the local device. If the new key is not configured on the neighbor device, MD5/HMAC-MD5/HMAC-SHA-256 authentication key rollover is triggered. During key rollover, OSPF sends multiple packets that contain both the new and old MD5/HMAC-MD5/HMAC-SHA-256 authentication keys to ensure that the neighbor device can pass the authentication.
2. Configure the new MD5/HMAC-MD5/HMAC-SHA-256 authentication key on the neighbor device. When the local device receives packets with the new key from the neighbor device, it exits MD5 key rollover.
3. Delete the old MD5/HMAC-MD5/HMAC-SHA-256 authentication key from the local device and the neighbor. This step helps prevent attacks from devices that use the old key for communication and reduces system resources and bandwidth consumption caused by key rollover.

When keychain authentication is configured for an OSPF virtual link, OSPF performs the following operations before sending a packet:

1. Obtains a valid send key from the keychain.

   OSPF does not send the packet if it fails to obtain a valid send key.
2. Uses the key ID, authentication algorithm, and key string to authenticate the packet.

   If the key ID is greater than 255, OSPF does not send the packet.

When keychain authentication is configured for an OSPF virtual link, OSPF performs the following operations after receiving a packet:

1. Uses the key ID carried in the packet to obtain a valid accept key from the keychain.

   OSPF discards the packet if it fails to obtain a valid accept key.
2. Uses the authentication algorithm and key string for the valid accept key to authenticate the packet.

   If the authentication fails, OSPF discards the packet.

OSPF supports only the MD5, HMAC-SM3, HMAC-MD5, and HMAC-SHA-256 authentication algorithms for keychain authentication.

The ID of keys used for keychain authentication can only be in the range of 0 to 255.

Examples

Configure a virtual link to the neighbor with router ID 1.1.1.1.

```
<Sysname> system-view
```

```
[Sysname] ospf 100
[Sysname-ospf-100] area 2
[Sysname-ospf-100-area-0.0.0.2] vlink-peer 1.1.1.1
```

Related commands

authentication-mode

display ospf vlink

Contents

OSPFv3 commands

abr-summary

Use **abr-summary** to configure route summarization on an ABR.

Use **undo abr-summary** to remove the configuration.

Syntax

abr-summary *ipv6-address prefix-length* [**not-advertise**] [**cost** *cost-value*]

undo abr-summary *ipv6-address prefix-length*

Default

Route summarization is not configured on an ABR.

Views

OSPFv3 area view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address: Specifies the destination IPv6 address of the summary route.

prefix-length: Specifies the prefix length of the destination IPv6 address, in the range of 0 to 128. This argument specifies the number of consecutive 1s of the prefix, which defines the network ID.

not-advertise: Specifies not to advertise the summary IPv6 route. If you do not specify this keyword, the command advertises the IPv6 summary route.

cost *cost-value*: Specifies the cost of the summary route, in the range of 1 to 16777215. The default cost is the largest cost value among routes that are summarized.

Usage guidelines

This command applies only to an ABR to summarize multiple contiguous networks into one network.

To enable ABR to advertise specific routes that have been summarized, use the **undo abr-summary** command.

Examples

Summarize networks 2000:1:1:1::/64 and 2000:1:1:2::/64 in Area 1 into 2000:1:1::/48.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] area 1
[Sysname-ospfv3-1-area-0.0.0.1] abr-summary 2000:1:1:: 48
```

area

Use **area** to create an OSPFv3 area and enter OSPFv3 area view.

Use **undo area** to remove an OSPFv3 area.

Syntax

area *area-id*

undo area *area-id*

Default

No OSPFv3 areas exist.

Views

OSPFv3 view

Predefined user roles

network-admin

context-admin

Parameters

area-id: Specifies an area by its ID, an IPv4 address or a decimal integer in the range of 0 to 4294967295 that is translated into the IPv4 address format.

Examples

Create OSPFv3 Area 0 and enter its view.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] area 0
[Sysname-ospfv3-1-area-0.0.0.0]
```

asbr-summary

Use **asbr-summary** to configure route summarization on an ASBR.

Use **undo asbr-summary** to remove the configuration.

Syntax

asbr-summary *ipv6-address prefix-length* [**cost** *cost-value* | **not-advertise** | **nssa-only** | **tag** *tag*] *

undo asbr-summary *ipv6-address prefix-length*

Default

Route summarization is not configured on an ASBR.

Views

OSPFv3 view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address: Specifies the destination IPv6 address of the summary route.

prefix-length: Specifies the prefix length in the range of 0 to 128.

cost *cost-value*: Specifies the cost of the summary route, in the range of 1 to 16777214. If you do not specify this option, the largest cost among the summarized routes applies. If the routes in

Type-5 LSAs translated from Type-7 LSAs are Type-2 external routes, the largest cost among the summarized routes plus 1 applies.

not-advertise: Disables advertising the summary route. If you do not specify this keyword, the command advertises the route.

nssa-only: Limits the route advertisement to the NSSA area by setting the P-bit of Type-7 LSAs to 0. By default, the P-bit of Type-7 LSAs is set to 1. If the ASBR is also an ABR and **FULL** state neighbors exist in the backbone area, the P-bit of Type-7 LSAs originated by the ASBR is set to 0. This keyword applies to the NSSA ASBR.

tag *tag*: Specifies a tag for the summary route, in the range of 0 to 4294967295.

Usage guidelines

An ASBR can summarize routes in the following LSAs:

- Type-5 LSAs.
- Type-7 LSAs in an NSSA area.
- Type-5 LSAs translated by the ASBR (also an ABR) from Type-7 LSAs in an NSSA area.

  If the ASBR (ABR) is not a translator, it cannot summarize routes in Type-5 LSAs translated from Type-7 LSAs.

To enable ASBR to advertise specific routes that have been summarized, use the **undo asbr-summary** command.

Examples

Configure a summary route 2000::/16, and specify a cost of 100 and a tag value of 2 for the summary route.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] asbr-summary 2000:: 16 cost 100 tag 2
```

authentication-mode

Use **authentication-mode** to specify an authentication mode for an OSPFv3 area.

Use **undo authentication-mode** to restore the default.

Syntax

authentication-mode keychain *keychain-name*

undo authentication-mode

Default

No authentication is performed for an area.

Views

OSPFv3 area view

Predefined user roles

network-admin

context-admin

Parameters

keychain: Specifies the keychain authentication mode.

keychain-name: Specifies a keychain by its name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

The authentication mode specified for an OSPFv3 interface has a higher priority than the mode specified for an OSPFv3 area.

When keychain authentication is configured for an OSPFv3 area, OSPFv3 performs the following operations before sending a packet:

1. Obtains a valid send key from the keychain.

   OSPFv3 does not send the packet if it fails to obtain a valid send key.
2. Uses the key ID, authentication algorithm, and key string to authenticate the packet.

   If the key ID is greater than 65535, OSPFv3 does not send the packet.

When keychain authentication is configured for an OSPFv3 area, OSPFv3 performs the following operations after receiving a packet:

1. Uses the key ID carried in the packet to obtain a valid accept key from the keychain.

   OSPFv3 discards the packet if it fails to obtain a valid accept key.
2. Uses the authentication algorithm and key string for the valid accept key to authenticate the packet.

   If the authentication fails, OSPFv3 discards the packet.

OSPFv3 supports the HMAC-SHA-256 and HMAC-SM3 authentication algorithms for keychain authentication.

The ID of keys used for keychain authentication can only be in the range of 0 to 65535.

Examples

Configure OSPFv3 area 1 to use keychain **test** for packet authentication.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] area 1
[Sysname-ospfv3-1-area-0.0.0.1] authentication-mode keychain test
```

bandwidth-reference

Use **bandwidth-reference** to set a reference bandwidth value for link cost calculation.

Use **undo bandwidth-reference** to restore the default.

Syntax

bandwidth-reference *value*

undo bandwidth-reference

Default

The reference bandwidth value is 100 Mbps for link cost calculation.

Views

OSPFv3 view

Predefined user roles

network-admin

context-admin

Parameters

value: Specifies the reference bandwidth value for link cost calculation, in the range of 1 to 4294967 Mbps.

Usage guidelines

You can configure an OSPFv3 cost for an interface with one of the following methods:

- Configure the cost value in interface view.
- Configure a bandwidth reference value. OSPFv3 computes the cost automatically based on the bandwidth reference value by using the following formula: Interface OSPFv3 cost = Bandwidth reference value / Interface bandwidth.
  - If the calculated cost is greater than 65535, the value of 65535 is used.
  - If the calculated cost is smaller than 1, the value of 1 is used.

If no cost value is configured for an interface, OSPFv3 computes the interface cost value automatically.

Examples

Set the reference bandwidth value to 1000 Mbps.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] bandwidth-reference 1000
```

default tag

Use **default tag** to set a tag for redistributed routes.

Use **undo default tag** to restore the default.

Syntax

default tag *tag*

undo default tag

Default

The tag of redistributed routes is 1.

Views

OSPFv3 view

Predefined user roles

network-admin

context-admin

Parameters

tag: Specifies a tag for redistributed routes, in the range of 0 to 4294967295.

Usage guidelines

If you do not set a tag for redistributed routes by using the **default-route-advertise**, **import-route**, or **route-tag** command, the tag specified by the **default tag** command applies.

Examples

Set the tag for redistributed routes to 2.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] default tag 2
```

Related commands

default-route-advertise

import-route

default-cost

Use **default-cost** to set a cost for the default route advertised to the stub area or NSSA area.

Use **undo default-cost** to restore the default.

Syntax

default-cost *cost*

undo default-cost

Default

The cost is 1.

Views

OSPFv3 area view

Predefined user roles

network-admin

context-admin

Parameters

value: Specifies a cost for the default route advertised to the stub area or NSSA area, in the range of 0 to 16777214.

Usage guidelines

This command takes effect only on the ABR of a stub area or the ABR or ASBR of an NSSA area.

Examples

Configure Area 1 as a stub area, and set the cost of the default route advertised to the stub area to 60.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] area 1
[Sysname-ospfv3-1-area-0.0.0.1] stub
[Sysname-ospfv3-1-area-0.0.0.1] default-cost 60
```

Related commands

nssa

stub

default-route-advertise

Use **default-route-advertise** to redistribute a default route into the OSPFv3 routing domain.

Use **undo default-route-advertise** to restore the default.

Syntax

default-route-advertise [[**always** | **permit-calculate-other**] | **cost** *cost-value* | **route-policy** *route-policy-name* | **tag** *tag* | **type** *type*] *

undo default-route-advertise

Default

No default route is redistributed into the OSPFv3 routing domain.

Views

OSPFv3 view

Predefined user roles

network-admin

context-admin

Parameters

always: Redistributes a default route in an AS-external-LSA into the OSPFv3 routing domain regardless of whether a default route exists in the routing table. If you do not specify this keyword, the router redistributes a default route in an AS-external-LSA into the OSPFv3 routing domain only when the default route exists in the routing table.

permit-calculate-other: Enables OSPFv3 to calculate default routes received from other routers. If you do not specify this keyword, OSPFv3 does not calculate default routes from other routers. If the router does not redistribute any default route in an AS-external-LSA into the OSPFv3 routing domain, the router calculates default routes from other routers. It calculates these routes regardless of whether this keyword is specified.

cost *cost-value*: Specifies a cost for the default route, in the range of 0 to 16777214. The default is 1.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters. When the routing policy is matched and one of the following conditions is met, the command redistributes a default route in an AS-external-LSA into the OSPFv3 routing domain:

- A default route exists in the routing table.
- The **always** keyword is specified.

The routing policy modifies values in the AS-external-LSA.

tag *tag*: Specifies a tag for the default route, in the range of 0 to 4294967295. If you do not specify this option, the tag specified by the **default tag** command applies.

type *type*: Specifies a type for the AS-external-LSA, 1 or 2. The default is 2.

Usage guidelines

This command redistributes a default route in an AS-external-LSA, which cannot be redistributed with the **import-route** command. If the local routing table has no default route, you must provide the **always** keyword for the command.

Examples

Redistribute a default route into the OSPFv3 routing domain. (The default route does not exist in the local router.)

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] default-route-advertise always
```

Related commands

import-route

display ospfv3

Use **display ospfv3** to display OSPFv3 process information.

Syntax

display ospfv3 [*process-id*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays information about all OSPFv3 processes.

verbose: Displays detailed OSPFv3 process information. If you do not specify this keyword, the command displays brief OSPFv3 process information.

Examples

Display detailed information about all OSPFv3 processes.

```
<Sysname> display ospfv3 verbose

               OSPFv3 Process 1 with Router ID 1.1.1.1

 RouterID: 1.1.1.1          Router type:  ABR  ASBR  NSSA
 Route tag: 0
 Route tag check: Disabled
 Multi-VPN-Instance: Disabled
 Type value of extended community attributes:
    Domain ID : 0x0005
    Route type: 0x0306
    Router ID : 0x0107
 Domain-id: 0.0.0.0
 DN-bit check: Enabled
 DN-bit set: Enabled
 Originating router-LSAs with maximum metric
    Condition: On startup for 600 seconds, State: Inactive
    Advertise summary-LSAs with metric 16711680
    Advertise external-LSAs with metric 16711680
    Advertise intra-area-prefix-LSAs with maximum metric
 Originating LSAs with metric 65500 controlled by RBM
 SPF-schedule-interval: 5 50 200
 LSA generation interval: 5
 LSA arrival interval: 1000
 Transmit pacing: Interval: 20 Count: 3
 Default ASE parameters: Tag: 1
```

```
Route preference: 10
ASE route preference: 150
FRR backup mode: LFA
SPF calculation count: 0
External LSA count: 0
LSA originated count: 0
LSA received count: 0
SNMP trap rate limit interval: 10  Count: 7
Area count: 2  Stub area count: 0  NSSA area count: 1
ExChange/Loading neighbors: 0
Max equal cost paths: 32
Up interfaces: 1
Full neighbors: 1
Normal areas with up interfaces: 1
Calculation trigger type: Full
Current calculation type: SPF calculation
Current calculation phase: Calculation area topology
Redistribute timer: Off
Redistribute schedule type: RIB
Redistribute route count: 0
Process reset state: N/A
Current reset type: N/A
Next reset type: N/A
Reset prepare message replied: -/-/-/-
Reset process message replied: -/-/-/-
Reset phase of module:
  M-N/A, P-N/A, S-N/A, C-N/A, R-N/A

Area: 0.0.0.0
Area flag: Normal
SPF scheduled count: 0
ExChange/Loading neighbors: 0
LSA count: 0
Keychain authentication: Enabled (chris)
Up interfaces: 0
MTU: 1440
Default cost: 1
Created by Vlink
Process reset state: N/A
Current reset type: N/A
Reset prepare message replied: -/-/-/-
Reset process message replied: -/-/-/-
Reset phase of module:
  M-N/A, P-N/A, S-N/A, C-N/A, R-N/A

Area: 0.0.0.2
Area flag: Normal
SPF scheduled count: 0
```

```
ExChange/Loading neighbors: 0
LSA count: 0
IPsec profile name: Profile000
Up interfaces: 1
MTU: 1500
Default cost: 1
Process reset state: N/A
Current reset type: N/A
Reset prepare message replied: -/-/-/-
Reset process message replied: -/-/-/-
Reset phase of module:
  M-N/A, P-N/A, S-N/A, C-N/A, R-N/A

Area: 0.0.0.3
Area flag: NSSA
7/5 translator state: Disabled
7/5 translate stability timer interval: 0
SPF Scheduled Count: 0
ExChange/Loading neighbors: 0
LSA Count: 0
Up interfaces: 0
MTU: 1440
Default cost: 1
Process reset flag: N/A
Current reset type: N/A
Reset prepare message replied: -/-/-/-
Reset process message replied: -/-/-/-
Reset phase of module:
  M-N/A, P-N/A, S-N/A, C-N/A, R-N/A
```

Table 1 Command output

Field	Description
OSPFv3 Process 1 with Router ID 1.1.1.1	OSPFv3 process is 1, and router ID is 1.1.1.1.
Router type	Router type: • ABR. • ASBR. • NSSA. • Null.
Route tag	Tag of the routes redistributed into the OSPFv3 process.
Route tag check	Whether the check is enabled for the route tag in OSPFv3 LSAs of the OSPFv3 process.
Multi-VPN-Instance	Whether the OSPFv3 process supports multiple VPN instances: • **Multi-VPN-Instance: Disabled**—The process does not support multiple VPN instances. • **Multi-VPN-Instance: Enabled**—The process supports multiple VPN instances.

Field	Description
DN-bit check	Whether the check is enabled for the DN bit in OSPFv3 LSAs of the OSPFv3 process.
DN-bit set	Whether the DN bit is set for OSPFv3 LSAs in the OSPFv3 process.
Condition	Time when the router acts as a stub router: • Always. • On startup while BGP is converging for *xxx* seconds, where *xxx* is specified by the user. • On startup for *xxx* seconds, where *xxx* is specified by the user.
State	State of the stub router: • Active. • Inactive.
Originating LSAs with metric *xxx* controlled by RBM	The device is the backup device in Remote Backup Management (RBM). • **Originating LSAs with metric +*n* controlled by RBM**—When OSPFv3 generates an LSA, the cost is the sum of the original cost and *n.* • **Originating LSAs with metric *n* controlled by RBM**—When OSPFv3 generates an LSA, the cost is *n.* This field is displayed only when RBM has adjusted the OSPFv3 cost.
SPF-schedule-interval	Interval for SPF calculations.
Transmit pacing	LSU advertisement rate: • **Interval**—Specifies the interval for sending LSUs. • **Count**—Specifies the maximum number of LSUs sent at each interval.
Default ASE parameters	Default parameters of redistributed routes. **Tag** represents the route tag of the redistributed routes.
Route preference	Internal route preference.
ASE route preference	AS-external route preference.
FRR backup mode	FRR backup mode: • **LFA**—Uses the LFA algorithm to calculate a backup next hop for all routes. **LFA ABR-only** indicates that only the next hop of the route to the ABR can be used as the backup next hop. • **route-policy** *route-policy-name*—Specifies a backup next hop by using a routing policy.
LSA originated count	Number of originated LSAs.
LSA received count	Number of received LSAs.
SNMP trap rate limit interval: 10 Count: 7	OSPFv3 can output a maximum of 7 SNMP notifications within 10 seconds.
Area count	Total number of areas.
Stub area count	Number of stub areas.
NSSA area count	Number of NSSA areas.
ExChange/Loading neighbors	Neighbors in ExChange/Loading state.

Field	Description
Calculation trigger type	Route calculation trigger type: • **Full**—Calculation of all routes is triggered. • **Area topology change**—Topology change in an area. • **Intra router change**—Incremental intra-area route change. • **ASBR change**—Incremental ASBR route change. • **Full IP prefix**—Calculation of all IP prefixes is triggered. • **Full intra AS**—Calculation of all intra-AS prefixes is triggered. • **Inc intra AS**—Calculation of incremental intra-AS prefixes is triggered. • **Full inter AS**—Calculation of all AS-external prefixes is triggered. • **Inc inter AS**—Calculation of incremental AS-external prefixes is triggered. • **Nexthop calculation**—Calculation of next hops is triggered. • **N/A**—Route calculation is not triggered.
Current calculation type	Current route calculation type: • SPF calculation. • **Intra router calculation**—Intra-area route calculation. • **ASBR calculation**—Inter-area ASBR route calculation. • **Inc intra router**—Incremental intra-area route calculation. • **Inc ASBR calculation**—Incremental inter-area ASBR route calculation. • **Full intra AS**—Calculation of all intra-AS prefixes. • **Inc intra AS**—Calculation of incremental intra-AS prefixes. • **Full inter AS**—Calculation of all AS-external prefixes. • **Inc inter AS**—Calculation of incremental AS-external prefixes. • **N/A**—Route calculation is not triggered.
Current calculation phase	Current route calculation phase: • **Calculation area topology**—Calculating area topology. • **Calculation router**—Calculating routes on routers. • **Calculation intra AS**—Calculating intra-AS routes. • **Calculation ASBR**—Calculating routes on ASBRs. • **Calculation inter AS**—Calculating AS-external routes. • **Calculation end**—Ending phase of calculation. • **N/A**—Route calculation is not triggered.
Redistribute timer	Route redistribution timer status: on or off.
Redistribute schedule type	Route redistribution scheduling type: • **RIB**—Redistribute routes through the RIB table. • **Self**—Redistribute routes through the routing table. • **N/A**—Route redistribution is not triggered.
Redistribute route count	Number of redistributed routes.

Field	Description
Process reset state	Process reset state: • **N/A**—The process is not reset. • **Under reset**—The process is in the reset progress. • **Under RIB smooth**—The process is synchronizing RIB routes.
Current reset type	Current process reset type: • **N/A**—The process is not reset. • **GR quit**—Normal reset when GR quits abnormally. • **Delete**—Delete OSPFv3 process. • **Undo router-id**—Delete router ID. • **Set router-id**—Set router ID.
Next reset type	Next process reset type: • **N/A**—The process is not reset. • **GR quit**—Normal reset when GR quits abnormally. • **Delete**—Delete OSPFv3 process. • **Undo router-id**—Delete router ID. • **Set router-id**—Set router ID.
Reset prepare message replied	Modules that reply reset prepare messages: • **P**—Neighbor maintenance module. • **S**—LSDB synchronization module. • **C**—Route calculation module. • **R**—Route redistribution module.
Reset process message replied	Modules that reply reset process messages: • **P**—Neighbor maintenance module. • **S**—LSDB synchronization module. • **C**—Route calculation module. • **R**—Route redistribution module.

Reset phase of module	Reset phase of each module:
	• LSDB synchronization (S) module:
	  ◦ **N/A**—Not reset.
	  ◦ **Delete ASE**—Delete all ASE LSAs.
	  ◦ **Delete area LSA**—Delete LSAs from an area.
	  ◦ **Delete area IF**—Delete interfaces from an area.
	• Route calculation (C) module:
	  ◦ **N/A**—Not reset.
	  ◦ **Delete topology**—Delete area topology.
	  ◦ **Delete router**—Delete routes of routers.
	  ◦ **Delete intra AS**—Delete intra-AS routes
	  ◦ **Delete inter AS**—Delete AS-external routes.
	  ◦ **Delete ASBR**—Delete ASBR routes.
	• Route redistribution (R) module:
	  ◦ **N/A**—Not reset.
	  ◦ **Delete import**—Delete redistributed routes.

IPsec profile name	IPsec profile applied to the area.
Keychain authentication: Enabled (test)	Keychain authentication is enabled for the area, and keychain **test** is used.
Created by Vlink	The area is created through virtual link.

Field	Description
7/5 translator state	State of the translator that translates Type-7 LSAs to Type-5 LSAs: • **Enabled**—The translator is specified through commands. • **Elected**—The translator is designated through election. • **Disabled**—The device is not a translator.
7/5 translate stability timer interval	Stability interval (in seconds) for Type-7 LSA-to-Type-5 LSA translation.

display ospfv3 abr-asbr

Use **display ospfv3 abr-asbr** to display information about the routes to OSPFv3 ABR and ASBR.

Syntax

display ospfv3 [*process-id*] **abr-asbr**

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays information about all the routes to the OSPFv3 ABR and ASBR.

Examples

Display information about all the routes to the OSPFv3 ABR and ASBR.

```
<Sysname> display ospfv3 abr-asbr

              OSPFv3 Process 1 with Router ID 1.1.1.1

Destination : 1.1.1.2                                Rtr Type : ABR
 Area        : 0.0.0.0                                Path Type: Intra
 Interface   : GE1/0/2                               BkInterface: GE1/0/1
 NextHop     : FE80:1:1::1
 BkNexthop   : FE80:1:2::2
 Cost        : 1

 Destination : 1.1.1.3                                Rtr Type : ASBR
 Area        : 0.0.0.0                                Path Type: Intra
 Interface   : GE1/0/3                               BkInterface: GE1/0/4
 NextHop     : FE80:2:1::1
```

```
BkNexthop   : FE80:1:2::4
Cost        : 1
```

Table 2 Command output

Field	Description
OSPFv3 Process 1 with Router ID 1.1.1.1	OSPFv3 process is 1, and router ID is 1.1.1.1.
Destination	Router ID of an ABR or ASBR.
Rtr Type	Router type: ABR or ASBR.
Area	Area ID of the next hop.
Path Type	Type of the route to the ABR or ASBR: • **Intra**—Intra-area route. • **Inter**—Inter-area route.
Interface	Output interface.
BkInterface	Backup output interface.
NextHop	Next hop address.
BkNexthop	Backup next hop address.
Cost	Cost from the router to the ABR or ASBR.

display ospfv3 abr-summary

Use **display ospfv3 abr-summary** to display ABR summary route information.

Syntax

display ospfv3 [*process-id*] [**area** *area-id*] **abr-summary** [*ipv6-address prefix-length*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays information about ABR summary routes for all OSPFv3 processes.

area *area-id*: Specifies an OSPFv3 area by its ID. The area ID is an IP address or a decimal integer in the range of 0 to 4294967295 that is translated into the IP address format. If you do not specify this option, the command displays information about ABR summary routes for all OSPFv3 areas.

ipv6-address prefix-length: Specifies an IPv6 address. The *ipv6-address* argument specifies an IPv6 prefix. The *prefix-length* argument specifies a prefix length in the range of 0 to 128. If you do not specify this argument, the command displays information about all summary routes on the ABR.

verbose: Displays detailed ABR summary route information. If you do not specify this keyword, the command displays brief ABR summary route information.

Examples

Display brief ABR summary route information in OSPFv3 process 1.

```
<Sysname> display ospfv3 1 abr-summary

            OSPFv3 Process 1 with Router ID 2.2.2.2

                    Area: 1.1.1.1
 Total summary addresses: 1

 Prefix      : 1000:4::/32
 Status      : Advertise
 NULL0       : Active
 Cost        : 1 (Configured)
 Routes count: 2
```

Table 3 Command output

Field	Description
Area	Area to which the summary routes belong.
Total summary addresses	Total number of summary routes.
Prefix	Prefix of the summary route.
Status	Advertisement status of the summary route.
NULL0	Null 0 route.
Cost	Cost of the summary route.
Routes count	Number of summarized routes.

Display detailed ABR summary route information in OSPFv3 process 1.

```
<Sysname> display ospfv3 1 abr-summary verbose

            OSPFv3 Process 1 with Router ID 2.2.2.2

                       Area: 1.1.1.1
Total summary addresses: 1

 Prefix      : 1000:4::/32
 Status      : Advertise
 NULL0       : Active
 Cost        : 1 (Configured)
 Routes count: 2
   Destination                                    Metric
   1000:4:10:3::/96                               1
   1000:4:11:3::/96                               1
```

Table 4 Command output

Field	Description
Destination	Destination address of a summarized route.
Metric	Metric of a summarized route.

display ospfv3 asbr-summary

Use **display ospfv3 asbr-summary** to display ASBR summary route information.

Syntax

display ospfv3 [*process-id*] **asbr-summary** [*ipv6-address prefix-length*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays information about ASBR summary routes for all OSPFv3 processes.

ipv6-address prefix-length: Specifies an IPv6 address. The *ipv6-address* argument specifies an IPv6 prefix. The *prefix-length* argument specifies a prefix length in the range of 0 to 128. If you do not specify this argument, the command displays information about all ASBR summary routes.

verbose: Displays detailed ASBR summary route information. If you do not specify this keyword, the command displays brief ASBR summary route information.

Examples

Display brief ASBR summary route information in OSPFv3 process 1.

```
<Sysname> display ospfv3 1 asbr-summary

              OSPFv3 Process 1 with Router ID 2.2.2.2

 Total summary addresses: 1

 Prefix      : 1000:4::/32
 Status      : Advertise
 NULL0       : Active
 Cost        : 1 (Configured)
 Tag         : (Not configured)
 Nssa-only   : (Not configured)
 Routes count: 2
```

Table 5 Command output

Field	Description
Total summary addresses	Total number of summary routes.
Prefix	Prefix and prefix length of the summary route.
Status	Advertisement status of the summary route: • **Advertise**—The summary route has been advertised. • **Not-advertise**—The summary route has not been advertised.
NULL0	Status of the Null 0 route: • Active. • Inactive.
Cost	Cost of the summary route: • Configured. • Not configured.
Tag	Tag of the summary route: • Configured. • Not configured.
Nssa-only	Whether the **nssa-only** attribute is configured: • Configured. • Not configured.
Routes count	Number of summarized routes.

Display detailed ASBR summary route information in OSPFv3 process 1.

```
<Sysname> display ospfv3 1 asbr-summary verbose

              OSPFv3 Process 1 with Router ID 2.2.2.2

 Total summary addresses: 1

 Prefix      : 1000:4::/32
 Status      : Advertise
 NULL0       : Active
 Cost        : 1 (Configured)
 Tag         : (Not configured)
 Nssa-only   : (Not configured)
 Routes count: 2
  Destination                                Protocol Process Type Metric
  1000:4:10:3::/96                           Static   0       2    1
  1000:4:11:3::/96                           Static   0       2    1
```

Table 6 Command output

Field	Description
Destination	Prefix and prefix length of the summarized route.
Protocol	Routing protocol from which the route was redistributed.

Field	Description
Process	Process of the routing protocol from which the route was redistributed.
Type	Type of the summarized route.
Metric	Metric of the summarized route.

display ospfv3 event-log

Use **display ospfv3 event-log** to display OSPFv3 log information.

Syntax

display ospfv3 [*process-id*] **event-log** { **lsa-flush** | **peer** | **spf** }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays OSPFv3 log information for all processes.

lsa-flush: Specifies LSA aging log information.

peer: Specifies neighbor log information.

spf: Specifies route calculation log information.

Usage guidelines

Route calculation logs show the number of routes newly installed in the IPv6 routing table.

Neighbor logs include information about the following events:

- The OSPFv3 neighbor state goes down.
- The OSPFv3 neighbor state goes backward because the local end receives BadLSReq, SeqNumberMismatch, and 1-Way events.

Examples

Display OSPFv3 LSA aging log information for OSPFv3 process 1.

```
<Sysname>display ospfv3 1 event-log lsa-flush

              OSPFv3 Process 1 with Router ID 1.3.3.3

 2014-09-02 07:55:25 Received MaxAge LSA from 1.1.1.1
 Type: 3   LS ID: 0.0.0.2         AdvRtr: 1.1.1.1          Seq#: 80000001

 2014-09-02 07:55:22 Flushed MaxAge LSA by itself
 Type: 3   LS ID: 0.0.0.2         AdvRtr: 1.3.3.3          Seq#: 80000001
```

```
2014-09-02 07:55:07 Flushed MaxAge LSA by itself
Type: 3   LS ID: 0.0.0.40        AdvRtr: 1.3.3.3          Seq#: 80000001

2014-09-02 07:55:07 Flushed MaxAge LSA by itself
Type: 3   LS ID: 0.0.0.39        AdvRtr: 1.3.3.3          Seq#: 80000001
```

Table 7 Command output

Field	Description
Received MaxAge LSA from X.X.X.X	The device received an LSA that has reached the maximum age from X.X.X.X.
Flushed MaxAge LSA by itself	The device flushed the LSA that has reached the maximum age.
Type	LSA type.
LS ID	LSA link state ID.
AdvRtr	Advertising router.
Seq#	LSA sequence number.

Display OSPFv3 route calculation log information for OSPFv3 process 1.

```
<Sysname>display ospfv3 1 event-log spf

              OSPFv3 Process 1 with Router ID 1.3.3.3

Date       Time     Duration   Intra   Inter   External Reason
2014-09-02 07:55:30 0.258827   0       0       0        Intra-area LSA
2014-09-02 07:55:30 0.679      0       0       0        Intra-area LSA
2014-09-02 07:55:30 0.51576    0       0       0        Intra-area LSA
2014-09-02 07:55:30 0.372      0       0       0        Intra-area LSA
2014-09-02 07:55:25 4.948353   0       0       0        Intra-area LSA
2014-09-02 07:55:25 0.5288     0       0       0        Area 0 full neighbor
2014-09-02 07:55:21 1.66013    0       0       0        Intra-area LSA
2014-09-02 07:55:20 0.450905   0       0       0        Intra-area LSA
2014-09-02 07:55:15 0.253688   0       0       0        Interface state change
2014-09-02 07:55:15 0.5693     0       0       0        Intra-area LSA
```

Table 8 Command output

Field	Description
Date	Date when the route calculation starts, in YYYY-MM-DD format. YYYY represents the year, MM represents the month, and DD represents the day.
Time	Time when the route calculation starts, in hh:mm:ss format. hh represents the hours, mm represents the minutes, and ss represents the seconds.
Duration	Duration of the route calculation, in seconds.
Intra	Number of intra-area routes newly installed in the IPv6 routing table.
Inter	Number of inter-area routes newly installed in the IPv6 routing table.
External	Number of external routes newly installed in the IPv6 routing table.

Field	Description
Reason	Reasons why the route calculation is performed: • **Intra-area LSA**—Intra-area LSA changes. • **Inter-area LSA**—Inter-area LSA changes. • **External LSA**—External LSA changes. • **Configuration**—Configuration changes. • **Area 0 full neighbor**—Number of **FULL**-state neighbors in Area 0 changes. • **Area 0 up interface**—Number of interfaces in up state in Area 0 changes. • **AS number**—AS number changes. • **ABR summarization**—ABR summarization changes. • **GR end**—GR ends. • **Routing policy**—Routing policy changes. • **Intra-area tunnel**—Intra-area tunnel changes. • **Others**—Other reasons.

Display OSPFv3 neighbor log information for OSPFv3 process 1.

```
<Sysname> display ospfv3 1 event-log peer

              OSPFv3 Process 1 with Router ID 1.1.1.1

Date       Time     Router ID       Reason       InstID  Interface
2014-09-02 16:39:13 1.3.3.3         IntPhyChange 0       GE1/0/1
2014-09-02 16:36:46 1.3.3.3         IntPhyChange 0       GE1/0/1
2014-09-02 16:34:49 1.3.3.3         BFDDown      0       GE1/0/1
2014-09-02 10:08:45 1.3.3.3         DeadExpired  0       GE1/0/2
2014-09-02 10:08:39 1.3.3.3         DeadExpired  0       VLINK1
2014-09-02 10:08:08 1.3.3.3         BFDDown      0       GE1/0/1
```

Table 9 Command output

Field	Description
Date	Date when the neighbor state changes, in YYYY-MM-DD format. YYYY represents the year, MM represents the month, and DD represents the day.
Time	Time when the neighbor state changes, in hh:mm:ss format. hh represents the hours, mm represents the minutes, and ss represents the seconds.
Router ID	Neighbor router ID.

Field	Description
Reason	Reasons for neighbor state changes: • **ResetConnect**—The connection is lost due to insufficient memory. • **IntChange**—The interface parameter has changed. • **ResetOspfv3**—The OSPFv3 process is reset. • **UndoOspfv3**—The OSPFv3 process is deleted. • **UndoArea**—The OSPFv3 area is deleted. • **UndoInt**—The interface is disabled. • **IntLogChange**—The logical attribute of the interface has changed. • **IntPhyChange**—The physical attribute of the interface has changed. • **DeadExpired**—The dead timer expires. • **Retrans**—Excessive retransmissions. • **BFDDown**—The interface is shut down by BFD. • **SilentInt**—The interface is configured as a silent interface. • **ConfStubArea**—The interface is configured with stub area parameters. • **ConfNssaArea**—The interface is configured with NSSA area parameters. • **VlinkDown**—The virtual link goes down. • **BadLSReq**—The interface receives BadLSReq events. • **SeqMismatch**—The interface receives SeqNumberMismatch events. • **Way**—The interface receives 1-Way events.
InstID	Instance ID for an interface.
Interface	Interface name.

display ospfv3 graceful-restart

Use **`display ospfv3 graceful-restart`** to display GR information.

Syntax

`display ospfv3` [*`process-id`*] **`graceful-restart`** [**`verbose`**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

`process-id`: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays GR information for all processes.

`verbose`: Displays detailed GR information. If you do not specify this keyword, the command displays brief GR information.

Examples

Display brief GR information for all OSPFv3 processes (GR restarter).

```
<Sysname> display ospfv3 graceful-restart

               OSPFv3 Process 1 with Router ID 3.3.3.3

 Graceful-restart capability     : Enable
 Graceful-restart support        : Planned and un-planned, Partial
 Helper capability               : Enable
 Helper support                  : Planned and un-planned
 Current GR state                : Normal
 Graceful-restart period         : 120 seconds
 Number of neighbors under helper: 0
 Number of restarting neighbors  : 0
 Last exit reason:
   Restarter: None
   Helper   : None
```

Table 10 Command output

Field	Description
OSPFv3 Process 1 with Router ID 3.3.3.3	The GR status of OSPFv3 process 1 with router ID 3.3.3.3 is displayed.
Graceful-restart capability	Whether OSPFv3 GR is enabled: • Enabled. • Disabled.
Graceful-restart support	GR modes that the process supports (displayed only when GR is enabled): • **Planned and un-planned**—Supports both planned and unplanned GR. • **Planned only**—Supports only planned GR. • **Partial**—Supports partial GR. • **Global**—Supports global GR.
Helper capability	Whether OSPFv3 GR helper is enabled: • Enabled. • Disabled.
Helper support	Policies and GR modes that the GR helper supports (displayed only when GR helper is enabled): • **Strict LSA check**—The GR helper supports strict LSA checking. • **Planned and un-planned**—The GR helper supports both planned and unplanned GR. • **Planned only**—The GR helper supports only planned GR.
Current GR state	GR status: • **Normal**—GR is not in progress or has completed. • **Under GR**—GR is in progress. • **Under Helper**—The process is acting as GR helper.
Graceful-restart period	GR restart interval.

Field	Description
Number of neighbors under helper	Number of neighbors in GR helper status.
Number of restarting neighbors	Number of neighbors in GR restarter status.

Last exit reason	Last exit reason:
	• **Restarter**—Reason that the restarter exited most recently:
	  ○ None.
	  ○ **Completed**—GR is completed.
	  ○ **Interval timer is fired**—The GR timer expires.
	  ○ **Interface state change**—An interface state change occurs.
	  ○ **Received 1-way hello**—The device receives 1-way hello packets from the neighbor.
	  ○ **Reset neighbor**—The neighbor is reset.
	  ○ **DR or BDR change**—The DR or BDR changes.
	• **Helper**—Reason that the helper exited most recently:
	  ○ None.
	  ○ **Completed**—GR is completed.
	  ○ **Received 1-way hello**—The device receives 1-way hello packets from the neighbor.
	  ○ **Grace Period timer is fired**—The GR timer expires.
	  ○ **Lsa check failed**—An LSA change on the GR helper is detected.
	  ○ **Reset neighbor**—The neighbor is reset.
	  ○ **Received MAXAGE gracelsa but neighbor is not full**—The device receives Grace-LSAs that reached the maximum age, but the neighbor is not in Full state.

Display detailed GR information for all OSPFv3 processes (GR restarter).

```
<Sysname> display ospfv3 graceful-restart verbose

               OSPFv3 Process 1 with Router ID 3.3.3.3

 Graceful-restart capability     : Enable
 Graceful-restart support        : Planned and un-planned, Partial
 Helper capability               : Enable
 Helper support                  : Planned and un-planned
 Current GR state                : Normal
 Graceful-restart period         : 120 seconds
 Number of neighbors under helper: 0
 Number of restarting neighbors  : 0
 Last exit reason:
   Restarter: None
   Helper   : None

 Area: 0.0.0.0
 Area flag: Normal
 Area up interface count: 1
```

```
Virtual-link Neighbor-ID: 100.1.1.1, Neighbor-state: Full
Restarter state: Normal   State: P-2-P    Type: Virtual
Interface: 6696 (GigabitEthernet1/0/2), Instance-ID: 0
Local  IPv6 address: 200:1:FFFF::1
Remote IPv6 address: 201:FFFF::2
Transit area: 0.0.0.1
Last exit reason:
  Restarter: None
  Helper   : None
Neighbor       GR state       Last helper exit reason
100.1.1.1      Normal         None

Area: 0.0.0.1
Area flag: Transit
Area up interface count: 3

Interface: 5506 (GigabitEthernet1/0/3), Instance-ID: 0
Restarter state: Normal   State: DR       Type: Broadcast
Last exit reason:
  Restarter: None
  Helper   : None
Neighbor count of this interface: 0
Number of neighbors under helper: 0

Interface: 6696 (GigabitEthernet1/0/2), Instance-ID: 0
Restarter state: Normal   State: DR       Type: Broadcast
Last exit reason:
  Restarter: None
  Helper   : None
Neighbor count of this interface: 1
Number of neighbors under helper: 0
Neighbor       GR state       Last helper exit reason
100.1.1.1      Normal         None

Sham-link Neighbor-ID: 100.1.1.1, Neighbor-state: Full
Restarter state: Normal   State: P-2-P    Type: Sham
Interface-ID: 2147483649, Instance-ID: 0
Source      : 8000:88::FFFF
Destination : 7000:77::FFFF
Last exit reason:
  Restarter: None
  Helper   : None
Neighbor       GR state       Last helper exit reason
100.1.1.1      Normal         None

Area: 0.0.0.5
Area flag: NSSANoSummaryNoImportRoute
```

```
7/5 translator state: Disabled
7/5 translate stability timer interval: 0
Area up interface count: 0
```

Table 11 Command output

Field	Description
Area	Area ID.
Area flag	Type of the area: • Normal. • Transit. • Stub. • **StubNoSummary**—Totally stub area. • NSSA. • **NSSANoSummary**—Totally NSSA area. • **NSSANoSummaryNoImportRoute**—Totally NSSA area with the **no-import-route** keyword configured.
7/5 translator state	State of the translator that translates Type-7 LSAs to Type-5 LSAs: • **Enabled**—The translator is specified through commands. • **Elected**—The translator is designated through election. • **Disabled**—The device is not a translator.
7/5 translate stability timer interval	Stability interval (in seconds) for Type-7 LSA-to-Type-5 LSA translation.
Area up interface count	Number of up interfaces in the area.
Interface	Interface in the area, or the output interface of the virtual link.
Restarter state	Restarter state on the interface.
State	Interface state.
Type	Interface network type.
Neighbor count of this interface	Number of neighbors on the interface.
Neighbor	Neighbor router ID.
GR state	Neighbor GR state: • **Normal**—GR is not in progress or has completed. • **Under GR**—GR is in process. • **Under Helper**—The process is acting as GR helper.
Last helper exit reason	Reason that the helper exited most recently.
Virtual-link Neighbor-ID	Router ID of the virtual link's neighbor.
Neighbor-State	Neighbor or virtual link state: Down, Init, 2-Way, ExStart, Exchange, Loading, and Full.
Local IPv6 address	Local IPv6 address of the neighbor relationship.
Remote IPv6 address	Peer IPv6 address of the neighbor relationship.
Transit area	Transit area ID.

display ospfv3 interface

Use **display ospfv3 interface** to display OSPFv3 interface information.

Syntax

display ospfv3 [*process-id*] **interface** [*interface-type interface-number* | **verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535.

interface-type interface-number: Specifies an interface by its type and number.

verbose: Displays detailed information about all OSPFv3 interfaces.

Usage guidelines

If you do not specify a process, this command displays brief OSPFv3 interface information for all processes.

If you do not specify the *interface-type interface-number* argument or the **verbose** keyword, this command displays brief information about all OSPFv3 interfaces.

Examples

Display OSPFv3 information about GigabitEthernet 1/0/1.

```
<Sysname> display ospfv3 interface gigabitethernet 1/0/1

               OSPFv3 Process 1 with Router ID 1.1.1.1

 Area: 0.0.0.0
----------------------------------------------------------------------------
 GigabitEthernet1/0/1 is up, line protocol is up
  Interface ID 3        Instance ID 0
  IPv6 prefixes
    FE80::200:12FF:FE34:1  (Link-Local address)
    2001::1
  Cost: 1       State: BDR       Type: Broadcast    MTU: 1500
  Priority: 1
  Designated router: 2.2.2.2
  Backup designated router: 1.1.1.1
  Timers: Hello 10, Dead 40, Poll 40, Retransmit 5, Transmit delay 1
  FRR backup: Enabled
  Neighbor count is 1, Adjacent neighbor count is 1
  Primary path detection mode: BFD echo
  IPsec profile name: profile001
```

```
Exchanging/Loading neighbors: 0
Wait timer: Off,  LsAck timer: Off
Prefix-suppression is enabled
```

Table 12 Command output

Field	Description
Area	Area ID that the interface belongs to.
Interface ID	Interface ID.
Instance ID	Instance ID.
IPv6 prefixes	IPv6 prefix.
Cost	Cost value of the interface.
State	Interface state: • **DOWN**—No protocol traffic can be sent or received on the interface. • **Waiting**—The interface starts sending and receiving Hello packets. The router is trying to determine the identity of the (Backup) designated router for the network. • **P-2-P**—The interface will send Hello packets at the hello interval, and try to establish an adjacency with the neighbor. • **DR**—The router is the designated router on the network. • **BDR**—The router is the backup designated router on the network. • **DROther**—The router is a DR Other router on the attached network.
Type	Network type of the interface: PTP (P2P), PTMP (P2MP), Broadcast, or NBMA.
MTU	MTU value of the interface.
Priority	DR priority of the interface.
Designated router	DR on this link.
Backup designated router	BDR on this link.
Timers	Time intervals in seconds configured on the interface: • **Hello**—Hello interval. • **Dead**—Dead interval. • **Poll**—Polling interval on an NBMA network. • **Retransmit**—LSA retransmission interval.
Transmit Delay	LSA transmission delay on the interface, in seconds.
FRR backup	Whether LFA calculation is enabled on an interface: • **Enabled**. • **Disabled**.
Neighbor count	Number of neighbors on the interface.
Primary path detection mode	Primary link detection mode: • **BFD ctrl**—BFD control packet mode. • **BFD echo**—BFD echo packet mode.
Adjacent neighbor count	Number of adjacencies on the interface.

Field	Description
IPsec profile name	IPsec profile applied to the interface. The **inherited** attribute indicates that the interface is using the IPsec profile specified for the area to which the interface belongs.

display ospfv3 lsdb

Use **display ospfv3 lsdb** to display OSPFv3 LSDB information.

Syntax

display ospfv3 [*process-id*] **lsdb** [{ **external** | **grace** | **inter-prefix** | **inter-router** | **intra-prefix** | **link** | **network** | **nssa** | **router** | **unknown** [*type*] } [*link-state-id*] [**originate-router** *router-id* | **self-originate**] | **statistics** | **total** | **verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays LSDB information for all processes.

external: Displays AS external LSAs (Type-5 LSAs).

grace: Displays Grace-LSAs (Type-11 LSAs).

inter-prefix: Displays Inter-area-prefix LSAs (Type-3 LSAs).

inter-router: Displays Inter-area-router LSAs (Type-4 LSAs).

intra-prefix: Displays Intra-area-prefix LSAs (Type-9 LSAs).

link: Displays Link-LSAs (Type-8 LSAs).

network: Displays Network-LSAs (Type-2 LSAs).

nssa: Displays NSSA LSAs (Type-7 LSAs).

router: Displays Router-LSAs (Type-1 LSAs).

unknown: Displays unknown LSAs.

type: Specifies an LSA type, a hexadecimal string of 0 to ffff. If you do not specify this argument, the command displays all unknown LSAs.

link-state-id: Specifies a link state ID in IPv4 address format.

originate-router *router-id*: Specifies an advertising router by its ID.

self-originate: Displays locally originated LSAs.

statistics: Displays LSA statistics.

total: Displays the total number of LSAs in the LSDB.

verbose: Displays detailed information. If you do not specify this keyword, the command displays brief information.

Examples

Display OSPFv3 LSDB information.

```
<Sysname> display ospfv3 lsdb
               OSPFv3 Process 1 with Router ID 1.1.1.1
                  Link-LSA (Interface GigabitEthernet1/0/1)
------------------------------------------------------------------------
 Link state ID   Origin router    Age   SeqNumber  Checksum  Prefix
 0.15.0.8        2.2.2.2          0691  0x80000041 0x8315         1
 0.0.0.3         1.1.1.1          0623  0x80000001 0x0fee         1
                  Router-LSA (Area 0.0.0.1)
------------------------------------------------------------------------
 Link state ID   Origin router    Age   SeqNumber  Checksum    Link
 0.0.0.0         1.1.1.1          0013  0x80000068 0x5d5f         2
 0.0.0.0         2.2.2.2          0024  0x800000ea 0x1e22         0
                  Network-LSA (Area 0.0.0.1)
------------------------------------------------------------------------
 Link state ID   Origin router    Age   SeqNumber  Checksum
 0.15.0.8        2.2.2.2          0019  0x80000007 0x599e
                  Intra-Area-Prefix-LSA (Area 0.0.0.1)
------------------------------------------------------------------------
 Link state ID   Origin router    Age   SeqNumber  Checksum  Prefix  Reference
 0.0.0.2         2.2.2.2          3600  0x80000002 0x2eed         2  Network-LSA
 0.0.0.1         2.2.2.2          0018  0x80000001 0x1478         1  Network-LSA
```

Table 13 Command output

Field	Description
Origin router	Originating router.
Age	Age of LSAs.
SeqNumber	LSA sequence number.
Checksum	LSA checksum.
Prefix	Number of prefixes.
Link	Number of links.
Reference	Type of referenced LSA.

Display Link LSA information in the LSDB.

```
<Sysname> display ospfv3 lsdb link
               OSPFv3 Process 1 with Router ID 1.1.1.1
                  Link-LSA (Interface GigabitEthernet1/0/1)
------------------------------------------------------------------------
  LS age            : 833
  LS type           : Link-LSA
  Link state ID     : 0.15.0.8
  Originating router: 2.2.2.2
  LS seq number     : 0x80000041
```

```
  Checksum          : 0x8315
  Length            : 56
  Priority          : 1
  Options           : 0x000013 (-|R|-|x|E|V6)
  Link-Local address: fe80::200:5eff:fe00:100
  Number of prefixes: 1
      Prefix        : 1001::/64
      Prefix options: 0 (-|-|x|-|-)
```

Table 14 Command output

Field	Description
LS age	Age of LSA.
LS type	Type of LSA.
Link state ID	Link state ID.
Originating router	Originating router.
LS seq number	LSA sequence number.
Checksum	LSA checksum.
Length	LSA length.
Priority	Router priority.
Options	Options.
Link-Local address	Link-local address.
Number of prefixes	Number of prefixes.
Prefix	Address prefix.
Prefix options	Prefix options.

Display LSA statistics.

```
<System> display ospfv3 lsdb statistics

               OSPFv3 Process 1 with Router ID 1.1.1.1
------------------------------------------------------------------------------
 Area ID         Router Network IntePre  InteRou IntraPre NSSA
 0.0.0.1         2      0       0        0       2        0
 0.0.0.3         1      0       0        0       1        1
 Total           3      0       0        0       3        1
------------------------------------------------------------------------------
                 Link   Grace   ASE
 Total           4      0       0
```

Table 15 Command output

Field	Description
Area ID	Area ID.
Router	Number of Type-1 LSAs.
Network	Number of Type-2 LSAs.

Field	Description
IntePre	Number of Type-3 LSAs.
InteRou	Number of Type-4 LSAs.
IntraPre	Number of Type-9 LSAs.
NSSA	Number of Type-7 LSAs.
Link	Number of Type-8 LSAs.
Grace	Number of Type-11 LSAs.
ASE	Number of Type-5 LSAs.

Display detailed OSPFv3 LSDB information.

```
<Sysname> display ospfv3 lsdb verbose
               OSPFv3 Process 1 with Router ID 1.1.1.1
                  Link-LSA (Interface GigabitEthernet1/0/1)
------------------------------------------------------------------------------
 Link state ID   Origin router    Age   SeqNumber  Checksum  Prefix
 0.15.0.8        2.2.2.2          0691  0x80000041 0x8315         1
                 SendCnt: 0       RxmtCnt: 0       Status: Stale
 0.0.0.3         1.1.1.1          0623  0x80000001 0x0fee         1
                 SendCnt: 0       RxmtCnt: 0       Status: Stale
                  Router-LSA (Area 0.0.0.1)
------------------------------------------------------------------------------
 Link state ID   Origin router    Age   SeqNumber  Checksum    Link
 0.0.0.0         1.1.1.1          0013  0x80000068 0x5d5f         2
                 SendCnt: 0       RxmtCnt: 0       Status: Stale
 0.0.0.0         2.2.2.2          0024  0x800000ea 0x1e22         0
                 SendCnt: 0       RxmtCnt: 0       Status: Stale
                  Network-LSA (Area 0.0.0.1)
------------------------------------------------------------------------------
 Link state ID   Origin router    Age   SeqNumber  Checksum
 0.15.0.8        2.2.2.2          0019  0x80000007 0x599e
                 SendCnt: 0       RxmtCnt: 0       Status: Stale
                  Intra-Area-Prefix-LSA (Area 0.0.0.1)
------------------------------------------------------------------------------
 Link state ID   Origin router    Age   SeqNumber  Checksum  Prefix  Reference
 0.0.0.2         2.2.2.2          3600  0x80000002 0x2eed         2  Network-LSA
                 SendCnt: 0       RxmtCnt: 0       Status: Stale
 0.0.0.1         2.2.2.2          0018  0x80000001 0x1478         1  Network-LSA
                 SendCnt: 0       RxmtCnt: 0       Status: Stale
```

Table 16 Command output

Field	Description
SendCnt	Number of interfaces to send the LSA.
RxmtCnt	Number of LSAs in the link state retransmission list.

Field	Description
Status	LSA status: • Normal. • Delayed. • **Maxage routed**—The LSA has reached its maximum age. • Self originated. • **Stale**—A self-originated LSA is received during the GR process.

display ospfv3 nexthop

Use **display ospfv3 nexthop** to display OSPFv3 next hop information.

Syntax

display ospfv3 [*process-id*] **nexthop**

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays next hop information for all OSPFv3 processes.

Examples

Display next hop information for OSPFv3 process 1.

```
<Sysname> display ospfv3 1 nexthop

              OSPFv3 Process 1 with Router ID 1.1.1.1

 Nexthop : FE80::20C:29FF:FED7:F308              Interface: GE1/0/2
 RefCount: 4                                     Status   : Valid
 NbrID   : 1.1.1.1                               NbrIntID : 21

 Nexthop : FE80::20C:29FF:FED7:F312              Interface: GE1/0/3
 RefCount: 3                                     Status   : Valid
 NbrID   : 1.1.1.1                               NbrIntID : 38
```

Table 17 Command output

Field	Description
Nexthop	Next hop address.
Interface	Output interface.

Field	Description
RefCount	Reference count (routes that use the next hop).
Status	Next hop status: valid or invalid.
NbrId	Neighbor router ID.
NbrIntID	Neighbor interface ID.

display ospfv3 non-stop-routing

Use **display ospfv3 non-stop-routing** to display OSPFv3 NSR information.

Syntax

display ospfv3 [*process-id*] **non-stop-routing**

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays OSPFv3 NSR information for all OSPFv3 processes.

Examples

Display OSPFv3 NSR information.

```
<Sysname> display ospfv3 non-stop-routing

              OSPFv3 Process 1 with Router ID 3.3.3.3

 Nonstop Routing capability: Enabled
 Upgrade phase             : Normal
```

Table 18 Command output

Field	Description
Nonstop Routing capability	NSR status: enabled or disabled.
Upgrade phase	NSR phase: • **Normal**—Normal status. • **Preparation**—Upgrade preparation phase. • **Smooth**—Upgrade phase. • **Precalculation**—Route pre-calculation phase. • **Calculation**—Route calculation phase. • **Redistribution**—Route redistribution phase.

display ospfv3 peer

Use **display ospfv3 peer** to display information about OSPFv3 neighbors.

Syntax

display ospfv3 [*process-id*] [**area** *area-id*] **peer** [[*interface-type interface-number*] [**verbose**] | *peer-router-id* | **statistics**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify a process, this command displays neighbor information for all processes.

area *area-id*: Specifies an area by its ID, an IPv4 address or a decimal integer in the range of 0 to 4294967295 that is translated into the IPv4 address format. If you do not specify an area, this command displays neighbor information for all areas.

interface-type interface-number: Specifies an interface by its type and number.

verbose: Displays detailed neighbor information.

peer-router-id: Specifies a neighbor.

statistics: Displays OSPFv3 neighbor statistics.

Usage guidelines

If you do not specify an interface and a neighbor, this command displays neighbor information for all interfaces.

Examples

Display neighbor information for OSPFv3 process 1.

```
<Sysname> display ospfv3 1 peer

              OSPFv3 Process 1 with Router ID 1.1.1.1

 Area: 0.0.0.1
----------------------------------------------------------------------------
 Router ID       Pri State            Dead-Time InstID Interface
 2.2.2.2         1   Full/DR          00:00:33  0      GE1/0/1

 Sham link destination: 3::3
 Router ID       Pri State            Dead-Time InstID
 100.1.1.1       1   Full/ -          00:00:39  0
```

Table 19 Command output

Field	Description
Router ID	Neighbor router ID.
Pri	Neighboring router priority.
State	Neighbor state.
Dead-Time	Dead time remained.
InstID	Instance ID.
Interface	Interface connected to the neighbor.
Sham link destination	IPv6 destination address of the OSPFv3 sham link.

Display detailed neighbor information for OSPFv3 process 1.

```
<Sysname> display ospfv3 1 peer verbose

              OSPFv3 Process 1 with Router ID 1.1.1.1

 Area 0.0.0.1 interface GE1/0/2's neighbors
 Router ID: 2.2.2.2          Address: FE80::200:5EFF:FE00:100
   State: Full  Mode: Nbr is master  Priority: 1
   DR: 2.2.2.2  BDR: None   MTU: 1500
   Options is 0x000013 (-|R|-|x|E|V6)
   Dead timer due in 00:00:38
   Neighbor is up for 00:19:07
   Neighbor state change count: 120
   Database Summary List 0
   Link State Request List 0
   Link State Retransmission List 3
   Neighbor interface ID: 8037
   GR state: Normal
   Grace period: 0           Grace period timer: Off
   DD Rxmt Timer: Off        LS Rxmt Timer: On

 Sham link neighbor with address: 3::3
 Router ID: 100.1.1.1        Area: 0.0.0.1
   State: Full  Mode: Nbr is slave  Priority: 1
   DR: None   BDR: None   MTU: 0
   Options is 0x000013 (-|-|-|-|-|-|R|-|x|E|V6)
   Dead timer due in 00:00:36
   Neighbor is up for 00:13:55
   Authentication sequence: (high) 0, (low) 0
   Neighbor state change count: 5
   Database Summary List 0
   Link State Request List 0
   Link State Retransmission List 0
   Neighbor interface ID: 2147483649
   GR state: Normal
   Grace period: 0           Grace period timer: Off
```

```
DD Rxmt Timer: Off        LS Rxmt Timer: Off
```

Table 20 Command output

Field	Description
Router ID	Neighbor router ID.
Address	Link-local address of the interface.
State	Neighbor state.
Mode	Neighbor mode for LSDB synchronization.
Priority	Neighboring router priority.
DR	DR on the interface's network segment.
BDR	BDR on the interface's network segment.
MTU	Interface MTU.
Options	LSA options: • **DC**—The originating router supports OSPFv3 over on-demand circuits. • **R**—Whether the originating router is an active router. • **N**—Whether the originating router supports NSSA LSAs. • **x**—Reserved. • **E**—Whether the originating router can receive AS External LSAs. • **V6**—Whether the originating router takes part in IPv6 route calculation.
Dead timer due in hh:mm:ss	Remaining time for the dead timer, in hh:mm:ss format. hh represents the hours, mm represents the minutes, and ss represents the seconds.
Neighbor is up for hh:mm:ss	Uptime for the neighbor, in hh:mm:ss format. hh represents the hours, mm represents the minutes, and ss represents the seconds.
Neighbor state change count	Count of neighbor state changes.
Database Summary List	Number of LSAs sent in DD packet.
Link State Request List	Number of LSAs in the link state request list.
Link State Retransmission List	Number of LSAs in the link state retransmission list.
Neighbor interface ID	Interface ID of the neighbor.
GR state	GR state: • **Normal**—GR is not in progress. • **Doing GR**—Acting as the GR restarter. • Complete GR. • **Helper**—Acting as the GR helper.
Grace period	Grace-LSA sending interval.
Grace period timer	Grace-LSA sending interval timer.
DD Rxmt Timer	DD packet retransmission timer.
LS Rxmt Timer	LSU retransmission timer.
Sham link neighbor with address	IPv6 neighbor address of the OSPFv3 sham link.

Display OSPFv3 neighbor statistics.

```
<Sysname> display ospfv3 peer statistics

               OSPFv3 Process 1 with Router ID 1.1.1.1
--------------------------------------------------------------------------
 Area ID         Down Attempt Init 2-Way ExStart Exchange Loading Full Total
 0.0.0.0         0    0       0    0     0       0        0       1    1
 Total           0    0       0    0     0       0        0       1    1
 Sham links' neighbors(Total: 1):
 Down: 0,Init: 0,2-Way: 0,ExStart: 0,Exchange: 0,Loading: 0,Full: 1
```

Table 21 Command output

Field	Description
Area ID	Area ID.
Down	In this state, neighbor initial state, the router has not received any information from a neighboring router for a period of time.
Attempt	This state is available only in an NBMA network. In this state, the OSPFv3 router has not received any information from a neighbor for a period. The router can send Hello packets at a longer interval to keep the neighbor relationship.
Init	In this state, the device received a Hello packet from the neighbor but the packet contains no router ID of the neighbor. Mutual communication is not setup.
2-Way	Mutual communication between the router and its neighbor is available. DR/BDR election is finished under this state (or higher).
ExStart	In this state, the router decides on the initial DD sequence number and active/standby relationship of the two parties.
Exchange	In this state, the router exchanges DD packets with the neighbor.
Loading	In this state, the router sends LSRs to request the neighbor for needed LSAs.
Full	LSDB synchronization has been accomplished between neighbors.
Total	Total number of neighbors under the same state.
Sham links' neighbors(Total: *xx*)	Statistics about sham links' neighbors. The **Total** field displays the total number of neighbors.

display ospfv3 request-queue

Use **display ospfv3 request-queue** to display OSPFv3 request list information.

Syntax

display ospfv3 [*process-id*] [**area** *area-id*] **request-queue** [*interface-type interface-number*] [*neighbor-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify an OSPFv3 process, this command displays OSPFv3 request list information for all OSPFv3 processes.

area *area-id*: Specifies an area by its ID, an IPv4 address or a decimal integer in the range of 0 to 4294967295 that is translated into the IPv4 address format. If you do not specify an OSPFv3 area, this command displays OSPFv3 request list information for all areas.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays OSPFv3 request list information for all interfaces.

neighbor-id: Specifies a neighbor's router ID. If you do not specify a neighbor, this command displays OSPFv3 request list information for all OSPFv3 neighbors.

Examples

Display OSPFv3 request list information.

```
<Sysname> display ospfv3 request-queue

               OSPFv3 Process 1 with Router ID 1.1.1.1

                   Area: 0.0.0.0
                   Interface GigabitEthernet1/0/1
----------------------------------------------------------------------------
                   Nbr-ID 1.3.3.3 Request List
 Type    LinkState ID    AdvRouter       SeqNum       Age   CkSum
 0x4005  0.0.34.127      1.3.3.3         0x80000001   0027  0x274d
 0x4005  0.0.34.128      1.3.3.3         0x80000001   0027  0x2d45
 0x4005  0.0.34.129      1.3.3.3         0x80000001   0027  0x333d
 0x4005  0.0.34.130      1.3.3.3         0x80000001   0027  0x3935
```

Table 22 Command output

Field	Description
Area	Area ID.
Interface	Interface type and sequence number.
Nbr-ID	Neighbor ID.
Request list	Request list information.
Type	LSA type.
LinkState ID	Link state ID.
AdvRouter	Advertising router.
SeqNum	LSA sequence number.
Age	LSA age.
CkSum	Checksum.

display ospfv3 retrans-queue

Use **display ospfv3 retrans-queue** to display retransmission list information.

Syntax

display ospfv3 [*process-id*] [**area** *area-id*] **retrans-queue** [*interface-type interface-number*] [*neighbor-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify an OSPFv3 process, this command displays retransmission list information for all OSPFv3 processes.

area *area-id*: Specifies an area by its ID, an IPv4 address or a decimal integer in the range of 0 to 4294967295 that is translated into the IPv4 address format. If you do not specify an OSPFv3 area, this command displays retransmission list information for all OSPFv3 areas.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays retransmission list information for all interfaces.

neighbor-id: Specifies a neighbor's router ID. If you do not specify a neighbor, this command displays retransmission list information for all neighbors.

Examples

Display OSPFv3 retransmission list information.

```
<Sysname> display ospfv3 retrans-queue

                OSPFv3 Process 1 with Router ID 1.1.1.1

                    Area: 0.0.0.0
                    Interface GigabitEthernet1/0/1
--------------------------------------------------------------------------
                    Nbr-ID 1.2.2.2 Retransmit List
 Type    LinkState ID    AdvRouter       SeqNum       Age   CkSum
 0x2009  0.0.0.0         1.3.3.3         0x80000001   3600  0x49fb
```

Table 23 Command output

Field	Description
Area	Area ID.
Interface	Interface type and sequence number.
Nbr-ID	Neighbor ID.
Retransmit List	Retransmission list information.
Type	LSA type.
LinkState ID	Link state ID.
AdvRouter	Advertising router.

Field	Description
SeqNum	LSA sequence number.
Age	LSA age.
CkSum	Checksum.

display ospfv3 routing

Use **display ospfv3 routing** to display OSPFv3 route information.

Syntax

display ospfv3 [*process-id*] **routing** [*ipv6-address prefix-length*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays the OSPFv3 route information for all processes.

ipv6-address prefix-length: Specifies an IPv6 address. The *ipv6-address* argument specifies an IPv6 prefix. The *prefix-length* argument specifies a prefix length in the range of 0 to 128.

Examples

Display OSPFv3 routing information.

```
<Sysname> display ospfv3 routing

               OSPFv3 Process 1 with Router ID 9.9.9.9
------------------------------------------------------------------------
 I  - Intra area route,  E1 - Type 1 external route,  N1 - Type 1 NSSA route
 IA - Inter area route,  E2 - Type 2 external route,  N2 - Type 2 NSSA route
 *  - Selected route

 *Destination: 1::/64
  Type       : IA                        Area       : 0.0.0.1
  AdvRouter  : 2.2.2.2                   Preference : 10
  NibID      : 0x23000003                Cost       : 2
  Interface  : GE1/0/1                   BkInterface: GE1/0/2
  Nexthop    : FE80::6AC7:45FF:FE5C:206
  BkNexthop  : N/A

 *Destination: 23::/64
  Type       : I                         Area       : 0.0.0.1
```

```
  AdvRouter  : 3.3.3.3                  Preference : 10
  NibID      : 0x23000001               Cost       : 1
  Interface  : GE1/0/1                  BkInterface: GE1/0/2
  Nexthop    : ::
  BkNexthop  : N/A

*Destination: 8::/64
  Type       : E2                       Tag        : 1
  AdvRouter  : 1.1.1.1                  Preference : 150
  NibID      : 0x23000004               Cost       : 1
  Interface  : GE1/0/1                  BkInterface: GE1/0/2
  Nexthop    : FE80::6AC7:45FF:FE5C:206
  BkNexthop  : N/A

 Total: 3
 Intra area: 3         Inter area: 0         ASE: 0         NSSA: 0
```

Table 24 Command output

Field	Description
Destination	Destination network segment.
Type	Route type.
Area	Area ID.
AdvRouter	Advertising router.
Preference	OSPFv3 route preference.
NibID	Next hop ID.
Cost	Route cost value.
Interface	Output interface.
BkInterface	Backup output interface.
Nexthop	Primary next hop IP address.
BkNexthop	Backup next hop IP address.
Interface	Output interface.
AdvRouter	Advertising router.
Area	Area ID.
Tag	Tag of external routes.
Preference	Route preference.
Total	Total number of routes.
Intra area	Number of intra-area routes.
Inter area	Number of inter-area routes.
ASE	Number of Type-5 external routes.
NSSA	Number of Type-7 external routes.

display ospfv3 spf-tree

Use **display ospfv3 spf-tree** to display OSPFv3 SPF tree information.

Syntax

display ospfv3 [*process-id*] [**area** *area-id*] **spf-tree** [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify a process, this command displays SPF tree information for all OSPFv3 processes.

area *area-id*: Specifies an OSPFv3 area by its ID. The area ID is an IP address or a decimal integer in the range of 0 to 4294967295 that is translated into the IP address format. If you do not specify an area, this command displays SPF tree information for all OSPFv3 areas.

verbose: Displays detailed OSPFv3 SPF tree information. If you do not specify this keyword, the command displays brief OSPFv3 SPF tree information.

Examples

Display brief SPF tree information for Area 0 in OSPFv3 process 1.

```
<Sysname> display ospfv3 1 area 0 spf-tree

               OSPFv3 Process 1 with Router ID 1.1.1.1

 Flags: S-Node is on SPF tree       R-Node is directly reachable
        I-Node or Link is init      D-Node or Link is to be deleted
        P-Neighbor is parent        A-Node is in candidate list
        C-Neighbor is child         H-Nexthop changed
        N-Link is a new path        V-Link is involved

                 Area: 0.0.0.0  Shortest Path Tree

 SPFNode         Type   Flag         SPFLink         Type   Cost  Flag
>1.1.1.1         Router S R
                                  -->2.2.2.2         RT2RT  1     C
                                  -->2.2.2.2         RT2RT  1     P
```

Table 25 Command output

Field	Description
SPFNode	SPF node, represented by the advertising router ID. Node type: • **Network**—Network node. • **Router**—Router node. Node flag: • **I**—The node is in initialization state. • **A**—The node is on the candidate list. • **S**—The node is on the SPF tree. • **R**—The node is directly connected to the root node. • **D**—The node is to be deleted.
SPFLink	SPF link, representing the advertising router ID. Link type: • **RT2RT**—Router to router. • **NET2RT**—Network to router. • **RT2NET**—Router to network. Link flag: • **I**—The link is in initialization state. • **P**—The peer is the parent node. • **C**—The peer is the child node. • **D**—The link is to be deleted. • **H**—The next hop is changed. • **V**—When the peer node is deleted or added, the peer node is not on the SPF tree or is deleted. • **N**—The link is newly added, and both end nodes are on the SPF tree. • **L**—The link is on the area change list.

Display detailed SPF tree information for Area 0 in OSPFv3 process 1.

```
<Sysname> display ospfv3 1 area 0 spf-tree verbose

               OSPFv3 Process 1 with Router ID 1.1.1.1

 Flags: S-Node is on SPF tree       R-Node is directly reachable
        I-Node or Link is init      D-Node or Link is to be deleted
        P-Neighbor is parent        A-Node is in candidate list
        C-Neighbor is child         H-Nexthop changed
        N-Link is a new path        V-Link is involved

           Area: 0.0.0.0  Shortest Path Tree

>SPFNode[0]
  AdvID        : 1.1.1.1                LsID       : 0.0.0.0
  NodeType     : Router                 Distance   : 1
  NodeFlag     : S R
  Nexthop count: 1
 -->NbrID      : 1.1.1.1                NbrIntID   : 21
    Interface  : GE1/0/2                NhFlag     : Valid
```

```
   BkInterface: GE1/0/3                 RefCount    : 4
   Nexthop    : FE80::20C:29FF:FED7:F308
   BkNexthop  : FE80::4
 SPFLink count: 1
-->AdvID      : 1.1.1.1                 LsID        : 0.0.0.0
   IntID      : 232                     NbrIntID    : 465
   NbrID      : 2.2.2.2                 LinkType    : RT2RT
   LinkCost   : 1                       LinkNewCost: 1
   LinkFlag   : C                       NexthopCnt : 0
 ParentLink count: 1
-->AdvID      : 1.1.1.1                 LsID        : 0.0.0.0
   IntID      : 215                     NbrIntID    : 466
   NbrID      : 2.2.2.2                 LinkType    : RT2RT
   LinkCost   : 1                       LinkNewCost: 1
   LinkFlag   : P                       NexthopCnt : 0
```

Table 26 Command output

Field	Description
SPFNode	SPF node.
AdvID	ID of the advertising router.
LsID	Link state ID.
NodeType	Node type.
Distance	Cost to the root node.
NodeFlag	Node flag.
Nexthop count	Number of next hops.
NbrID	Neighbor router ID.
NbrIntID	Neighbor interface ID.
Interface	Output interface.
NhFlag	Next hop flag: valid or invalid.
BkInterface	Backup output interface.
RefCount	Reference count (routes that use the backup next hop).
Nexthop	Next hop.
BkNexthop	Backup next hop.
SPFLink count	Number of SPF links.
IntID	Interface ID.
LinkType	Link type: • **RT2RT**—Router to router. • **NET2RT**—Network to router. • **RT2NET**—Router to network.
LinkCost	Link cost.
LinkNewCost	New link cost.

Field	Description
LinkFlag	Link flag: • **I**—The link is in initialization state. • **P**—The peer is the parent node. • **C**—The peer is the child node. • **D**—The link is to be deleted. • **H**—The next hop is changed. • **V**—When the peer node is deleted or added, the peer node is not on the SPF tree or is deleted. • **N**—The link is newly added, and both end nodes are on the SPF tree. • **L**—The link is on the area change list.
NexthopCnt	Number of next hops.
ParentLinkCnt	Number of parent links.

display ospfv3 statistics

Use **display ospfv3 statistics** to display OSPFv3 statistics.

Syntax

display ospfv3 [*process-id*] **statistics** [**error** | **packet** [*interface-type interface-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays OSPFv3 statistics for all processes.

error: Displays error statistics. If you do not specify this keyword, the command displays OSPFv3 packet, LSA, and route statistics.

packet: Displays packet statistics.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify this argument, the command displays statistics for all interfaces.

Examples

Display OSPFv3 statistics.

```
<Sysname> display ospfv3 statistics

                OSPFv3 Process 1 with Router ID 1.1.1.1
                    Packet Statistics
----------------------------------------------------------
```

```
 Type                          Recv               Send
 Hello                         1746               1284
 DB Description                505                941
 Ls Req                        252                136
 Ls Upd                        851                1553
 Ls Ack                        416                450

            Local Originated LSAs Statistics
-------------------------------------------------------------
 Type                                             Count
 Router-LSA                                       192
 Network-LSA                                      0
 Inter-Area-Prefix-LSA                            0
 Inter-Area-Router-LSA                            0
 AS-external-LSA                                  0
 NSSA-LSA                                         0
 Link-LSA                                         10
 Intra-Area-Prefix-LSA                            112
 Grace-LSA                                        0
 Unknown-LSA                                      0
 Total                                            314

                  Routes Statistics
-------------------------------------------------------------
 Type                                             Count
 Intra Area                                       0
 Inter Area                                       0
 ASE                                              0
 NSSA                                             0
```

Table 27 Command output

Field	Description
Packet Statistics	Statistics about inbound and outbound packets.
Hello	Hello packet.
DB Description	DB description packet.
Ls Req	Link state request packet.
Ls Upd	Link state update packet.
Ls Ack	Link state acknowledgment packet.
Local Originated LSAs Statistics	Statistics about generated LSAs.
Router-LSA	Number of Type-1 LSAs.
Network-LSA	Number of Type-2 LSAs.
Inter-Area-Prefix-LSA	Number of Type-3 LSAs.
Inter-Area-Router-LSA	Number of Type-4 LSAs.
AS-external-LSA	Number of Type-5 LSAs.

Field	Description
NSSA-LSA	Number of Type-7 LSAs.
Link-LSA	Number of Type-8 LSAs.
Intra-Area-Prefix-LSA	Number of Type-9 LSAs.
Grace-LSA	Number of Type-11 LSAs.
Unknown-LSA	Number of Unknown-LSAs.
Total	Total number.
Routes Statistics	Number of routes.
Intra Area	Intra-area routes.
Inter Area	Inter-area routes.
ASE	Type-5 external routes.
NSSA	Type-7 external routes.

Display OSPFv3 error statistics.

```
<Sysname> display ospfv3 statistics error

                OSPFv3 Process 1 with Router ID 1.1.1.1

 0          : Transmit error               0          : Neighbor state low
 0          : Packet too small             0          : Bad version
 0          : Bad checksum                 0          : Unknown neighbor
 0          : Bad area ID                  0          : Bad packet
 0          : Packet dest error            0          : Inactive area packet
 0          : Router ID confusion          0          : Bad virtual link
 0          : HELLO: Hello-time mismatch   0          : HELLO: Dead-time mismatch
 0          : HELLO: Ebit option mismatch  0          : DD: Ebit option mismatch
 0          : DD: Unknown LSA type         0          : DD: MTU option mismatch
 0          : REQ: Empty request           0          : REQ: Bad request
 0          : UPD: LSA checksum bad        0          : UPD: Unknown LSA type
 0          : UPD: Less recent LSA         0          : UPD: LSA length bad
 0          : UPD: LSA AdvRtr id bad       0          : ACK: Bad ack packet
 0          : ACK: Invalid ack             0          : Interface down
 0          : Multicast incapable          0          : Authentication failure
 0          : AuthSeqNumber error
```

Table 28 Command output

Field	Description
Transmit error	Packets with error when being transmitted.
Neighbor state low	Packets received in low neighbor state.
Packet too small	Packets too small in length.
Bad version	Packets with wrong version.
Bad checksum	Packets with wrong checksum.
Unknown neighbor	Packets received from unknown neighbors.

Field	Description
Bad area ID	Packets with invalid area ID.
Bad packet	Packets illegal.
Packet dest error	Packets with wrong destination addresses.
Inactive area packet	Packets received in inactive areas.
Router ID confusion	Packets with duplicate router ID.
Bad virtual link	Packets on wrong virtual links.
HELLO: Hello-time mismatch	Hello packets with mismatched hello timer.
HELLO: Dead-time mismatch	Hello packets with mismatched dead timer.
HELLO: Ebit option mismatch	Hello packets with mismatched E-bit in the option field.
DD: Ebit option mismatch	DD packets with mismatched E-bit in the option field.
DD: Unknown LSA type	DD packets with unknown LSA type.
DD: MTU option mismatch	DD packets with mismatched MTU.
REQ: Empty request	LSR packets with no request information.
REQ: Bad request	Bad LSR packets.
UPD: LSA checksum bad	LSU packets with wrong LSA checksum.
UPD: Unknown LSA type	LSU packets with unknown LSA type.
UPD: Less recent LSA	LSU packets without the most recent LSA.
UPD: LSA length bad	LSU packets with wrong LSA length.
UPD: LSA AdvRtr id bad	LSU packets with wrong LSA advertising router.
ACK: Bad ack packet	Bad LSAck packets for LSU packets.
ACK: Invalid ack	Invalid LSAck packets.
Interface down	Shutdown times of the interface.
Multicast incapable	Failures to join the multicast group.
Authentication failure	Received packets with authentication failures.
AuthSeqNumber error	Received packets with incorrect sequence numbers.

Display OSPFv3 packet statistics for all processes and interfaces.

```
<Sysname> display ospfv3 statistics packet

          OSPFv3 Process 1 with Router ID 1.1.1.1

         Hello      DD         LSR        LSU        ACK        Total
 Input : 8727       128        28         1584       929        11396
 Output: 8757       159        86         987        1513       11502

 Area: 0.0.0.0

 Area: 0.0.0.1
 Interface: GigabitEthernet1/0/1
         DD         LSR        LSU        ACK        Total
```

```
Input : 16         0          45         7          68
Output: 17         1          7          44         69
Interface: GigabitEthernet1/0/2
        DD         LSR        LSU        ACK        Total
Input : 41         13         720        719        1493
Output: 54         41         750        713        1558
```

Table 29 Command output

Field	Description
Total	Total number of packets.
Input	Number of received packets.
Output	Number of sent packets.
Area	Area ID.
Interface	Interface name.

display ospfv3 vlink

Use **display ospfv3 vlink** to display OSPFv3 virtual link information.

Syntax

display ospfv3 [*process-id*] **vlink**

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays the OSPFv3 virtual link information for all OSPFv3 processes.

Examples

Display OSPFv3 virtual link information.

```
<Sysname> display ospfv3 vlink

              OSPFv3 Process 1 with Router ID 1.1.1.1

 Virtual-link Neighbor-ID: 12.2.2.2, Neighbor-state: Full
 Interface: 2348 (GigabitEthernet1/0/2), Instance-ID: 0
 Local  IPv6 address: 3:3333::12
 Remote IPv6 address: 2:2222::12
 Cost: 1  State: P-2-P  Type: Virtual
 Transit area: 0.0.0.1
```

```
Timers: Hello 10, Dead 40, Retransmit 5, Transmit delay 1
IPsec profile name: profile001
```

Table 30 Command output

Field	Description
Virtual-link Neighbor-ID	ID of the neighbor on the virtual link.
Neighbor-State	Neighbor state: Down, Init, 2-Way, ExStart, Exchange, Loading, or Full.
Interface	Number and name of the local interface on the virtual link.
Cost	Interface route cost.
State	Interface state.
Type	Virtual link.
Transit Area	Transit area ID. This field is displayed when a virtual link is present on the interface.
Timers	Values of OSPFv3 timers (in seconds): **Hello**, **Dead**, and **Retransmit**.
Transmit delay	LSA transmission delay on the interface, in seconds.
IPsec profile name	IPsec profile applied to the virtual link. The **inherited** attribute indicates that the virtual link is using the IPsec profile specified for the backbone area.
Keychain authentication: Enabled (test)	Keychain authentication is enabled for the virtual link, and keychain **test** is used. The **inherited** attribute indicates that the virtual link is using the authentication mode specified for the backbone area.

enable ipsec-profile

Use **`enable ipsec-profile`** to apply an IPsec profile to an OSPFv3 area.

Use **`undo enable ipsec-profile`** to remove the IPsec profile from the OSPFv3 area.

Syntax

`enable ipsec-profile` *`profile-name`*

`undo enable ipsec-profile`

Default

No IPsec profile is applied to an area.

Views

OSPFv3 area view

Predefined user roles

network-admin

context-admin

Parameters

`profile-name`: Specifies an IPsec profile by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

To protect routing information and prevent attacks, OSPFv3 can authenticate protocol packets by using an IPsec profile. For more information about IPsec profiles, see *Security Configuration Guide*.

Examples

Apply IPsec profile **profile001** to Area 0 in OSPFv3 process 1.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] area 0
[Sysname-ospfv3-1-area-0.0.0.0] enable ipsec-profile profile001
```

event-log

Use **event-log** to set the maximum number of OSPFv3 logs.

Use **undo event-log** to remove the configuration.

Syntax

event-log { **lsa-flush** | **peer** | **spf** } **size** *count*

undo event-log { **lsa-flush** | **peer** | **spf** } **size**

Default

The maximum number of LSA aging logs, neighbor logs, or route calculation logs is 10.

Views

OSPFv3 view

Predefined user roles

network-admin

context-admin

Parameters

lsa-flush: Specifies the maximum number of LSA aging logs.

peer: Specifies the maximum number of neighbor logs.

spf: Specifies the maximum number of route calculation logs.

size *count*: Specifies the maximum number of OSPFv3 logs, in the range of 0 to 65535.

Examples

Set the maximum number of route calculation logs to 50 in OSPFv3 process 100.

```
<Sysname> system-view
[Sysname] ospfv3 100
[Sysname-ospfv3-100] event-log spf size 50
```

fast-reroute

Use **fast-reroute** to configure OSPFv3 FRR.

Use **undo fast-reroute** to restore the default.

Syntax

fast-reroute { **lfa** [**abr-only**] | **route-policy** *route-policy-name* }

undo fast-reroute

Default

OSPFv3 FRR is disabled.

Views

OSPFv3 view

Predefined user roles

network-admin

context-admin

Parameters

lfa: Uses the LFA algorithm to calculate a backup next hop for all routes.

abr-only: Uses the next hop of the route to the ABR as the backup next hop.

route-policy *route-policy-name*: Uses a routing policy to designate a backup next hop. The *route-policy-name* argument is a case-sensitive string of 1 to 63 characters.

Usage guidelines

Do not use the **fast-reroute lfa** command together with the **vlink-peer** command.

Examples

Enable FRR to calculate a backup next hop for all routes by using LFA algorithm in OSPFv3 process 1.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] fast-reroute lfa
```

filter

Use **filter** to configure inbound/outbound Inter-Area-Prefix-LSA filtering on an ABR.

Use **undo filter** to remove the configuration.

Syntax

filter { *ipv6-acl-number* | **prefix-list** *prefix-list-name* | **route-policy** *route-policy-name* } { **export** | **import** }

undo filter { **export** | **import** }

Default

Inter-Area-Prefix-LSAs are not filtered.

Views

OSPFv3 area view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-acl-number: Specifies an IPv6 ACL by its number in the range of 2000 to 3999 to filter inbound/outbound Inter-Area-Prefix-LSAs.

prefix-list *prefix-list-name*: Specifies an IPv6 prefix list by its name, a case-sensitive string of 1 to 63 characters, to filter inbound/outbound Inter-Area-Prefix-LSAs.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to filter inbound/outbound Inter-Area-Prefix-LSAs.

export: Filters Inter-Area-Prefix-LSAs advertised to other areas.

import: Filters Inter-Area-Prefix-LSAs advertised into the local area.

Usage guidelines

This command applies only to an ABR.

When you specify an ACL, follow these guidelines:

- If the ACL does not exist or has no rules, the ABR does not filter Inter-Area-Prefix-LSAs.
- If a rule in the ACL is applied to a VPN instance, the rule will deny all Inter-Area-Prefix-LSAs.

To use an advanced ACL (with a number from 3000 to 3999) in the command, configure the ACL using one of the following methods:

- To deny or permit Inter-Area-Prefix-LSAs with the specified address prefix, use the **rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour-addr sour-prefix* command.
- To deny or permit Inter-Area-Prefix-LSAs with the specified address prefix and prefix length, use the **rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour-addr sour-prefix* **destination** *dest-addr dest-prefix* command.

The **source** keyword specifies the address prefix in an Inter-Area-Prefix LSA and the **destination** keyword specifies the prefix length of the address prefix. For the prefix length configuration to take effect, specify a contiguous prefix length.

Examples

Use IPv6 prefix list **my-prefix-list** to filter inbound Inter-Area-Prefix-LSAs. Use IPv6 basic ACL 2000 to filter outbound Inter-Area-Prefix-LSAs in OSPFv3 Area 1.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] area 1
[Sysname-ospfv3-1-area-0.0.0.1] filter prefix-list my-prefix-list import
[Sysname-ospfv3-1-area-0.0.0.1] filter 2000 export
```

filter-policy export

Use **filter-policy export** to configure OSPFv3 to filter redistributed routes.

Use **undo filter-policy export** to remove the configuration.

Syntax

filter-policy { *ipv6-acl-number* | **prefix-list** *prefix-list-name* } **export** [**bgp4+** | **direct** | { **isisv6** | **ospfv3** | **ripng** } [*process-id*] | **static**]

undo filter-policy export [**bgp4+** | **direct** | { **isisv6** | **ospfv3** | **ripng** } [*process-id*] | **static**]

Default

Redistributed routes are not filtered.

Views

OSPFv3 view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-acl-number: Specifies an IPv6 ACL by its number in the range of 2000 to 3999 to filter redistributed routes by destination address.

prefix-list *prefix-list-name*: Specifies an IPv6 prefix list by its name, a case-sensitive string of 1 to 63 characters, to filter redistributed routes by destination address.

bgp4+: Filters redistributed IPv6 BGP routes.

direct: Filters redistributed direct routes.

isisv6: Filters redistributed IPv6 IS-IS routes.

ospfv3: Filters redistributed OSPFv3 routes.

ripng: Filters redistributed RIPng routes.

process-id: Specifies a process by its ID in the range of 1 to 65535. The default value is 1.

static: Filters redistributed static routes.

Usage guidelines

When you specify an ACL, follow these guidelines:

- If the ACL does not exist or has no rules, OSPFv3 does not filter redistributed routes.
- If a rule in the ACL is applied to a VPN instance, the rule will deny all redistributed routes.

To use an advanced ACL (with a number from 3000 to 3999) in the command, configure the ACL in one of the following ways:

- To deny or permit a route with the specified destination, use **rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix*.
- To deny or permit a route with the specified destination and prefix, use **rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix* **destination** *dest dest-prefix*.

The **source** keyword specifies the destination address of a route, and the **destination** keyword specifies the prefix of the route. For the configuration to take effect, specify a contiguous prefix.

Using the **filter-policy export** command filters only routes redistributed by the **import-route** command. If the **import-route** command is not configured to redistribute routes from other protocols and other OSPFv3 processes, the **filter-policy export** command does not take effect.

If you do not specify a routing protocol, the command filters all redistributed routes.

Examples

Use IPv6 prefix list **abc** to filter redistributed routes.

```
<Sysname> system-view
[Sysname] ipv6 prefix-list abc permit 2002:1:: 64
[Sysname] ospfv3
[Sysname-ospfv3-1] filter-policy prefix-list abc export
```

Configure IPv6 advanced ACL 3000 to permit only route 2001::1/128. Use ACL 3000 to filter redistributed routes.

```
<Sysname> system-view
[Sysname] acl ipv6 advanced 3000
[Sysname-acl-ipv6-adv-3000] rule 10 permit ipv6 source 2001::1 128 destination
ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff 128
[Sysname-acl-ipv6-adv-3000] rule 100 deny ipv6
[Sysname-acl-ipv6-adv-3000] quit
```

```
[Sysname] ospfv3
[Sysname-ospfv3-1] filter-policy 3000 export
```

filter-policy import

Use **filter-policy import** to configure OSPFv3 to filter routes calculated using received LSAs.

Use **undo filter-policy import** to remove the configuration.

Syntax

filter-policy { *ipv6-acl-number* [**gateway** *prefix-list-name*] | **prefix-list** *prefix-list-name* [**gateway** *prefix-list-name*] | **gateway** *prefix-list-name* | **route-policy** *route-policy-name* } **import**

undo filter-policy import

Default

Routes calculated using received LSAs are not filtered.

Views

OSPFv3 view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-acl-number: Specifies an IPv6 ACL by its number in the range of 2000 to 3999 to filter routes by destination.

gateway *prefix-list-name*: Specifies an IPv6 prefix list by its name, a case-sensitive string of 1 to 63 characters, to filter routes by next hop. If you do not specify this option, the command does not filter routes by next hop.

prefix-list *prefix-list-name*: Specifies an IPv6 prefix list by its name, a case-sensitive string of 1 to 63 characters, to filter routes by destination.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to filter received routes.

Usage guidelines

When you specify an ACL, follow these guidelines:

- If the ACL does not exist or has no rules, OSPFv3 does not filter calculated routes.
- If a rule in the ACL is applied to a VPN instance, the rule will deny all calculated routes.

To use an advanced ACL (with a number from 3000 to 3999) in the command, configure the ACL in one of the following ways:

- To deny or permit a route with the specified destination, use **rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix*.
- To deny or permit a route with the specified destination and prefix, use **rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix* **destination** *dest dest-prefix*.

The **source** keyword specifies the destination address of a route, and the **destination** keyword specifies the prefix of the route. For the configuration to take effect, specify a contiguous prefix.

Using the **filter-policy import** command filters only routes computed by OSPFv3. Routes that fail to pass the filter are not added to the routing table.

Examples

Use IPv6 prefix list **abc** to filter received routes.

```
<Sysname> system-view
[Sysname] ipv6 prefix-list abc permit 2002:1:: 64
[Sysname] ospfv3
[Sysname-ospfv3-1] filter-policy prefix-list abc import
```

Configure IPv6 advanced ACL 3000 to permit only route 2001::1/128 to pass. Use ACL 3000 to filter received routes.

```
<Sysname> system-view
[Sysname] acl ipv6 advanced 3000
[Sysname-acl-ipv6-adv-3000] rule 10 permit ipv6 source 2001::1 128 destination
ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff 128
[Sysname-acl-ipv6-adv-3000] rule 100 deny ipv6
[Sysname-acl-ipv6-adv-3000] quit
[Sysname] ospfv3
[Sysname-ospfv3-1] filter-policy 3000 import
```

graceful-restart enable

Use **graceful-restart enable** to enable the GR capability for OSPFv3.

Use **undo graceful-restart enable** to disable the GR capability for OSPFv3.

Syntax

graceful-restart enable [**global** | **planned-only**] *

undo graceful-restart enable

Default

The GR capability for OSPFv3 is disabled.

Views

OSPFv3 view

Predefined user roles

network-admin

context-admin

Parameters

global: Enables global GR. In global GR mode, a GR process can be completed only when all GR helpers exist. A GR process fails if a GR helper fails (for example, the interface connected to the GR helper goes down). If you do not specify this keyword, the command enables partial GR. In partial GR mode, a GR process can be completed as long as one GR helper exists.

planned-only: Enables planned GR only. If you do not specify this keyword, the command enables both planned GR and unplanned GR.

Usage guidelines

GR includes planned GR and unplanned GR.

- **Planned GR**—Manually restarts OSPFv3 or performs an active/standby switchover. Before OSPFv3 restart or active/standby switchover, the GR restarter sends Grace-LSAs to GR helpers.
- **Unplanned GR**—OSPFv3 restarts or an active/standby switchover occurs because of device failure. Before OSPFv3 restart or active/standby switchover, the GR restarter does not send Grace-LSAs to GR helpers.

OSPFv3 GR and OSPFv3 NSR are mutually exclusive. Do not configure the **graceful-restart enable** command and the **non-stop-routing** command at the same time.

To prevent service interruption after a master/backup switchover, a GR restarter running OSPFv3 must perform the following tasks:

- Keep the GR restarter forwarding entries stable during reboot.
- Establish all adjacencies and obtain complete topology information after reboot.

Examples

Enable the GR capability for OSPFv3 process 1.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] graceful-restart enable
```

Related commands

graceful-restart helper enable

graceful-restart helper enable

Use **graceful-restart helper enable** to enable the GR helper capability for OSPFv3.

Use **undo graceful-restart helper enable** to disable the GR helper capability for OSPFv3.

Syntax

graceful-restart helper enable [**planned-only**]

undo graceful-restart helper enable

Default

The GR helper capability for OSPFv3 is enabled.

Views

OSPFv3 view

Predefined user roles

network-admin

context-admin

Parameters

planned-only: Enables only planned GR for the GR helper. If you do not specify this keyword, the command enables both planned GR and unplanned GR for the GR helper.

Usage guidelines

Upon receiving the Grace-LSA, the neighbors with the GR helper capability enter the helper mode (and are called GR helpers). Then, the GR restarter retrieves its adjacencies and LSDB with the help of the GR helpers.

Examples

Enable the GR helper capability for OSPFv3 process 1.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] graceful-restart helper enable
```

Related commands

graceful-restart enable

graceful-restart helper strict-lsa-checking

Use **graceful-restart helper strict-lsa-checking** to enable strict LSA checking for the GR helper.

Use **undo graceful-restart helper strict-lsa-checking** to disable strict LSA checking for the GR helper.

Syntax

graceful-restart helper strict-lsa-checking

undo graceful-restart helper strict-lsa-checking

Default

Strict LSA checking for the GR helper is disabled.

Views

OSPFv3 view

Predefined user roles

network-admin

context-admin

Usage guidelines

With GR helper enabled, when an LSA change on the GR helper is detected, the GR helper device exits the GR helper mode.

Examples

Enable strict LSA checking for the GR helper in OSPFv3 process 1.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] graceful-restart helper strict-lsa-checking
```

Related commands

graceful-restart helper enable

graceful-restart interval

Use **graceful-restart interval** to set the GR restart interval.

Use **undo graceful-restart interval** to restore the default.

Syntax

graceful-restart interval *interval*

undo graceful-restart interval

Default

The GR restart interval is 120 seconds.

Views

OSPFv3 view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies GR restart interval in the range of 40 to 1800 seconds.

Usage guidelines

For GR restart to succeed, the value of the GR restart interval cannot be smaller than the maximum OSPFv3 neighbor dead time of all the OSPFv3 interfaces.

Examples

Set the GR restart interval for OSPFv3 process 1 to 100 seconds.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] graceful-restart interval 100
```

Related commands

ospfv3 timer dead

import-route

Use **import-route** to enable route redistribution.

Use **undo import-route** to disable route redistribution.

Syntax

import-route bgp4+ [*as-number*] [**allow-ibgp**] [**cost** *cost-value* | **nssa-only** | **route-policy** *route-policy-name* | **tag** *tag* | **type** *type*] *

undo import-route bgp4+

import-route { **direct** | **guard** | **static** } [**cost** *cost-value* | **nssa-only** | **route-policy** *route-policy-name* | **tag** *tag* | **type** *type*] *

undo import-route { **direct** | **guard** | **static** }

import-route { **isisv6** | **ospfv3** | **ripng** } [*process-id* | **all-processes**] [**allow-direct** | **cost** *cost-value* | **nssa-only** | **route-policy** *route-policy-name* | **tag** *tag* | **type** *type*] *

undo import-route { **isisv6** | **ospfv3** | **ripng** } [*process-id* | **all-processes**]

Default

OSPFv3 does not redistribute routes.

Views

OSPFv3 view

Predefined user roles

network-admin

context-admin

Parameters

bgp4+: Redistributes IPv6 BGP routes.

direct: Redistributes direct routes.

guard: Redistributes guard routes.

static: Redistributes static routes.

isisv6: Redistributes IPv6 IS-IS routes.

ospfv3: Redistributes OSPFv3 routes.

ripng: Redistributes RIPng routes.

as-number: Redistributes routes from an AS specified by its number in the range of 1 to 4294967295. If you do not specify this argument, this command redistributes all IPv6 EBGP routes. As a best practice, specify an AS number to prevent the system from redistributing excessive IPv6 EBGP routes.

process-id: Specifies the process ID of a routing protocol, in the range of 1 to 65536. The default is 1.

all-processes: Redistributes routes from all the processes of the specified routing protocol.

allow-ibgp: Redistributes IBGP routes. The **import-route bgp4+** command redistributes only EBGP routes. The **import-route bgp4+ allow-ibgp** command redistributes both EBGP and IBGP routes, and might cause routing loops. Therefore, use it with caution.

allow-direct: Redistributes the networks of the local interfaces enabled with the specified routing protocol. If you do not specify this keyword, the networks of the local interfaces are not redistributed. If you specify both the **allow-direct** keyword and the **route-policy** *route-policy-name* option, make sure the **if-match** rule defined in the routing policy does not conflict with the **allow-direct** keyword. For example, if you specify the **allow-direct** keyword, do not configure the **if-match route-type** rule for the routing policy. Otherwise, the **allow-direct** keyword does not take effect.

cost *cost-value*: Specifies a cost for redistributed routes, in the range of 1 to 16777214. The default is 1.

nssa-only: Limits the route advertisement to the NSSA area by setting the P-bit of Type-7 LSAs to 0. If you do not specify this keyword, the P-bit of Type-7 LSAs is set to 1. If the router acts as both an ASBR and an ABR and **FULL** state neighbors exist in the backbone area, the P-bit of Type-7 LSAs originated by the router is set to 0. This keyword applies to NSSA routers.

route-policy *route-policy-name*: Specifies a routing policy to filter redistributed routes. The *route-policy-name* argument is a case-sensitive string of 1 to 63 characters.

tag *tag*: Specifies a tag for external LSAs, in the range of 0 to 4294967295. If you do not specify this option, the tag specified by the **default tag** command applies.

type *type*: Specifies the type for redistributed routes, 1 or 2. The default is 2.

Usage guidelines

An external route is a route to a destination outside the OSPFv3 AS. External routes include the following types:

- **Type-1 external routes**—Have high credibility. The cost of Type-1 external routes is comparable with the cost of OSPFv3 internal routes. The cost of a Type-1 external route equals the cost from the router to the ASBR plus the cost from the ASBR to the external route's destination.

- **Type-2 external routes**—Have low credibility. OSPFv3 considers the cost from the ASBR to a Type-2 external route is much bigger than the cost from the ASBR to an OSPFv3 internal router. The cost of a Type-2 external route equals the cost from the ASBR to the Type-2 external route's destination.

The **import-route** command cannot redistribute default routes.

The **import-route nssa-only** command redistributes AS-external routes in Type-7 LSAs only into the NSSA area.

Examples

Configure OSPFv3 process 1 to redistribute routes from RIPng and specify the type as type 2 and cost as 50.

```
<Sysname> system-view
[Sysname] ospfv3
[Sysname-ospfv3-1] import-route ripng 10 type 2 cost 50
```

Configure OSPFv3 process 100 to redistribute the routes discovered by OSPFv3 process 160.

```
<Sysname> system-view
[Sysname] ospfv3 100
[Sysname-ospfv3-100] import-route ospfv3 160
```

Related commands

default-route-advertise

log-peer-change

Use **log-peer-change** to enable logging for neighbor state changes.

Use **undo log-peer-change** to disable logging for neighbor state changes.

Syntax

log-peer-change

undo log-peer-change

Default

Logging for neighbor state changes is enabled.

Views

OSPFv3 view

Predefined user roles

network-admin

context-admin

Usage guidelines

This feature enables the device to deliver logs about neighbor state changes to its information center. The information center processes logs according to user-defined output rules (whether and where to output logs). For more information about the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Disable logging for neighbor state changes for OSPFv3 process 100.

```
<Sysname> system-view
[Sysname] ospfv3 100
[Sysname-ospfv3-100] undo log-peer-change
```

lsa-generation-interval

Use **lsa-generation-interval** to set the OSPFv3 LSA generation interval.

Use **undo lsa-generation-interval** to restore the default.

Syntax

lsa-generation-interval *maximum-interval* [*minimum-interval* [*incremental-interval*]]

undo lsa-generation-interval

Default

The maximum interval is 5 seconds, the minimum interval is 0 milliseconds, and the incremental interval is 0 milliseconds.

Views

OSPFv3 view

Predefined user roles

network-admin

context-admin

Parameters

maximum-interval: Specifies the maximum OSPFv3 LSA generation interval in the range of 1 to 60 seconds.

minimum-interval: Specifies the minimum OSPFv3 LSA generation interval in the range of 10 to 60000 milliseconds. The default is 0, which indicates that the minimum interval can be any value.

incremental-interval: Specifies the OSPFv3 LSA generation incremental interval in the range of 10 to 60000 milliseconds.

Usage guidelines

When network changes are infrequent, LSAs are generated at the minimum interval. If network changes become frequent, the LSA generation interval increases by the incremental interval × 2^{n-2} for each generation until the maximum interval is reached. The value *n* is the number of generation times.

The minimum interval and the incremental interval cannot be greater than the maximum interval.

Examples

Set the maximum LSA generation interval to 2 seconds, minimum interval to 100 milliseconds, and incremental interval to 100 milliseconds.

```
<Sysname> system-view
[Sysname] ospfv3 100
[Sysname-ospfv3-100] lsa-generation-interval 2 100 100
```

maximum load-balancing

Use **maximum load-balancing** to set the maximum number of equal-cost multi-path (ECMP) routes.

Use **undo maximum load-balancing** to restore the default.

Syntax

maximum load-balancing *number*

undo maximum load-balancing

Default

The maximum number of OSPFv3 ECMP routes equals the maximum number of ECMP routes supported by the system.

Views

OSPFv3 view

Predefined user roles

network-admin

context-admin

Parameters

number: Specifies the maximum number of ECMP routes. When the maximum number is 1, OSPFv3 does not perform load balancing.

Usage guidelines

The value range for the *number* argument of the **maximum load-balancing** command depends on the maximum number of ECMP routes supported by the system. You can use the **max-ecmp-num** command to set the maximum number of ECMP routes supported by the system to *m*. After a reboot, the value range for the *number* argument is 1 to *m*.

Examples

Set the maximum number of ECMP routes to 2.

```
<Sysname> system-view
[Sysname] ospfv3 100
[Sysname-ospfv3-100] maximum load-balancing 2
```

non-stop-routing

Use **non-stop-routing** to enable OSPFv3 NSR.

Use **undo non-stop-routing** to disable OSPFv3 NSR.

Syntax

non-stop-routing

undo non-stop-routing

Default

OSPFv3 NSR is disabled.

Views

OSPFv3 view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command takes effect only for the current process. As a best practice, enable OSPFv3 NSR for each process if multiple OSPFv3 processes exist.

OSPFv3 NSR and OSPFv3 GR are mutually exclusive. Do not configure the **non-stop-routing** command and the **graceful-restart enable** command at the same time.

Examples

Enable NSR for OSPFv3 process 100.

```
<Sysname> system-view
[Sysname] ospfv3 100
[Sysname-ospfv3-100] non-stop-routing
```

nssa

Use **nssa** to configure an area as an NSSA area.

Use **undo nssa** to restore the default.

Syntax

nssa [**default-route-advertise** [**cost** *cost-value* | **nssa-only** | **route-policy** *route-policy-name* | **tag** *tag* | **type** *type*] * | **no-import-route** | **no-summary** | [**translate-always** | **translate-never**] | **suppress-fa** | **translator-stability-interval** *value*] *

undo nssa

Default

No area is configured as an NSSA area.

Views

OSPFv3 area view

Predefined user roles

network-admin

context-admin

Parameters

default-route-advertise: Used on an NSSA ABR or an ASBR only. If it is configured on an NSSA ABR, the ABR redistributes a default route in a Type-7 LSA into the NSSA area. It redistributes a default route regardless of whether a default route exists in the routing table. If it is configured on an ASBR, the ASBR redistributes a default route in a Type-7 LSA only when the default route exists in the routing table.

cost *cost-value*: Specifies a cost for the default route, in the range of 0 to 16777214. If you do not specify this option, the default cost specified by the **default-cost** command applies.

nssa-only: Limits the default route advertisement to the NSSA area by setting the P-bit of Type-7 LSAs to 0. If you do not specify this keyword, the P-bit of Type-7 LSAs is set to 1. If the router acts as both an ASBR and an ABR and **FULL** state neighbors exist in the backbone area, the P-bit is set to 0.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters. When the specified routing policy is matched, the command redistributes a default route in a Type-7 LSA into the OSPFv3 routing domain. The routing policy modifies values in the Type-7 LSA.

tag *tag*: Specifies a tag for the default route, in the range of 0 to 4294967295.

type *type*: Specifies a type for the Type-7 LSA, 1 or 2. The default is 2.

no-import-route: Used on an NSSA ABR to control the **import-route** command to not redistribute routes into the NSSA area.

no-summary: Used only on an ABR to advertise a default route in a Type-3 summary LSA into the NSSA area and to not advertise other summary LSAs into the area. The area is a totally NSSA area.

translate-always: Always translates Type-7 LSAs to Type-5 LSAs. This keyword takes effect only on an NSSA ABR.

translate-never: Never translates Type-7 LSAs to Type-5 LSAs. This keyword takes effect only on an NSSA ABR.

suppress-fa: Suppresses the forwarding address in the Type-7 LSAs from being placed in the Type-5 LSAs.

translator-stability-interval *value*: Specifies the stability interval of the translator. During the interval, the translator can maintain its translating capability after another device becomes the new translator. The *value* argument is the stability interval in the range of 0 to 900 seconds. The default interval is 0. A value of 0 means the translator does not maintain its translating capability when a new translator arises.

Usage guidelines

All routers attached to an NSSA area must be configured with the **nssa** command in area view.

Examples

Configure Area 1 as an NSSA area.

```
<Sysname> system-view
[Sysname] ospfv3 120
[Sysname-ospfv3-120] area 1
[Sysname-ospfv3-120-area-0.0.0.1] nssa
```

Related commands

default-cost

ospfv3

Use **ospfv3** to enable an OSPFv3 process and enter OSPFv3 view.

Use **undo ospfv3** to disable an OSPFv3 process.

Syntax

ospfv3 [*process-id* | **vpn-instance** *vpn-instance-name*] *

undo ospfv3 [*process-id*]

Default

No OSPFv3 process is enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. The default process ID is 1.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the OSPFv3 process runs on the public network.

Usage guidelines

Specify a router ID for the OSPFv3 process. Otherwise, the OSPFv3 process cannot generate LSAs.

Examples

Enable OSPFv3 process 120 and set the router ID to 1.1.1.1.

```
<Sysname> system-view
[Sysname] ospfv3 120
[Sysname-ospfv3-120] router-id 1.1.1.1
```

ospfv3 area

Use **ospfv3 area** to enable an OSPFv3 process on an interface and specify an area for the interface.

Use **undo ospfv3 area** to disable an OSPFv3 process on an interface.

Syntax

ospfv3 *process-id* **area** *area-id* [**instance** *instance-id*]

undo ospfv3 *process-id* **area** *area-id* [**instance** *instance-id*]

Default

No OSPFv3 processes are enabled on an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535.

area-id: Specifies an area by its ID, an IPv4 address or a decimal integer in the range of 0 to 4294967295 that is translated into the IPv4 address format.

instance *instance-id*: Specifies an instance by its ID in the range of 0 to 255. The default is 0.

Examples

Configure GigabitEthernet 1/0/1 to run instance 1 of OSPFv3 process 1 in Area 1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospfv3 1 area 1 instance 1
```

ospfv3 bfd enable

Use **ospfv3 bfd enable** to enable BFD on an OSPFv3 interface.

Use **undo ospfv3 bfd enable** to disable BFD on an OSPFv3 interface.

Syntax

ospfv3 bfd enable [**instance** *instance-id*]

undo ospfv3 bfd enable [**instance** *instance-id*]

Default

BFD is disabled on an OSPFv3 interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

instance *instance-id*: Specifies an instance by its ID in the range of 0 to 255. The default is 0.

Usage guidelines

BFD provides a mechanism to quickly detect the connectivity of links between OSPFv3 neighbors, improving the convergence speed of OSPFv3.

OSPFv3 uses BFD to implement bidirectional control detection.

Examples

Enable BFD on GigabitEthernet 1/0/1 in instance 1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospfv3 bfd enable instance 1
```

ospfv3 cost

Use **ospfv3 cost** to set an OSPFv3 cost for an interface in an instance.

Use **undo ospfv3 cost** to remove the configuration.

Syntax

ospfv3 cost *cost-value* [**instance** *instance-id*]

undo ospfv3 cost [**instance** *instance-id*]

Default

The cost is 1 for a VLAN interface, is 0 for a loopback interface, and is computed according to the interface bandwidth for other interfaces.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

cost-value: Specifies an OSPFv3 cost in the range of 0 to 65535 for a loopback interface, and in the range of 1 to 65535 for other interfaces.

instance *instance-id*: Specifies an instance by its ID in the range of 0 to 255. The default is 0.

Examples

Set the OSPFv3 cost to 33 for GigabitEthernet 1/0/1 in instance 1.

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospfv3 cost 33 instance 1
```

ospfv3 dr-priority

Use **ospfv3 dr-priority** to set the router priority for an interface in an instance.

Use **undo ospfv3 dr-priority** to remove the configuration.

Syntax

ospfv3 dr-priority *priority* [**instance** *instance-id*]

undo ospfv3 dr-priority [**instance** *instance-id*]

Default

An interface has a router ID of 1.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

priority: Specifies a router priority in the range of 0 to 255.

instance *instance-id*: Specifies an instance by its ID in the range of 0 to 255. The default is 0.

Usage guidelines

An interface's router priority determines its privilege in DR/BDR selection.

Examples

Set the router priority for GigabitEthernet 1/0/1 in instance 1 to 8.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospfv3 dr-priority 8 instance 1
```

ospfv3 fast-reroute lfa-backup exclude

Use **ospfv3 fast-reroute lfa-backup exclude** to disable LFA on an interface.

Use **undo ospfv3 fast-reroute lfa-backup exclude** to remove the configuration.

Syntax

ospfv3 fast-reroute lfa-backup exclude [**instance** *instance-id*]

undo ospfv3 fast-reroute lfa-backup exclude [**instance** *instance-id*]

Default

LFA is enabled on an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

instance *instance-id*: Specifies an instance by its ID in the range of 0 to 255. The default is 0.

Usage guidelines

An interface enabled with LFA can be selected as a backup interface. After you disable LFA on the interface, it cannot be selected as a backup interface.

Examples

Disable GigabitEthernet 1/0/1 from calculating a backup next hop by using the LFA algorithm.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospfv3 fast-reroute lfa-backup exclude
```

ospfv3 ipsec-profile

Use **ospfv3 ipsec-profile** to apply an IPsec profile to an OSPFv3 interface.

Use **undo ospfv3 ipsec-profile** to remove the IPsec profile from the OSPFv3 interface.

Syntax

ospfv3 ipsec-profile *profile-name* [**instance** *instance-id*]

undo ospfv3 ipsec-profile [**instance** *instance-id*]

Default

No IPsec profile is applied to an OSPFv3 interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

profile-name: Specifies an IPsec profile by its name, a case-insensitive string of 1 to 63 characters.

instance *instance-id*: Specifies an instance by its ID in the range of 0 to 255. The default is 0.

Usage guidelines

An IPsec profile must be specified in this command. For more information about IPsec profiles, see *Security Configuration Guide*.

Examples

Apply IPsec profile **profile001** to GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospfv3 ipsec-profile profile001
```

ospfv3 mib-binding

Use **ospfv3 mib-binding** to bind an OSPFv3 process to MIB.

Use **undo ospfv3 mib-binding** to restore the default.

Syntax

ospfv3 mib-binding *process-id*

undo ospfv3 mib-binding

Default

MIB is bound to the OSPFv3 process with the smallest process ID.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535.

Usage guidelines

If the specified process ID does not exist, the MIB binding configuration fails.

Deleting an OSPFv3 process that has been bound to MIB unbinds the OSPFv3 process from MIB, and re-binds MIB to the OSPFv3 process with the smallest process ID.

Examples

Bind OSPFv3 process 100 to MIB.

```
<Sysname> system-view
[Sysname] ospfv3 mib-binding 100
```

ospfv3 mtu-ignore

Use **ospfv3 mtu-ignore** to configure an interface to ignore MTU check during DD packet exchange.

Use **undo ospfv3 mtu-ignore** to remove the configuration.

Syntax

ospfv3 mtu-ignore [**instance** *instance-id*]

undo ospfv3 mtu-ignore [**instance** *instance-id*]

Default

An interface performs MTU check during DD packet exchange.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

instance *instance-id*: Specifies an instance by its ID in the range of 0 to 255. The default is 0.

Usage guidelines

A neighbor relationship can be established only if the interface's MTU is the same as that of the peer.

Examples

Configure GigabitEthernet 1/0/1 that belongs to instance 1 to ignore MTU check during DD packet exchange.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospfv3 mtu-ignore instance 1
```

ospfv3 network-type

Use **ospfv3 network-type** to specify the network type for an OSPFv3 interface.

Use **undo ospfv3 network-type** to remove the configuration.

Syntax

ospfv3 network-type { **broadcast** | **nbma** | **p2mp** [**unicast**] | **p2p** } [**instance** *instance-id*]

undo ospfv3 network-type [**instance** *instance-id*]

Default

The network type of an OSPFv3 interface is broadcast.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

broadcast: Specifies the network type as broadcast.

nbma: Specifies the network type as NBMA.

p2mp: Specifies the network type as P2MP.

unicast: Specifies the P2MP interface to unicast OSPFv3 packets. By default, a P2MP interface multicasts OSPFv3 packets.

p2p: Specifies the network type as P2P.

instance *instance-id*: Specifies an instance by its ID in the range of 0 to 255. The default is 0.

Usage guidelines

If a router on a broadcast network does not support multicast, configure the network type for the connected interfaces as NBMA.

If any two routers on an NBMA network are directly connected through a virtual link, the network is fully meshed. You can configure the network type for the connected interfaces as NBMA. If two routers are not directly connected, configure the P2MP network type so that the two routers can exchange routing information through another router.

When the network type of an interface is NBMA or P2MP unicast, you must use the **peer** command to specify the neighbor.

When the network type of an interface is P2MP unicast, all OSPFv3 packets are unicast by the interface.

Examples

Specify the OSPFv3 network type for GigabitEthernet 1/0/1 as NBMA.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospfv3 network-type nbma
```

Related commands

ospfv3 dr-priority

ospfv3 peer

Use **ospfv3 peer** to specify a neighbor and the DR priority of the neighbor.

Use **undo ospfv3 peer** to remove the configuration.

Syntax

ospfv3 peer *ipv6-address* [**cost** *cost-value* | **dr-priority** *priority*] [**instance** *instance-id*]

undo ospfv3 peer *ipv6-address* [**instance** *instance-id*]

Default

No link-local address is specified for the neighbor interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address: Specifies the link-local IPv6 address of the neighbor.

cost *cost-value*: Specifies the cost of the neighbor, in the range of 1 to 65535.

dr-priority *priority*: Specifies the DR priority of the neighbor, in the range of 0 to 255. The default is 1.

instance *instance-id:* Specifies an instance by its ID in the range of 0 to 255. The default is 0.

Usage guidelines

For NBMA and P2MP interfaces (only when in unicast mode), you must specify the link-local IPv6 addresses of their neighbors because these interfaces cannot find neighbors through broadcasting hello packets. For NBMA interfaces, you can also specify DR priorities for their neighbors.

Examples

On GigabitEthernet 1/0/1, specify the link-local address of its neighbor as FE80::1111.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ospfv3 peer fe80::1111
```

ospfv3 prefix-suppression

Use **ospfv3 prefix-suppression** to disable an OSPFv3 interface from advertising all its prefixes.

Use **undo ospfv3 prefix-suppression** to remove the configuration.

Syntax

ospfv3 prefix-suppression [**disable**] [**instance** *instance-id*]

undo ospfv3 prefix-suppression [**instance** *instance-id*]

Default

Prefix suppression is disabled on an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

disable: Disables prefix suppression for an interface.

instance *instance-id*: Specifies an instance by its ID in the range of 0 to 255. The default is 0.

Usage guidelines

To disable prefix suppression for an interface associated with an OSPFv3 process that has been enabled with prefix suppression, use the **ospfv3 prefix-suppression disable** command on that interface.

Examples

Enable prefix suppression for GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospfv3 prefix-suppression
```

Related commands

prefix-suppression

ospfv3 primary-path-detect bfd

Use **ospfv3 primary-path-detect bfd** to enable BFD for OSPFv3 FRR.

Use **undo ospfv3 primary-path-detect bfd** to disable BFD for OSPFv3 FRR.

Syntax

ospfv3 primary-path-detect bfd { **ctrl** | **echo** } [**instance** *instance-id*]

undo ospfv3 primary-path-detect bfd [**instance** *instance-id*]

Default

BFD is disabled for OSPFv3 FRR.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ctrl: Enables BFD control packet mode.

echo: Enables BFD echo packet mode.

instance *instance-id*: Specifies an instance by its ID in the range of 0 to 255. The default is 0.

Usage guidelines

This command enables OSPFv3 FRR to use BFD to detect primary link failures.

For an interface to run the BFD session in echo packet mode correctly, make sure the interface has an IPv6 global unicast address. For more information about IPv6 global unicast addresses, see IPv6 basics configuration in *Layer 3—IP Services Configuration Guide*.

Examples

On GigabitEthernet 1/0/1, enable BFD echo packet mode for OSPFv3 FRR.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] fast-reroute lfa
[Sysname-ospfv3-1] quit
[Sysname] bfd echo-source-ipv6 1::1
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospfv3 primary-path-detect bfd echo
```

ospfv3 timer dead

Use **ospfv3 timer dead** to set the OSPFv3 neighbor dead time.

Use **undo ospfv3 timer dead** to remove the configuration.

Syntax

ospfv3 timer dead *seconds* [**instance** *instance-id*]

undo ospfv3 timer dead [**instance** *instance-id*]

Default

The OSPFv3 neighbor dead time is 40 seconds for P2P and broadcast interfaces, and is 120 seconds for P2MP and NBMA interfaces.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies the dead time in the range of 1 to 65535 seconds.

instance *instance-id*: Specifies an instance by its ID in the range of 0 to 255. The default is 0.

Usage guidelines

If an interface receives no hello packet from a neighbor within the dead time, the interface determines that the neighbor is down.

The dead time must be a minimum of four times the hello time and must be identical on interfaces attached to the same network segment.

Examples

Set the OSPFv3 neighbor dead time to 60 seconds for GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospfv3 timer dead 60
```

Related commands

ospfv3 timer hello

ospfv3 timer hello

Use **ospfv3 timer hello** to set the hello interval for an interface.

Use **undo ospfv3 timer hello** to remove the configuration.

Syntax

ospfv3 timer hello *seconds* [**instance** *instance-id*]

undo ospfv3 timer hello [**instance** *instance-id*]

Default

The hello interval is 10 seconds for P2P and broadcast interfaces, and is 30 seconds for P2MP or NBMA interfaces.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies the hello interval in the range of 1 to 65535 seconds.

instance *instance-id*: Specifies an instance by its ID in the range of 0 to 255. The default is 0.

Usage guidelines

The shorter the hello interval is, the faster the topology converges and the more resources are consumed. Make sure the hello interval on two neighboring interfaces is the same.

Examples

Set the hello interval to 20 seconds for GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospfv3 timer hello 20
```

Related commands

ospfv3 timer dead

ospfv3 timer poll

Use **ospfv3 timer poll** to set the poll interval on an NBMA interface.

Use **undo ospfv3 timer poll** to remove the configuration.

Syntax

ospfv3 timer poll *seconds* [**instance** *instance-id*]

undo ospfv3 timer poll [**instance** *instance-id*]

Default

The poll interval is 120 seconds on an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies the poll interval in the range of 1 to 65535 seconds.

instance *instance-id*: Specifies an interface instance by its ID in the range of 0 to 255. The default is 0.

Usage guidelines

When an NBMA interface finds its neighbor is down, it sends hello packets at the poll interval.

The poll interval must be a minimum of four times the hello interval.

Examples

Set the poll interval on GigabitEthernet 1/0/1 to 120 seconds.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospfv3 timer poll 120
```

Related commands

ospfv3 timer hello

ospfv3 timer retransmit

Use **ospfv3 timer retransmit** to set the LSA retransmission interval for an interface.

Use **undo ospfv3 timer retransmit** to remove the configuration.

Syntax

ospfv3 timer retransmit *seconds* [**instance** *instance-id*]

undo ospfv3 timer retransmit [**instance** *instance-id*]

Default

The interval is 5 seconds.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies the LSA retransmission interval in the range of 1 to 3600 seconds.

instance *instance-id*: Specifies an instance by its ID in the range of 0 to 255. The default is 0.

Usage guidelines

After the device sends an LSA to its neighbor, it waits for an acknowledgment. If the device receives no acknowledgment after the LSA retransmission interval elapses, it will retransmit the LSA.

To avoid unnecessary retransmissions, set an appropriate retransmission interval. For example, you can set a large retransmission interval value on a low-speed link.

Examples

Set the LSA retransmission interval to 12 seconds on GigabitEthernet 1/0/1 in instance 1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospfv3 timer retransmit 12 instance 1
```

ospfv3 trans-delay

Use **ospfv3 trans-delay** to set the transmission delay for an interface.

Use **undo ospfv3 trans-delay** to remove the configuration.

Syntax

ospfv3 trans-delay *seconds* [**instance** *instance-id*]

undo ospfv3 trans-delay [**instance** *instance-id*]

Default

The transmission delay is 1 second.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies the transmission delay in the range of 1 to 3600 seconds.

instance *instance-id*: Specifies an instance by its ID in the range of 0 to 255. The default is 0.

Usage guidelines

Each LSA in the LSDB has an age that increases by 1 every second, but the age does not change during transmission. Adding a transmission delay into the age time is important in low speed networks.

Examples

Set the transmission delay to 3 seconds for GigabitEthernet 1/0/1 in instance 1.

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospfv3 trans-delay 3 instance 1
```

preference

Use **preference** to set a preference for OSPFv3 routes.

Use **undo preference** to remove the configuration.

Syntax

preference [**ase**] { *preference* | **route-policy** *route-policy-name* } *

undo preference [**ase**]

Default

The preference is 10 for OSPFv3 internal routes and 150 for OSPFv3 external routes.

Views

OSPFv3 view

Predefined user roles

network-admin

context-admin

Parameters

ase: Specifies a preference for OSPFv3 external routes. If you do not specify this keyword, the command sets a preference for OSPFv3 internal routes.

preference: Specifies the preference value in the range of 1 to 255. A smaller value represents a higher preference.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to set a preference for matching routes.

Usage guidelines

If multiple routing protocols find multiple routes to the same destination, the router uses the route found by the protocol with the highest preference.

Examples

Set a preference of 150 for OSPFv3 routes.

```
<Sysname> system-view
[Sysname] OSPFv3
[Sysname-OSPFv3-1] preference 150
```

prefix-suppression

Use **prefix-suppression** to disable an OSPFv3 process from advertising all prefixes except for the prefixes of loopback interfaces and passive interfaces.

Use **undo prefix-suppression** to restore the default.

Syntax

prefix-suppression

undo prefix-suppression

Default

An OSPFv3 process advertises all prefixes.

Views

OSPFv3 view

Predefined user roles

network-admin

context-admin

Usage guidelines

By default, an OSPFv3 interface advertises all of its prefixes in LSAs. To speed up OSPFv3 convergence, you can suppress interfaces from advertising all of their prefixes. This feature helps improve network security by preventing IP routing to the suppressed networks.

To disable an OSPFv3 process from advertising the prefixes of loopback and passive interfaces, configure prefix suppression on the interfaces by using the **ospfv3 prefix-suppression** command.

When prefix suppression is enabled:

- OSPFv3 does not advertise the prefixes of suppressed interfaces in Type-8 LSAs.
- On broadcast and NBMA networks, the DR does not advertise the prefixes of suppressed interfaces in Type-9 LSAs that reference Type-2 LSAs.
- On P2P and P2MP networks, OSPFv3 does not advertise the prefixes of suppressed interfaces in Type-9 LSAs that reference Type-1 LSAs.

Examples

Enable prefix suppression for OSPFv3 process 100.

```
<Sysname> system-view
[Sysname] ospfv3 100
[Sysname-ospfv3-100] prefix-suppression
```

Related commands

ospfv3 prefix-suppression

reset ospfv3 event-log

Use **reset ospfv3 event-log** to clear OSPFv3 log information.

Syntax

reset ospfv3 [*process-id*] **event-log** [**lsa-flush** | **peer** | **spf**]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command clears OSPFv3 log information for all OSPFv3 processes.

lsa-flush: Clears LSA aging log information.

peer: Clears neighbor log information.

spf: Clears route calculation log information.

Usage guidelines

If you do not specify a log type, this command clears all log information.

Examples

Clear OSPFv3 route calculation log information for all OSPFv3 processes.

```
<Sysname> reset ospfv3 event-log spf
```

Related commands

display ospfv3 event-log

reset ospfv3 process

Use **reset ospfv3 process** to restart OSPFv3 processes.

Syntax

reset ospfv3 [*process-id*] **process** [**graceful-restart**]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command restarts all OSPFv3 processes.

graceful-restart: Restarts the OSPFv3 process by using GR.

Usage guidelines

The **reset ospfv3 process** command performs the following actions:

- Clears all invalid LSAs without waiting for their timeouts.
- Starts a new DR/BDR election.
- Keeps previous OSPFv3 configurations.

The system prompts you to select whether to restart OSPFv3 process upon execution of this command.

Examples

Restart all OSPFv3 processes.

```
<Sysname> reset ospfv3 process
Reset OSPFv3 process? [Y/N]:y
```

reset ospfv3 redistribution

Use **reset ospfv3 redistribution** to restart route redistribution.

Syntax

reset ospfv3 [*process-id*] **redistribution**

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command restarts route redistribution for all OSPFv3 processes.

Examples

Restart route redistribution.

```
<Sysname> reset ospfv3 redistribution
```

reset ospfv3 statistics

Use **reset ospfv3 statistics** to clear OSPFv3 statistics.

Syntax

reset ospfv3 [*process-id*] **statistics**

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command clears statistics for all OSPFv3 processes.

Examples

Clear statistics for all OSPFv3 processes.

```
<Sysname> reset ospfv3 statistics
```

router-id

Use **router-id** to configure a router ID.

Use **undo router-id** to restore the default.

Syntax

router-id *router-id*

undo router-id

Default

No router ID is configured.

Views

OSPFv3 view

Predefined user roles

network-admin

context-admin

Parameters

router-id: Specifies a router ID in IPv4 address format.

Usage guidelines

The router ID is the unique identifier for the device to run OSPFv3 in the AS. An OSPFv3 process cannot run without a router ID.

You must specify a unique router ID for each OSPFv3 process in an AS. When you run multiple OSPFv3 processes on a router, specify a unique router ID for each OSPFv3 process as a best practice.

Examples

Configure the router ID 10.1.1.3 for OSPFv3 process 1.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] router-id 10.1.1.3
```

Related commands

ospfv3

silent-interface

Use **silent-interface** to disable the specified interface from receiving and sending OSPFv3 packets.

Use **undo silent-interface** to remove the configuration.

Syntax

silent-interface { *interface-type interface-number* | **all** }

undo silent-interface { *interface-type interface-number* | **all** }

Default

An interface can receive and send OSPFv3 packets.

Views

OSPFv3 view

Predefined user roles

network-admin

context-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

all: Specifies all interfaces.

Usage guidelines

Multiple processes can disable the same interface from receiving and sending OSPFv3 packets. However, the **silent-interface** command takes effect only on interfaces enabled with the current process.

Examples

Disable GigabitEthernet 1/0/1 from receiving and sending OSPFv3 packets in OSPFv3 processes 100 and 200.

```
<Sysname> system-view
[Sysname] ospfv3 100
[Sysname-ospfv3-100] router-id 10.100.1.9
[Sysname-ospfv3-100] silent-interface gigabitethernet 1/0/1
[Sysname-ospfv3-100] quit
[Sysname] ospfv3 200
[Sysname-ospfv3-200] router-id 20.100.1.9
[Sysname-ospfv3-200] silent-interface gigabitethernet 1/0/1
```

snmp context-name

Use **snmp context-name** to configure an SNMP context for OSPFv3.

Use **undo snmp context-name** to restore the default.

Syntax

snmp context-name *context-name*

undo snmp context-name

Default

No SNMP contexts exist for OSPFv3.

Views

OSPFv3 view

Predefined user roles

network-admin

context-admin

Parameters

context-name: Specifies a context name, a case-sensitive string of 1 to 32 characters.

Usage guidelines

The standard OSPFv3 MIB provides only single-instance MIB objects. For SNMP to correctly identify OSPFv3 management information in the standard OSPFv3 MIB, you must configure a unique context name for OSPFv3. If multiple OSPFv3 processes exist, you must assign a unique context to each process.

Context is a method introduced to SNMPv3 for multiple-instance management. For SNMPv1/v2c, you must specify a community name as a context name for protocol identification.

Examples

Configure the SNMP context name as **mib** for OSPFv3 process 1.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] snmp context-name mib
```

snmp trap rate-limit

Use **snmp trap rate-limit** to set the SNMP notification output interval and the maximum number of SNMP notifications that can be output at each interval.

Use **undo snmp trap rate-limit** to restore the default.

Syntax

snmp trap rate-limit interval *trap-interval* **count** *trap-number*

undo snmp trap rate-limit

Default

OSPFv3 outputs a maximum of seven SNMP notifications within 10 seconds.

Views

OSPFv3 view

Predefined user roles

network-admin

context-admin

Parameters

interval *trap-interval*: Specifies the SNMP notification output interval in the range of 2 to 60 seconds.

count *trap-number*: Specifies the number of SNMP notifications output by OSPFv3 at each interval, in the range of 0 to 300. The value of 0 indicates that OSPFv3 does not output SNMP notifications.

Examples

Configure OSPFv3 to output a maximum of 10 SNMP notifications within 5 seconds.

```
<Sysname> system-view
[Sysname] ospfv3 100
[Sysname-ospfv3-100] snmp trap rate-limit interval 5 count 10
```

snmp-agent trap enable ospfv3

Use **snmp-agent trap enable ospfv3** to enable SNMP notifications for OSPFv3.

Use **undo snmp-agent trap enable ospfv3** to disable SNMP notifications for OSPFv3.

Syntax

snmp-agent trap enable ospfv3 [**grrestarter-status-change** | **grhelper-status-change** | **if-state-change** | **if-cfg-error** | **if-bad-pkt** | **neighbor-state-change** | **nssatranslator-status-change** | **virtif-bad-pkt** | **virtif-cfg-error** | **virtif-state-change** | **virtgrhelper-status-change** | **virtneighbor-state-change**] *

undo snmp-agent trap enable ospfv3 [**grrestarter-status-change** | **grhelper-status-change** | **if-state-change** | **if-cfg-error** | **if-bad-pkt** | **neighbor-state-change** | **nssatranslator-status-change** | **virtif-bad-pkt** | **virtif-cfg-error** | **virtif-state-change** | **virtgrhelper-status-change** | **virtneighbor-state-change**] *

Default

SNMP notifications for OSPFv3 are enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

grrestarter-status-change: Specifies notifications about GR restarter state changes.

grhelper-status-change: Specifies notifications about GR helper state changes.

if-state-change: Specifies notifications about interface state changes.

if-cfg-error: Specifies notifications about error configuration of an interface.

if-bad-pkt: Specifies notifications about error messages received on an interface.

neighbor-state-change: Specifies notifications about neighbor state changes.

nssatranslator-status-change: Specifies notifications about NSSA translator state changes.

virtif-bad-pkt: Specifies notifications about error messages received on a virtual interface.

virtif-cfg-error: Specifies notifications about error configuration of a virtual interface.

virtif-state-change: Specifies notifications about virtual interface state changes.

virtgrhelper-status-change: Specifies notifications about neighbor GR helper state changes of a virtual interface.

virtneighbor-state-change: Specifies notifications about the neighbor state changes of a virtual interface.

Examples

Disable SNMP notifications for OSPFv3.

```
<Sysname> system-view
[Sysname] undo snmp-agent trap enable ospfv3
```

spf-schedule-interval

Use **spf-schedule-interval** to set the OSPFv3 SPF calculation interval.

Use **undo spf-schedule-interval** to restore the default.

Syntax

spf-schedule-interval *maximum-interval* [*minimum-interval* [*incremental-interval*]]

undo spf-schedule-interval

Default

The maximum SPF calculation interval is 5 seconds, the minimum interval is 50 milliseconds, and the incremental interval is 200 milliseconds.

Views

OSPFv3 view

Predefined user roles

network-admin

context-admin

Parameters

maximum-interval: Specifies the maximum OSPFv3 route calculation interval in the range of 1 to 60 seconds.

minimum-interval: Specifies the minimum OSPFv3 route calculation interval in the range of 10 to 60000 milliseconds.

incremental-interval: Specifies the incremental OSPFv3 route calculation interval in the range of 10 to 60000 milliseconds.

Usage guidelines

Based on the LSDB, an OSPFv3 router uses SPF to calculate a shortest path tree with itself being the root. OSPFv3 uses the shortest path tree to determine the next hop to a destination. By adjusting the SPF calculation interval, you can prevent overconsumption of bandwidth and router resources due to frequent topology changes.

For a stable network, the minimum interval is used. If network changes become frequent, the SPF calculation interval increases by the incremental interval × 2^{n-2} for each calculation until the maximum interval is reached. The value *n* is the number of calculation times.

The minimum interval and the incremental interval cannot be greater than the maximum interval.

Examples

Set the maximum SPF calculation interval to 10 seconds, minimum interval to 500 milliseconds, and incremental interval to 300 milliseconds.

```
<Sysname> system-view
[Sysname] ospfv3 100
[Sysname-ospfv3-100] spf-schedule-interval 10 500 300
```

stub

Use **stub** to configure an area as a stub area.

Use **undo stub** to restore the default.

Syntax

stub [**default-route-advertise-always** | **no-summary**] *

undo stub

Default

No area is configured as a stub area.

Views

OSPFv3 area view

Predefined user roles

network-admin

context-admin

Parameters

default-route-advertise-always: Enables the ABR to always advertise a default route into the stub area.

no-summary: Enables the ABR to advertise only a default route in an Inter-Area-Prefix-LSA into the stub area. No AS-external-LSA, Inter-Area-Prefix-LSA, or other Inter-Area-Router-LSA is advertised in the area. The area is a totally stub area.

Usage guidelines

To remove the **no-summary** configuration on an ABR, execute the **stub** command again to overwrite it.

To configure an area as a stub area, execute the **stub** command on all routers attached to the area.

Examples

Configure OSPFv3 area 1 as a stub area.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] area 1
[Sysname-ospfv3-1-area-0.0.0.1] stub
```

Related commands

default-cost

stub-router

Use **stub-router** to configure a router as a stub router.

Use **undo stub-router** to restore the default.

Syntax

stub-router r-bit [**include-stub** | **on-startup** { *seconds* | **wait-for-bgp** [*seconds*] }] *

stub-router max-metric [**external-lsa** [*max-metric-value*] | **summary-lsa** [*max-metric-value*] | **include-stub** | **on-startup** { *seconds* | **wait-for-bgp** [*seconds*] }] *

undo stub-router

Default

The router is not configured as a stub router.

Views

OSPFv3 view

Predefined user roles

network-admin

context-admin

Parameters

r-bit: Clears the R-bit of the Option field in Type-1 LSAs.

max-metric: Advertises the locally generated Type-1 LSAs with the maximum cost of 65535.

external-lsa *max-metric-value*: Specifies a cost for external LSAs, in the range of 1 to 16777215. The default is 16711680.

summary-lsa *max-metric-value*: Specifies a cost for Type-3 and Type-4 LSAs, in the range of 1 to 16777215. The default is 16711680.

include-stub: Specifies the cost for Type-9 LSAs that reference Type-1 LSAs to the maximum value 65535.

on-startup *seconds*: Specifies the router as a stub router during reboot, and specifies the timeout time in the range of 5 to 86400 seconds.

wait-for-bgp *seconds*: Specifies the router as a stub router during BGP route convergence after reboot, and specifies the timeout time in the range of 5 to 86400 seconds. The default timeout time is 600 seconds.

Usage guidelines

You can use the **stub-router r-bit** command or **stub-router max-metric** command to configure a router as a stub router.

- The **stub-router r-bit** command clears the R-bit of the Option field in Type-1 LSAs. When the R-bit is clear, the OSPFv3 router can participate in OSPFv3 topology distribution without forwarding traffic.
- The **stub-router max-metric** command specifies the OSPFv3 max-metric router LSA feature. This feature enables OSPFv3 to advertise its locally generated Type-1 LSAs with a maximum cost of 65535. Neighbors do not send packets to the stub router as long as they have a route with a smaller cost.

Examples

Configure a stub router.

```
<Sysname> system-view
[Sysname] ospfv3 100
[Sysname-ospfv3-100] stub-router r-bit
```

transmit-pacing

Use **transmit-pacing** to set the LSU transmission interval and the maximum number of LSU packets that can be sent at each interval.

Use **undo transmit-pacing** to restore the default.

Syntax

transmit-pacing interval *interval* **count** *count*

undo transmit-pacing

Default

An OSPFv3 interface sends a maximum of three LSU packets every 20 milliseconds.

Views

OSPFv3 view

Predefined user roles

network-admin

context-admin

Parameters

interval *interval*: Specifies an interval at which an interface sends LSU packets, in the range of 10 to 1000 milliseconds. If the router has multiple OSPFv3 interfaces, increase the interval to reduce the total number of LSU packets sent by the router every second.

count *count*: Specifies the maximum number of LSU packets sent by an interface at each interval, in the range of 1 to 200. If the router has multiple OSPFv3 interfaces, decrease the maximum number to reduce the total number of LSU packets sent by the router every second.

Examples

Configure all the interfaces running OSPFv3 process 1 to send a maximum of 10 LSU packets every 30 milliseconds.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] transmit-pacing interval 30 count 10
```

vlink-peer

Use **vlink-peer** to configure a virtual link.

Use **undo vlink-peer** to remove a virtual link.

Syntax

vlink-peer *router-id* [**dead** *seconds* | **hello** *seconds* | **instance** *instance-id* | **ipsec-profile** *profile-name* | **keychain** *keychain-name* | **retransmit** *seconds* | **trans-delay** *seconds*] *

undo vlink-peer *router-id* [**dead** | **hello** | **ipsec-profile** | **keychain** | **retransmit** | **trans-delay**] *

Default

No virtual links exist.

Views

OSPFv3 area view

Predefined user roles

network-admin

context-admin

Parameters

router-id: Specifies the router ID of the neighbor on the virtual link.

dead *seconds*: Specifies the dead interval in the range of 1 to 32768 seconds. The default is 40. The dead interval must be identical with that on the virtual link neighbor, and must be a minimum of four times the hello interval.

hello *seconds*: Specifies the hello interval in the range of 1 to 8192 seconds. The default is 10. It must be identical with the hello interval on the virtual link neighbor.

instance *instance-id*: Specifies the instance ID of a virtual link, in the range of 0 to 255. The default is 0.

ipsec-profile *profile-name:* Specifies an IPsec profile by its name, a case-insensitive string of 1 to 63 characters. For more information about IPsec profiles, see *Security Configuration Guide*.

keychain: Specifies the keychain authentication mode.

keychain-name: Specifies a keychain by its name, a case-sensitive string of 1 to 63 characters.

retransmit *seconds*: Specifies the retransmission interval in the range of 1 to 3600 seconds. The default is 5.

trans-delay *seconds*: Specifies the transmission delay interval in the range of 1 to 3600 seconds. The default is 1.

Usage guidelines

You can configure a virtual link to maintain connectivity between a non-backbone area and the backbone, or maintain connectivity within the backbone. A virtual link is similar to an interface with OSPFv3 enabled. You can configure parameters such as **hello**, **dead**, **retransmit** and **trans-delay** for the virtual link.

Both ends of a virtual link must be ABRs that are configured with the **vlink-peer** command.

The following guidelines apply to parameters:

- The smaller the hello interval is, the faster the network converges, and the more network resources are consumed.
- For a low speed link, set a large retransmission interval to avoid unnecessary retransmissions.
- Specify a transmission delay with the **trans-delay** keyword depending on the interface delay.

The authentication mode specified for an OSPFv3 virtual link has a higher priority than the mode specified for the backbone area. If no authentication mode is specified for the virtual link, the mode specified for the backbone area applies.

When keychain authentication is configured for an OSPFv3 virtual link, OSPFv3 performs the following operations before sending a packet:

1. Obtains a valid send key from the keychain.

   OSPFv3 does not send the packet if it fails to obtain a valid send key.
2. Uses the key ID, authentication algorithm, and key string to authenticate the packet.

   If the key ID is greater than 65535, OSPFv3 does not send the packet.

When keychain authentication is configured for an OSPFv3 virtual link, OSPFv3 performs the following operations after receiving a packet:

1. Uses the key ID carried in the packet to obtain a valid accept key from the keychain.

   OSPFv3 discards the packet if it fails to obtain a valid accept key.
2. Uses the authentication algorithm and key string for the valid accept key to authenticate the packet.

   If the authentication fails, OSPFv3 discards the packet.

OSPFv3 supports the HMAC-SHA-256 and HMAC-SM3 authentication algorithms for keychain authentication.

The ID of keys used for keychain authentication can only be in the range of 0 to 65535.

Examples

Configure a virtual link to 10.10.0.3.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] area 1
[Sysname-ospfv3-1-area-0.0.0.1] vlink-peer 10.10.0.3
```

Related commands

display ospfv3 vlink

Contents

IS-IS commands

address-family ipv4

Use **address-family ipv4** to create the IS-IS IPv4 address family and enter its view.

Use **undo address-family ipv4** to delete the IS-IS IPv4 address family and all configurations in the view.

Syntax

address-family ipv4 [**unicast**]

undo address-family ipv4 [**unicast**]

Default

No IS-IS IPv4 address family exists.

Views

IS-IS view

Predefined user roles

network-admin

context-admin

Parameters

unicast: Specifies the unicast address family (the default).

Examples

Create the IS-IS IPv4 address family and enter its view.

```
<Sysname> system-view
[Sysname] isis 100
[Sysname-isis-100] address-family ipv4
[Sysname-isis-100-ipv4]
```

address-family ipv6

Use **address-family ipv6** to create the IS-IS IPv6 address family and enter its view.

Use **undo address-family ipv6** to remove the IS-IS IPv6 address family and all configurations in the view.

Syntax

address-family ipv6 [**unicast**]

undo address-family ipv6 [**unicast**]

Default

No IS-IS IPv6 address family exists.

Views

IS-IS view

Predefined user roles

network-admin

context-admin

Parameters

unicast: Specifies the unicast address family (the default).

Usage guidelines

This command enables IPv6 for an IS-IS process.

Examples

Create the IS-IS IPv6 address family and enter its view.

```
<Sysname> system-view
[Sysname] isis 100
[Sysname-isis-100] address-family ipv6
[Sysname-isis-100-ipv6]
```

area-authentication send-only

Use **area-authentication send-only** to configure IS-IS not to check the authentication information in the received Level-1 packets, including LSPs, CSNPs, and PSNPs.

Use **undo area-authentication send-only** to restore the default.

Syntax

area-authentication send-only

undo area-authentication send-only

Default

When area authentication mode and key are configured, a Level-1 or Level-1-2 router checks the authentication information in the received packets.

Views

IS-IS view

Predefined user roles

network-admin

context-admin

Usage guidelines

When area authentication mode and key are configured, a Level-1 or Level-1-2 router adds the key in the specified mode into transmitted Level-1 packets (including LSPs, CSNPs, and PSNPs). It also checks the key in the received Level-1 packets.

To prevent packet exchange failure in case of an authentication key change, configure IS-IS not to check the authentication information in the received packets.

Examples

Configure IS-IS not to check the authentication information in the received packets.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] area-authentication send-only
```

Related commands

area-authentication-mode

domain-authentication send-only

isis authentication send-only

area-authentication-mode

Use **area-authentication-mode** to specify an area authentication mode and a key.

Use **undo area-authentication-mode** to restore the default.

Syntax

area-authentication-mode { { **gca** *key-id* { **hmac-sha-1** | **hmac-sha-224** | **hmac-sha-256** | **hmac-sha-384** | **hmac-sha-512** } [**nonstandard**] | **md5** | **simple** } { **cipher** | **plain** } *string* | **keychain** *keychain-name* } [**ip** | **osi**]

undo area-authentication-mode

Default

No area authentication mode or key is configured.

Views

IS-IS view

Predefined user roles

network-admin

context-admin

Parameters

gca: Specifies the Generic Cryptographic Authentication (GCA) mode.

key-id: Uniquely identifies an SA in the range of 1 to 65535. The sender inserts the Key ID into the authentication TLV, and the receiver authenticates the packet by using the SA that is selected based on the Key ID.

hmac-sha-1: Specifies the HMAC-SHA-1 algorithm.

hmac-sha-224: Specifies the HMAC-SHA-224 algorithm.

hmac-sha-256: Specifies the HMAC-SHA-256 algorithm.

hmac-sha-384: Specifies the HMAC-SHA-384 algorithm.

hmac-sha-512: Specifies the HMAC-SHA-512 algorithm.

nonstandard: Specifies the nonstandard GCA mode.

md5: Specifies the MD5 authentication mode.

simple: Specifies the simple authentication mode.

cipher: Specifies a key in encrypted form.

plain: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. Its plaintext form is a case-sensitive string of 1 to 16 characters. Its encrypted form is a case-sensitive string of 33 to 53 characters.

keychain: Specifies the keychain authentication mode.

keychain-name: Specifies a keychain by its name, a case-sensitive string of 1 to 63 characters.

ip: Checks IP-related fields in LSPs.

osi: Checks OSI-related fields in LSPs.

Usage guidelines

Area authentication enables IS-IS to discard routes from untrusted routers.

The key in the specified mode is inserted into all outbound Level-1 packets (LSP, CSNP, and PSNP) and is used to authenticate inbound Level-1 packets.

IS-IS keychain authentication supports the HMAC-MD5 and HMAC-SM3 authentication algorithms. For the HMAC-SM3 authentication algorithm, only key IDs in the range of 0 to 65535 are supported. When keychain authentication is used, IS-IS receives and sends packets as follows:

- Before IS-IS sends a Level-1 packet, it uses the valid send key obtained from the keychain to authenticate the packet. If no valid send key exists or the valid send key does not use the HMAC-MD5 or HMAC-SM3 algorithm, the authentication fails and the packet does not contain authentication information.
- After IS-IS receives a Level-1 packet, it processes the packet as follows:
  - If the authentication algorithm of the packet is HMAC-MD5, IS-IS uses a valid accept key obtained from the keychain to authenticate the packet. If no valid accept key exists or all valid accept keys fail to authenticate the packet, the authentication fails and the packet is discarded.
  - If the authentication algorithm of the packet is HMAC-SM3, IS-IS uses the key ID of the received packet to obtain the corresponding valid accept key from the keychain. Then, IS-IS uses the accept key to authenticate the packet. If IS-IS cannot find a valid accept key based on the key ID of the received packet or the packet fails the authentication, the packet is discarded.

Routers in an area must have the same authentication mode and key.

If neither **ip** nor **osi** is specified, OSI-related fields are checked.

When you specify the GCA mode, follow these guidelines:

- If you do not specify the **nonstandard** keyword, the device can communicate only with devices that use the GCA mode.
- If you specify the **nonstandard** keyword, the device can communicate only with devices that use the nonstandard GCA mode.

Examples

Set the area authentication mode to **simple**, and set the plaintext key to 123456.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] area-authentication-mode simple plain 123456
```

Related commands

area-authentication send-only

domain-authentication-mode

isis authentication-mode

auto-cost enable

Use **auto-cost enable** to enable automatic link cost calculation.

Use **undo auto-cost enable** to disable automatic link cost calculation.

Syntax

auto-cost enable

undo auto-cost enable

Default

Automatic link cost calculation is disabled.

Views

IS-IS view

IS-IS IPv6 unicast address family view

Predefined user roles

network-admin

context-admin

Usage guidelines

After automatic link cost calculation is enabled, the link cost is automatically calculated based on the bandwidth reference value of an interface. When the **cost-style** is **wide** or **wide-compatible**, the cost value of an interface is calculated by using the following formula: Cost = (Reference bandwidth value / Link bandwidth) × 10. For other cost styles, Table 1 applies.

Table 1 Automatic cost calculation scheme for cost styles other than wide and wide-compatible

Interface bandwidth	Cost
≤10 Mbps	60
≤100 Mbps	50
≤155 Mbps	40
≤622 Mbps	30
≤2500 Mbps	20
>2500 Mbps	10

Examples

Enable automatic link cost calculation for IS-IS process 1.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] auto-cost enable
```

Related commands

bandwidth-reference

cost-style

isis cost

isis ipv6 cost

bandwidth-reference

Use **bandwidth-reference** to set the bandwidth reference value for automatic link cost calculation.

Use **undo bandwidth-reference** to restore the default.

Syntax

bandwidth-reference *value*

undo bandwidth-reference

Default

The bandwidth reference value is 100 Mbps.

Views

IS-IS view

IS-IS IPv6 unicast address family view

Predefined user roles

network-admin

context-admin

Parameters

value: Specifies the bandwidth reference value in the range of 1 to 2147483648 Mbps.

Examples

Set the bandwidth reference of IS-IS process 1 to 200 Mbps.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] bandwidth-reference 200
```

Related commands

auto-cost enable

isis cost

circuit-cost

Use **circuit-cost** to set a global IS-IS link cost.

Use **undo circuit-cost** to remove the configuration.

Syntax

circuit-cost *cost-value* [**level-1** | **level-2**]

undo circuit-cost [**level-1** | **level-2**]

Default

No global link cost is configured.

Views

IS-IS view

IS-IS IPv6 unicast address family view

Predefined user roles

network-admin

context-admin

Parameters

cost-value: Specifies the link cost value. The value range varies by cost style.

- For styles **narrow**, **narrow-compatible**, and **compatible**, the cost value is in the range of 0 to 63.
- For styles **wide** and **wide-compatible**, the cost value is in the range of 0 to 16777215.

level-1: Applies the link cost to Level-1.

level-2: Applies the link cost to Level-2.

Usage guidelines

If no level is specified, the specified cost applies to both Level-1 and Level-2.

Examples

Set the global Level-1 link cost to 11 for IS-IS process 1.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] circuit-cost 11 level-1
```

Related commands

cost-style

isis cost

cost-style

Use **cost-style** to set a cost style.

Use **undo cost-style** to restore the default.

Syntax

cost-style { **narrow** | **wide** | **wide-compatible** | { **compatible** | **narrow-compatible** } [**relax-spf-limit**] }

undo cost-style

Default

The IS-IS cost style is **narrow**.

Views

IS-IS view

Predefined user roles

network-admin

context-admin

Parameters

narrow: Receives and sends only narrow cost style packets. The narrow cost is in the range of 0 to 63.

wide: Receives and sends only wide cost style packets. The wide cost is in the range of 0 to 16777215.

compatible: Receives and sends both wide and narrow cost style packets.

narrow-compatible: Receives both narrow and wide cost style packets, but sends only narrow cost style packets.

wide-compatible: Receives both narrow and wide cost style packets, but sends only wide cost style packets.

relax-spf-limit: Allows receiving routes with a cost greater than 1023. If you do not specify this keyword, routes with a cost bigger than 1023 will be discarded. This keyword is available only when **compatible** or **narrow-compatible** is used.

Examples

Configure the router to send only narrow cost style packets, but receive both narrow and wide cost style packets.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] cost-style narrow-compatible
```

Related commands

circuit-cost

isis cost

default-route-advertise

Use **default-route-advertise** to advertise a default route of 0.0.0.0/0.

Use **undo default-route-advertise** to restore the default.

Syntax

default-route-advertise [**avoid-learning** | [**level-1** | **level-1-2** | **level-2**] | **route-policy** *route-policy-name* | **tag** *tag*] *

undo default-route-advertise

Default

Default route advertisement is disabled.

Views

IS-IS IPv4 unicast address family view

IS-IS IPv6 unicast address family view

Predefined user roles

network-admin

context-admin

Parameters

avoid-learning: Avoids learning the default route received in LSPs or generated by using the ATT bit to avoid routing loops.

level-1: Advertises a Level-1 default route.

level-1-2: Advertises both Level-1 and Level-2 default routes.

level-2: Advertises a Level-2 default route.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters.

tag *tag*: Specifies the tag value for the default route, in the range of 1 to 4294967295.

Usage guidelines

If no level is specified, a Level-2 default route is advertised.

The Level-1 default route is advertised to other routers in the same area, and the Level-2 default route is advertised to all the Level-2 and Level-1-2 routers.

You can use a routing policy to specify a level for the default route. The **apply isis level-1** command in routing policy view can generate a Level-1 default route. The **apply isis level-2** command in routing policy view can generate a Level-2 default route. The **apply isis**

level-1-2 command in routing policy view can generate both a Level-1 default route and Level-2 default route.

The tag value specified in the routing policy takes precedence over the tag value specified in this command.

Examples

Configure IS-IS process 1 to advertise a Level-2 default route.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] address-family ipv4
[Sysname-isis-1-ipv4] default-route-advertise
```

display isis

Use **display isis** to display configuration information for an IS-IS process.

Syntax

display isis [*process-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

process-id: Specifies a process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays configuration information for all IS-IS processes.

Examples

Display IS-IS configuration information.

```
<Sysname> display isis

          IS-IS(1) Protocol Information

Network entity                  : 10.0000.0000.0001.00
IS level                        : level-1-2
Cost style                      : Wide
Fast reroute                    : Disabled
ECMP group                      : Disabled
Fast-reroute TI-LFA
    level-1                     : Disabled
    level-2                     : Disabled
Microloop-avoidance
    level-1                     : Disabled
    level-2                     : Disabled
Microloop-avoidance RIB-update-delay
    level-1                     : 5000
```

```
    level-2                     : 5000
Fast-reroute remote-LFA
    level-1                     : Disabled
    level-2                     : Disabled
Node-protecting preference
    level-1                     : 40
    level-2                     : 40
Lowest-cost preference
    level-1                     : 20
    level-2                     : 20
SRLG preference
    level-1                     : 10
    level-2                     : 10
Preference                      : 15
LSP length receive              : 1497
LSP length originate
    level-1                     : 1497
    level-2                     : 1497
Maximum imported routes         : 1000
Timers
    LSP-max-age                 : 1200
    LSP-refresh                 : 900
    SPF mode                    : Normal
    SPF intervals               : 5 50 200
IPv6 enabled
    Fast reroute                : Disabled
    ECMP group                  : Disabled
    Preference                  : 15
    Maximum imported routes     : 1000
    SPF intervals               : 5 50 200
Segment routing
    MPLS                        : Disabled
    Adjacency                   : Disabled
    Configured SRGB             : 17000 18000
    Effective SRGB              : 17000 18000
    Level-1 tunnel count        : 0
    Level-2 tunnel count        : 0
    Local block                 : 15000 15999
```

Table 2 Command output

Field	Description
Network entity	Network entity name.
IS level	IS-IS routing level.
Cost style	Cost style.

Field	Description
Fast reroute	IS-IS FRR status: • **Disabled**—IS-IS FRR is disabled. • **LFA**—IS-IS FRR automatically calculates a backup next hop. • **Route-policy**—IS-IS FRR specifies a backup next hop by using a routing policy.
ECMP group	ECMP route grouping state: **Disabled** or **Enabled**.
Fast-reroute TI-LFA	Topology independent LFA (TI-LFA) FRR status: Disabled or Enabled.
Microloop-avoidance	Microloop avoidance status: **Disabled** or **Enabled**.
Microloop-avoidance RIB-update-delay	Microloop avoidance delay timer.
Fast-reroute TI-LFA	Remote LFA FRR status: **Disabled** or **Enabled**.
Node-protecting preference	Priority of the node-protection backup path selection policy.
Lowest-cost preference	Priority of the lowest-cost backup path selection policy.
SRLG preference	Priority of the shared risk link group (SRLG)-disjoint backup path selection policy.
Preference	IS-IS route preference.
LSP length receive	Maximum LSP that can be received.
LSP length originate	Maximum LSP that can be generated.
Maximum imported routes	Maximum number of redistributed Level-1/Level-2 IPv4/IPv6 routes.
Timers	Timers: • **LSP-max-age**—Maximum life period of LSPs. • **LSP-refresh**—Refresh interval of LSPs. • **SPF mode**—SPF interval calculation mode. • **SPF intervals**—Interval between SPF calculations.
IPv6 enabled	IPv6 is enabled.
Segment routing	Segment routing is supported.
Configured SRGB	Configured SRGB range. This field is displayed when SRGB is configured.
Effective SRGB	SRGB range that takes effect.
Level-1 tunnel count	Number of Level-1 SR tunnels.
Level-2 tunnel count	Number of Level-2 SR tunnels.
Local block	Minimum and maximum label values of the SRLB.

display isis event-log lsp

Use **display isis event-log lsp** to display IS-IS LSP log information.

Syntax

display isis event-log lsp { **purged** | **refreshed** } [**level-1** | **level-2**] [*process-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

purged: Displays log information about purged LSPs.

refreshed: Displays log information about refreshed LSPs, including generated and received LSPs.

level-1: Displays Level-1 LSP log information.

level-2: Displays Level-2 LSP log information.

process-id: Specifies a process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays LSP log information for all IS-IS processes.

Usage guidelines

If you do not specify a level, the command displays both Level-1 and Level-2 LSP log information.

Examples

Displays log information about purged LSPs.

```
<Sysname> display isis event-log lsp purged

                              LSP log for IS-IS(1)
                              --------------------

                                Level-1 LSP log
                                ---------------

Date       Time     LSP ID               Seq Num    Event
--------------------------------------------------------------------------------
2017-07-31 10:19:48 1111.1111.1111.01-00 0x00000001 Generated LSP purge packet
2017-07-31 10:19:48 1111.1111.1111.01-00 0x00000001 Received LSP purge packet
2017-07-31 10:15:29 2222.2222.2222.01-00 0x00000005 Generated LSP purge packet

                                Level-2 LSP log
                                ---------------

Date       Time     LSP ID               Seq Num    Event
--------------------------------------------------------------------------------
2017-07-31 10:19:48 1111.1111.1111.01-00 0x00000001 Generated LSP purge packet
2017-07-31 10:19:48 1111.1111.1111.01-00 0x00000001 Received LSP purge packet
2017-07-31 10:15:29 2222.2222.2222.01-00 0x00000005 Generated LSP purge packet
```

Displays log information about refreshed LSPs.

```
<Sysname> display isis event-log lsp refreshed
```

```
                                LSP log for IS-IS(1)
                                --------------------

                                  Level-1 LSP log
                                  ---------------

Date       Time     LSP ID                Seq Num    Event
-------------------------------------------------------------------------------
2017-06-06 17:18:48 0000.0000.0012.00-00 0x00000038 Received LSP
2017-06-06 17:18:48 0000.0000.0011.00-00 0x00000042 Received LSP
2017-06-06 17:18:48 0000.0000.0012.00-00 0x00000039 Generated LSP
2017-06-06 17:18:48 0000.0000.0012.00-00 0x00000038 Received LSP
2017-06-06 17:18:48 0000.0000.0011.00-00 0x00000042 Received LSP
2017-06-06 17:18:48 0000.0000.0012.00-00 0x00000002 Generated LSP
2017-06-06 17:18:48 0000.0000.0011.01-00 0x00000032 Received LSP
2017-06-06 17:18:48 0000.0000.0011.02-00 0x00000035 Received LSP
2017-06-06 17:18:48 0000.0000.0011.01-00 0x00000032 Received LSP
2017-06-06 17:18:48 0000.0000.0011.02-00 0x00000035 Received LSP
2017-06-06 17:18:47 0000.0000.0012.00-00 0x00000001 Generated LSP

                                  Level-2 LSP log
                                  ---------------

Date       Time     LSPID                 Seq Num    Event
-------------------------------------------------------------------------------
2017-06-06 17:18:48 0000.0000.0012.00-00 0x00000002 Generated LSP
2017-06-06 17:18:47 0000.0000.0012.00-00 0x00000001 Generated LSP
```

Table 3 Command output

Field	Description
Date	Date of the LSP change.
Time	Time of the LSP change.
LSPID	LSP ID.
Seq Num	LSP sequence number.

Related commands

reset isis event-log lsp

display isis event-log spf

Use **display isis event-log spf** to display IS-IS route calculation log information.

Syntax

display isis event-log spf [**ipv4** | **ipv6**] [[**level-1** | **level-2**] | **verbose**] * [*process-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ipv4: Displays IS-IS IPv4 route calculation log information.

ipv6: Displays IS-IS IPv6 route calculation log information.

level-1: Displays Level-1 route calculation log information.

level-2: Displays Level-2 route calculation log information.

verbose: Displays detailed route calculation log information. If you do not specify this keyword, the command displays brief route calculation log information.

process-id: Specifies a process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays route calculation log information for all IS-IS processes.

Usage guidelines

If you specify neither the **ipv4** nor **ipv6** keyword, the command displays IS-IS IPv4 route calculation log information for the public network.

If you do not specify a level, the command displays both Level-1 and Level-2 route calculation log information.

Examples

Display brief IS-IS route calculation log information.

```
<Sysname> display isis event-log spf

                              SPF Log for IS-IS(1)
                              --------------------

                                Level-1 SPF Log
                                ---------------

Date       Time     Duration   Count      Trigger event
--------------------------------------------------------------------------------
2018-12-07 11:11:45 0.003      2          LDP label changed
2018-12-07 11:11:10 0          2          Remote LFA configuration changed
2018-12-07 11:10:45 0          4          Interface metric changed
2018-12-07 09:26:40 0          4          LSP updated
2018-12-07 09:26:28 0          2          DIS changed
2018-12-07 09:26:21 0.001      2          LSP updated
2018-12-07 09:26:07 0.001      3          Direct route changed

                                Level-2 SPF Log
                                ---------------

Date       Time     Duration   Count      Trigger event
--------------------------------------------------------------------------------
2018-12-07 11:11:45 0.003      2          LDP label changed
```

```
2018-12-07 11:11:10 0          2          Remote LFA configuration changed
2018-12-07 11:10:45 0          4          Interface metric changed
2018-12-07 09:26:40 0          4          LSP updated
2018-12-07 09:26:28 0          2          DIS changed
2018-12-07 09:26:21 0          2          LSP updated
2018-12-07 09:26:07 0          3          Direct route changed
```

Display detailed IS-IS route calculation log information.

```
<Sysname> display isis event-log spf verbose

                           SPF Log for IS-IS(1)
                           --------------------

                             Level-1 SPF Log
                             ---------------

 Log date      : 2018-12-07 11:10:45
 Log key       : 5
 Trigger count : 4
 Trigger event : Interface metric changed
 SPF details   :
   Phase             Duration     Description
   TE tunnel ADJ     0            TE SPF nodes: 0
   Topology          0            SPF nodes: 3
   BSPF              0            Candidate NBRs: 1
   TI/R-LFA prepare  0            TI/R-LFA links: 0, TI/R-LFA nodes: 0
   Link PSPF         0
   Link PQ           0
   Node PSPF         0
   Node PQ           0
   LFA               0            LFA SPF nodes: 1
   Area              0            Area addresses: 1
   PRC               0            Add: 0 modify: 1 delete: 0
                                  Last 10 routes:
                                  1.1.1.0/24
   Route summary     0            Summary route nodes: 0
   Total             0

 Log date      : 2018-12-07 09:26:40
 Log key       : 4
 Trigger count : 4
 Trigger event : LSP updated
 SPF details   :
   Phase             Duration     Description
   TE tunnel ADJ     0            TE SPF nodes: 0
   Topology          0            SPF nodes: 3
   BSPF              0            Candidate NBRs: 1
   TI/R-LFA prepare  0            TI/R-LFA links: 0, TI/R-LFA nodes: 0
   Link PSPF         0
```

```
  Link PQ           0
  Node PSPF         0
  Node PQ           0
  LFA               0            LFA SPF nodes: 1
  Area              0            Area addresses: 1
  PRC               0            Add: 0 modify: 0 delete: 0
  Route summary     0            Summary route nodes: 0
  Total             0
Log date      : 2018-12-07 09:26:28
Log key       : 3
Trigger count : 2
Trigger event : DIS changed
SPF details   :
  Phase             Duration     Description
  TE tunnel ADJ     0            TE SPF nodes: 0
  Topology          0            SPF links changed: 1
  BSPF              0            Candidate NBRs: 0
  TI/R-LFA prepare  0            TI/R-LFA links: 0, TI/R-LFA nodes: 0
  Link PSPF         0
  Link PQ           0
  Node PSPF         0
  Node PQ           0
  LFA               0            LFA SPF nodes: 0
  Area              0            Area addresses: 0
  PRC               0            Add: 0 modify: 0 delete: 0
  Route summary     0            Summary route nodes: 0
  Total             0

Log date      : 2018-12-07 09:26:21
Log key       : 2
Trigger count : 2
Trigger event : LSP updated
SPF details   :
  Phase             Duration     Description
  TE tunnel ADJ     0            TE SPF nodes: 0
  Topology          0            SPF nodes: 0
  BSPF              0            Candidate NBRs: 0
  TI/R-LFA prepare  0            TI/R-LFA links: 0, TI/R-LFA nodes: 0
  Link PSPF         0
  Link PQ           0
  Node PSPF         0
  Node PQ           0
  LFA               0            LFA SPF nodes: 0
  Area              0            Area addresses: 1
  PRC               0.001        Add: 0 modify: 0 delete: 0
  Route summary     0            Summary route nodes: 0
  Total             0.001
```

```
Log date      : 2018-12-07 09:26:07
Log key       : 1
Trigger count : 3
Trigger event : Direct route changed
SPF details   :
  Phase             Duration     Description
  TE tunnel ADJ     0            TE SPF nodes: 0
  Topology          0            SPF nodes: 0
  BSPF              0            Candidate NBRs: 0
  TI/R-LFA prepare  0            TI/R-LFA links: 0, TI/R-LFA nodes: 0
  Link PSPF         0
  Link PQ           0
  Node PSPF         0
  Node PQ           0
  LFA               0            LFA SPF nodes: 0
  Area              0            Area addresses: 1
  PRC               0.001        Add: 1 modify: 0 delete: 0
                                 Last 10 routes:
                                 1.1.1.0/24
  Route summary     0            Summary route nodes: 0
  Total             0.001
                                  Level-2 SPF Log
                                  ---------------

Log date      : 2018-12-07 11:10:45
Log key       : 5
Trigger count : 4
Trigger event : Interface metric changed
SPF details   :
  Phase             Duration     Description
  TE tunnel ADJ     0            TE SPF nodes: 0
  Topology          0            SPF nodes: 3
  BSPF              0            Candidate NBRs: 1
  TI/R-LFA prepare  0            TI/R-LFA links: 0, TI/R-LFA nodes: 0
  Link PSPF         0
  Link PQ           0
  Node PSPF         0
  Node PQ           0
  LFA               0            LFA SPF nodes: 1
  Area              0            Area addresses: 1
  PRC               0            Add: 0 modify: 0 delete: 0
  Route summary     0            Summary route nodes: 0
  Total             0

Log date      : 2018-12-07 09:26:40
Log key       : 4
Trigger count : 4
Trigger event : LSP updated
```

```
SPF details   :
  Phase             Duration     Description
  TE tunnel ADJ     0            TE SPF nodes: 0
  Topology          0            SPF nodes: 3
  BSPF              0            Candidate NBRs: 1
  TI/R-LFA prepare  0            TI/R-LFA links: 0, TI/R-LFA nodes: 0
  Link PSPF         0
  Link PQ           0
  Node PSPF         0
  Node PQ           0
  LFA               0            LFA SPF nodes: 1
  Area              0            Area addresses: 1
  PRC               0            Add: 0 modify: 0 delete: 0
  Route summary     0            Summary route nodes: 0
  Total             0

Log date      : 2018-12-07 09:26:28
Log key       : 3
Trigger count : 2
Trigger event : DIS changed
SPF details   :
  Phase             Duration     Description
  TE tunnel ADJ     0            TE SPF nodes: 0
  Topology          0            SPF links changed: 1
  BSPF              0            Candidate NBRs: 0
  TI/R-LFA prepare  0            TI/R-LFA links: 0, TI/R-LFA nodes: 0
  Link PSPF         0
  Link PQ           0
  Node PSPF         0
  Node PQ           0
  LFA               0            LFA SPF nodes: 0
  Area              0            Area addresses: 0
  PRC               0            Add: 0 modify: 0 delete: 0
  Route summary     0            Summary route nodes: 0
  Total             0

Log date      : 2018-12-07 09:26:21
Log key       : 2
Trigger count : 2
Trigger event : LSP updated
SPF details   :
  Phase             Duration     Description
  TE tunnel ADJ     0            TE SPF nodes: 0
  Topology          0            SPF nodes: 0
  BSPF              0            Candidate NBRs: 0
  TI/R-LFA prepare  0            TI/R-LFA links: 0, TI/R-LFA nodes: 0
  Link PSPF         0
  Link PQ           0
```

```
  Node PSPF         0
  Node PQ           0
  LFA               0           LFA SPF nodes: 0
  Area              0           Area addresses: 1
  PRC               0           Add: 0 modify: 0 delete: 0
  Route summary     0           Summary route nodes: 0
  Total             0

Log date      : 2018-12-07 09:26:07
Log key       : 1
Trigger count : 3
Trigger event : Direct route changed
SPF details   :
  Phase             Duration    Description
  TE tunnel ADJ     0           TE SPF nodes: 0
  Topology          0           SPF nodes: 0
  BSPF              0           Candidate NBRs: 0
  TI/R-LFA prepare  0           TI/R-LFA links: 0, TI/R-LFA nodes: 0
  Link PSPF         0
  Link PQ           0
  Node PSPF         0
  Node PQ           0
  LFA               0           LFA SPF nodes: 0
  Area              0           Area addresses: 1
  PRC               0           Add: 0 modify: 0 delete: 0
  Route summary     0           Summary route nodes: 0
  Total             0
```

Table 4 Command output

Field	Description
Date	Start date of route calculation.
Time	Start time of route calculation.
Duration	Route calculation duration in seconds. The value is accurate to six decimal places.
Count	Number of events that trigger the current route calculation.
Trigger event	Type of the most recent event that triggers route calculation: • NextHop changed. • DIS changed. • Interface metric changed. • SPF link changed. • Default route changed. • Summary route changed. • TE tunnel updated. • TE tunnel metric changed. • IPv6 mode changed. • FRR configuration changed. • Prefix priority configuration changed. • Route preference changed.

	• ISPF configuration changed. • Import filter policy changed. • ECMP configuration changed. • PIC configuration changed. • Interface LFA exclude changed. • ATT configuration changed. • GR/NSR first SPF. • GR over. • T3 timeout. • Direct route changed. • Logic interface changed. • Route leakage configuration changed. • NSR over. • Entered overload state. • Exited overload state. • Area address changed. • Route policy changed. • Redistributed route updated. • LSP updated. • MT disabled. • MT enabled. • TE tunnel configuration changed. • TE tunnel destination changed. • RIB smooth. • Remote LFA configuration changed. • LDP label changed.
Log date	Generation time of the route calculation logs.
Log key	Route calculation log key.
Trigger count	Number of events that trigger the current route calculation.
SPF details	Detailed information about the route calculation phases.
Phase	Route calculation phase: • **TE tunnel ADJ**—TE tunnel adjacency calculation. • **Topology**—Topology calculation. • **BSPF**—Backup SPF calculation. • **TI/R-LFA prepare**—TI-LFA/Remote LFA calculation preparation. • **Link PSPF**—SPF calculation after PSPF convergence for link protection. • **Link PQ**—P space and Q space calculation for link protection. • **Node PSPF**—SPF calculation after PSPF convergence for node protection. • **Node PQ**—P space and Q space calculation for node protection. • **LFA**—LFA calculation. • **Area**—Area calculation. • **PRC**—Prefix calculation. • **Route summary**—Route summarization calculation.
Description	Route calculation phase description: • **TE SPF nodes**—Number of SPF nodes for TE tunnel adjacency calculation. • **SPF nodes**—Number of SPF nodes for topology calculation. • **Candidate NBRs**—Number of candidate neighbors.

	• **TI/R-LFA links**—Number of TI-LFA/remote LFA protected links. • **TI/R-LFA nodes**—Number of TI-LFA/remote LFA protected nodes. • **LFA SPF nodes**—Number of SPF nodes for LFA calculation. • **Area addresses**—Number of area addresses. • **Add**, **modify**, and **delete**—Prefix calculation summary. • **Last 10 routes**—10 routes that are most recently calculated. • **Summary route nodes**—Number of summarized routes.
Total	Total duration time of all route calculation phases.

Display brief IPv6 IS-IS route calculation log information.

```
<Sysname> display isis event-log spf ipv6

                            SPF Log for IS-IS(1)
                            --------------------

                              Level-1 SPF Log
                              ---------------

Date       Time     Duration   Count      Trigger event
--------------------------------------------------------------------------------
2015-09-07 11:10:45 0          4          Interface metric changed
2015-09-07 09:26:40 0          4          LSP updated
2015-09-07 09:26:28 0          2          DIS changed
2015-09-07 09:26:21 0.001      2          LSP updated
2015-09-07 09:26:07 0.001      3          Direct route changed

                              Level-2 SPF Log
                              ---------------

Date       Time     Duration   Count      Trigger event
--------------------------------------------------------------------------------
2015-09-07 11:10:45 0          4          Interface metric changed
2015-09-07 09:26:40 0          4          LSP updated
2015-09-07 09:26:28 0          2          DIS changed
2015-09-07 09:26:21 0          2          LSP updated
2015-09-07 09:26:07 0          3          Direct route changed
```

Display detailed IPv6 IS-IS route calculation log information.

```
<Sysname> display isis event-log spf ipv6 verbose

                            SPF Log for IS-IS(1)
                            --------------------

                              Level-1 SPF Log
                              ---------------

 Log date      : 2015-09-07 02:18:09
 Log key       : 10
 Trigger count : 2
```

```
Trigger event : LSP updated
SPF details   :
  Phase          Duration     Description
  TE tunnel ADJ  0            TE SPF nodes: 0
  Topology       0            SPF nodes: 0
  BSPF           0            Candidate NBRs: 0
  TI-LFA prepare 0            TI-LFA links: 0, TI-LFA nodes: 0
  Link PSPF      0
  Link PQ        0
  Node PSPF      0
  Node PQ        0
  LFA            0            LFA SPF nodes: 0
  Area           0            Area addresses: 0
  PRC            0            Add: 0 modify: 0 delete: 0
  Route summary  0            Summary route nodes: 0
  Total          0

Log date      : 2015-09-07 02:18:09
Log key       : 9
Trigger count : 2
Trigger event : NextHop changed
SPF details   :
  Phase          Duration     Description
  TE tunnel ADJ  0            TE SPF nodes: 0
  Topology       0.003        SPF nodes: 3
  BSPF           0            Candidate NBRs: 0
  TI-LFA prepare 0            TI-LFA links: 0, TI-LFA nodes: 0
  Link PSPF      0
  Link PQ        0
  Node PSPF      0
  Node PQ        0
  LFA            0            LFA SPF nodes: 0
  Area           0            Area addresses: 1
  PRC            0            Add: 0 modify: 0 delete: 0
  Route summary  0            Summary route nodes: 0
  Total          0.003

Log date      : 2011-01-01 02:17:40
Log key       : 8
Trigger count : 2
Trigger event : Logic interface changed
SPF details   :
  Phase          Duration     Description
  TE tunnel ADJ  0            TE SPF nodes: 0
  Topology       0            SPF nodes: 0
  BSPF           0            Candidate NBRs: 0
  TI-LFA prepare 0            TI-LFA links: 0, TI-LFA nodes: 0
  Link PSPF      0
```

```
  Link PQ        0
  Node PSPF      0
  Node PQ        0
  LFA            0            LFA SPF nodes: 0
  Area           0            Area addresses: 0
  PRC            0.005        Add: 1 modify: 0 delete: 0
                              Last 10 routes:
                              10::/64
  Route summary  0            Summary route nodes: 0
  Total          0.005

Log date      : 2015-09-07 02:17:38
Log key       : 7
Trigger count : 1
Trigger event : Logic interface changed
SPF details   :
  Phase          Duration     Description
  TE tunnel ADJ  0            TE SPF nodes: 0
  Topology       0            SPF nodes: 0
  BSPF           0            Candidate NBRs: 0
  TI-LFA prepare 0            TI-LFA links: 0, TI-LFA nodes: 0
  Link PSPF      0
  Link PQ        0
  Node PSPF      0
  Node PQ        0
  LFA            0            LFA SPF nodes: 0
  Area           0            Area addresses: 0
  PRC            0            Add: 0 modify: 0 delete: 0
  Route summary  0            Summary route nodes: 0
  Total          0

Log date      : 2015-09-07 02:17:33
Log key       : 6
Trigger count : 5
Trigger event : NextHop changed
SPF details   :
  Phase          Duration     Description
  TE tunnel ADJ  0            TE SPF nodes: 0
  Topology       0            SPF links changed: 1
  BSPF           0            Candidate NBRs: 0
  TI-LFA prepare 0            TI-LFA links: 0, TI-LFA nodes: 0
  Link PSPF      0
  Link PQ        0
  Node PSPF      0
  Node PQ        0
  LFA            0            LFA SPF nodes: 0
  Area           0            Area addresses: 0
  PRC            0.003        Add: 0 modify: 0 delete: 1
```

```
                              Last 10 routes:
                              3::/24
  Route summary  0            Summary route nodes: 0
  Total          0.003

Log date      : 2015-09-07 02:17:21
Log key       : 5
Trigger count : 1
Trigger event : Direct route changed
SPF details   :
  Phase          Duration     Description
  TE tunnel ADJ  0            TE SPF nodes: 0
  Topology       0            SPF nodes: 0
  BSPF           0            Candidate NBRs: 0
  TI-LFA prepare 0            TI-LFA links: 0, TI-LFA nodes: 0
  Link PSPF      0
  Link PQ        0
  Node PSPF      0
  Node PQ        0
  LFA            0            LFA SPF nodes: 0
  Area           0            Area addresses: 0
  PRC            0.006        Add: 1 modify: 0 delete: 0
                              Last 10 routes:
                              3::/24
  Route summary  0            Summary route nodes: 0
  Total          0.006

Log date      : 2015-09-07 02:17:11
Log key       : 4
Trigger count : 1
Trigger event : IPv6 mode changed
SPF details   :
  Phase          Duration     Description
  TE tunnel ADJ  0            TE SPF nodes: 0
  Topology       0            SPF nodes: 3
  BSPF           0            Candidate NBRs: 0
  TI-LFA prepare 0            TI-LFA links: 0, TI-LFA nodes: 0
  Link PSPF      0
  Link PQ        0
  Node PSPF      0
  Node PQ        0
  LFA            0            LFA SPF nodes: 0
  Area           0            Area addresses: 1
  PRC            0            Add: 0 modify: 0 delete: 0
  Route summary  0            Summary route nodes: 0
  Total          0

Log date      : 2015-09-07 01:09:33
```

```
Log key       : 3
Trigger count : 2
Trigger event : DIS changed
SPF details   :
  Phase          Duration     Description
  TE tunnel ADJ  0            TE SPF nodes: 0
  Topology       0.001        SPF nodes: 3
  BSPF           0            Candidate NBRs: 0
  TI-LFA prepare 0            TI-LFA links: 0, TI-LFA nodes: 0
  Link PSPF      0
  Link PQ        0
  Node PSPF      0
  Node PQ        0
  LFA            0            LFA SPF nodes: 0
  Area           0            Area addresses: 1
  PRC            0            Add: 0 modify: 0 delete: 0
  Route summary  0            Summary route nodes: 0
  Total          0.001

Log date      : 2015-09-07 01:09:25
Log key       : 2
Trigger count : 2
Trigger event : LSP updated
SPF details   :
  Phase          Duration     Description
  TE tunnel ADJ  0            TE SPF nodes: 0
  Topology       0            SPF links changed: 1
  BSPF           0            Candidate NBRs: 0
  TI-LFA prepare 0            TI-LFA links: 0, TI-LFA nodes: 0
  Link PSPF      0
  Link PQ        0
  Node PSPF      0
  Node PQ        0
  LFA            0            LFA SPF nodes: 0
  Area           0            Area addresses: 1
  PRC            0            Add: 0 modify: 0 delete: 0
  Route summary  0            Summary route nodes: 0
  Total          0

Log date      : 2015-09-07 01:08:49
Log key       : 1
Trigger count : 1
Trigger event : Area address changed
SPF details   :
  Phase          Duration     Description
  TE tunnel ADJ  0            TE SPF nodes: 0
  Topology       0            SPF nodes: 0
  BSPF           0            Candidate NBRs: 0
```

```
  TI-LFA prepare 0            TI-LFA links: 0, TI-LFA nodes: 0
  Link PSPF      0
  Link PQ        0
  Node PSPF      0
  Node PQ        0
  LFA            0            LFA SPF nodes: 0
  Area           0            Area addresses: 1
  PRC            0            Add: 0 modify: 0 delete: 0
  Route summary  0            Summary route nodes: 0
  Total          0

                               Level-2 SPF Log
                               ---------------

Log date      : 2015-09-07 02:18:09
Log key       : 10
Trigger count : 2
Trigger event : LSP updated
SPF details   :
  Phase          Duration     Description
  TE tunnel ADJ  0            TE SPF nodes: 0
  Topology       0            SPF nodes: 0
  BSPF           0            Candidate NBRs: 0
  TI-LFA prepare 0            TI-LFA links: 0, TI-LFA nodes: 0
  Link PSPF      0
  Link PQ        0
  Node PSPF      0
  Node PQ        0
  LFA            0            LFA SPF nodes: 0
  Area           0            Area addresses: 0
  PRC            0            Add: 0 modify: 0 delete: 0
  Route summary  0            Summary route nodes: 0
  Total          0

Log date      : 2015-09-07 02:18:09
Log key       : 9
Trigger count : 2
Trigger event : NextHop changed
SPF details   :
  Phase          Duration     Description
  TE tunnel ADJ  0            TE SPF nodes: 0
  Topology       0.002        SPF nodes: 3
  BSPF           0            Candidate NBRs: 0
  TI-LFA prepare 0            TI-LFA links: 0, TI-LFA nodes: 0
  Link PSPF      0
  Link PQ        0
  Node PSPF      0
  Node PQ        0
```

```
  LFA            0            LFA SPF nodes: 0
  Area           0            Area addresses: 1
  PRC            0            Add: 0 modify: 0 delete: 0
  Route summary  0.001        Summary route nodes: 0
  Total          0.003

Log date      : 2015-09-07 02:17:40
Log key       : 8
Trigger count : 2
Trigger event : Logic interface changed
SPF details   :
  Phase          Duration     Description
  TE tunnel ADJ  0            TE SPF nodes: 0
  Topology       0            SPF nodes: 0
  BSPF           0            Candidate NBRs: 0
  TI-LFA prepare 0            TI-LFA links: 0, TI-LFA nodes: 0
  Link PSPF      0
  Link PQ        0
  Node PSPF      0
  Node PQ        0
  LFA            0            LFA SPF nodes: 0
  Area           0            Area addresses: 0
  PRC            0            Add: 0 modify: 0 delete: 0
  Route summary  0            Summary route nodes: 0
  Total          0

Log date      : 2015-09-07 02:17:38
Log key       : 7
Trigger count : 1
Trigger event : Logic interface changed
SPF details   :
  Phase          Duration     Description
  TE tunnel ADJ  0            TE SPF nodes: 0
  Topology       0            SPF nodes: 0
  BSPF           0            Candidate NBRs: 0
  TI-LFA prepare 0            TI-LFA links: 0, TI-LFA nodes: 0
  Link PSPF      0
  Link PQ        0
  Node PSPF      0
  Node PQ        0
  LFA            0            LFA SPF nodes: 0
  Area           0            Area addresses: 0
  PRC            0            Add: 0 modify: 0 delete: 0
  Route summary  0            Summary route nodes: 0
  Total          0

Log date      : 2015-09-07 02:17:33
Log key       : 6
```

```
Trigger count : 5
Trigger event : NextHop changed
SPF details   :
  Phase          Duration     Description
  TE tunnel ADJ  0            TE SPF nodes: 0
  Topology       0            SPF links changed: 1
  BSPF           0            Candidate NBRs: 0
  TI-LFA prepare 0            TI-LFA links: 0, TI-LFA nodes: 0
  Link PSPF      0
  Link PQ        0
  Node PSPF      0
  Node PQ        0
  LFA            0            LFA SPF nodes: 0
  Area           0            Area addresses: 0
  PRC            0.001        Add: 0 modify: 0 delete: 0
  Route summary  0            Summary route nodes: 0
  Total          0.001

Log date      : 2015-09-07 02:17:21
Log key       : 5
Trigger count : 1
Trigger event : Direct route changed
SPF details   :
  Phase          Duration     Description
  TE tunnel ADJ  0            TE SPF nodes: 0
  Topology       0            SPF nodes: 0
  BSPF           0            Candidate NBRs: 0
  TI-LFA prepare 0            TI-LFA links: 0, TI-LFA nodes: 0
  Link PSPF      0
  Link PQ        0
  Node PSPF      0
  Node PQ        0
  LFA            0            LFA SPF nodes: 0
  Area           0            Area addresses: 0
  PRC            0            Add: 0 modify: 0 delete: 0
  Route summary  0            Summary route nodes: 0
  Total          0

Log date      : 2015-09-07 02:17:11
Log key       : 4
Trigger count : 1
Trigger event : IPv6 mode changed
SPF details   :
  Phase          Duration     Description
  TE tunnel ADJ  0            TE SPF nodes: 0
  Topology       0.001        SPF nodes: 3
  BSPF           0            Candidate NBRs: 0
  TI-LFA prepare 0            TI-LFA links: 0, TI-LFA nodes: 0
```

```
  Link PSPF      0
  Link PQ        0
  Node PSPF      0
  Node PQ        0
  LFA            0            LFA SPF nodes: 0
  Area           0            Area addresses: 1
  PRC            0            Add: 0 modify: 0 delete: 0
  Route summary  0            Summary route nodes: 0
  Total          0.001

Log date      : 2015-09-07 01:09:33
Log key       : 3
Trigger count : 2
Trigger event : DIS changed
SPF details   :
  Phase          Duration     Description
  TE tunnel ADJ  0            TE SPF nodes: 0
  Topology       0            SPF nodes: 3
  BSPF           0            Candidate NBRs: 0
  TI-LFA prepare 0            TI-LFA links: 0, TI-LFA nodes: 0
  Link PSPF      0
  Link PQ        0
  Node PSPF      0
  Node PQ        0
  LFA            0            LFA SPF nodes: 0
  Area           0            Area addresses: 1
  PRC            0            Add: 0 modify: 0 delete: 0
  Route summary  0            Summary route nodes: 0
  Total          0

Log date      : 2015-09-07 01:09:25
Log key       : 2
Trigger count : 2
Trigger event : LSP updated
SPF details   :
  Phase          Duration     Description
  TE tunnel ADJ  0            TE SPF nodes: 0
  Topology       0            SPF links changed: 1
  BSPF           0            Candidate NBRs: 0
  TI-LFA prepare 0            TI-LFA links: 0, TI-LFA nodes: 0
  Link PSPF      0
  Link PQ        0
  Node PSPF      0
  Node PQ        0
  LFA            0            LFA SPF nodes: 0
  Area           0            Area addresses: 1
  PRC            0            Add: 0 modify: 0 delete: 0
  Route summary  0            Summary route nodes: 0
```

```
  Total          0

Log date      : 2015-09-07 01:08:49
Log key       : 1
Trigger count : 1
Trigger event : Area address changed
SPF details   :
  Phase          Duration     Description
  TE tunnel ADJ  0            TE SPF nodes: 0
  Topology       0            SPF nodes: 0
  BSPF           0            Candidate NBRs: 0
  TI-LFA prepare 0            TI-LFA links: 0, TI-LFA nodes: 0
  Link PSPF      0
  Link PQ        0
  Node PSPF      0
  Node PQ        0
  LFA            0            LFA SPF nodes: 0
  Area           0            Area addresses: 1
  PRC            0            Add: 0 modify: 0 delete: 0
  Route summary  0            Summary route nodes: 0
  Total          0
```

Table 5 Command output

Field	Description
Date	Start date of route calculation.
Time	Start time of route calculation.
Duration	Route calculation duration in seconds. The value is accurate to six decimal places.
Count	Number of events that trigger the current route calculation.
Trigger event	Type of the most recent event that triggers route calculation: • NextHop changed. • DIS changed. • Interface metric changed. • SPF link changed. • Default route changed. • Summary route changed. • TE tunnel updated. • TE tunnel metric changed. • IPv6 mode changed. • FRR configuration changed. • Prefix priority configuration changed. • Route preference changed. • ISPF configuration changed. • Import filter policy changed. • ECMP configuration changed. • PIC configuration changed. • Interface LFA exclude changed. • ATT configuration changed. • GR/NSR first SPF.

	• GR over. • T3 timeout. • Direct route changed. • Logic interface changed. • Route leakage configuration changed. • NSR over. • Entered overload state. • Exited overload state. • Area address changed. • Route policy changed. • Redistributed route updated. • LSP updated. • MT disabled. • MT enabled. • TE tunnel configuration changed. • TE tunnel destination changed. • RIB smooth.
Log date	Generation time of the route calculation logs.
Log key	Route calculation log key.
Trigger count	Number of events that trigger the current route calculation.
SPF details	Detailed information about the route calculation phases.
Phase	Route calculation phase: • **TE tunnel ADJ**—TE tunnel adjacency calculation. • **Topology**—Topology calculation. • **BSPF**—Backup SPF calculation. • **TI-LFA prepare**—TI-LFA calculation preparation. • **Link PSPF**—SPF calculation after PSPF convergence for link protection. • **Link PQ**—P space and Q space calculation for link protection. • **Node PSPF**—SPF calculation after PSPF convergence for node protection. • **Node PQ**—P space and Q space calculation for node protection. • **LFA**—LFA calculation. • **Area**—Area calculation. • **PRC**—Prefix calculation. • **Route summary**—Route summarization calculation.
Description	Route calculation phase description: • **TE SPF nodes**—Number of SPF nodes for TE tunnel adjacency calculation. • **SPF nodes**—Number of SPF nodes for topology calculation. • **Candidate NBRs**—Number of candidate neighbors. • **TI-LFA links**—Number of TI-LFA protected links. • **TI-LFA nodes**—Number of TI-LFA protected nodes. • **LFA SPF nodes**—Number of SPF nodes for LFA calculation. • **Area addresses**—Number of area addresses. • **Add, modify, and delete**—Prefix calculation summary. • **Last 10 routes**—10 routes that are most recently calculated. • **Summary route nodes**—Number of summarized routes.
Total	Total duration time of all route calculation phases.

Related commands

reset isis event-log spf

display isis graceful-restart event-log

Use **display isis graceful-restart event-log** to display IS-IS GR log information.

Syntax

display isis graceful-restart event-log slot *slot-number*

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its ID.

Examples

Display IS-IS GR log information for the specified slot.

```
<Sysname> display isis graceful-restart event-log slot 1
IS-IS loginfo :
Sep 18 08:48:24 2015 slot 1 Process 1 enter GR restarting phase(Initialization).
Sep 18 08:48:24 2015 slot 1 Process 1 enter GR phase (LSDB synchronization).
Sep 18 08:48:24 2015 slot 1 Process 1 enter GR phase (TE tunnel prepare).
Sep 18 08:48:24 2015 slot 1 Process 1 enter GR phase (First SPF computation).
Sep 18 08:48:25 2015 slot 1 Process 1 enter GR phase (Redistribution).
Sep 18 08:48:25 2015 slot 1 Process 1 enter GR phase (Second SPF computation).
Sep 18 08:48:25 2015 slot 1 Process 1 enter GR phase (LSP stability).
Sep 18 08:48:25 2015 slot 1 Process 1 enter GR phase (LSP generation).
Sep 18 08:48:25 2015 slot 1 Process 1 enter GR phase (Finish).
Sep 18 08:48:25 2015 slot 1 Process 1 GR complete.
```

Table 6 Command output

Field	Description
GR phase	GR phase: • **Initialization**. • **LSDB synchronization**. • **TE tunnel prepare**—Preparing for TE tunnel computation. • **First SPF computation**. • **Redistribution**. • **Second SPF computation**. • **LSP stability**—Ready to generate LSPs. • **LSP generation**. • **Finish**.

display isis graceful-restart status

Use **display isis graceful-restart status** to display IS-IS GR state.

Syntax

display isis graceful-restart status [**level-1** | **level-2**] [*process-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

level-1: Displays the IS-IS Level-1 GR state.

level-2: Displays the IS-IS Level-2 GR state.

process-id: Specifies a process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays GR state of all IS-IS processes.

Examples

Display IS-IS GR state.

```
<Sysname> display isis graceful-restart status

                        Restart information for IS-IS(1)
                        --------------------------------
Restart status: COMPLETE
Restart phase: Finish
Restart t1: 3, count 10; Restart t2: 60; Restart t3: 300
SA Bit: supported

                          Level-1 restart information
                          ---------------------------
Total number of interfaces: 1
Number of waiting LSPs: 0

                          Level-2 restart information
                          ---------------------------
Total number of interfaces: 1
Number of waiting LSPs: 0
```

Table 7 Command output

Field	Description
Restart status	Current GR state: • **RESTARTING**—In this state, forwarding can be ensured. • **STARTING**—In this state, forwarding cannot be ensured. • **COMPLETE**—GR is completed.
Restart phase	Current Restart phase: • **Initialization**. • **LSDB synchronization**. • **TE tunnel prepare**. • **First SPF computation**. • **Redistribution**. • **Second SPF computation**. • **LSP stability**—Ready to generate LSPs. • **LSP generation**. • **Finish**.
Restart t1	T1 timer, in seconds.
count	Number of T1 timer expirations.
Restart t2	T2 timer, in seconds.
Restart t3	T3 timer, in seconds.
SA Bit	Whether SA is supported.
Total number of interfaces	Total number of IS-IS interfaces.
Number of waiting LSPs	Number of LSPs not obtained by the GR restarter from GR helpers during LSDB synchronization.

display isis interface

Use **`display isis interface`** to display IS-IS interface information.

Syntax

`display isis interface` [[*`interface-type interface-number`*] [**`verbose`**] | **`statistics`**] [*`process-id`*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

`interface-type interface-number`: Displays information for a specified IS-IS interface. If you do not specify this argument, the command displays information about all interfaces.

verbose: Displays detailed information about an interface. If you do not specify this keyword, the command displays brief information about an interface.

statistics: Displays IS-IS interface statistics.

process-id: Displays IS-IS interface information for an IS-IS process specified by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays interface information for all IS-IS processes.

Examples

Display brief IS-IS interface information.

```
<Sysname> display isis interface

                    Interface information for IS-IS(1)
                    ----------------------------------

  Interface:  GigabitEthernet1/0/2
  Index     IPv4 state      IPv6 state     Circuit ID   MTU   Type   DIS
  00001     Up              Down           1            1497  L1/L2  No/No
```

Display detailed IS-IS interface information.

```
<Sysname> display isis interface verbose

                    Interface information for IS-IS(1)
                    ----------------------------------

  Interface:  GigabitEthernet1/0/2
  Index     IPv4 state      IPv6 state     Circuit ID   MTU   Type   DIS
  00001     Up              Down           1            1497  L1/L2  No/No
  SNPA address                    : 000c-29e8-1bd5
  IP address                      : 192.168.220.10
  Secondary IP address(es)        :
  IPv6 link-local address         :
  Extended circuit ID             : 1
  CSNP timer value                : L1        10  L2        10
  Hello timer value               :           10
  Hello multiplier value          :            3
  LSP timer value                 : L12       33
  LSP transmit-throttle count     : L12        5
  Cost                            : L1       100  L2        100
  IPv6 cost                       : L1        10  L2        10
  Priority                        : L1        64  L2        64
  Retransmit timer value          : L12        5
  IPv4 BFD                        : Disabled
  IPv6 BFD                        : Disabled
  IPv4 BFD session-restrict-adj   : Enabled
  IPv6 BFD session-restrict-adj   : Disabled
  IPv4 FRR LFA backup             : Enabled
  IPv6 FRR LFA backup             : Enabled
  IPv4 FRR TI-LFA                 : L1   Enabled  L2   Enabled
  IPv4 FRR remote-LFA             : L1   Enabled  L2   Enabled
  IPv4 prefix-suppression         : Disabled
```

```
  IPv6 prefix-suppression          : Disabled
  IPv4 tag                         : 1
  IPv6 tag                         : 4294967295
  IPv4 primary path detection mode: BFD ctrl
  IPv6 primary path detection mode: BFD ctrl
```

Display detailed information about interfaces enabled with SR.

```
<Sysname> display isis interface verbose

                     Interface information for IS-IS(1)
                     ----------------------------------


  Interface:  LoopBack1
  Index     IPv4 state      IPv6 state     Circuit ID   MTU   Type   DIS
  00003     Up              Down           1            1536  L1/L2  --
  SNPA address                     : 0000-0000-0000
  IP address                       : 111.111.111.111
  Secondary IP addresses         :
  IPv6 link-local address          :
  Extended circuit ID              : 3
  CSNP timer value                 : L1        10  L2        10
  Hello timer value                :           10
  Hello multiplier value           :            3
  LSP timer value                  : L12       33
  LSP transmit-throttle count      : L12        5
  Cost                             : L1         0  L2         0
  IPv6 cost                        : L1         0  L2         0
  Priority                         : L1        64  L2        64
  Retransmit timer value           : L12        5
  IPv4 BFD                         : Disabled
  IPv6 BFD                         : Disabled
  IPv4 BFD session-restrict-adj    : Enabled
  IPv6 BFD session-restrict-adj    : Disabled
  IPv4 FRR LFA backup              : Enabled
  IPv6 FRR LFA backup              : Enabled
  IPv4 FRR TI-LFA                  : L1   Enabled  L2   Enabled
  IPv4 FRR remote-LFA              : L1   Enabled  L2   Enabled
  IPv4 prefix suppression          : Disabled
  IPv6 prefix suppression          : Disabled
  IPv4 tag                         : 0
  IPv6 tag                         : 0
  Prefix-SID type                  : Index
  Value                            : 2
  Prefix-SID validity              : Valid
```

Table 8 Command output

Field	Description
Interface	Interface type and number.
Index	Interface index.

Field	Description
IPv4 state	IPv4 state: • **Up**—The interface is up at both the link layer and network layer. • **Down**—The interface is down at the link layer and network layer. • **Lnk:Up/IP:Dn**—The interface is up at the link layer but is down at the network layer.
IPv6 state	IPv6 state: • **Up**—The interface is up at both the link layer and network layer. • **Down**—The interface is down at the link layer and network layer. • **Lnk:Up/IP:Dn**—The interface is up at the link layer but is down at the network layer.
Circuit ID	Circuit ID.
MTU	Interface MTU.
Type	Interface link adjacency type.
DIS	Indicates whether the interface is elected as the Level-1/Level-2 DIS. On a P2P network, this field displays a hyphen (-) because DIS election is not performed.
SNPA address	Subnet access point address.
IP address	Primary IP address.
Secondary IP address(es)	Secondary IP addresses.
IPv6 link-local address	IPv6 link local address.
Extended circuit ID	Extended circuit ID for a P2P link.
CSNP timer value	Interval for sending CSNP packets.
Hello timer value	Interval for sending Hello packets.
Hello multiplier value	Number of invalid Hello packets.
LSP timer value	Minimum interval for sending LSP packets.
LSP transmit-throttle count	Number of LSP packets sent each time.
Cost	Cost of the interface.
IPv6 cost	IPv6 link cost of the interface.
Priority	DIS priority.
Retransmit timer value	Retransmission interval for LSPs on a P2P link.
IPv4 BFD	Whether BFD for IS-IS is enabled: • **Disabled**. • **Enabled**.
IPv6 BFD	Whether BFD for IPv6 IS-IS is enabled: • **Disabled**. • **Enabled**.
IPv4 BFD session-restrict-adj	Whether IPv4 adjacency establishment and maintenance control based on BFD session state is enabled: • **Disabled**. • **Enabled**.

Field	Description
IPv6 BFD session-restrict-adj	Whether IPv6 adjacency establishment and maintenance control based on BFD session state is enabled: • **Disabled**. • **Enabled**.
IPv4 FRR LFA backup	Whether LFA calculation is enabled for IPv4 FRR: • **Disabled**. • **Enabled**.
IPv6 FRR LFA backup	Whether LFA calculation is enabled for IPv6 FRR: • **Disabled**. • **Enabled**.
IPv4 FRR TI-LFA	IPv4 TI-LFA calculation status: • **Disabled**. • **Enabled**.
IPv4 FRR remote-LFA	IPv4 remote LFA calculation status: • **Disabled**. • **Enabled**.
IPv4 prefix suppression	Whether IPv4 IS-IS prefix suppression is enabled: • **Disabled**. • **Enabled**.
IPv6 prefix suppression	Whether IPv6 IS-IS prefix suppression is enabled: • **Disabled**. • **Enabled**.
IPv4 tag	IPv4 tag value of the interface.
IPv6 tag	IPv6 tag value of the interface.
IPv4 primary path detection mode	IPv4 primary path detection mode: • **BFD ctrl**—BFD control packet mode. • **BFD echo**—BFD echo packet mode.
IPv6 primary path detection mode	IPv6 primary path detection mode: • **BFD ctrl**—BFD control packet mode. • **BFD echo**—BFD echo packet mode.
Prefix-SID type	Prefix SID type: • **Absolute**—Absolute value of the prefix SID. • **Index**—Index value of the prefix SID.
Value	Prefix SID value.
Prefix-SID validity	Whether the prefix SID is valid: • **Invalid**—The prefix SID is invalid because it is out of the SRGB range. • **Valid**—The prefix SID is valid.
Nexthop	Next hop address. This field displays 0.0.0.0 for a P2P network.
Type	Adjacency SID type: • **Absolute**—Absolute value of the adjacency SID. • **Index**—Index value of the adjacency SID.

Display IS-IS interface statistics.

```
<Sysname> display isis interface statistics
```

```
                Interface statistics information for IS-IS(1)
                ----------------------------------------
Type            IPv4 up/down          IPv6 up/down
LAN                   1/0                   0/0
P2P                   0/0                   0/0
```

Table 9 Command output

Field	Description
Type	Network type of the interface: • **LAN**—Broadcast network. • **P2P**—Point-to-point network.
IPv4 up	Number of IS-IS interfaces in up state.
IPv4 down	Number of IS-IS interfaces in down state.
IPv6 up	Number of IS-ISv6 interfaces in up state.
IPv6 down	Number of IS-ISv6 interfaces in down state.

display isis lsdb

Use **display isis lsdb** to display IS-IS LSDB information.

Syntax

display isis lsdb [[**level-1** | **level-2**] | **local** | [**lsp-id** *lspid* | **lsp-name** *lspname*] | **verbose**] * [*process-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

level-1: Displays the level-1 LSDB.

level-2: Displays the level-2 LSDB.

local: Displays LSP information generated locally.

lsp-id *lspid*: Specifies an LSP ID, in the form of *sysID. Pseudo ID-fragment num*, where *sysID* represents the originating node or pseudo node. *Pseudo ID* is separated by a dot from sysID and by a hyphen from *fragment num*.

lsp-name *lspname*: Specifies the LSP name, in the form of *Symbolic name.Pseudo ID-fragment num*, where *Pseudo ID* is separated by a dot from *Symbolic name* and by a hyphen from *fragment num*. If the Pseudo ID is 0, specify the LSP name in the form *Symbolic name-fragment num*.

verbose: Displays LSDB detailed information. If you do not specify this keyword, the command displays brief information about LSDB.

process-id: Specifies an IS-IS process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays LSDBs for all IS-IS processes.

Usage guidelines

If no level is specified, the command displays both Level-1 and Level-2 LSDB information.

Examples

Display brief Level-1 LSDB information.

```
<Sysname> display isis lsdb level-1

                        Database information for IS-IS(1)
                        ---------------------------------

                          Level-1 Link State Database
                          ---------------------------

LSPID                 Seq Num      Checksum      Holdtime      Length  ATT/P/OL
--------------------------------------------------------------------------------
0000.0000.0001.00-00* 0x00000087   0xf846        1152          183     0/0/0
0000.0000.0003.00-00  0x00000005   0x4bee        520           177     0/0/0
0000.0000.0003.00-01  0x00000004   0x7245        520           45      0/0/0
0000.0000.0011.00-00  0x0000000b   0xcdf6        815           183     0/0/0

    *-Self LSP, +-Self LSP(Extended), ATT-Attached, P-Partition, OL-Overload
```

Display detailed Level-1 LSDB information.

```
<Sysname> display isis lsdb level-1 verbose

                        Database information for IS-IS(1)
                        ---------------------------------

                          Level-1 Link State Database
                          ---------------------------

LSPID                 Seq Num      Checksum      Holdtime      Length  ATT/P/OL
--------------------------------------------------------------------------------
0000.0000.0001.00-00* 0x00000080   0x73f         1185          183     0/0/0
 Source       0000.0000.0001.00
 NLPID        IPv4
 Area address 10
 IPv4 address 192.168.220.10
 MT ID        0000   (-/-)
 MT ID        0002   (-/-)
 MT ID        0006   (-/-)
 +NBR  ID
     0000.0000.0011.00               Cost: 100
 IPv6 unicast NBR ID
     6464.6464.6464.01               Cost: 10         MT ID: 2
 MT NBR ID
     6464.6464.6464.01               Cost: 10         MT ID: 6
 +IP-Extended
     192.168.220.0   255.255.255.0    Cost: 100
```

```
 +IP-Extended
     14.159.100.2    255.255.255.255  Cost: 0
     Prefix-SID: 3333            Algorithm: 0
     Prefix-SID flags (R/N/P/E/V/L): 0/1/0/0/0/0
 IPv4 unicast
     1.1.1.1         255.255.255.255  Cost: 0          MT ID: 6
 IPv4 unicast
     10.10.10.0      255.255.255.0    Cost: 10         MT ID: 6
 Router ID    1.1.1.1

0000.0000.0003.00-00  0x00000005   0x4bee        887           177     0/0/0
 Source       0000.0000.0003.00
 NLPID        IPv4
 Area address 10
 IPv4 address 10.10.10.10
 IPv4 address 192.168.220.20
 +NBR  ID
     0000.0000.0001.00               Cost: 10
 Router ID    3.3.3.3

0000.0000.0003.00-01  0x00000004   0x7245        887           45      0/0/0
 Source       0000.0000.0003.00
 +IP-Extended
         10.10.10.0      255.255.255.0    Cost: 10
 +IP-Extended
         192.168.220.0   255.255.255.0    Cost: 10


*-Self LSP, +-Self LSP(Extended), ATT-Attached, P-Partition, OL-Overload
```

Table 10 Command output

Field	Description
LSPID	LSP ID.
Seq Num	LSP sequence number.
Checksum	LSP checksum.
Holdtime	LSP lifetime, which decreases as time elapses.
Length	LSP length.
ATT/P/OL	• **ATT**—Attach bit. • **P**—Partition bit. • **OL**—Overload bit. 1 means the LSP bit is set and 0 means the LSP bit is not set.
Source	System ID of the originating router.
HOST NAME	Dynamic host name of the originating router.
ORG ID	Original system ID of the virtual system of the originating router.
NLPID	Network layer protocol the originating router runs.
Area address	Area address of the originating router.

Field	Description
IPv4 address	IP address of the originating router's IS-IS interface.
IPv6 address	IPv6 address of the originating router's IS-ISv6 interface.
MT ID 0000 (-/-) MT ID 0002 (-/-) MT ID 0006 (-/-)	Topology supported by the originating router (0/0/0 indicates ATT/P/OL): • **0000**—Base topology. • **(-/-)**—Attach bit/overload bit.
NBR ID	Neighbor ID of the originating router.
IPv6 unicast NBR ID	IPv6 unicast neighbor information about the originating router.
Router ID	Router ID.
IP-Internal	Internal IP address and mask of the originating router.
IP-External	External IP address and mask of the originating router.
IP-Extended	Extended IP address and mask of the originating router.
Cost	Cost.
Auth	Authentication information of the originating router.
IPv4 unicast	IPv4 unicast reachability information about the originating router.
LAN-ADJ-SID	SID advertisement information from the LAN adjacency path.
P2P-ADJ-SID	SID advertisement information from the P2P adjacency path.
Flags (F/B/V/L/S)	Adjacency SID flag: • **F**—Address family flag. If set, the adjacency SID refers to an IPv6 adjacency. If not set, the adjacency SID refers to an IPv4 adjacency. • **B**—Backup flag. If set, the adjacency SID is eligible for link protection. • **V**—Value/Index flag. If set, the adjacency SID carries an absolute value. If not set, the adjacency SID carries an index value. • **L**—Local flag. If set, the adjacency SID has local significance. If not set, the adjacency SID has global significance. • **S**—Set flag. If set, the adjacency SID refers to a set of adjacencies.
Weight	Adjacency path weight.
System ID	System ID.
Adjacency SID	SID advertised by the adjacency path.
Prefix-SID flags (R/N/P/E/V/L)	Prefix SID flag: • **R**—Re-advertisement flag. If set, inter-level propagation or route redistribution exists. • **N**—Node-SID flag. If set, the prefix SID is the SID to an SR node. • **P**—No-PHP flag. If set, the penultimate node cannot pop the prefix SID. • **E**—Explicit null flag. If set, the upstream neighbor must replace the prefix SID with an explicit null flag before forwarding the packets. • **V**—Value/Index flag. If set, the prefix SID carries an absolute value. • **L**—Local flag. If set, the prefix SID has local significance.
Perfix-SID	Prefix SID value.
Algorithm	Prefix related algorithm. Only SPF is supported in the current software version.
Router capability	Router capability sub-TLV information.

Field	Description
Flags (D/S)	Inter-level leaking flag: • **D**—D flag. If set, the router capability TLV cannot be leaked from Level-1 to Level-2. • **S**—S flag. If set, the router capability TLV must be flooded across the entire routing domain. If not set, the router capability TLV cannot be leaked between levels.
SRGB base	Minimum label value of the SRGB range.
SRGB range	Number of labels of the SRGB.
SRLB base	Minimum label value of the SRGB range.
SRLB range	Number of labels of the SRGB.
SRLG NBR ID	SRLG neighbor information about the originating router.
Interface IP address	IP address of the local interface.
Neighbor IP address	IP address of the remote interface.
Shared risk link group	Number of the SRLG to which the local interface belongs.
SID binding	Prefix-SID mapping information.
Flags (F/M/S/D/A)	Mapping flags: • **F**—Address family flag. If set, the peer is an IPv6 peer. If not set, the peer is an IPv4 peer. • **M**—Mirror context flag. If set, the SID is used for SR node protection. • **S**—Scope flag. If set, the route capability TLV can be leaked from Level-1 to Level-2. • **D**—Down flag. If set, the SID/Label Binding TLV is advertised from Level-2 to Level-1. • **A**—Attached flag. If set, the prefix and SID are advertised by a directly connected peer.
Range	Number of consecutive SIDs assigned.

display isis name-table

Use **`display isis name-table`** to display the host name-to-system ID mapping table.

Syntax

`display isis name-table` [*`process-id`*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

`process-id`: Displays the host name to system ID mapping table for an IS-IS process specified by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays the host name to system ID mapping table for all IS-IS processes.

Examples

Display the IS-IS host name to system ID mapping table.

```
<Sysname> display isis name-table
                     Name table information for IS-IS(1)
                     ----------------------------------
 System ID           Hostname                          Type       Level
 6789.0000.0001      RUTA                              DYNAMIC    Level-1
 6789.0000.0001      RUTA                              DYNAMIC    Level-2
 0000.0000.0041      RUTB                              STATIC     Level-1
 0000.0000.0041      RUTB                              STATIC     Level-2
 6789.0000.0001.01   DIS-A                             DYNAMIC    Level-1
 0000.0000.0041.01   DIS-B                             DYNAMIC    Level-2
```

Table 11 Command output

Field	Description
System ID	System ID.
Hostname	Host name.
Type	Mapping type: • **STATIC**. • **DYNAMIC**.
Level	Level on which the system ID-to-host name mapping takes effect: **Level-1** or **Level-2**.

display isis non-stop-routing event-log

Use **display isis non-stop-routing event-log** to display IS-IS NSR log information.

Syntax

display isis non-stop-routing event-log slot *slot-number*

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its ID.

Examples

Display IS-IS NSR log information for the specified slot.

```
<Sysname> display isis non-stop-routing event-log slot 1
IS-IS loginfo :
Sep 18 10:20:44 2015 slot 1 Enter HA Block status
Sep 18 10:20:44 2015 slot 1 Exit HA Block status
```

```
Sep 18 10:24:00 2015 slot 1 Process 100 enter NSR phase (Initialization).
Sep 18 10:24:00 2015 slot 1 Process 100 enter NSR phase (Smooth).
Sep 18 10:24:00 2015 slot 1 Process 100 enter NSR phase (TE tunnel prepare).
Sep 18 10:24:00 2015 slot 1 Process 100 enter NSR phase (First SPF computation).
Sep 18 10:24:00 2015 slot 1 Process 100 enter NSR phase (Redistribution).
Sep 18 10:24:00 2015 slot 1 Process 100 enter NSR phase (Second SPF computation).
Sep 18 10:24:00 2015 slot 1 Process 100 enter NSR phase (LSP stability).
Sep 18 10:24:00 2015 slot 1 Process 100 enter NSR phase (LSP generation).
Sep 18 10:24:00 2015 slot 1 Process 100 enter NSR phase (Finish).
Sep 18 10:24:00 2015 slot 1 Process 100 NSR complete.
```

Table 12 Command output

Field	Description
NSR phase	NSR phase: • **Initialization**. • **Smooth**. • **TE tunnel prepare**—Preparing for TE tunnel computation. • **First SPF computation**. • **Redistribution**. • **Second SPF computation**. • **LSP stability**—Ready to generate LSPs. • **LSP generation**. • **Finish**.

display isis non-stop-routing status

Use **`display isis non-stop-routing status`** to display IS-IS NSR status.

Syntax

`display isis non-stop-routing status`

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display IS-IS NSR status.

```
<Sysname> display isis non-stop-routing status

                      Nonstop Routing information for IS-IS(1)
                    ----------------------------------------
NSR phase: Finish
```

Table 13 Command output

Field	Description
NSR phase	NSR phase: • **Initialization**. • **Smooth**. • **TE tunnel prepare**. • **First SPF computation**. • **Redistribution**. • **Second SPF computation**. • **LSP stability**—Ready to generate LSPs. • **LSP generation**. • **Finish**.

display isis peer

Use **display isis peer** to display IS-IS neighbor information.

Syntax

display isis peer [**statistics** | **verbose**] [*process-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

statistics: Displays IS-IS neighbor statistics.

verbose: Displays detailed IS-IS neighbor information. If you do not specify this keyword, the command displays brief IS-IS neighbor information.

process-id: Displays IS-IS neighbor information for an IS-IS process specified by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays neighbor information for all IS-IS processes.

Examples

Display brief IS-IS neighbor information.

```
<Sysname> display isis peer

                        Peer information for IS-IS(1)
                        ------------------------------

 System ID: 0000.0000.0001
 Interface: GE1/0/2                Circuit Id:  0000.0000.0001.01
 State: Up     HoldTime:  27s      Type: L1(L1L2)     PRI: 64

 System ID: 0000.0000.0001
```

```
 Interface: GE1/0/2                Circuit Id:  0000.0000.0001.01
 State: Up     HoldTime:  27s      Type: L2(L1L2)     PRI: 64
```

Display detailed IS-IS neighbor information.

```
<Sysname> display isis peer verbose

                        Peer information for IS-IS(1)
                        ----------------------------

 System ID: 0000.1111.2222
 Interface: GE1/0/2                Circuit Id:  0000.1111.2222.01
 State: Up     Holdtime:   6s      Type: L1(L1L2)     PRI: 64
 Area address(es): 49
 Peer IP address(es): 12.0.0.2
 Peer local circuit ID: 1
 Peer circuit SNPA address: 000c-293b-c4be
 Uptime: 00:05:07
 Adj protocol:  IPv4
 IPv4 adjacency state: Up
 Adj P2P three-way handshake: No
Graceful Restart capable
   Restarting signal: No
   Suppress adjacency advertisement: No
 Local topology:
   0
 Remote topology:
   0    2
 Local BFD support:
   (MTID:0, IPv4)
 Remote BFD support:
   (MTID:0, IPv4)

 System ID: 0000.0000.0002
 Interface: GE1/0/3                Circuit Id:  001
 State: Up     HoldTime: 27s       Type: L1L2         PRI: --
 Area address(es): 49
 Peer IP address(es): 192.168.220.30
 Peer local circuit ID: 1
 Peer circuit SNPA address: 000c-29fd-ed69
 Uptime: 00:05:07
 Adj protocol:  IPv4
 IPv4 adjacency state: Up
 Adj P2P three-way handshake: Yes
   Peer extended circuit ID: 2
 Graceful Restart capable
   Restarting signal: No
   Suppress adjacency advertisement: No
 Local topology:
   0
```

```
Remote topology:
  0
Local BFD support:
  (MTID:0, IPv4)
Remote BFD support:
  (MTID:0, IPv4)
```

Table 14 Command output

Field	Description
System ID	System ID of the neighbor.
Interface	Interface connecting to the neighbor.
Circuit Id	Circuit ID.
State	Circuit state.
HoldTime	Within the holdtime, if no hellos are received from the neighbor, the neighbor is considered down. If a hello is received, the holdtime is reset to the initial value.
Type	Circuit type: • **L1**—Means the circuit type is Level-1 and the neighbor is a Level-1 router. • **L2**—Means the circuit type is Level-2 and the neighbor is a Level-2 router. • **L1(L1L2)**—Means the circuit type is Level-1 and the neighbor is a Level-1-2 router. • **L2(L1L2)**—Means the circuit type is Level-2 and the neighbor is a Level-1-2 router.
PRI	DIS priority of the neighbor.
Area address(es)	Area address of the neighbor.
Peer IP address(es)	IP address of the neighbor.
Peer IPv6 address(es)	IPv6 address of the neighbor.
Uptime	Time elapsed since the neighbor relationship was formed.
Adj Protocol	Adjacency protocol: IPv4 or IPv6.
IPv4 adjacency state	IPv4 adjacency state: **Up** or **Down**. This field is not displayed if IPv4 is not supported.
IPv6 adjacency state	IPv6 adjacency state: **Up** or **Down**. This field is not displayed if IPv6 is not supported.
Adjacency not up	Reason why the adjacency relationship is down: **Waiting for BFD session to come up**. This field is no longer displayed after the adjacency relationship comes up.
Peer local circuit ID	Circuit ID of the neighbor.
Peer circuit SNPA address	SNPA address of the neighbor.
Adj P2P three-way handshake	Indicates whether the neighbor supports P2P three-way handshake.
Peer extended circuit ID	Extended circuit ID of the neighbor interface. This field is available when the neighbor supports three-way handshake.
Graceful Restart capable	The neighbor has the GR helper capability.

Field	Description
Restarting signal	RR flag.
Suppress adjacency advertisement	SA flag.
Local topology	List of topologies supported by the local interface.
Remote topology	List of topologies supported by the neighbor interface.
Local BFD support	Support of the local end for adjacency establishment and maintenance control based on BFD session state: • **(MTID:0, IPv4)**—Adjacency establishment and maintenance control based on BFD session state is supported in IPv4 unicast topology 0. • **(MTID:0, IPv6)**—Adjacency establishment and maintenance control based on BFD session state is supported in IPv6 unicast topology 0. • **(MTID:2, IPv6)**—Adjacency establishment and maintenance control based on BFD session state is supported in IPv6 unicast topology 2. This field is not displayed if the local end does not support adjacency establishment and maintenance control based on BFD session state.
Remote BFD support	Support of the remote end for adjacency establishment and maintenance control based on BFD session state: • **(MTID:0, IPv4)**—Adjacency establishment and maintenance control based on BFD session state is supported in IPv4 unicast topology 0. • **(MTID:0, IPv6)**—Adjacency establishment and maintenance control based on BFD session state is supported in IPv6 unicast topology 0. • **(MTID:2, IPv6)**—Adjacency establishment and maintenance control based on BFD session state is supported in IPv6 unicast topology 2. This field is not displayed if the remote end does not support adjacency establishment and maintenance control based on BFD session state.

Display IS-IS neighbor statistics.

```
<Sysname> display isis peer statistics

                  Peer Statistics information for IS-IS(1)
                  ----------------------------------------
  Type              IPv4 Up/Init              IPv6 Up/Init
  LAN Level-1             1/0                       0/0
  LAN Level-2             1/0                       0/0
  P2P                     0/0                       0/0
```

Table 15 Command output

Field	Description
Type	Neighbor type: • **LAN Level-1**—Number of Level-1 neighbors whose network type is broadcast. • **LAN Level-2**—Number of Level-2 neighbors whose network type is broadcast. • **P2P**—Number of neighbors whose network type is P2P.
IPv4 Up	Number of IPv4 neighbors in up state.
IPv4 Init	Number of IPv4 neighbors in init state.
IPv6 Up	Number of IPv6 neighbors in up state.
IPv6 Init	Number of IPv6 neighbors in init state.

display isis redistribute

Use **display isis redistribute** to display the redistributed IS-IS routing information.

Syntax

display isis redistribute [**ipv4** [*ip-address mask-length*] | **ipv6** [*ipv6-address prefix-length*]] [**level-1** | **level-2**] [*process-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ipv4: Displays the redistributed IPv4 routing information.

ipv6: Displays the redistributed IPv6 routing information.

ipv6-address prefix-length: Displays redistributed routes for the specified IPv6 address and mask length. The value range for the *prefix-length* argument is 1 to 128.

ip-address mask-length: Specifies the destination IP address and mask length.

process-id: Specifies the IS-IS process by its ID in the range of 1 to 65535.

level-1: Displays the IS-IS Level-1 routing information.

level-2: Displays the IS-IS Level-2 routing information.

Usage guidelines

If you do not specify the **ipv4** or **ipv6** keyword, the command displays redistributed IPv4 routing information.

If you do not specify an IS-IS level, this command displays both Level-1 and Level-2 routing information.

Examples

Display redistributed IPv4 IS-IS routing information.

```
<Sysname> display isis redistribute 1

                        Route information for IS-IS(1)
                        ------------------------------

                       Level-1 IPv4 Redistribute Table
                       -------------------------------
 Type IPv4 Destination     IntCost    ExtCost    Tag        State
--------------------------------------------------------------------------------
 D    192.168.30.0/24      0          0                     Active
 D    11.11.11.11/32       0          0
 D    10.10.10.0/24        0          0
```

Table 16 Command output

Field	Description
Route information for IS-IS(1)	IS-IS process of the redistributed routing information.
Level-1 IPv4 Redistribute Table	Redistributed IPv4 routing information of IS-IS Level-1.
Level-2 IPv4 Redistribute Table	Redistributed IPv4 routing information of IS-IS Level-2.
Type	Redistributed route type.
IPv4 Destination	IPv4 destination address.
IntCost	Internal cost of the route.
ExtCost	External cost of the route.
Tag	Tag value.
State	Indicates whether the route is valid.

Display redistributed IPv6 IS-IS routing information.

```
<Sysname> display isis redistribute ipv6 1

                        Route information for IS-IS(1)
                        ------------------------------

                       Level-1 IPv6 Redistribute Table
                       --------------------------------
Type       : direct    Destination: 12:1::/64
IntCost    : 0         Tag        :
State      : Active


                       Level-2 IPv6 Redistribute Table
                       --------------------------------
Type       : direct    Destination: 12:1::/64
IntCost    : 0         Tag        :
State      : Active
```

Table 17 Command output

Field	Description
Route information for IS-IS(1)	Redistributed routing information for IPv6 IS-IS process 1.
Level-1 IPv6 Redistribute Table	Redistributed IPv6 IS-IS Level-1 routing information.
Level-2 IPv6 Redistribute Table	Redistributed IPv6 IS-IS Level-2 routing information.
Type	Redistributed route types: • Direct. • IS-ISv6. • Static. • OSPFv3. • BGP4+. • RIPng.

Destination	IPv6 destination address.
IntCost	Internal route cost.
Tag	Tag value.
State	Indicates whether the redistributed route is valid.

display isis route

Use **display isis route** to display IS-IS routing information.

Syntax

display isis route [**ipv4** [*ip-address mask-length*] | **ipv6** [*ipv6-address prefix-length*]] [[**level-1** | **level-2**] | **verbose**] * [*process-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ipv4: Displays IPv4 IS-IS routing information.

ip-address mask-length: Displays IPv4 IS-IS routing information for the specified IP address. The *mask-length* argument is in the range of 0 to 32.

ipv6: Displays IPv6 IS-IS routing information.

ipv6-address prefix-length: Displays IPv6 IS-IS routing information for the specified IPv6 address. The *prefix-length* argument is in the range of 0 to 128.

verbose: Displays detailed IS-IS routing information. If you do not specify this keyword, the command displays brief IS-IS routing information

process-id: Displays IS-IS routing information for an IS-IS process specified by its ID in the range of 1 to 65535. If you do not specify an IS-IS process, this command displays routing information for all IS-IS processes.

level-1: Displays Level-1 IS-IS routes.

level-2: Displays Level-2 IS-IS routes.

Usage guidelines

If you do not specify the **ipv4** or **ipv6** keyword, the command displays IPv4 IS-IS routing information.

If you do not specify a level, this command displays both Level-1 and Level-2 routing information.

Examples

Display brief IPv4 IS-IS routing information.

```
<Sysname> display isis route

                        Route information for IS-IS(1)
```

```
                          ----------------------------

                          Level-1 IPv4 Forwarding Table
                          ----------------------------

 IPv4 Destination     IntCost    ExtCost ExitInterface   NextHop         Flags
--------------------------------------------------------------------------------
 8.8.8.0/24           10         NULL    GE1/0/2         Direct          D/L/-
 9.9.9.0/24           20         NULL    GE1/0/2         8.8.8.5         R/L/-

      Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set

                          Level-2 IPv4 Forwarding Table
                          ----------------------------

 IPv4 Destination     IntCost    ExtCost ExitInterface   NextHop         Flags
--------------------------------------------------------------------------------
 8.8.8.0/24           10         NULL                                    D/L/-

      Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set
```

Table 18 Command output

Field	Description
Route information for IS-IS(1)	Route information for IS-IS process 1.
Level-1 IPv4 Forwarding Table	IPv4 IS-IS routing information for Level-1.
Level-2 IPv4 Forwarding Table	IPv4 IS-IS routing information for Level-2.
IPv4 Destination	IPv4 destination address.
IntCost	Internal cost.
ExtCost	External cost.
ExitInterface	Output interface.
NextHop	Next hop.
Flags	Routing state flag: • **D**—Direct route. • **R**—The route has been added into the routing table. • **L**—The route has been advertised in an LSP. • **U**—Penetration flag. Setting it to UP can prevent an LSP sent from L2 to L1 from being sent back to L2.

Display detailed IPv4 IS-IS routing information.

```
<Sysname> display isis route verbose

                          Route information for IS-IS(1)
                          ----------------------------

                          Level-1 IPv4 Forwarding Table
```

```
                        ----------------------------

IPv4 Dest : 8.8.8.0/24          Int. Cost  : 10              Ext. Cost  : NULL
Admin Tag : -                   Src Count  : 2               Flag       : D/L/-
InLabel   : 4294967295          InLabel Flag: -/-/-/-/-/-
NextHop   :                     Interface  :                ExitIndex  :
   Direct                             GE1/0/2                  0x00000000
Nib ID    : 0x0                 OutLabel   : 4294967295      OutLabelFlag: -

IPv4 Dest : 9.9.9.0/24          Int. Cost  : 20              Ext. Cost  : NULL
Admin Tag : -                   Src Count  : 1               Flag       : R/L/-
InLabel   : 4294967295          InLabel Flag: -/-/-/-/-/-
NextHop   :                     Interface :                ExitIndex :
   8.8.8.5                            GE1/0/2                  0x00000003
Nib ID    : 0x0                 OutLabel   : 4294967295      OutLabelFlag: -

     Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set

     InLabel flags: R-Readvertisement, N-Node SID, P-no PHP
                    E-Explicit null, V-Value, L-Local

     OutLabelFlags: E-Explicit null, I-Implicit null, N-Nomal, P-SR label prefer

                        Level-2 IPv4 Forwarding Table
                        ----------------------------

IPv4 Dest : 8.8.8.0/24          Int. Cost  : 10              Ext. Cost  : NULL
Admin Tag : -                   Src Count  : 2               Flag       : D/L/-
InLabel   : 4294967295          InLabel Flag: -/-/-/-/-/-
NextHop   :                     Interface  :                ExitIndex  :
   Direct                             GE1/0/2                  0x00000000
Nib ID    : 0x14000003          OutLabel   : 4294967295      OutLabelFlag: -

IPv4 Dest : 90.0.0.0/8          Int. Cost  : 10              Ext. Cost  : 0
Admin Tag : -                   Src Count  : 2               Flag       : R/-/-
InLabel   : 4294967295          InLabel Flag: -/-/-/-/-/-    ECMP group : 0x1400000b
NextHop   :                     Interface  :                ExitIndex  :
   30.40.0.3                          GE1/0/3                  0x00000004
Nib ID    : 0x14000009          OutLabel   : 4294967295      OutLabelFlag: -
   20.40.0.2                          GE1/0/4                  0x00000005
Nib ID    : 0x1400000a          OutLabel   : 4294967295      OutLabelFlag: -

     Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set

     InLabel flags: R-Readvertisement, N-Node SID, P-no PHP
                    E-Explicit null, V-Value, L-Local

     OutLabelFlags: E-Explicit null, I-Implicit null, N-Nomal, P-SR label prefer
```

Table 19 Command output

Field	Description
Route information for IS-IS(1)	Route information for IS-IS process 1.
Level-1 IPv4 Forwarding Table	IPv4 IS-IS routing information for Level-1.
Level-2 IPv4 Forwarding Table	IPv4 IS-IS routing information for Level-2.
IPv4 Dest	IPv4 destination.
Int. Cost	Internal cost.
Ext. Cost	External cost.
Admin Tag	Tag.
Src Count	Count of advertising sources.
Flag	Route state flag: • **R**—The route has been installed into the routing table. • **L**—The route has been flooded in an LSP. • **U**—Route leaking flag. Setting it to UP can prevent an LSP sent from L2 to L1 from being sent back to L2.
NextHop	Next hop.
Interface	Output interface.
ExitIndex	Index of the output interface.
Nib ID	ID assigned by the routing management module (next hop index).
ECMP group	ECMP route group ID. This field is displayed only when ECMP route groups exist.
InLabel	Incoming label.
InLabel flag	Incoming label flag: • **R**—Re-advertisement flag. If set, inter-level propagation or route redistribution exists. • **N**—Node-SID flag. If set, the prefix SID is the SID to an SR node. • **P**—No-PHP flag. If set, the penultimate node cannot pop the prefix SID. • **E**—Explicit null flag. If set, the upstream neighbor must replace the prefix SID with an explicit null flag before forwarding the packets. • **V**—Value/Index flag. If set, the prefix SID carries an absolute value. • **L**—Local flag. If set, the prefix SID has local significance.
LabelSrc	Label source: • **SR**—The label is allocated by the SR node. • **SRMS**—The label is allocated by the segment routing mapping server (SRMS). • **N/A**—No label exists.
Delay Flag	Microloop avoidance delay flag: • **D**—Microloop avoidance is configured. Route convergence is delayed. • **N/A**—Microloop avoidance is not configured or the microloop avoidance delay timer has expired. Route convergence is in progress.
OutLabel	Outgoing label.

Field	Description
OutLabelFlag	Outgoing label flag: • **E**—Explicit null flag. The upstream neighbor must replace the SID with an explicit null flag before forwarding the packets. • **I**—Implicit null flag. The upstream neighbor must replace the SID with an implicit null flag before forwarding the packets. This flag is not supported in the current software version. • **N**—Normal flag. • **P**—SR label preferred flag.
TI-LFA	TI-LFA backup information.
BKNextHop	TI-LFA/Remote LFA backup next hop.
LsIndex	Label stack index.
Backup label stack(top->bottom)	Backup path label stack. **N/A** indicates that no label stack exists.
Remote-LFA	Remote LFA backup information.
Tunnel destination address	LDP tunnel destination address.
Backup label	Backup label to the PQ node. **N/A** indicates that no label exists.

Display IPv6 IS-IS routing information.

```
<Sysname> display isis route ipv6

                      Route information for IS-IS(1)
                      ------------------------------

                      Level-1 IPv6 forwarding table
                      ------------------------------

 Destination: 2001:1::                              PrefixLen: 64
 Flag       : R/L/-                                 Cost     : 20
 Next hop   : FE80::200:5EFF:FE64:8905              Interface: GE1/0/1

 Destination: 2001:2::                              PrefixLen: 64
 Flag       : D/L/-                                 Cost     : 10
 Next hop   : Direct                                Interface: GE1/0/1

       Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set

                      Level-2 IPv6 forwarding table
                      ------------------------------

 Destination: 2001:1::                              PrefixLen: 64
 Flag       : -/-/-                                 Cost     : 20


 Destination: 2001:2::                              PrefixLen: 64
 Flag       : D/L/-                                 Cost     : 10

       Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set
```

Table 20 Command output

Field	Description
Destination	IPv6 destination prefix.
PrefixLen	Length of the prefix.
Flag/Flags	Route flag: • **D**—This is a direct route. • **R**—The route has been added into the routing table. • **L**—The route has been advertised in an LSP. • **U**—Route leaking flag, indicating that the Level-1 route is from Level-2. **U** means the route will not be returned to Level-2.
Cost	Route cost.
Next hop	Next hop.
Interface	Output interface.

Display detailed IPv6 IS-IS routing information.

```
<Sysname> display isis route ipv6 verbose

                      Route information for IS-IS(1)
                      ------------------------------

                      Level-1 IPv6 forwarding table
                      ------------------------------

 IPv6 dest   : 2::2/128
 Flag        : R/L/-                       Cost        : 10
 Admin tag   : -                           Src count   : 1
 Nexthop     : FE80::86FB:DDFF:FE3F:1007
 Interface   : GE1/0/2
 BkNexthop   : FE80::86FB:D4FF:FE1B:E05
 BkInterface : GE1/0/1
 Nib ID      : 0x24000004

 IPv6 dest   : 2012::/64
 Flag        : D/L/-                       Cost        : 10
 Admin tag   : -                           Src count   : 2
 Nexthop     : Direct
 Interface   : GE1/0/2
 Nib ID      : 0x0

 IPv6 dest   : 2023::/64
 Flag        : R/L/-                       Cost        : 20
 Admin tag   : -                           Src count   : 2
 Nexthop     : FE80::86FB:D4FF:FE1B:E05
 Interface   : GE1/0/1
 Nib ID      : 0x24000002

 Nexthop     : FE80::86FB:DDFF:FE3F:1007
```

```
Interface   : GE1/0/2
Nib ID      : 0x24000003

IPv6 dest   : 2013::/64
Flag        : D/L/-                         Cost        : 10
Admin tag   : -                             Src count   : 2
Nexthop     : Direct
Interface   : GE1/0/1
Nib ID      : 0x0

     Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set

                      Level-2 IPv6 forwarding table
                      -----------------------------

IPv6 dest : 2::2/128
Flag      : -/-/-                       Cost      : 10
Admin tag : -                           Src count : 2
Nexthop   : -
Interface : -
Nib ID    : -

IPv6 dest   : 2012::/64
Flag        : D/L/-                         Cost        : 10
Admin tag   : -                             Src count   : 3
Nexthop     : Direct
Interface   : GE1/0/2
Nib ID      : 0x0

IPv6 dest : 2023::/64
Flag      : -/-/-                       Cost      : 20
Admin tag : -                           Src count : 2
Nexthop   : -
Interface : -
Nib ID    : -

IPv6 dest   : 2013::/64
Flag        : D/L/-                         Cost        : 10
Admin tag   : -                             Src count   : 3
Nexthop     : Direct
Interface   : GE1/0/1
Nib ID      : 0x0

     Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set
```

Table 21 Command output

Field	Description
IPv6 dest	IPv6 destination address and prefix.

Flag/Flags	Route flag: • **D**—This is a direct route. • **R**—The route has been added into the routing table. • **L**—The route has been advertised in an LSP. • **U**—Route leaking flag, indicating the Level-1 route is from Level-2. **U** means the route will not be returned to Level-2.
Cost	Route cost.
Admin tag	Administrative tag.
Src count	Number of advertisement sources.
ECMP group	ECMP route group ID. This field is displayed only when ECMP route groups exist.
Nexthop	Next hop.
Interface	Output interface.
BkNexthop	Backup next hop.
BkInterface	Backup output interface.
Nib ID	Next hop index assigned by the routing management module.

display isis spf-tree

Use **display isis spf-tree** to display IS-IS SPF tree information.

Syntax

display isis spf-tree [**ipv4** | **ipv6**] [[**level-1** | **level-2**] | [**source-id** *source-id* | **verbose**]] * [*process-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ipv4: Displays IPv4 IS-IS SPF tree information.

ipv6: Displays IPv6 IS-IS SPF tree information.

level-1: Displays Level-1 IS-IS SPF tree information. If you do not specify a level, the command displays both Level-1 and Level-2 SPF tree information.

level-2: Displays Level-2 SPF tree information. If you do not specify a level, the command displays both Level-1 and Level-2 SPF tree information.

source-id *source-id*: Displays detailed information about an SPF node. The *source-id* argument represents the system ID of the SPF node, in XXXX.XXXX.XXXX.XX format.

verbose: Displays detailed IS-IS SPF tree information. If you do not specify this keyword, the command displays brief IS-IS SPF tree information.

process-id: Specifies an IS-IS process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays SPF tree information for all IS-IS processes.

Usage guidelines

If you do not specify the **ipv4** or **ipv6** keyword, the command displays IPv4 IS-IS SPF tree information.

Examples

Display brief IPv4 IS-IS SPF tree information.

```
<Sysname> display isis spf-tree

                      Shortest Path Tree for IS-IS(1)
                      -------------------------------

      Flags: S-Node is on SPF tree       T-Node is on tent list
             O-Node is overload          R-Node is directly reachable
             I-Node or Link is isolated  D-Node or Link is to be deleted
             C-Neighbor is child         P-Neighbor is parent
             V-Link is involved          N-Link is a new path
             L-Link is on change list    U-Protocol usage is changed
             H-Nexthop is changed

                         Level-1 Shortest Path Tree
                         --------------------------

SpfNode            NodeFlag       SpfLink            LinkCost LinkFlag
-------------------------------------------------------------------------------
0000.0000.0032.00  S/-/-/-/-/-
                              -->0000.0000.0032.01  10       -/-/C/-/-/-/-/-/-
                              -->0000.0000.0064.00  10       -/-/C/-/-/-/-/-/-
0000.0000.0032.01  S/-/-/R/-/-
                              -->0000.0000.0064.00  0        -/-/C/-/-/-/-/-/-
                              -->0000.0000.0032.00  0        -/-/-/P/-/-/-/-/-
0000.0000.0064.00  S/-/-/R/-/-
                              -->0000.0000.0032.00  10       -/-/-/P/-/-/-/-/-
                              -->0000.0000.0032.01  10       -/-/-/P/-/-/-/-/-

                         Level-2 Shortest Path Tree
                         --------------------------

SpfNode            NodeFlag       SpfLink            LinkCost LinkFlag
-------------------------------------------------------------------------------
0000.0000.0032.00  S/-/-/-/-/-
                              -->0000.0000.0032.01  10       -/-/C/-/-/-/-/-/-
                              -->0000.0000.0064.00  10       -/-/C/-/-/-/-/-/-
0000.0000.0032.01  S/-/-/R/-/-
                              -->0000.0000.0064.00  0        -/-/C/-/-/-/-/-/-
                              -->0000.0000.0032.00  0        -/-/-/P/-/-/-/-/-
0000.0000.0064.00  S/-/-/R/-/-
                              -->0000.0000.0032.00  10       -/-/-/P/-/-/-/-/-
```

```
                              -->0000.0000.0032.01  10       -/-/-/P/-/-/-/-/-
```

Display detailed IPv4 IS-IS SPF tree information.

```
<Sysname> display isis spf-tree verbose

                      Shortest Path Tree for IS-IS(1)
                      -------------------------------

     Flags: S-Node is on SPF tree       T-Node is on tent list
            O-Node is overload          R-Node is directly reachable
            I-Node or Link is isolated  D-Node or Link is to be deleted
            C-Neighbor is child         P-Neighbor is parent
            V-Link is involved          N-Link is a new path
            L-Link is on change list    U-Protocol usage is changed
            H-Nexthop is changed

                         Level-1 Shortest Path Tree
                         --------------------------

 SpfNode        : 0000.0000.0001.00
 Distance       : 0
 TE distance    : 0
 NodeFlag       : S/-/-/-/-/-
 RelayNibID     : 0x0
 TE tunnel count: 0
 Nexthop count  : 0
 SpfLink count  : 1
 -->0000.0000.0004.04
    LinkCost    : 10
    LinkNewCost : 10
    LinkFlag    : -/-/C/-/-/-/-/-/-
    LinkSrcCnt  : 1
        Type       : Adjacent     Interface : N/A
        Cost       : 10           Nexthop   : N/A
        InterfaceIP: N/A          NeighborIP: N/A

 SpfNode        : 0000.0000.0004.00
 Distance       : 10
 Te Distance    : 10
 NodeFlag       : S/-/-/-/-/-
 RelayNibID     : 0x14000000
 TE tunnel count: 1
     Destination: 4.4.4.4                 Interface  : Tun0
     TE cost    : 10                      Final cost : 10
     Add nexthop: YES                     Add TLV    : YES
 Nexthop count  : 2
     Neighbor   : 0000.0000.0004.00       Interface  : Tun0
     Nexthop    : 4.4.4.4
     BkNeighbor : N/A                     BkInterface: N/A
```

```
    BkNexthop  : N/A
    Neighbor   : 0000.0000.0004.00        Interface  : GE1/0/1
    Nexthop    : 1.1.1.3
    BkNeighbor : N/A                      BkInterface: N/A
    BkNexthop  : N/A
SpfLink count  : 1
-->0000.0000.0004.04
   LinkCost    : 10
   LinkNewCost : 10
   LinkFlag    : -/-/-/P/-/-/-/-/-
   LinkSrcCnt  : 1
       Type       : Remote       Interface : N/A
       Cost       : 10           Nexthop   : N/A
       InterfaceIP: N/A          NeighborIP: N/A
       AdvMtID    : 0

SpfNode        : 0000.0000.0004.04
Distance       : 10
TE distance    : 10
NodeFlag       : S/-/-/R/-/-
RelayNibID     : 0x14000001
TE tunnel count: 0
Nexthop count  : 0
SpfLink count  : 2
-->0000.0000.0001.00
   LinkCost    : 0
   LinkNewCost : 0
   LinkFlag    : -/-/-/P/-/-/-/-/-
   LinkSrcCnt  : 1
       Type: Remote              Interface : N/A
       Cost: 0                   Nexthop   : N/A
       InterfaceIP: N/A          NeighborIP: N/A
-->0000.0000.0004.00
   LinkCost    : 0
   LinkNewCost : 0
   LinkFlag    : -/-/C/-/-/-/-/-/-
   LinkSrcCnt  : 1
       Type       : Remote       Interface : GE1/0/1
       Cost       : 0            Nexthop   : 1.1.1.3
       InterfaceIP: N/A          NeighborIP: N/A

                        Level-2 Shortest Path Tree
                        --------------------------

SpfNode        : 0000.0000.0001.00
Distance       : 0
TE distance    : 0
NodeFlag       : S/-/-/-/-/-
```

```
RelayNibID     : 0x0
TE tunnel count: 0
Nexthop count  : 0
SpfLink count  : 1
-->0000.0000.0004.04
   LinkCost    : 10
   LinkNewCost : 10
   LinkFlag    : -/-/C/-/-/-/-/-/-
   LinkSrcCnt  : 1
       Type       : Adjacent     Interface : N/A
       Cost       : 10           Nexthop   : N/A
       InterfaceIP: N/A          NeighborIP: N/A

SpfNode        : 0000.0000.0004.00
Distance       : 10
TE distance    : 10
NodeFlag       : S/-/-/-/-/-
RelayNibID     : 0x0
TE tunnel count: 1
    Destination: 4.4.4.4                 Interface  : Tun0
    TE cost    : 10                      Final cost : 10
    Add nexthop: YES                     Add TLV    : YES
Nexthop count  : 2
    Neighbor   : 0000.0000.0004.00       Interface  : Tun0
    Nexthop    : 4.4.4.4
    BkNeighbor : N/A                     BkInterface: N/A
    BkNexthop  : N/A
    Neighbor   : 0000.0000.0004.00       Interface  : GE1/0/1
    Nexthop    : 1.1.1.3
    BkNeighbor : N/A                     BkInterface: N/A
    BkNexthop  : N/A
SpfLink count  : 1
-->0000.0000.0004.04
   LinkCost    : 10
   LinkNewCost : 10
   LinkFlag    : -/-/-/P/-/-/-/-/-
   LinkSrcCnt  : 1
       Type       : Remote       Interface : N/A
       Cost       : 10           Nexthop   : N/A
       InterfaceIP: N/A          NeighborIP: N/A
       AdvMtID    : 0

SpfNode        : 0000.0000.0004.04
Distance       : 10
TE distance    : 10
NodeFlag       : S/-/-/R/-/-
RelayNibID     : 0x0
TE tunnel count: 0
```

```
Nexthop count  : 0
SpfLink count  : 2
-->0000.0000.0001.00
   LinkCost    : 0
   LinkNewCost : 0
   LinkFlag    : -/-/-/P/-/-/-/-/-
   LinkSrcCnt  : 1
       Type       : Remote       Interface : N/A
       Cost       : 0            Nexthop   : N/A
       InterfaceIP: N/A          NeighborIP: N/A
-->0000.0000.0004.00
   LinkCost    : 0
   LinkNewCost : 0
   LinkFlag    : -/-/C/-/-/-/-/-/-
   LinkSrcCnt  : 1
       Type       : Remote       Interface : GE1/0/1
       Cost       : 0            Nexthop   : 1.1.1.3
       InterfaceIP: N/A          NeighborIP: N/A
```

Table 22 Command output

Field	Description
SpfNode	ID of the topology node.
Distance	Shortest distance from the root node to the local node.
TE distance	Shortest distance from the root node to the local node (including tunnel links). If tunnel is not configured, TE distance equals to Distance.
NodeFlag	Node flag: • **S**—The node is on the SPF tree. • **T**—The node is on the tent list. • **O**—The node is overloaded. • **R**—The node is directly connected. • **I**—The node is isolated. • **D**—The node is to be deleted.
RelayNibID	Next hop ID of the node after route recursion.
TE tunnel count	Number of tunnels destined to this node.
Destination	Destination router.
Nexthop count	Next hop count.
Nexthop	Primary next hop of the node or the link advertising source.
AdvMtID	Topology from which the routing information is learned: • **0**—Base topology. • **6-4094**—Other topologies.
Interface	Primary output interface of the node or the link advertising source.
BkNexthop	Backup next hop.
BkInterface	Backup output interface.
Neighbor	ID of the primary next hop neighbor.
BkNeighbor	ID of the backup next hop neighbor.

Field	Description
TiLfaNeighbor	ID of the TI-LFA backup next hop neighbor.
TiLfaInterface	Output interface of the TI-LFA backup next hop.
TiLfaNexthop	TI-LFA backup next hop.
PNode SrcID	Source ID of the P node.
QNode SrcID	Source ID of the Q node.
PNode prefix	Prefix of the P node. **N/A** indicates that the prefix of the destination node is not displayed in the P space.
PNode SidIndex	Index value of the prefix SID for the P node. **N/A** indicates that the prefix SID of the destination node is not displayed in the P space.

Protect	TI-LFA/Remote LFA traffic protection type:
	• **Link**—Link protection that excludes the direct primary link from backup path calculation.
	• **Node**—Node protection that excludes the primary next hop node from backup path calculation.
	• **SrlgLink**—SRLG-disjoint link protection that excludes the following links from backup path calculation:
	  ○ Direct primary link.
	  ○ Local links in the same SRLG as the direct primary link.
	• **SrlgNode**—SRLG-disjoint node protection that excludes the following nodes from backup path calculation:
	  ○ Primary next hop node.
	  ○ Local links in the same SRLG as the direct primary link.

Label stack	Label stack. **N/A** indicates that no label stack exists.
SpfLink	Topology link.
SpfLink count	Number of topology links.
LinkCost	Link cost.
LinkNewCost	New link cost.
LinkFlag	Link flag: • **I**—The link is isolated. • **D**—The link is to be deleted. • **C**—The neighbor is a child node. • **P**—The neighbor is the parent node. • **V**—The link is involved. • **N**—The link is a new path. • **L**—The link is on the change list. • **U**—The protocol usage of the link is changed. • **H**—The next hop of the link is changed.
LinkSrcCnt	Number of link advertising sources.
Type	Type of the link advertising source: • **Adjacent**—The link advertising source is a local neighbor. • **Remote**—The link advertising source is advertised by a remote node in an LSP.
Cost	Cost of the link advertising source.
InterfaceIP	Interface IP address.
NeighborIP	Neighbor IP address.

Field	Description
Remote-LFA	Remote LFA backup information.
RLfaNeighbor	System ID of the remote LFA backup next hop.
PQNode	System ID of the PQ node.
PQNodePrefix	PQ node prefix.
OutLabel	Backup label to the PQ node.

Display brief IPv6 IS-IS SPF tree information.

```
<Sysname> display isis spf-tree ipv6

                      Shortest Path Tree for IS-IS(1)
                      -------------------------------

      Flags: S-Node is on SPF tree       T-Node is on tent list
             O-Node is overload          R-Node is directly reachable
             I-Node or Link is isolated  D-Node or Link is to be deleted
             C-Neighbor is child         P-Neighbor is parent
             V-Link is involved          N-Link is a new path
             L-Link is on change list    U-Protocol usage is changed
             H-Nexthop is changed

                      Level-1 Shortest Path Tree
                      ----------------------------------

SpfNode            NodeFlag       SpfLink            LinkCost LinkFlag
--------------------------------------------------------------------------------
0000.0000.0032.00  S/-/-/-/-/-
                               -->0000.0000.0032.01  10       -/-/C/-/-/-/-/-/-
                               -->0000.0000.0064.00  10       -/-/C/-/-/-/-/-/-
0000.0000.0032.01  S/-/-/R/-/-
                               -->0000.0000.0064.00  0        -/-/C/-/-/-/-/-/-
                               -->0000.0000.0032.00  0        -/-/-/P/-/-/-/-/-
0000.0000.0064.00  S/-/-/R/-/-
                               -->0000.0000.0032.00  10       -/-/-/P/-/-/-/-/-
                               -->0000.0000.0032.01  10       -/-/-/P/-/-/-/-/-

                      Level-2 Shortest Path Tree
                      ----------------------------------

SpfNode            NodeFlag       SpfLink            LinkCost LinkFlag
--------------------------------------------------------------------------------
0000.0000.0032.00  S/-/-/-/-/-
                               -->0000.0000.0032.01  10       -/-/C/-/-/-/-/-/-
                               -->0000.0000.0064.00  10       -/-/C/-/-/-/-/-/-
0000.0000.0032.01  S/-/-/R/-/-
                               -->0000.0000.0064.00  0        -/-/C/-/-/-/-/-/-
                               -->0000.0000.0032.00  0        -/-/-/P/-/-/-/-/-
```

```
0000.0000.0064.00  S/-/-/R/-/-
                               -->0000.0000.0032.00  10       -/-/-/P/-/-/-/-/-
                               -->0000.0000.0032.01  10       -/-/-/P/-/-/-/-/-
```

Display detailed Level-1 IPv6 IS-IS SPF tree information.

```
<Sysname> display isis spf-tree ipv6 level-1 verbose
                       Shortest Path Tree for IS-IS(1)
                       -------------------------------

      Flags: S-Node is on SPF tree       T-Node is on tent list
             O-Node is overload          R-Node is directly reachable
             I-Node or Link is isolated  D-Node or Link is to be deleted
             C-Neighbor is child         P-Neighbor is parent
             V-Link is involved          N-Link is a new path
             L-Link is on change list    U-Protocol usage is changed
             H-Nexthop is changed

                          Level-1 Shortest Path Tree
                          --------------------------

 SpfNode        : 0000.0000.0032.00
 Distance       : 0
 TE distance    : 0
 NodeFlag       : S/-/-/-/-/-
 RelayNibID     : 0x0
 TE tunnel count: 0
 Nexthop count  : 0
 SpfLink count  : 2
 -->0000.0000.0032.01
    LinkCost    : 10
    LinkNewCost : 10
    LinkFlag    : -/-/C/-/-/-/-/-/-
    LinkSrcCnt  : 1
     Type       : Adjacent     Interface : N/A
     Cost       : 10           Nexthop   : N/A
     InterfaceIP: N/A          NeighborIP: N/A
-->0000.0000.0064.00
    LinkCost    : 10
    LinkNewCost : 10
    LinkFlag    : -/-/C/-/-/-/-/-/-
    LinkSrcCnt  : 1
     Type       : Adjacent     Interface : Tun1
     Cost       : 10           Nexthop   : FE80::A0A:A40
     InterfaceIP: N/A          NeighborIP: N/A

SpfNode        : 0000.0000.0032.01
 Distance       : 10
 TE distance    : 10
 NodeFlag       : S/-/-/R/-/-
```

```
 RelayNibID     : 0x0
 TE tunnel count: 0
 Nexthop count  : 0
 SpfLink count  : 2
 -->0000.0000.0064.00
    LinkCost    : 0
    LinkNewCost : 0
    LinkFlag    : -/-/C/-/-/-/-/-/-
    LinkSrcCnt  : 1
     Type       : Adjacent     Interface : GE1/0/2
     Cost       : 10           Nexthop   : FE80::200:12FF:FE34:1
     InterfaceIP: N/A          NeighborIP: N/A
-->0000.0000.0032.00
    LinkCost    : 0
    LinkNewCost : 0
    LinkFlag    : -/-/-/P/-/-/-/-/-
    LinkSrcCnt  : 1
     Type       : Adjacent     Interface : N/A
     Cost       : 0            Nexthop   : N/A
     InterfaceIP: N/A          NeighborIP: N/A

SpfNode        : 0000.0000.0064.00
 Distance       : 10
 TE distance    : 10
 NodeFlag       : S/-/-/R/-/-
 RelayNibID     : 0x0
 TE tunnel count: 0
 Nexthop count  : 2
     Neighbor  : 0000.0000.0064.00        Interface  : GE1/0/2
     NextHop   : FE80::200:12FF:FE34:1
     BkNeighbor: N/A                      BkInterface: N/A
     BkNextHop : N/A
     Neighbor  : 0000.0000.0064.00        Interface  : Tun1
     NextHop   : FE80::A0A:A40
     BkNeighbor: N/A                      BkInterface: N/A
     BkNextHop : N/A
 SpfLink count  : 2
 -->0000.0000.0032.00
    LinkCost    : 10
    LinkNewCost : 10
    LinkFlag    : -/-/-/P/-/-/-/-/-
    LinkSrcCnt  : 1
     Type       : Remote       Interface : N/A
     Cost       : 10           Nexthop   : N/A
     InterfaceIP: N/A          NeighborIP: N/A
        AdvMtID : 0
-->0000.0000.0064.00
    LinkCost    : 10
```

```
LinkNewCost : 10
LinkFlag    : -/-/C/-/-/-/-/-/-
LinkSrcCnt  : 1
 Type       : Remote       Interface : Tun1
 Cost       : 10           Nexthop   : FE80::A0A:A40
 InterfaceIP: N/A          NeighborIP: N/A
    AdvMtID : 0
```

Table 23 Command output

Field	Description
SpfNode	ID of the topology node.
Distance	Shortest distance from the root node to the current node.
TE distance	Shortest distance from the root node to the current node (including tunnel links). If no tunnels are configured, TE distance equals Distance.
NodeFlag	Node flag: • **S**—The node is on the SPF tree. • **T**—The node is on the tent list. • **O**—The node is overloaded. • **R**—The node is directly connected. • **I**—The node is isolated. • **D**—The node is to be deleted.
TE tunnel count	Number of tunnels destined for this node.
Nexthop count	Number of next hops.
NextHop	Primary next hop of the node or the link advertising source.
AdvMtID	Topology from which the routing information is learned: • **2**—IPv6 unicast topology. • **6-4094**—Other topologies.
Interface	Primary output interface of the node or the link advertising source.
BkNextHop	Backup next hop.
BkInterface	Backup output interface.
Neighbor	ID of the primary next hop neighbor.
BkNeighbor	ID of the backup next hop neighbor.
SpfLink	Topology link.
SpfLink count	Number of topology links.
LinkCost	Link cost.
LinkNewCost	New link cost.
LinkFlag	Link flag: • **I**—The link is isolated. • **D**—The link is to be deleted. • **C**—The neighbor is a child node. • **P**—The neighbor is the parent node. • **V**—The link is involved. • **N**—The link is a new path.

	• **L**—The link is on the change list. • **U**—The protocol of the link is changed. • **H**—The next hop of the link is changed.
LinkSrcCnt	Number of link advertising sources.
Type	Type of the link advertising source: • **Adjacent**—The link advertising source is a local neighbor. • **Remote**—The link advertising source is advertised by a remote node in an LSP.
Cost	Cost of the link advertising source.

display isis statistics

Use **display isis statistics** to display IS-IS statistics.

Syntax

display isis statistics [**ipv4** | **ipv6**] [**level-1** | **level-1-2** | **level-2**] [*process-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ipv4: Displays IPv4 IS-IS statistics. If you do not specify this option, the command displays both IPv4 and IPv6 statistics.

ipv6: Displays IPv6 IS-IS statistics.

level-1: Displays IS-IS Level-1 statistics.

level-1-2: Displays IS-IS Level-1-2 statistics.

level-2: Displays IS-IS Level-2 statistics.

process-id: Displays statistics for an IS-IS process specified by its ID in the range of 1 to 65535. If you do not specify an IS-IS process, this command displays the statistics for all IS-IS processes.

Usage guidelines

If you do not specify a level, this command displays both Level-1 and Level-2 routing information.

Examples

Display IS-IS statistics.

```
<Sysname> display isis statistics

                    Statistics information for IS-IS(1)
                    -----------------------------------

                           Level-1 Statistics
```

```
                              ------------------

Learnt routes information:
        Total IPv4 Learnt Routes in IPv4 Routing Table: 1
Imported routes information:
        IPv4 Imported Routes:
                        Static: 0       Direct: 0
                        ISIS:   0       BGP:    0
                        RIP:    0       OSPF:   0
                        EIGRP:  0
                        Total Number:   0
Learnt routes information:
        Total IPv6 Learnt Routes in IPv6 Routing Table: 0
Imported routes information:
        IPv6 Imported Routes:
                        Static: 0       Direct: 0
                        ISISv6: 0       BGP4+:  0
                        RIPng:  0       OSPFv3: 0
                        Total Number:   0
Lsp information:
                  LSP Source ID:          No. of used LSPs
                  7777.8888.1111                  001
                              Level-2 Statistics
                              ------------------
Learnt routes information:
         Total IPv4 Learnt Routes in IPv4 Routing Table: 0
Imported routes information:
        IPv4 Imported Routes:
                        Static: 0       Direct: 0
                        ISIS:   0       BGP:    0
                        RIP:    0       OSPF:   0
                        EIGRP:  0
                        Total Number:   0
Learnt routes information:
         Total IPv6 Learnt Routes in IPv6 Routing Table: 0
Imported routes information:
         IPv6 Imported Routes:
                         Static: 0       Direct: 0
                         ISISv6: 0       BGP4+:  0
                         RIPng:  0       OSPFv3: 0
                         Total Number:   0
Lsp information:
                  LSP Source ID:          No. of used LSPs
                  7777.8888.1111                  001
```

Table 24 Command output

Field	Description
Statistics information for IS-IS(*processid*)	Statistics for the IS-IS process.

Field	Description
Level-1 Statistics	Level-1 statistics.
Level-2 Statistics	Level-2 statistics.
Learnt routes information	• **Total IPv4 Learnt Routes in IPv4 Routing Table**—Number of learned IPv4 routes. • **Total IPv6 Learnt Routes in IPv6 Routing Table**—Number of learned IPv6 routes.
IPv4 Imported Routes	Numbers of different types of redistributed IPv4 routes, including static, direct, IS-IS, BGP, RIP, OSPF, and EIGRP routes. EIGRP routes are not supported in the current software version.
IPv6 Imported Routes	Numbers of different types of redistributed IPv6 routes, including static, direct, IS-ISv6, BGP4+, RIPng, and OSPFv3 routes.
Lsp information	LSP information: • **LSP Source ID**—ID of the source system. • **No. of used LSPs**—Number of used LSPs.

display osi

Use **display osi** to display OSI connection information.

Syntax

display osi [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays OSI connection information for all member devices.

Examples

Display OSI connection information.

```
<Sysname> display osi
Total OSI socket number: 2

 Location: slot 0
 Creator: isisd[1539]
 State: N/A
 Options: SO_FILTER
 Error: 0
 Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 1048576 / 1 / 0 / N/A
 Sending buffer(cc/hiwat/lowat/state): 0 / 262144 / 512 / N/A
```

```
Type: 2
Enabled interfaces:
 GigabitEthernet1/0/1
  MAC address: 0180-c200-0014

Location: slot 0
Creator: isisd[1539]
State: N/A
Options: SO_FILTER
Error: 0
Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 1048576 / 1 / 0 / N/A
Sending buffer(cc/hiwat/lowat/state): 0 / 262144 / 512 / N/A
Type: 2
Enabled interfaces:
 GigabitEthernet1/0/1
  MAC address: 0180-c200-0014
```

Table 25 Command output

Field	Description
Total OSI socket number	Total number of OSI sockets.
Creator	Name of the socket creator. The process ID of the creator is displayed in the square brackets.
State	This field always displays **N/A**.
Options	Socket options: • **SO_FILTER**—Filter option is configured. • **N/A**—No option is configured.
Error	Number of errors that affect the socket session.
Receiving buffer(cc/hiwat/lowat/drop/state)	Receiving buffer information, including the current used space, maximum space, minimum space, number of dropped packets, and status.
Sending buffer(cc/hiwat/lowat/state)	Sending buffer information, including the current used space, maximum space, minimum space, and status.
Type	Type 2 socket, corresponding to unreliable connectionless-oriented transport layer protocols.
Enabled interfaces	Input interfaces and matched multicast MAC addresses. Only packets received from Ethernet link-layer interfaces need to match the multicast MAC addresses.

display osi statistics

Use **display osi statistics** to display OSI packet statistics.

Syntax

display osi statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays OSI packet statistics for all member devices.

Examples

Display OSI packet statistics.

```
<Sysname> display osi statistics
Received packets:
     Total: 35
     Relay received: 35
     Relay forwarded: 35
     Invalid service slot: 0
     No matched socket: 0
     Not delivered, input socket full: 0
Sent packets:
     Total: 19
     Relay forwarded: 19
     Relay received: 19
     Failed: 0
```

Table 26 Command output

Field	Description
Received packets	Statistics of received packets: • **Total**—Total number of received link layer packets. • **Relay received**—Number of inbound packets on LPUs relayed from other cards. This count is not included in the total count of received packets. • **Relay forwarded**—Number of inbound packets relayed to LPUs. • **Invalid service slot**—Number of discarded packets due to unavailable LPUs. • **No matched socket**—Number of discarded packets due to mismatches in input interfaces, MAC addresses, or connection filter criteria. • **Not delivered, input socket full**—Number of undelivered packets due to a socket receiving buffer overflow.

Field	Description
Sent packets	Statistics of sent packets: • **Total**—Total number of packets that IS-IS sent over OSI connections. • **Relay forwarded**—Number of outbound packets relayed to the cards that hosts the output interfaces. This count is not included in the total count of sent packets. • **Relay received**—Number of outbound packets on the cards that hosts the output interfaces. These packets are relayed from other cards. • **Failed**—Number of packets failed to be sent.

Related commands

`reset osi statistics`

distribute bgp-ls

Use **`distribute bgp-ls`** to advertise IS-IS link state information to BGP.

Use **`undo distribute bgp-ls`** to restore the default.

Syntax

`distribute bgp-ls` [**`instance-id`** *`id`*] [**`level-1`** | **`level-2`**]

`undo distribute bgp-ls` [**`level-1`** | **`level-2`**]

Default

The device does not advertise IS-IS link state information to BGP.

Views

IS-IS view

Predefined user roles

network-admin

context-admin

Parameters

`instance-id` *`id`*: Specifies an instance by its ID in the range of 0 to 65535. If you do not specify this option, the command advertises IS-IS link state information of instance 0 to BGP.

`level-1`: Advertises the Level-1 IS-IS link state information to BGP.

`level-2`: Advertises the Level-2 IS-IS link state information to BGP.

Usage guidelines

After the device advertises IS-IS link state information to BGP, BGP can advertise the information for intended applications.

If multiple IS-IS processes have the same instance ID and link state information, only the link state information of the IS-IS process with the smallest process ID is advertised.

To advertise the same link state information of different IS-IS processes to BGP, specify different instance IDs for the IS-IS processes.

If you do not specify a level for the **`distribute bgp-ls`** command, both Level-1 and Level-2 IS-IS link state information are advertised to BGP.

If you do not specify a level for the **undo distribute bgp-ls** command, neither Level-1 nor Level-2 IS-IS link state information can be advertised to BGP.

Examples

Advertise link state information of IS-IS process 1 to BGP.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] distribute bgp-ls
```

domain-authentication send-only

Use **domain-authentication send-only** to configure IS-IS not to check the authentication information in the received Level-2 packets, including LSPs, CSNPs, and PSNPs.

Use **undo domain-authentication send-only** to restore the default.

Syntax

domain-authentication send-only

undo domain-authentication send-only

Default

When domain authentication mode and key are configured, a Level-2 or Level-1-2 router checks the authentication information in the received packets.

Views

IS-IS view

Predefined user roles

network-admin

context-admin

Usage guidelines

When domain authentication mode and key are configured, a Level-2 or Level-1-2 router adds the key in the specified mode into transmitted Level-2 packets (including LSPs, CSNPs, and PSNPs). It also checks the key in the received Level-2 packets.

To prevent packet exchange failure in case of an authentication key change, configure IS-IS not to check the authentication information in the received packets.

Examples

Configure IS-IS not to check the authentication information in the received packets.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] domain-authentication send-only
```

Related commands

area-authentication send-only

domain-authentication-mode

isis authentication send-only

domain-authentication-mode

Use **domain-authentication-mode** to specify the routing domain authentication mode and a key.

Use **undo domain-authentication-mode** to restore the default.

Syntax

domain-authentication-mode { { **gca** *key-id* { **hmac-sha-1** | **hmac-sha-224** | **hmac-sha-256** | **hmac-sha-384** | **hmac-sha-512** } [**nonstandard**] | **md5** | **simple** } { **cipher** | **plain** } *string* | **keychain** *keychain-name* } [**ip** | **osi**]

undo domain-authentication-mode

Default

No routing domain authentication mode or key is configured.

Views

IS-IS view

Predefined user roles

network-admin

context-admin

Parameters

gca: Specifies the GCA mode.

key-id: Uniquely identifies an SA in the range of 1 to 65535. The sender inserts the Key ID into the authentication TLV, and the receiver authenticates the packet by using the SA that is selected based on the Key ID.

hmac-sha-1: Specifies the HMAC-SHA-1 algorithm.

hmac-sha-224: Specifies the HMAC-SHA-224 algorithm.

hmac-sha-256: Specifies the HMAC-SHA-256 algorithm.

hmac-sha-384: Specifies the HMAC-SHA-384 algorithm.

hmac-sha-512: Specifies the HMAC-SHA-512 algorithm.

nonstandard: Specifies the nonstandard GCA authentication mode.

md5: Specifies the MD5 authentication mode.

simple: Specifies the simple authentication mode.

cipher: Specifies a key in encrypted form.

plain: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. Its plaintext form is a case-sensitive string of 1 to 16 characters. Its encrypted form is a case-sensitive string of 33 to 53 characters.

keychain: Specifies the keychain authentication mode.

keychain-name: Specifies a keychain by its name, a case-sensitive string of 1 to 63 characters.

ip: Checks IP-related fields in LSPs.

osi: Checks OSI-related fields in LSPs.

Usage guidelines

The configured key in the specified mode is inserted into all outgoing Level-2 packets (LSP, CSNP, and PSNP) and is used for authenticating the incoming Level-2 packets.

IS-IS keychain authentication supports the HMAC-MD5 and HMAC-SM3 authentication algorithms. For the HMAC-SM3 authentication algorithm, only key IDs in the range of 0 to 65535 are supported. When keychain authentication is used, IS-IS receives and sends packets as follows:

- Before IS-IS sends a Level-2 packet, it uses the valid send key obtained from the keychain to authenticate the packet. If no valid send key exists or the valid send key does not use the HMAC-MD5 or HMAC-SM3 algorithm, the authentication fails and the packet does not contain the authentication information.
- After IS-IS receives a Level-2 packet, it processes the packet as follows:
  - If the authentication algorithm of the packet is HMAC-MD5, IS-IS uses a valid accept key obtained from the keychain to authenticate the packet. If no valid accept key exists or all valid accept keys fail to authenticate the packet, the authentication fails and the packet is discarded.
  - If the authentication algorithm of the packet is HMAC-SM3, IS-IS uses the key ID of the received packet to obtain the corresponding valid accept key from the keychain. Then, IS-IS uses the accept key to authenticate the packet. If IS-IS cannot find a valid accept key based on the key ID of the received packet or the packet fails the authentication, the packet is discarded.

All the backbone routers must have the same authentication mode and key.

If neither **ip** nor **osi** is specified, the OSI-related fields in LSPs are checked.

When you specify the GCA mode, follow these guidelines:

- If you do not specify the **nonstandard** keyword, the device can communicate only with devices that use the GCA mode.
- If you specify the **nonstandard** keyword, the device can communicate only with devices that use the nonstandard GCA mode.

Examples

Set the routing domain authentication mode to **simple**, and set the plaintext key to **123456**.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] domain-authentication-mode plain 123456
```

Related commands

area-authentication-mode

domain-authentication send-only

isis authentication-mode

ecmp-group enable

Use **ecmp-group enable** to enable IS-IS to group ECMP routes.

Use **undo ecmp-group enable** to restore the default.

Syntax

ecmp-group enable

undo ecmp-group enable

Default

IS-IS does not group ECMP routes.

Views

IS-IS IPv4 unicast address family view

IS-IS IPv6 unicast address family view

Predefined user roles

network-admin

context-admin

Usage guidelines

Configure this command to enable IS-IS to group ECMP routes by prefix to speed up route convergence.

This command is applicable to a network when the network has a large number of ECMP routes and different route prefixes in the network have the same next hops. For example, IS-IS learns 10000 route prefixes and all route prefixes have the same 16 next hops (1.1.1.1 to 1.1.1.16). If you do not configure this command, IS-IS has to send all ECMP routes of every route prefix (10000 × 16 routes) to the route management module. After you configure this command, IS-IS groups the ECMP routes by prefix and sends the route groups (10000 route groups) to the route management module.

If the output interfaces to the next hops of ECMP routes are TE tunnel interfaces, IS-IS groups the ECMP routes regardless of whether you enable this feature or not.

Examples

Enable IS-IS process 1 to group ECMP routes.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] address-family ipv4
[Sysname-isis-1-ipv4] ecmp-group enable
```

fast-reroute

Use **fast-reroute** to configure IS-IS FRR.

Use **undo fast-reroute** to disable IS-IS FRR.

Syntax

fast-reroute { **lfa** [**level-1** | **level-2**] | **route-policy** *route-policy-name* }

undo fast-reroute { **lfa** [**level-1** | **level-2**] | **route-policy** }

Default

IS-IS FRR is disabled.

Views

IS-IS IPv4 unicast address family view

IS-IS IPv6 unicast address family view

Predefined user roles

network-admin

context-admin

Parameters

lfa: Calculates a backup next hop through Loop Free Alternate (LFA) calculation for all routes.

level-1: Specifies Level-1 routes.

level-2: Specifies Level-2 routes.

route-policy *route-policy-name*: Uses the specified routing policy to designate a backup next hop. The *route-policy-name* argument is a case-sensitive string of 1 to 63 characters.

Usage guidelines

ECMP routes do not support FRR.

The LFA calculation of FRR and IS-IS TE are mutually exclusive.

Example

Enable FRR for IS-IS process 1 and configure IS-IS FRR to calculate a backup next hop through LFA calculation for all routes.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] address-family ipv4
[Sysname-isis-1-ipv4] fast-reroute lfa
```

fast-reroute tiebreaker

Use **fast-reroute tiebreaker** to set the priority for the node-protection or lowest-cost backup path selection policy.

Use **undo fast-reroute tiebreaker** to restore the default.

Syntax

In IS-IS IPv4 unicast address family view:

fast-reroute tiebreaker { **lowest-cost** | **node-protecting** | **srlg-disjoint** } **preference** *preference* [**level-1** | **level-2**]

undo fast-reroute tiebreaker { **lowest-cost** | **node-protecting** | **srlg-disjoint** } [**level-1** | **level-2**]

In IS-IS IPv6 unicast address family view:

fast-reroute tiebreaker { **lowest-cost** | **node-protecting** } **preference** *preference* [**level-1** | **level-2**]

undo fast-reroute tiebreaker { **lowest-cost** | **node-protecting** } [**level-1** | **level-2**]

Default

The priority values of the node-protection, lowest-cost, and SRLG-disjoint backup path selection policies are 40, 20, and 10, respectively.

Views

IS-IS IPv4 unicast address family view

IS-IS IPv6 unicast address family view

Predefined user roles

network-admin

context-admin

Parameters

lowest-cost: Sets a priority value for the lowest-cost backup path selection policy.

node-protecting: Sets a priority value for the node-protection backup path selection policy.

srlg-disjoint: Sets a priority value for the SRLG-disjoint backup path selection policy.

preference *preference*: Specifies a priority value in the range of 1 to 255. A higher value indicates a higher priority.

level-1: Applies the configuration to Level-1 areas.

level-2: Applies the configuration to the Level-2 area.

Usage guidelines

IS-IS FRR uses specific policies for backup path calculation. This command defines the priority for the backup path selection policy. The higher the value, the higher the priority of the associated backup path selection policy. Changing the backup path selection policy priority can affect the backup path calculation result for IS-IS FRR. The backup paths can provide node protection or link protection for traffic, or provide both node protection and link protection.

IS-IS FRR supports the following backup path selection policies that are used to generate different topologies for backup path calculation:

- **Node protection**—IS-IS FRR performs backup path calculation after excluding the primary next hop node.
- **Lowest cost**—IS-IS FRR performs backup path calculation after excluding the direct primary link.
- **SRLG disjoint**—When one link in the SRLG fails, the other links in the SRLG might also fail. If you use a link in this SRLG as the backup link for the failed link, protection does not take effect. To avoid this issue, IS-IS FRR excludes the local links in the same SRLG as the direct primary link and then performs backup path calculation.

For IS-IS FRR, the SRLG disjoint policy depends on the node protection and lowest cost policies.

If multiple backup path selection policies exist in an IS-IS process, the policy with the highest priority is used to calculate the backup path. If the policy fails to calculate the backup path, another policy with higher priority is used. IS-IS performs backup path calculation by using the node protection and lowest cost policies as follows:

- If the node protection policy has higher priority and fails to calculate the backup path, IS-IS uses the lowest cost policy to calculate the backup path. If the lowest cost policy still fails to calculate the backup path, reliability cannot be ensured upon primary link failure.
- If the lowest cost policy has higher priority and fails to calculate the backup path, IS-IS does not perform further backup path calculation with the node protection policy. Reliability cannot be ensured upon primary link failure.

You can execute this command multiple times to specify the priorities for the lowest cost, node protection, and SRLG disjoint policies, respectively.

If you execute this command multiple times for a backup path selection policy, the most recent configuration takes effect.

If you do not specify a level, the command takes effect on both Level-1 and Level-2 areas.

Examples

Set the priority value of the node-protection backup path selection policy to 100.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] address-family ipv4
[Sysname-isis-1-ipv4] fast-reroute tiebreaker node-protecting preference 100
```

Related commands

fast-reroute

filter-policy export

Use **filter-policy export** to configure IS-IS to filter redistributed routes.

Use **undo filter-policy export** to remove the configuration.

Syntax

In IS-IS IPv4 unicast address family view:

filter-policy { *ipv4-acl-number* | **prefix-list** *prefix-list-name* | **route-policy** *route-policy-name* } **export** [**bgp** | **direct** | { **isis** | **ospf** | **rip** } *process-id* | **static**]

undo filter-policy export [**bgp** | **direct** | { **isis** | **ospf** | **rip** } *process-id* | **static**]

In IS-IS IPv6 unicast address family view:

filter-policy { *ipv6-acl-number* | **prefix-list** *prefix-list-name* | **route-policy** *route-policy-name* } **export** [**bgp4+** | **direct** | { **isisv6** | **ospfv3** | **ripng** } *process-id* | **static**]

undo filter-policy export [**bgp4+** | **direct** | { **isisv6** | **ospfv3** | **ripng** } *process-id* | **static**]

Default

IS-IS does not filter redistributed routes.

Views

IS-IS IPv4 unicast address family view

IS-IS IPv6 unicast address family view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-acl-number: Specifies an IPv4 ACL by its number in the range of 2000 to 3999 to filter redistributed routes.

ipv6-acl-number: Specifies an IPv6 ACL by its number in the range of 2000 to 3999 to filter redistributed routes.

prefix-list *prefix-list-name*: Specifies a prefix list by its name, a case-sensitive string of 1 to 63 characters, to filter redistributed routes by destination address.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to filter redistributed routes.

bgp: Filters redistributed BGP routes.

direct: Filters redistributed direct routes.

isis: Filters redistributed IS-IS routes.

ospf: Filters redistributed OSPF routes.

rip: Filters redistributed RIP routes.

static: Filters redistributed static routes.

bgp4+: Filters redistributed IPv6 BGP routes.

isisv6: Filters redistributed IPv6 IS-IS routes.

ospfv3: Filters redistributed OSPFv3 routes.

ripng: Filters redistributed RIPng routes.

process-id: Specifies a process by its ID in the range of 1 to 65535.

Usage guidelines

This command filters routes redistributed by the **import-route** command. Only routes that have not been filtered can be advertised.

When you specify an ACL, follow these guidelines:

- If the ACL does not exist or has no rules, IS-IS does not filter redistributed routes.
- If a rule in the ACL is applied to a VPN instance, the rule will deny all redistributed routes.

To use an advanced ACL (with a number from 3000 to 3999) in the command, configure the ACL using one of the following methods:

- To deny/permit a route with the specified destination, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* command.
- To deny/permit a route with the specified destination and mask, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* **destination** *dest-addr dest-wildcard* command.

The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the subnet mask of the route. For the configuration to take effect, specify a contiguous subnet mask.

Examples

Use basic ACL 2000 to filter redistributed routes.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule deny source 192.168.10.0 0.0.0.255
[Sysname-acl-ipv4-basic-2000] quit
[Sysname] isis 1
[Sysname-isis-1] address-family ipv4
[Sysname-isis-1-ipv4] filter-policy 2000 export
```

Configure advanced ACL 3000 to permit only route 113.0.0.0/16 to pass. Use advanced ACL 3000 to filter redistributed routes.

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule 10 permit ip source 113.0.0.0 0 destination 255.255.0.0
0
[Sysname-acl-ipv4-adv-3000] rule 100 deny ip
[Sysname-acl-ipv4-adv-3000] quit
[Sysname] isis 1
[Sysname-isis 1] address-family ipv4
[Sysname-isis-1-ipv4] filter-policy 3000 export
```

Related commands

display isis route

filter-policy import

Use **filter-policy import** to configure IS-IS to filter routes calculated using received LSPs.

Use **undo filter-policy import** to restore the default.

Syntax

In IS-IS IPv4 unicast address family view:

filter-policy { *ipv4-acl-number* | **prefix-list** *prefix-list-name* | **route-policy** *route-policy-name* } **import**

undo filter-policy import

In IS-IS IPv6 unicast address family view:

filter-policy { *ipv6-acl-number* | **prefix-list** *prefix-list-name* | **route-policy** *route-policy-name* } **import**

undo filter-policy import

Default

IS-IS does not filter routes calculated using received LSPs.

Views

IS-IS IPv4 unicast address family view

IS-IS IPv6 unicast address family view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-acl-number: Specifies an IPv4 ACL by its number in the range of 2000 to 3999 to filter routes calculated using received LSPs.

ipv6-acl-number: Specifies an IPv6 ACL by its number in the range of 2000 to 3999 to filter routes calculated using received LSPs.

prefix-list *prefix-list-name*: Specifies a prefix list by its name, a case-sensitive string of 1 to 63 characters, to filter routes calculated using received LSPs by destination address.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to filter received routes.

Usage guidelines

This command filters received routes. Only routes that have not been filtered can be added into the routing table.

When you specify an ACL, follow these guidelines:

- If the ACL does not exist or has no rules, IS-IS does not filter received routes.
- If a rule in the ACL is applied to a VPN instance, the rule will deny all received routes.

To use an advanced ACL (with a number from 3000 to 3999) in the command, configure the ACL using one of the following methods:

- To deny/permit a route with the specified destination, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* command.

- To deny/permit a route with the specified destination and mask, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* **destination** *dest-addr dest-wildcard* command.

The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the subnet mask of the route. For the configuration to take effect, specify a contiguous subnet mask.

Examples

Use basic ACL 2000 to filter routes calculated using received LSPs.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule deny source 192.168.10.0 0.0.0.255
[Sysname-acl-ipv4-basic-2000] quit
[Sysname] isis 1
[Sysname-isis-1] address-family ipv4
[Sysname-isis-1-ipv4] filter-policy 2000 import
```

Use advanced ACL 3000 to filter routes calculated using received LSPs and install only route 113.0.0.0/16 to the IP routing table.

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule 10 permit ip source 113.0.0.0 0 destination 255.255.0.0
0
[Sysname-acl-ipv4-adv-3000] rule 100 deny ip
[Sysname-acl-ipv4-adv-3000] quit
[Sysname] isis 1
[Sysname-isis 1] address-family ipv4
[Sysname-isis-1-ipv4] filter-policy 3000 import
```

Related commands

display ip routing-table

flash-flood

Use **flash-flood** to enable IS-IS LSP flash flooding.

Use **undo flash-flood** to disable IS-IS LSP flash flooding.

Syntax

flash-flood [**flood-count** *flooding-count* | **max-timer-interval** *flooding-interval* | [**level-1** | **level-2**]] *

undo flash-flood [**level-1** | **level-2**]

Default

IS-IS LSP flash flooding is disabled.

Views

IS-IS view

Predefined user roles

network-admin

context-admin

Parameters

flood-count *flooding-count*: Specifies the maximum number of LSPs to be flooded before the next SPF calculation, in the range of 1 to 15. The default is 5.

max-timer-interval *flooding-interval*: Specifies the delay of the flash flooding, in the range of 10 to 50000 milliseconds. The default is 10.

level-1: Enables flash flooding for Level-1.

level-2: Enables flash flooding for Level-2.

Usage guidelines

If no level is specified, the command enables IS-IS LSP flash flooding for both Level-1 and Level-2.

Examples

Enable fast flooding, and set the maximum LSPs to be sent to 10 and the delay time to 100 milliseconds.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] flash-flood flood-count 10 max-timer-interval 100
```

graceful-restart

Use **graceful-restart** to enable IS-IS GR.

Use **undo graceful-restart** to disable IS-IS GR.

Syntax

graceful-restart

undo graceful-restart

Default

IS-IS GR is disabled.

Views

IS-IS view

Predefined user roles

network-admin

context-admin

Usage guidelines

IS-IS GR and IS-IS NSR are mutually exclusive. Therefore, do not configure the **graceful-restart** command and the **non-stop-routing** command at the same time.

Examples

Enable GR for IS-IS process 1.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] graceful-restart
```

Related commands

graceful-restart suppress-sa

graceful-restart suppress-sa

Use **graceful-restart suppress-sa** to suppress the Suppress-Advertisement (SA) bit during restart.

Use **undo graceful-restart suppress-sa** to restore the default.

Syntax

graceful-restart suppress-sa

undo graceful-restart suppress-sa

Default

The SA bit is set during restart.

Views

IS-IS view

Predefined user roles

network-admin

context-admin

Usage guidelines

Suppressing the SA bit is mainly for avoiding black hole route. If a router starts or reboots without keeping the local forwarding table, sending packets to the router might result in severe packet loss. To avoid this, you can set the SA bit of the hello packet sent by the GR restarter to 1. Upon receiving such hello packets, the GR helpers will not advertise the GR restarter through LSP.

Examples

Suppress the SA bit during graceful restart.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] graceful-restart suppress-sa
```

Related commands

graceful-restart

graceful-restart t1

Use **graceful-restart t1** to set the T1 timer.

Use **undo graceful-restart t1** to restore the default.

Syntax

graceful-restart t1 *seconds* **count** *count*

undo graceful-restart t1

Default

The T1 timer is 3 seconds and can expire 10 times.

Views

IS-IS view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies the T1 timer in the range of 3 to 10 seconds.

count: Specifies the number of times that the T1 timer can expire, in the range of 1 to 20.

Usage guidelines

The T1 timer specifies the number of times that GR restarter can send a Restart TLV with the RR bit set. After restart, the GR restarter sends a Restart TLV with the RR bit set to its neighbor. If the restarting router receives a Restart TLV with the RA set from its neighbor before the T1 timer expires, the GR process starts. Otherwise, the GR process fails.

To avoid configuration failure, follow these guidelines when you set the GR timers:

- The product of the T1 timer and the number of times that the T1 timer can expire must be smaller than the T2 timer.
- The T2 timer must be smaller than the T3 timer.

Examples

Set the T1 timer of IS-IS process 1 to 5 seconds, and the expiration times to 5.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] graceful-restart t1 5 count 5
```

Related commands

graceful-restart

graceful-restart t2

graceful-restart t3

graceful-restart t2

Use **graceful-restart t2** to set the T2 timer.

Use **undo graceful-restart t2** to restore the default.

Syntax

graceful-restart t2 *seconds*

undo graceful-restart t2

Default

The T2 timer is 60 seconds.

Views

IS-IS view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies the T2 timer in the range of 30 to 65535 seconds.

Usage guidelines

The T2 timer specifies the LSDB synchronization interval. Each LSDB has a T2 timer. The Level-1-2 router has two T2 timers: a Level-1 timer and a Level-2 timer. If the LSDBs have not achieved synchronization before the two timers expire, the GR process fails.

To avoid configuration failure, follow these guidelines when you set the GR timers:

- The product of the T1 timer and the number of times that the T1 timer can expire must be smaller than the T2 timer.
- The T2 timer must be smaller than the T3 timer.

Examples

Set the T2 timer of IS-IS process 1 to 50 seconds.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] graceful-restart t2 50
```

Related commands

graceful-restart

graceful-restart t1

graceful-restart t3

graceful-restart t3

Use **graceful-restart t3** to set the T3 timer.

Use **undo graceful-restart t3** to restore the default.

Syntax

graceful-restart t3 *seconds*

undo graceful-restart t3

Default

The T3 timer is 300 seconds.

Views

IS-IS view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies the T3 timer in the range of 300 to 65535 seconds.

Usage guidelines

The T3 timer specifies the GR interval. The GR interval is set as the holdtime in hello PDUs. Within the interval, the neighbors maintain their adjacency with the GR restarter. If the GR process has not completed within the holdtime, the neighbors tear down the neighbor relationship and the GR process fails.

To avoid configuration failure, follow these guidelines when you set the GR timers:

- The product of the T1 timer and the number of times that the T1 timer can expire must be smaller than the T2 timer.

- The T2 timer must be smaller than the T3 timer.

Examples

Set the T3 timer of IS-IS process 1 to 500 seconds.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] graceful-restart t3 500
```

Related commands

graceful-restart

graceful-restart t1

graceful-restart t2

ignore-att

Use **ignore-att** to configure IS-IS not to calculate the default route through the ATT bit.

Use **undo ignore-att** to restore the default.

Syntax

ignore-att

undo ignore-att

Default

IS-IS calculates the default route through the ATT bit.

Views

IS-IS view

Predefined user roles

network-admin

context-admin

Examples

Configure IS-IS not to calculate the default route through the ATT bit.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] ignore-att
```

import-route

Use **import-route** to redistribute routes from another routing protocol or another IS-IS process.

Use **undo import-route** to disable route redistribution.

Syntax

In IS-IS IPv4 unicast address family view:

import-route bgp [*as-number*] [**allow-ibgp**] [**cost** *cost-value* | **cost-type** { **external** | **internal** } | [**level-1** | **level-1-2** | **level-2**] | **route-policy** *route-policy-name* | **tag** *tag*] *

import-route { **direct** | **static** } [**cost** *cost-value* | **cost-type** { **external** | **internal** } | [**level-1** | **level-1-2** | **level-2**] | **route-policy** *route-policy-name* | **tag** *tag*] *

import-route { **isis** | **ospf** | **rip** } [*process-id* | **all-processes**] [**allow-direct** | **cost** *cost-value* | **cost-type** { **external** | **internal** } | [**level-1** | **level-1-2** | **level-2**] | **route-policy** *route-policy-name* | **tag** *tag*] *

undo import-route { **bgp** | **direct** | { **isis** | **ospf** | **rip** } [*process-id* | **all-processes**] | **static** }

In IS-IS IPv6 unicast address family view:

Default

IS-IS does not redistribute routes from other routing protocols or processes.

Views

IS-IS IPv4 unicast address family view

IS-IS IPv6 unicast address family view

Predefined user roles

network-admin

context-admin

Parameters

bgp: Redistributes BGP routes.

direct: Redistributes direct routes.

isis: Redistributes IS-IS routes.

ospf: Redistributes OSPF routes.

rip: Redistributes RIP routes.

static: Redistributes static routes.

bgp4+: Redistributes IPv6 BGP routes.

isisv6: Redistributes IPv6 IS-IS routes.

ospfv3: Redistributes OSPFv3 routes.

ripng: Redistributes RIPng routes.

as-number: Specifies an AS by its number in the range of 1 to 4294967295. If you do not specify this argument for the BGP or BGP4+ protocol, the command redistributes all IPv4 or IPv6 EBGP routes. As a best practice, specify an AS to prevent the system from redistributing excessive routes.

process-id: Specifies a process by its ID in the range of 1 to 65535.

all-processes: Redistributes routes from all the processes of the specified routing protocol.

allow-ibgp: Allows redistribution of IBGP routes.

allow-direct: Redistributes the networks of the local interfaces enabled with the specified routing protocol. By default, the networks of the local interfaces are not redistributed. If you specify both the **allow-direct** keyword and the **route-policy** *route-policy-name* option, make sure the **if-match** rule defined in the routing policy does not conflict with the **allow-direct** keyword. For example, if you specify the **allow-direct** keyword, do not configure the **if-match route-type** rule for the routing policy. Otherwise, the **allow-direct** keyword does not take effect.

cost *cost-value*: Specifies a cost for redistributed routes, which is in the range of 0 to 4261412864.

- For the styles of **narrow**, **narrow-compatible**, and **compatible**, the cost is in the range of 0 to 63.
- For the styles of **wide** and **wide-compatible**, the cost is in the range of 0 to 4261412864.

cost-type { **external** | **internal** }: Specifies the cost type. The **internal** type indicates internal routes, and the **external** type indicates external routes. If **external** is specified, the cost of a redistributed route is added by 64 to make internal routes take priority over external routes. The type is **external** by default. The keywords are available only when the cost type is **narrow, narrow-compatible**, or **compatible**.

level-1: Redistributes routes into the Level-1 routing table.

level-1-2: Redistributes routes into both Level-1 and Level-2 routing tables.

level-2: Redistributes routes into the Level-2 routing table. If no level is specified, the routes are redistributed into the Level-2 routing table by default.

route-policy *route-policy-name*: Redistributes only routes matching the specified routing policy. The *route-policy-name* argument is a case-sensitive string of 1 to 63 characters.

tag *tag*: Specifies a tag value for marking redistributed routes, in the range of 1 to 4294967295.

Usage guidelines

IS-IS takes all the redistributed routes as external routes to destinations outside the IS-IS routing domain.

The effective cost varies by cost style. For the styles of **narrow**, **narrow-compatible**, and **compatible**, the cost is in the range of 0 to 63. If the cost is more than 63, 63 is used. For the style of wide or wide-compatible, the configured value is the effective value.

This **import-route** command cannot redistribute default routes. The command redistributes only active routes. To display route state information, use the **display ip routing-table protocol** command.

The **import-route bgp** or **import-route bgp4+** command redistributes only EBGP routes.

The **import-route bgp allow-ibgp** or **import-route bgp4+ allow-ibgp** command redistributes both EBGP and IBGP routes. Because this command might cause routing loops, use it with caution.

The **undo import-route** { **isis** | **ospf** | **rip** } **all-processes** or **undo import-route** { **isisv6** | **ospfv3** | **ripng** } **all-processes** command removes only the configuration made by the **import-route** { **isis** | **ospf** | **rip** } **all-processes** or **import-route** { **isisv6** | **ospfv3** | **ripng** } **all-processes** command, instead of the configuration made by the **import-route** { **isis** | **ospf** | **rip** } *process-id* or **import-route** { **isisv6** | **ospfv3** | **ripng** } *process-id* command.

Examples

Redistribute static routes into IS-IS, and set the cost for redistributed routes to 15.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] address-family ipv4
[Sysname-isis-1-ipv4] import-route static cost 15
```

Related commands

import-route limit

import-route isis level-1 into level-2

Use **import-route isis level-1 into level-2** to enable route advertisement from Level-1 to Level-2.

Use **undo import-route isis level-1 into level-2** to disable route advertisement from Level-1 to Level-2.

Syntax

import-route isis level-1 into level-2 [**filter-policy** { *ipv4-acl-number* | **prefix-list** *prefix-list-name* | **route-policy** *route-policy-name* } | **tag** *tag*] *

undo import-route isis level-1 into level-2

Default

Route advertisement from Level-1 to Level-2 is enabled.

Views

IS-IS IPv4 unicast address family view

Predefined user roles

network-admin

context-admin

Parameters

filter-policy: Specifies a filtering policy.

ipv4-acl-number: Specifies an ACL by its number in the range of 2000 to 3999 to filter routes from Level-1 to Level-2.

prefix-list *prefix-list-name*: Specifies an IPv4 prefix list by its name, a case-sensitive string of 1 to 63 characters, to filter routes from Level-1 to Level-2 by destination address.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to filter routes from Level-1 to Level-2.

tag *tag*: Specifies a tag for marking redistributed routes, in the range of 1 to 4294967295.

Usage guidelines

If a routing policy is used, the routing policy must be specified in the **import-route isis level-1 into level-2** command to filter routes from Level-1 to Level-2. Other routing policies specified for route reception and redistribution do not affect the route leaking.

If a filtering policy is configured, only Level-1 routes not filtered out can be advertised into the Level-2 area.

When you specify an IPv4 ACL, follow these guidelines:

- If the ACL does not exist or has no rules, IS-IS does not filter routes advertised from Level-1 to Level-2.
- If a rule in the ACL is applied to a VPN instance, the rule will deny all routes advertised from Level-1 to Level-2.

Examples

Enable route advertisement from Level-1 to Level-2.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] address-family ipv4
```

```
[Sysname-isis-1-ipv4] import-route isis level-1 into level-2
```

Related commands

import-route

import-route isis level-1 into level-2

import-route isis level-2 into level-1

Use **import-route isis level-2 into level-1** to enable route advertisement from Level-2 to Level-1.

Use **undo import-route isis level-2 into level-1** to restore the default.

Syntax

import-route isis level-2 into level-1 [**filter-policy** { *ipv4-acl-number* | **prefix-list** *prefix-list-name* | **route-policy** *route-policy-name* } | **tag** *tag*] *

undo import-route isis level-2 into level-1

Default

Route advertisement from Level-2 to Level-1 is disabled.

Views

IS-IS IPv4 unicast address family view

Predefined user roles

network-admin

context-admin

Parameters

filter-policy: Specifies a filtering policy.

ipv4-acl-number: Specifies an ACL by its number in the range of 2000 to 3999 to filter routes from Level-2 to Level-1.

prefix-list *prefix-list-name*: Specifies an IPv4 prefix list by its name, a case-sensitive string of 1 to 63 characters, to filter routes from Level-2 to Level-1 by destination address.

route-policy *route-policy-name*: Uses the specified routing policy to filter routes from Level-2 to Level-1. The *route-policy-name* argument is a case-sensitive string of 1 to 63 characters.

tag *tag*: Specifies a tag for marking redistributed routes, in the range of 1 to 4294967295.

Usage guidelines

If a routing policy is used, the routing policy must be specified in the **import-route isis level-2 into level-1** command to filter routes from Level-2 to Level-1. Other routing policies specified for route reception and redistribution does not affect the route leaking.

If a filtering policy is configured, only Level-2 routes not filtered out can be advertised into the Level-1 area.

When you specify an IPv4 ACL, follow these guidelines:

- If the ACL does not exist or has no rules, IS-IS does not filter routes advertised from Level-2 to Level-1.
- If a rule in the ACL is applied to a VPN instance, the rule will deny all routes advertised from Level-2 to Level-1.

Examples

Enable route advertisement from Level-2 to Level-1.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] address-family ipv4
[Sysname-isis-1-ipv4] import-route isis level-2 into level-1
```

Related commands

import-route

import-route isis level-1 into level-2

import-route isisv6 level-1 into level-2

Use **import-route isisv6 level-1 into level-2** to enable route advertisement from Level-1 to Level-2.

Use **undo import-route isisv6 level-1 into level-2** to disable route advertisement from Level-1 to Level-2.

Syntax

import-route isisv6 level-1 into level-2 [**filter-policy** { *ipv6-acl-number* | **prefix-list** *prefix-list-name* | **route-policy** *route-policy-name* } | **tag** *tag*] *

undo import-route isisv6 level-1 into level-2

Default

Route advertisement from Level-1 to Level-2 is enabled.

Views

IS-IS IPv6 unicast address family view

Predefined user roles

network-admin

context-admin

Parameters

filter-policy: Specifies a filtering policy.

ipv6-acl-number: Specifies an IPv6 ACL by its number in the range of 2000 to 3999.

prefix-list *prefix-list-name*: Specifies an IPv6 prefix list by its name, a case-sensitive string of 1 to 63 characters.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters.

tag *tag*: Specifies an administrative tag for marking redistributed routes, in the range of 1 to 4294967295.

Usage guidelines

This command enables a Level-1-2 router to redistribute Level-1 routes to Level-2 routers and Level-1-2 routers in the local area.

When you specify an IPv6 ACL, follow these guidelines:

- If the ACL does not exist or has no rules, IS-IS does not filter routes advertised from Level-1 to Level-2.

- If a rule in the ACL is applied to a VPN instance, the rule will deny all routes advertised from Level-1 to Level-2.

Examples

Enable route advertisement from Level-1 to Level-2.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] address-family ipv6
[Sysname-isis-1-ipv6] import-route isisv6 level-1 into level-2
```

import-route isisv6 level-2 into level-1

Use **import-route isisv6 level-2 into level-1** to enable IPv6 IS-IS route advertisement from Level-2 to Level-1.

Use **undo import-route isisv6 level-2 into level-1** to restore the default.

Syntax

import-route isisv6 level-2 into level-1 [**filter-policy** { *ipv6-acl-number* | **prefix-list** *prefix-list-name* | **route-policy** *route-policy-name* } | **tag** *tag*] *

undo import-route isisv6 level-2 into level-1

Default

Route advertisement from Level-2 to Level-1 is disabled.

Views

IS-IS IPv6 unicast address family view

Predefined user roles

network-admin

context-admin

Parameters

filter-policy: Specifies a filtering policy.

ipv6-acl-number: Specifies an IPv6 ACL by its number in the range of 2000 to 3999.

prefix-list *prefix-list-name*: Specifies an IPv6 prefix list by its name, a case-sensitive string of 1 to 63 characters.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters.

tag: Specifies an administrative tag for marking redistributed routes, in the range of 1 to 4294967295.

Usage guidelines

This command enables a Level-1-2 router to redistribute Level-2 routes to the Level-1 and Level-1-2 routers in the local area.

When you specify an IPv6 ACL, follow these guidelines:

- If the ACL does not exist or has no rules, IS-IS does not filter routes advertised from Level-2 to Level-1.
- If a rule in the ACL is applied to a VPN instance, the rule will deny all routes advertised from Level-2 to Level-1.

Examples

Enable IPv6 IS-IS route advertisement from Level-2 to Level-1.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] address-family ipv6
[Sysname-isis-1-ipv6] import-route isisv6 level-2 into level-1
```

import-route limit

Use **import-route limit** to configure the maximum number of redistributed Level 1/Level 2 routes.

Use **undo import-route limit** to restore the default.

Syntax

import-route limit *number*

undo import-route limit

Default

The maximum number of redistributed Level 1/Level 2 routes is 1000000.

Views

IS-IS IPv4 unicast address family view

IS-IS IPv6 unicast address family view

Predefined user roles

network-admin

context-admin

Parameters

number: Specifies the maximum number of redistributed Level 1/Level 2 routes.The value range for this argument is 1 to 1000000.

Examples

Configure IS-IS process 1 to redistribute up to 1000 Level 1/Level 2 routes.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] address-family ipv4
[Sysname-isis-1-ipv4] import-route limit 1000
```

Related commands

import-route

isis

Use **isis** to enable IS-IS and enter IS-IS view.

Use **undo isis** to disable IS-IS.

Syntax

isis [*process-id*] [**vpn-instance** *vpn-instance-name*]

undo isis [*process-id*]

Default

IS-IS is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

process-id: Specifies an IS-IS process by its ID in the range of 1 to 65535. The default is 1.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If no VPN instance is specified, the IS-IS process runs on the public network.

Examples

Enable IS-IS process 1 and set the system ID to 0000.0000.0002 and area ID to 01.0001.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] network-entity 01.0001.0000.0000.0002.00
```

Related commands

isis enable

network-entity

isis authentication send-only

Use **isis authentication send-only** to configure an IS-IS interface not to check the authentication information in the received hello packets.

Use **undo isis authentication send-only** to remove the configuration.

Syntax

isis authentication send-only [**level-1** | **level-2**]

undo isis authentication send-only [**level-1** | **level-2**]

Default

When interface authentication mode and key are configured, an IS-IS interface checks the authentication information in the received packets.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

level-1: Configures IS-IS not to check the authentication information in the received Level-1 hello packets.

level-2: Configures IS-IS not to check the authentication information in the received Level-2 hello packets.

Usage guidelines

When peer authentication mode and key are configured, an IS-IS interface adds the key in the specified mode into transmitted hello packets. It also checks the key in the received hello packets.

To prevent packet exchange failure in case of an authentication key change, configure the IS-IS interface not to check the authentication information in the received packets.

Examples

Configure GigabitEthernet 1/0/1 not to check the authentication information in the received Level-1 hello packets.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] isis authentication send-only level-1
```

Related commands

area-authentication send-only

domain-authentication send-only

isis authentication-mode

isis authentication-mode

Use **isis authentication-mode** to specify the neighbor relationship authentication mode and a key.

Use **undo isis authentication-mode** to remove the configuration.

Syntax

isis authentication-mode { { **gca** *key-id* { **hmac-sha-1** | **hmac-sha-224** | **hmac-sha-256** | **hmac-sha-384** | **hmac-sha-512** } [**nonstandard**] | **md5** | **simple** } { **cipher** | **plain** } *string* | **keychain** *keychain-name* } [**level-1** | **level-2**] [**ip** | **osi**]

undo isis authentication-mode [**level-1** | **level-2**]

Default

No neighbor relationship authentication mode or key is configured.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

gca: Specifies the GCA mode.

key-id: Uniquely identifies an SA in the range of 1 to 65535. The sender inserts the Key ID into the authentication TLV, and the receiver authenticates the packet by using the SA that is selected based on the Key ID.

hmac-sha-1: Specifies the HMAC-SHA-1 algorithm.

hmac-sha-224: Specifies the HMAC-SHA-224 algorithm.

hmac-sha-256: Specifies the HMAC-SHA-256 algorithm.

hmac-sha-384: Specifies the HMAC-SHA-384 algorithm.

hmac-sha-512: Specifies the HMAC-SHA-512 algorithm.

nonstandard: Specifies the nonstandard GCA mode.

md5: Specifies the MD5 authentication mode.

simple: Specifies the simple authentication mode.

cipher: Specifies a key in encrypted form.

plain: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. Its plaintext form is a case-sensitive string of 1 to 16 characters. Its encrypted form is a case-sensitive string of 33 to 53 characters.

keychain: Specifies the keychain authentication mode.

keychain-name: Specifies a keychain by its name, a case-sensitive string of 1 to 63 characters.

level-1: Configures the key for Level-1.

level-2: Configures the key for Level-2.

ip: Checks IP-related fields in LSPs and SNPs.

osi: Checks OSI-related fields in LSPs and SNPs.

Usage guidelines

The key in the specified mode is inserted into all outbound hello packets and is used for authenticating inbound hello packets. Only if the authentication succeeds can the neighbor relationship be formed.

IS-IS keychain authentication supports the HMAC-MD5 and HMAC-SM3 authentication algorithms. For the HMAC-SM3 authentication algorithm, only key IDs in the range of 0 to 65535 are supported. When keychain authentication is used, IS-IS receives and sends packets as follows:

- Before IS-IS sends a Hello packet, it uses the valid send key obtained from the keychain to authenticate the packet. If no valid send key exists or the valid send key does not use the HMAC-MD5 or HMAC-SM3 algorithm, the authentication fails and the packet does not contain the authentication information.
- After IS-IS receives a Hello packet, it processes the packet as follows:
  - If the authentication algorithm of the packet is HMAC-MD5, IS-IS uses a valid accept key obtained from the keychain to authenticate the packet. If no valid accept key exists or all valid accept keys fail to authenticate the packet, the authentication fails and the packet is discarded.
  - If the authentication algorithm of the packet is HMAC-SM3, IS-IS uses the key ID of the received packet to obtain the corresponding valid accept key from the keychain. Then, IS-IS uses the accept key to authenticate the packet. If IS-IS cannot find a valid accept key based on the key ID of the received packet or the packet fails the authentication, the packet is discarded.

The **level-1** and **level-2** keywords are configurable on an interface that has had IS-IS enabled with the **isis enable** command.

If you configure a key without specifying a level, the key applies to both Level-1 and Level-2.

For two routers to become neighbors, the authentication mode and key at both ends must be identical.

If neither **ip** nor **osi** is specified, the OSI-related fields in LSPs are checked.

When you specify the GCA mode, follow these guidelines:

- If you do not specify the **nonstandard** keyword, the device can communicate only with devices that use the GCA mode.
- If you specify the **nonstandard** keyword, the device can communicate only with devices that use the nonstandard GCA mode.

Examples

On GigabitEthernet 1/0/1, set the authentication mode to **simple**, and set the plaintext key to **123456**.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] isis authentication-mode simple plain 123456
```

Related commands

area-authentication-mode

domain authentication-mode

isis authentication send-only

isis bfd enable

Use **isis bfd enable** to enable BFD.

Use **undo isis bfd enable** to disable BFD.

Syntax

isis bfd enable

undo isis bfd enable

Default

IS-IS BFD is disabled.

Views

Interface view

Predefined user roles

network-admin

context-admin

Examples

Enable BFD for IS-IS on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] isis enable
[Sysname-GigabitEthernet1/0/1] isis bfd enable
```

isis bfd session-restrict-adj

Use **isis bfd session-restrict-adj** to enable IPv4 adjacency establishment and maintenance control based on BFD session state.

Use **undo isis bfd session-restrict-adj** to disable IPv4 adjacency establishment and maintenance control based on BFD session state.

Syntax

isis bfd session-restrict-adj

undo isis bfd session-restrict-adj

Default

IPv4 adjacency establishment and maintenance control based on BFD session state is disabled.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

When BFD detects a Layer 3 forwarding failure between two routers, the BFD session goes down, which causes the IPv4 IS-IS adjacency to go down. If Layer 2 forwarding is still available, the routers can exchange IS-IS packets and re-establish the adjacency, which might cause traffic loss.

To avoid the issue, execute this command on the BFD-enabled interfaces of the local and remote routers, enabling the interfaces to carry BFD-enabled TLVs in hello packets. After the BFD session goes down, the routers do not establish an adjacency if the exchanged BFD-enabled TLVs are identical.

If you configure this command for an existing adjacency, the BFD session state does not affect the adjacency relationship within the hold time. This mechanism avoids adjacency flaps during the BFD session establishment.

Before configuring this command, enable IPv4 IS-IS BFD by using the **isis bfd enable** command.

Examples

Enable IPv4 adjacency establishment and maintenance control based on BFD session state on interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] isis enable
[Sysname-GigabitEthernet1/0/1] isis bfd enable
[Sysname-GigabitEthernet1/0/1] isis bfd session-restrict-adj
```

Enable IPv4 adjacency establishment and maintenance control based on BFD session state on interface VLAN-interface 11.

```
<Sysname> system-view
[Sysname] interface vlan-interface 11
[Sysname-Vlan-interface11] isis enable
[Sysname-Vlan-interface11] isis bfd enable
[Sysname-Vlan-interface11] isis bfd session-restrict-adj
```

Related commands

isis bfd enable

isis circuit-level

Use **isis circuit-level** to set the circuit level for the interface.

Use **undo isis circuit-level** to restore the default.

Syntax

isis circuit-level [**level-1** | **level-1-2** | **level-2**]

undo isis circuit-level

Default

An interface can establish either the Level-1 or Level-2 adjacency.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

level-1: Sets the circuit level to Level-1.

level-1-2: Sets the circuit level to Level-1-2.

level-2: Sets the circuit level to Level-2.

Usage guidelines

For a Level-1 (Level-2) router, the circuit level can only be Level-1 (Level-2). For a Level-1-2 router, you must specify a circuit level for a specific interface to form only the specified level neighbor relationship.

Examples

GigabitEthernet 1/0/1 is connected to a non-backbone router in the same area. Set the circuit level of Ethernet 1/1 to Level-1 to prevent sending and receiving Level-2 Hello packets.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] isis enable
[Sysname-GigabitEthernet1/0/1] isis circuit-level level-1
```

Related commands

is-level

isis circuit-type p2p

Use **isis circuit-type p2p** to set the network type of an interface to P2P.

Use **undo isis circuit-type** to restore the default.

Syntax

isis circuit-type p2p

undo isis circuit-type

Default

The network type of an interface varies by physical media. (The network type of a VLAN interface is broadcast.)

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

Use this command only on a broadcast network with two attached routers.

Interfaces with different network types operate differently. For example, broadcast interfaces must elect a DIS and flood CSNP packets to synchronize the LSDBs. P2P interfaces do not need to elect a DIS, and use a different LSDB synchronization mechanism.

If only two routers exist on a broadcast network, set the network type of attached interfaces to P2P to avoid DIS election and CSNP flooding. This saves network bandwidth and speeds up network convergence.

Examples

Set the network type of GigabitEthernet 1/0/1 to P2P.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] isis enable
[Sysname-GigabitEthernet1/0/1] isis circuit-type p2p
```

isis cost

Use **isis cost** to set the IS-IS cost for an interface.

Use **undo isis cost** to remove the configuration.

Syntax

isis cost *cost-value* [**level-1** | **level-2**]

undo isis cost [**level-1** | **level-2**]

Default

No IS-IS cost is configured for an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

cost-value: Specifies an IS-IS cost in the range of 1 to 16777215.

level-1: Applies the cost to Level-1.

level-2: Applies the cost to Level-2.

Usage guidelines

If neither **level-1** nor **level-2** is included, the cost applies to both Level-1 and Level-2.

Examples

Set the Level-2 IS-IS cost to 5 for GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] isis cost 5 level-2
```

Related commands

auto-cost enable

bandwidth-reference

isis dis-name

Use **isis dis-name** to configure a name for a DIS to represent the pseudo node on a broadcast network.

Use **undo isis dis-name** to restore the default.

Syntax

isis dis-name *symbolic-name*

undo isis dis-name

Default

No name is configured for the DIS.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

symbolic-name: Specifies a DIS name, a case-insensitive string of 1 to 64 characters.

Usage guidelines

This command takes effect only on routers that have dynamic system ID to host name mapping enabled. This command does not take effect on Point-to-Point interfaces.

Examples

Set the DIS name to **LOCALAREA**.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] isis dis-name LOCALAREA
```

Related commands

display isis name-table

is-name

isis dis-priority

Use **isis dis-priority** to specify a DIS priority at a specified level for an interface.

Use **undo isis dis-priority** to remove the configuration.

Syntax

isis dis-priority *priority* [**level-1** | **level-2**]

undo isis dis-priority [**level-1** | **level-2**]

Default

The priority of Level-1 and Level-2 is 64.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

priority: Specifies a DIS priority in the range of 0 to 127.

level-1: Applies the DIS priority to Level-1.

level-2: Applies the DIS priority to Level-2.

Usage guidelines

On an IS-IS broadcast network, a router must be elected as the DIS at each routing level. Specify a DIS priority at a level for an interface. The greater the interface's priority is, the more likelihood it becomes the DIS. If multiple routers in the broadcast network have the same highest DIS priority, the router with the highest Subnetwork Point of Attachment (SNPA) address becomes the DIS. SNPA addresses are MAC addresses on a broadcast network.

IS-IS has no backup DIS. The router with a priority of 0 can also participate in DIS election.

If neither **level-1** nor **level-2** is specified, the DIS priority applies to both Level-1 and Level-2.

Examples

Set the Level-2 DIS priority to 127 for GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] isis dis-priority 127 level-2
```

isis enable

Use **isis enable** to enable an IS-IS process on an interface.

Use **undo isis enable** to disable IS-IS.

Syntax

isis enable [*process-id*]

undo isis enable

Default

No IS-IS process is enabled on an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

process-id: Specifies an IS-IS process by its ID in the range of 1 to 65535. The default is 1.

Examples

Enable IS-IS process 1 globally and enable it on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] network-entity 10.0001.1010.1020.1030.00
[Sysname-isis-1] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] isis enable 1
```

Related commands

isis

network-entity

isis fast-reroute lfa-backup exclude

Use **isis fast-reroute lfa-backup exclude** to disable LFA calculation on an interface.

Use **undo isis fast-reroute lfa-backup exclude** to restore the default.

Syntax

isis fast-reroute lfa-backup exclude [**level-1** | **level-2**]

undo isis fast-reroute lfa-backup exclude [**level-1** | **level-2**]

Default

LFA calculation is enabled on an interface, and the interface can be elected as a backup interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

level-1: Disables LFA calculation on the interface whose circuit level is Level-1.

level-2: Disables LFA calculation on the interface whose circuit level is Level-2.

Usage guidelines

When this command is configured, the interface does not participate in the LFA calculation, and cannot be elected as a backup interface.

If you do not specify the **level-1** or **level-2** keyword, LFA calculation is disabled on the interface regardless of its circuit level.

Examples

Disable LFA calculation on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] network-entity 10.0001.1010.1020.1030.00
[Sysname-isis-1] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] isis enable 1
```

```
[Sysname-GigabitEthernet1/0/1] isis fast-reroute lfa-backup exclude
```

Related commands

fast-reroute

isis ipv6 bfd enable

Use **isis ipv6 bfd enable** to enable BFD for IPv6 IS-IS.

Use **undo isis ipv6 bfd enable** to disable BFD for IPv6 IS-IS.

Syntax

isis ipv6 bfd enable

undo isis ipv6 bfd enable

Default

BFD for IPv6 IS-IS is disabled.

Views

Interface view

Predefined user roles

network-admin

context-admin

Examples

Enable BFD for IPv6 IS-IS on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] isis ipv6 bfd enable
```

isis ipv6 bfd session-restrict-adj

Use **isis ipv6 bfd session-restrict-adj** to enable IPv6 adjacency establishment and maintenance control based on BFD session state.

Use **undo isis ipv6 bfd session-restrict-adj** to disable IPv6 adjacency establishment and maintenance control based on BFD session state.

Syntax

isis ipv6 bfd session-restrict-adj

undo isis ipv6 bfd session-restrict-adj

Default

IPv6 adjacency establishment and maintenance control based on BFD session state is disabled.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

When BFD detects a Layer 3 forwarding failure between two routers, the BFD session goes down, which causes the IPv6 IS-IS adjacency to go down. If Layer 2 forwarding is still available, the routers can exchange IS-IS packets and re-establish the adjacency, which might cause traffic loss.

To avoid the issue, execute this command on the BFD-enabled interfaces of the local and remote routers, enabling the interfaces to carry BFD-enabled TLVs in hello packets. After the BFD session goes down, the routers do not establish an adjacency if the exchanged BFD-enabled TLVs are identical.

If you configure this command for an existing adjacency, the BFD session state does not affect the adjacency relationship within the hold time. This mechanism avoids adjacency flaps during the BFD session establishment.

Before configuring this command, enable IPv6 IS-IS BFD by using the **isis ipv6 bfd enable** command.

Examples

Enable IPv6 adjacency establishment and maintenance control based on BFD session state on interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] isis ipv6 enable
[Sysname-GigabitEthernet1/0/1] isis ipv6 bfd enable
[Sysname-GigabitEthernet1/0/1] isis ipv6 bfd session-restrict-adj
```

Enable IPv6 adjacency establishment and maintenance control based on BFD session state on interface VLAN-interface 11.

```
<Sysname> system-view
[Sysname] interface vlan-interface 11
[Sysname-Vlan-interface11] isis ipv6 enable
[Sysname-Vlan-interface11] isis ipv6 bfd enable
[Sysname-Vlan-interface11] isis ipv6 bfd session-restrict-adj
```

Related commands

isis ipv6 bfd enable

isis ipv6 cost

Use **isis ipv6 cost** to set the IPv6 IS-IS cost for an interface.

Use **undo isis ipv6 cost** to remove the configuration.

Syntax

isis ipv6 cost *cost-value* [**level-1** | **level-2**]

undo isis ipv6 cost [**level-1** | **level-2**]

Default

No IPv6 IS-IS cost is configured for an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

cost-value: Specifies an IPv6 IS-IS cost in the range of 1 to 16777215.

level-1: Applies the cost to Level-1 routes.

level-2: Applies the cost to Level-2 routes.

Usage guidelines

This command applies to interfaces that are enabled with IPv6 IS-IS.

This command takes effect only when the standard MTR mode is enabled.

Examples

Set the IPv6 IS-IS cost to 10 for GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] isis 100
[Sysname-isis-100] address-family ipv6 unicast
[Sysname-isis-100-ipv6] quit
[Sysname-isis-100] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] isis ipv6 enable 100
[Sysname-GigabitEthernet1/0/1] isis ipv6 cost 10
```

isis ipv6 enable

Use **isis ipv6 enable** to enable IPv6 for IS-IS on an interface.

Use **undo isis ipv6 enable** to disable IPv6 for IS-IS on an interface.

Syntax

isis ipv6 enable [*process-id*]

undo isis ipv6 enable

Default

IPv6 is disabled for IS-IS on an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

process-id: Specifies an IS-IS process by its ID in the range of 1 to 65535. The default is 1.

Examples

Enable IPv6 for IS-IS on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] network-entity 10.0001.1010.1020.1030.00
[Sysname-isis-1] address-family ipv6 unicast
[Sysname-isis-1-ipv6] quit
[Sysname-isis-1] quit
```

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 address 2002::1/64
[Sysname-GigabitEthernet1/0/1] isis ipv6 enable 1
```

isis ipv6 fast-reroute lfa-backup exclude

Use **isis ipv6 fast-reroute lfa-backup exclude** to disable LFA calculation on an interface.

Use **undo isis ipv6 fast-reroute lfa-backup exclude** to restore the default.

Syntax

isis ipv6 fast-reroute lfa-backup exclude [**level-1** | **level-2**]

undo isis ipv6 fast-reroute lfa-backup exclude [**level-1** | **level-2**]

Default

LFA calculation is enabled on an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

level-1: Disables LFA calculation on the interface whose circuit level is Level-1.

level-2: Disables LFA calculation on the interface whose circuit level is Level-2.

Usage guidelines

If you do not specify the **level-1** or **level-2** keyword, LFA calculation is disabled on the interface regardless of its circuit level.

Examples

Disable LFA calculation on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] network-entity 10.0001.1010.1020.1030.00
[Sysname-isis-1] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] isis ipv6 enable 1
[Sysname-GigabitEthernet1/0/1] isis ipv6 fast-reroute lfa-backup exclude
```

Related commands

fast-reroute

isis ipv6 prefix-suppression

Use **isis ipv6 prefix-suppression** to enable prefix suppression on an interface.

Use **undo isis ipv6 prefix-suppression** to disable prefix suppression on an interface.

Syntax

isis ipv6 prefix-suppression

undo isis ipv6 prefix-suppression

Default

Prefix suppression is disabled on an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

By default, IS-IS interfaces advertise their IPv6 prefixes in LSPs. Use this command to disable an interface from advertising its IPv6 prefix in LSPs. This enhances network security by preventing IP routing to the internal nodes and speeds up network convergence.

Examples

Enable prefix suppression on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] isis ipv6 prefix-suppression
```

isis ipv6 primary-path-detect bfd

Use **isis ipv6 primary-path-detect bfd** to enable BFD for IPv6 IS-IS.

Use **undo isis ipv6 primary-path-detect bfd** to disable BFD for IPv6 IS-IS.

Syntax

isis ipv6 primary-path-detect bfd { **ctrl** | **echo** }

undo isis ipv6 primary-path-detect bfd

Default

BFD is disabled for IPv6 IS-IS.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ctrl: Enables BFD control packet mode.

echo: Enables BFD echo packet mode.

Usage guidelines

This command enables IPv6 IS-IS FRR or IPv6 IS-IS PIC to use BFD to detect primary link failures.

For an interface to run the BFD session in echo packet mode correctly, make sure the interface has an IPv6 global unicast address. For more information about IPv6 global unicast addresses, see IPv6 basics configuration in *Layer 3—IP Services Configuration Guide*.

Examples

Enable BFD control packet mode for IPv6 IS-IS FRR on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] address-family ipv6
[Sysname-isis-1-ipv6] fast-reroute lfa
[Sysname-isis-1-ipv6] quit
[Sysname-isis-1] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] isis ipv6 primary-path-detect bfd ctrl
```

Enable BFD echo packet mode for IPv6 IS-IS PIC on GigabitEthernet 1/0/2.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] pic additional-path-always
[Sysname-isis-1] quit
[Sysname] bfd echo-source-ipv6 1::1
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] isis ipv6 primary-path-detect bfd echo
```

isis ipv6 tag

Use **isis ipv6 tag** to configure the tag value on an interface.

Use **undo isis ipv6 tag** to restore the default.

Syntax

isis ipv6 tag *tag*

undo isis ipv6 tag

Default

No tag value is configured on an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

tag: Specifies a tag value in the range of 1 to 4294967295.

Usage guidelines

When IS-IS advertises an IPv6 prefix with a tag value, it adds the tag to the IPv6 reachability information TLV, regardless of the link cost style.

Examples

Set the tag value on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] isis ipv6 tag 4294967295
```

isis mib-binding

Use **isis mib-binding** to bind an IS-IS process to MIB.

Use **undo isis mib-binding** to restore the default.

Syntax

isis mib-binding *process-id*

undo isis mib-binding

Default

MIB operation is bound to the IS-IS process with the smallest process ID.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

process-id: Specifies an IS-IS process by its ID in the range of 1 to 65535.

Usage guidelines

If the specified the process ID does not exist, the MIB binding configuration fails.

Deleting an IS-IS process bound to MIB operation deletes the MIB binding configuration. MIB operation is bound to the IS-IS process with the smallest process ID.

Examples

Bind IS-IS process 100 to MIB.

```
<Sysname> system-view
[Sysname] isis mib-binding 100
```

isis peer-ip-check

Use **isis peer-ip-check** to enable source address check for hello packets on an IS-IS P2P interface. An IS-IS P2P interface can establish a neighbor relationship only with a peer on the same network.

Use **undo isis peer-ip-check** to restore the default.

Syntax

isis peer-ip-check

undo isis peer-ip-check

Default

An IS-IS P2P interface can have a peer on a different network.

Views

Interface view

Predefined user roles

network-admin

context-admin

Examples

Enable source address check for hello packets on interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] isis peer-ip-check
```

Related commands

isis circuit-type p2p

isis prefix-suppression

Use **isis prefix-suppression** to enable prefix suppression on an interface.

Use **undo isis prefix-suppression** to disable prefix suppression on an interface.

Syntax

isis prefix-suppression

undo isis prefix-suppression

Default

Prefix suppression is disabled on an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

Use this command to disable an interface from advertising its prefix in LSPs. This enhances network security by preventing IP routing to the interval nodes and speeds up network convergence.

This command is also applicable to the secondary IP address of the interface.

Examples

Enable prefix suppression on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] isis prefix-suppression
```

isis primary-path-detect bfd

Use **isis primary-path-detect bfd** to enable BFD for IS-IS FRR or IS-IS PIC.

Use **undo isis primary-path-detect bfd** to disable BFD for IS-IS FRR or IS-IS PIC.

Syntax

isis primary-path-detect bfd { **ctrl** | **echo** }

undo isis primary-path-detect bfd

Default

BFD is disabled for IS-IS FRR or IS-IS PIC.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ctrl: Specifies the BFD control packet mode.

echo: Specifies the BFD echo packet mode.

Usage guidelines

This command enables IS-IS FRR or IS-IS PIC to use BFD to detect primary link failures.

Examples

Enable BFD control packet mode for IS-IS FRR on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] address-family ipv4
[Sysname-isis-1-ipv4] fast-reroute lfa
[Sysname-isis-1-ipv4] quit
[Sysname-isis-1] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] isis primary-path-detect bfd ctrl
```

Enable BFD echo packet mode for IS-IS PIC on GigabitEthernet 1/0/2.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] pic additional-path-always
[Sysname-isis-1] quit
[Sysname] bfd echo-source-ip 1.1.1.1
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] isis primary-path-detect bfd echo
```

isis silent

Use **isis silent** to disable the interface from sending and receiving IS-IS packets.

Use **undo isis silent** to restore the default.

Syntax

isis silent

undo isis silent

Default

An interface can send and receive IS-IS packets.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command is not available in loopback interface view.

Examples

Disable GigabitEthernet 1/0/1 from sending and receiving IS-IS packets.

```
<<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] isis silent
```

isis small-hello

Use **isis small-hello** to configure the interface to send small hello packets without CLVs.

Use **undo isis small-hello** to restore the default.

Syntax

isis small-hello

undo isis small-hello

Default

An interface sends standard hello packets.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command is not available in loopback interface view.

Examples

Configure GigabitEthernet 1/0/1 to send small Hello packets.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] isis small-hello
```

isis tag

Use **isis tag** to configure the tag value for an interface.

Use **undo isis tag** to restore the default.

Syntax

isis tag *tag*

undo isis tag

Default

The interface is not configured with a tag value.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

tag: Specifies the tag value in the range of 1 to 4294967295.

Usage guidelines

When IS-IS advertises an IP prefix with a tag value, it adds the tag to the IP reachability information TLV if the link cost style is **wide**, **wide-compatible**, or **compatible**.

Examples

Configure the tag value for GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] isis tag 4294967295
```

isis timer csnp

Use **isis timer csnp** to set on the DIS of a broadcast network the interval for sending CSNP packets.

Use **undo isis timer csnp** to remove the configuration.

Syntax

isis timer csnp *seconds* [**level-1** | **level-2**]

undo isis timer csnp [**level-1** | **level-2**]

Default

The default CSNP interval is 10 seconds.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies on the DIS of a broadcast network the interval for sending CSNP packets. The value range is 1 to 600 seconds.

level-1: Applies the interval to Level-1.

level-2: Applies the interval to Level-2.

Usage guidelines

On a broadcast network, this command only applies to the DIS, because the DIS sends CSNP packets periodically for LSDB synchronization.

If no level is specified, the CSNP interval applies to both Level-1 and Level-2.

Examples

Configure Level-2 CSNP packets to be sent every 15 seconds over GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] isis timer csnp 15 level-2
```

isis timer hello

Use **isis timer hello** to set the interval for sending hello packets.

Use **undo isis timer hello** to remove the configuration.

Syntax

isis timer hello *seconds* [**level-1** | **level-2**]

undo isis timer hello [**level-1** | **level-2**]

Default

The hello interval is 10 seconds.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies the interval for sending hello packets, in the range of 1 to 255 seconds.

level-1: Specifies the interval for sending Level-1 hello packets.

level-2: Specifies the interval for sending Level-2 hello packets.

Usage guidelines

If a neighbor does not receive any hello packets from the router within the advertised hold time, it considers the router down and recalculates the routes. The hold time is the hello multiplier multiplied by the hello interval.

Level-1 and Level-2 hello packets are sent independently on a broadcast network, so you need to specify an interval for each level. On a P2P link, Level-1 and Level-2 packets are both sent in P2P hello packets, and you need not specify an interval for each level.

You can configure the **level-1** and **level-2** keywords only on broadcast interfaces. Before you configure the **level-1** or **level-2** keyword, enable IS-IS on the interface.

The shorter the interval, the more system resources will be occupied.

If no level is specified, the hello interval applies to both Level-1 and Level-2.

Examples

Configure Level-2 hello packets to be sent every 20 seconds over GigabitEthernet 1/0/1.

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] isis timer hello 20 level-2
```

Related commands

isis timer holding-multiplier

isis timer holding-multiplier

Use **isis timer holding-multiplier** to set the IS-IS hello multiplier.

Use **undo isis timer holding-multiplier** to remove the configuration.

Syntax

isis timer holding-multiplier *value* [**level-1** | **level-2**]

undo isis timer holding-multiplier [**level-1** | **level-2**]

Default

The default IS-IS hello multiplier is 3.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

value: Specifies the number of hello intervals, in the range of 3 to 1000.

level-1: Applies the number to the Level-1 IS-IS neighbor.

level-2: Applies the number to the Level-2 IS-IS neighbor.

Usage guidelines

The hello multiplier is the number of hello packets a neighbor must miss before declaring the router is down.

If a neighbor does not receive any hello packets from the router within the advertised hold time, it considers the router down and recalculates the routes. The hold time is the hello multiplier multiplied by the hello interval.

Level-1 and Level-2 hello packets are sent independently on a broadcast network, so you need to specify a hello multiplier for each level. On a P2P link, Level-1 and Level-2 packets are both sent in P2P hello packets, and you need not specify Level-1 or Level-2.

You can configure the **level-1** and **level-2** keywords only on broadcast interfaces. Before you configure the **level-1** or **level-2** keyword, enable IS-IS on the interface.

If no level is specified, the hello multiplier applies to both Level-1 and Level-2.

The value of hello multiplier multiplied by hello interval cannot be more than 65535.

Examples

Set the hello multiplier to 6 for GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] isis timer holding-multiplier 6 level-2
```

Related commands

isis timer hello

isis timer lsp

Use **isis timer lsp** to set the minimum interval for sending LSPs on the interface and specify the maximum number of LSPs that can be sent per time.

Use **undo isis timer lsp** to restore the default.

Syntax

isis timer lsp *time* [**count** *count*]

undo isis timer lsp

Default

The minimum interval for sending LSPs on the interface is 33 milliseconds, and the maximum number of LSPs that can be sent at a time is 5.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

time: Specifies the minimum interval for sending link-state packets, in the range of 1 to 1000 milliseconds.

count: Specifies the maximum number of link-state packets to be sent at one time, in the range of 1 to 1000.

Usage guidelines

If a change occurs in the LSDB, IS-IS advertises the changed LSP to neighbors. You can specify the minimum interval for sending these LSPs to control the amount of LSPs on the network.

Examples

Set the interval to 500 milliseconds for sending LSPs on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] isis timer lsp 500
```

Related commands

isis timer retransmit

isis timer retransmit

Use **isis timer retransmit** to configure the interval for retransmitting LSP packets over a point-to-point link.

Use **undo isis timer retransmit** to restore the default.

Syntax

isis timer retransmit *seconds*

undo isis timer retransmit

Default

The retransmission interval on a P2P link is 5 seconds.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies the interval for retransmitting LSP packets, in the range of 1 to 300 seconds.

Usage guidelines

On a P2P link, IS-IS requires an advertised LSP be acknowledged. If no acknowledgment is received within a configurable interval, IS-IS will retransmit the LSP.

You do not need to use this command over a broadcast link where CSNPs are periodically broadcast to implement LSDB synchronization.

Examples

Set the LSP retransmission interval on a P2P link to 50 seconds for GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] isis circuit-type p2p
[Sysname-GigabitEthernet1/0/1] isis timer retransmit 50
```

Related commands

isis circuit-type p2p

isis timer lsp

is-level

Use **is-level** to specify the IS level.

Use **undo is-level** to restore the default.

Syntax

is-level { **level-1** | **level-1-2** | **level-2** }

undo is-level

Default

The IS level is **level-1-2**.

Views

IS-IS view

Predefined user roles

network-admin

context-admin

Parameters

level-1: Specifies Level-1, which means IS-IS only calculates intra-area routes and maintains the Level-1 LSDB.

level-1-2: Specifies Level-1-2, which means IS-IS calculates routes and maintains the LSDBs for both Level-1 and Level-2.

level-2: Specifies Level-2, which means IS-IS calculates routes and maintains the LSDB for Level-2 only.

Usage guidelines

If only one area exists, configure all the routers as either Level-1 or Level-2, because the routers do not need to maintain two identical LSDBs at the same time.

If the only area is an IP network, configure all the routers as Level-2 for scalability.

Examples

Set the IS level to Level-1 for IS-IS process 1.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] is-level level-1
```

is-name

Use **is-name** to specify a host name for the IS and enable dynamic system ID to hostname mapping.

Use **undo is-name** to disable dynamic system ID to hostname mapping.

Syntax

is-name *sys-name*

undo is-name

Default

Dynamic system ID to hostname mapping is disabled, and no host name is configured for the IS.

Views

IS-IS view

Predefined user roles

network-admin

context-admin

Parameters

sys-name: Specifies a host name for the local IS, a case-insensitive string of 1 to 64 characters.

Usage guidelines

To display the host name rather than the system ID of an IS by using the **display isis lsdb** command, first enable dynamic system ID to hostname mapping.

Examples

Configure a host name for the local IS.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] is-name RUTA
```

Related commands

display isis name-table

is-name map

Use **is-name map** to configure a system ID to host name mapping for a remote IS.

Use **undo is-name map** to remove the mapping.

Syntax

is-name map *sys-id map-sys-name*

undo is-name map *sys-id*

Default

No system ID to host name mapping is configured for a remote IS.

Views

IS-IS view

Predefined user roles

network-admin

context-admin

Parameters

sys-id: Specifies the system ID or pseudonode ID of a remote IS.

map-sys-name: Specifies a host name for the remote IS, a case-insensitive string of 1 to 64 characters.

Usage guidelines

Each remote IS system ID corresponds to only one name.

Examples

Map the host name **RUTB** to the system ID 0000.0000.0041 of the remote IS.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] is-name map 0000.0000.0041 RUTB
```

Related commands

display isis name-table

ispf enable

Use **ispf enable** to enable incremental SPF (ISPF).

Use **undo ispf enable** to disable ISPF.

Syntax

ispf enable

undo ispf enable

Default

IS-IS ISPF is enabled.

Views

IS-IS view

IS-IS IPv6 unicast address family view

Predefined user roles

network-admin

context-admin

Usage guidelines

When a network topology is changed, ISPF recomputes only the affected part of the SPT, instead of the entire SPT.

Examples

Enable ISPF.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] ispf enable
```

log-peer-change

Use **log-peer-change** to enable the logging of neighbor state changes.

Use **undo log-peer-change** to disable the logging.

Syntax

log-peer-change

undo log-peer-change

Default

The logging of IS-IS neighbor state changes is enabled.

Views

IS-IS view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command enables sending logs about IS-IS neighbor state changes to the information center. For IS-IS neighbor state change logs to be sent correctly, you must also configure the information center parameters on the device. For more information about information center, see the network management and monitoring configuration guide for the device.

Examples

Disable the logging of IS-IS neighbor state changes.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] undo log-peer-change
```

lsp-fragments-extend

Use **lsp-fragments–extend** to enable LSP fragment extension for a level.

Use **undo lsp-fragments–extend** to restore the default.

Syntax

lsp-fragments-extend [**level-1** | **level-1-2** | **level-2**]

undo lsp-fragments-extend

Default

LSP fragment extension is disabled.

Views

IS-IS view

Predefined user roles

network-admin

context-admin

Parameters

level-1: Applies the fragment extension to Level-1 LSPs.

level-1-2: Applies the fragment extension to both Level-1 and Level-2 LSPs.

level-2: Applies the fragment extension to Level-2 LSPs.

Usage guidelines

If no level is specified, the command enables LSP fragment extension for both Level-1 and Level-2.

Examples

Enable LSP fragment extension for Level-2.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] lsp-fragments-extend level-2
```

lsp-length originate

Use **lsp-length originate** to configure the maximum size of generated Level-1 or Level-2 LSPs.

Use **undo lsp-length originate** to remove the configuration.

Syntax

lsp-length originate *size* [**level-1** | **level-2**]

undo lsp-length originate [**level-1** | **level-2**]

Default

The maximum size of generated Level-1 and Level-2 LSPs is 1497 bytes.

Views

IS-IS view

Predefined user roles

network-admin

context-admin

Parameters

size: Specifies the maximum size of LSP packets, in the range of 512 to 16384 bytes.

level-1: Applies the size to Level-1 LSP packets.

level-2: Applies the size to Level-2 LSP packets.

Usage guidelines

If neither Level-1 nor Level-2 is specified in the command, the configured maximum size applies to the current IS-IS level.

Examples

Set the maximum size of the generated Level-2 LSPs to 1024 bytes.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] lsp-length originate 1024 level-2
```

lsp-length receive

Use **lsp-length receive** to configure the maximum size of received LSPs.

Use **undo lsp-length receive** to restore the default.

Syntax

lsp-length receive *size*

undo lsp-length receive

Default

The maximum size of received LSPs is 1497 bytes.

Views

IS-IS view

Predefined user roles

network-admin

context-admin

Parameters

size: Specifies the maximum size of received LSPs, in the range of 512 to 16384 bytes.

Examples

Configure the maximum size of received LSPs to 1024 bytes.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] lsp-length receive 1024
```

maximum load-balancing

Use **maximum load-balancing** to configure the maximum number of ECMP routes for load balancing.

Use **undo maximum load-balancing** to restore the default.

Syntax

maximum load-balancing *number*

undo maximum load-balancing

Default

The maximum number of IS-IS ECMP routes equals the maximum number of ECMP routes supported by the system.

Views

IS-IS IPv4 unicast address family view

IS-IS IPv6 unicast address family view

Predefined user roles

network-admin

context-admin

Parameters

number: Specifies the maximum number of ECMP routes. The value of 1 indicates that IS-IS does not perform load balancing.

The following compatibility matrixes show the value ranges for the maximum number of ECMP routes:

Models	Value range
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280	1 to 16
NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	1 to 32

Usage guidelines

If you use the **max-ecmp-num** command to configure the maximum number of ECMP routes supported by the system as *m*:

- The default setting for the **maximum load-balancing** command is *m*.
- The value range for the *number* argument of the **maximum load-balancing** command is 1 to *m*.

Examples

Set the maximum number of ECMP routes to 2.

```
<Sysname> system-view
[Sysname] isis 100
[Sysname-isis-100] address-family ipv4
[Sysname-isis-100-ipv4] maximum load-balancing 2
```

Related commands

max-ecmp-num

multi-topology

Use **multi-topology** to enable IPv6 IS-IS MTR.

Use **undo multiple-topology** to disable IPv6 IS-IS MTR.

Syntax

multi-topology [**compatible**]

undo multi-topology

Default

IPv6 IS-IS MTR is disabled.

Views

IS-IS IPv6 address family view

Predefined user roles

network-admin

context-admin

Parameters

compatible: Specifies the compatible mode to advertise IPv6 prefixes to both IPv4 and IPv6 topologies. If you do not specify this keyword, the command advertises IPv6 prefixes only to the IPv6 topology.

Usage guidelines

This command enables separate route calculation in IPv4 and IPv6 topologies.

This command is available when the link cost style is **wide**, **compatible**, or **wide-compatible**.

Examples

Enable IPv6 IS-IS MTR.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] address-family ipv6
[Sysname-isis-1-ipv6] multi-topology
```

Related commands

cost-style

network-entity

Use **network-entity** to configure the Network Entity Title (NET) for an IS-IS process.

Use **undo network-entity** to delete a NET.

Syntax

network-entity *net*

undo network-entity *net*

Default

No NET is configured.

Views

IS-IS view

Predefined user roles

network-admin

context-admin

Parameters

net: Specifies a NET as a dotted hexadecimal string in the X…X.XXXX....XXXX.00 format. The X…X segment represents the area address, the XXXX....XXXX segment represents the system ID, and the 00 segment is the SEL.

Usage guidelines

CAUTION:

When you execute the **network-entity** command together with the **cost-style** and **is-level** commands for the same IS-IS process, execute the **network-entity** command at last. Incorrect configuration order might cause data loss because the IS-IS process will restart.

A NET is a special NSAP address with the SEL being 0. The length of the NET is in the range of 8 to 20 bytes.

A NET comprises the following parts:

- **Area ID**—With a length of 1 to 13 bytes.
- **System ID**—A system ID uniquely identifies a host or router in the area and has a fixed 6-byte length.
- **SEL**—It has a value of 0 and a fixed 1-byte length.

For example, a NET of ab.cdef.1234.5678.9abc.00 specifies the area ID ab.cdef, the system ID 1234.5678.9abc, and the SEL 00.

Examples

Set the NET to 10.0001.1010.1020.1030.00, of which 10.0001 is the area ID and 1010.1020.1030 is the system ID.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] network-entity 10.0001.1010.1020.1030.00
```

Related commands

cost-style

isis

isis enable

is-level

non-stop-routing

Use **non-stop-routing** to enable IS-IS NSR.

Use **undo non-stop-routing** to disable IS-IS NSR.

Syntax

non-stop-routing

undo non-stop-routing

Default

IS-IS NSR is disabled.

Views

IS-IS view

Predefined user roles

network-admin

context-admin

Usage guidelines

IS-IS NSR takes effect on a per-process basis. As a best practice, enable NSR for each IS-IS process.

IS-IS NSR and IS-IS GR are mutually exclusive. Therefore, do not configure the **non-stop-routing** command and the **graceful-restart** command at the same time.

Examples

Enable NSR for IS-IS process 1.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] non-stop-routing
```

pic

Use **pic** to enable IS-IS PIC.

Use **undo pic** to disable IS-IS PIC.

Syntax

pic [**additional-path-always**]

undo pic

Default

IS-IS PIC is disabled.

Views

IS-IS view

Predefined user roles

network-admin

context-admin

Parameters

additional-path-always: Allows the indirect suboptimal route as the backup route.

Usage guidelines

Prefix Independent Convergence (PIC) enables the device to speed up network convergence by ignoring the number of prefixes. PIC applies only to indirect routes.

When both IS-IS PIC and IS-IS FRR are configured, only IS-IS FRR takes effect.

Examples

Configure IS-IS PIC to support the indirect suboptimal route as the backup route.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] pic additional-path-always
```

preference

Use **preference** to configure the preference for IS-IS.

Use **undo preference** to restore the default.

Syntax

preference { *preference* | **route-policy** *route-policy-name* } *

undo preference

Default

IS-IS preference is 15.

Views

IS-IS IPv4 unicast address family view

IS-IS IPv6 unicast address family view

Predefined user roles

network-admin

context-admin

Parameters

preference: Specifies an IS-IS protocol preference in the range of 1 to 255.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to assign a priority to the matching routes.

Usage guidelines

If multiple routing protocols find routes to the same destination, the route found by the routing protocol with the highest preference is selected as the optimal route.

If a routing policy is specified in this command, the preference set by the routing policy applies to the matching routes. Other routes use the preference set by the **preference** command.

Examples

Set the preference for IS-IS to 25.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] address-family ipv4
[Sysname-isis-1-ipv4] preference 25
```

prefix-priority

Use **prefix-priority** to assign convergence priorities to specific IS-IS routes.

Use **undo prefix-priority** to remove the configuration.

Syntax

prefix-priority { **critical** | **high** | **medium** } { **prefix-list** *prefix-list-name* | **tag** *tag-value* }

prefix-priority route-policy *route-policy-name*

undo prefix-priority { **critical** | **high** | **medium** } [**prefix-list** | **tag**]

undo prefix-priority route-policy

Default

IS-IS routes have the lowest convergence priority.

Views

IS-IS IPv4 unicast address family view

IS-IS IPv6 unicast address family view

Predefined user roles

network-admin

context-admin

Parameters

critical: Specifies the highest convergence priority.

high: Specifies the high convergence priority.

medium: Specifies the medium convergence priority.

prefix-list *prefix-list-name*: Specifies a prefix list by its name, a case-sensitive string of 1 to 63 characters.

tag *tag-value*: Specifies a tag value in the range of 1 to 4294967295.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

The higher the convergence priority, the faster the convergence speed.

IS-IS host routes have a medium convergence priority.

Examples

Assign the high convergence priority to IS-IS routes permitted by IP prefix list **standtest**.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] address-family ipv4
[Sysname-isis-1-ipv4] prefix-priority high prefix-list standtest
```

reset isis all

Use **reset isis all** to clear all IS-IS data structure information.

Syntax

reset isis all [*process-id*] [**graceful-restart**]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

process-id: Specifies an IS-IS process by its ID in the range of 1 to 65535 to clear the data structure information for an IS-IS process.

graceful-restart: Recovers the data through graceful restart after the data is cleared.

Usage guidelines

If no IS-IS process is specified, the command clears data structure information for all IS-IS processes.

Use this command when LSPs must be updated immediately.

Examples

Clear all IS-IS data structure information.

```
<Sysname> reset isis all
```

reset isis event-log lsp

Use **reset isis event-log lsp** to clear IS-IS LSP log information.

Syntax

reset isis event-log lsp { **purged** | **refreshed** } [*process-id*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

purged: Clears log information about purged LSPs.

refreshed: Clears log information about refreshed LSPs.

process-id: Specifies an IS-IS process by its ID in the range of 1 to 65535. If you do not specify this argument, the command clears LSP log information for all IS-IS processes.

Examples

Clear log information about refreshed LSPs for IS-IS process 1.

```
<Sysname> reset isis event-log lsp refreshed 1
```

Related commands

display isis event-log lsp

reset isis graceful-restart event-log

Use **reset isis graceful-restart event-log** to clear IS-IS GR log information.

Syntax

reset isis graceful-restart event-log slot *slot-number*

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its ID.

Examples

Clear IS-IS GR log information for the specified slot.

```
<Sysname> reset isis graceful-restart event-log slot 1
```

reset isis non-stop-routing event-log

Use **reset isis non-stop-routing event-log** to clear IS-IS NSR log information.

Syntax

reset isis non-stop-routing event-log slot *slot-number*

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its ID.

Examples

Clear IS-IS NSR log information for the specified slot.

```
<Sysname> reset isis non-stop-routing event-log slot 1
```

reset isis peer

Use **reset isis peer** to clear data structure information for a specified IS-IS neighbor.

Syntax

reset isis peer *system-id* [*process-id*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

system-id: Specifies an IS-IS neighbor by its system ID.

process-id: Specifies an IS-IS process by its ID in the range of 1 to 65535 to clear data structure information for the neighbor in the specified IS-IS process.

Usage guidelines

Use this command when you re-establish an IS-IS neighbor relationship.

Examples

Clear the data structure information of the neighbor with the system ID 0000.0c11.1111.

```
<Sysname> reset isis peer 0000.0c11.1111
```

reset osi statistics

Use **reset osi statistics** to clear OSI packet statistics.

Syntax

reset osi statistics

Views

User view

Predefined user roles

network-admin

context-admin

Usage guidelines

To obtain OSI packet statistics from the specified time point, first clear the existing statistics.

Examples

Clear OSI packet statistics.

```
<Sysname> reset osi statistics
```

Related commands

display osi statistics

set-att

Use **set-att** to set the ATT bit of Level-1 LSPs.

Use **undo set-att** to restore the default.

Syntax

set-att { **always** | **never** }

undo set-att

Default

The Level-1-2 router sets the ATT bit for Level-1 LSPs in accordance with the default ATT bit setting rule.

Views

IS-IS view

Predefined user roles

network-admin

context-admin

Parameters

always: Sets the ATT bit of Level-1 LSPs.

never: Keeps the ATT bit of Level-1 LSPs not set.

Usage guidelines

The ATT bit is used to identify the connection status between a Level-1 area and other areas. By default, a Level-1-2 router sets the ATT bit for Level-1 LSPs as follows:

- The Level-1-2 router sets the ATT bit in Level-1 LSPs to inform the Level-1 routers that it can reach other areas. After a Level-1 router receives a Level-1 LSP with the ATT bit set, it generates a default route destined for the Level-1-2 router.
- The Level-1-2 router does not set the ATT bit in Level-1 LSPs if it can reach only one area.

To edit the default ATT bit setting rule for a Level-1-2 router, perform the following tasks as needed:

- To enable ATT bit setting for all Level-1 LSPs, execute the **set-att always** command on the Level-1-2 router.
- To disable a Level-1 router from generating a default route upon receiving an ATT-bit-set Level-1 LSP from the Level-1-2 router, you can perform one of the following tasks:
  - Execute the **ignore-att** command on the Level-1 router.

- Execute the **set-att never** command on the Level-1-2 router.

The **set-att** command is applicable to only Level-1-2 routers.

Examples

Set the ATT bit of Level-1 LSPs.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] set-att always
```

set-overload

Use **set-overload** to set the overload bit.

Use **undo set-overload** to restore the default.

Syntax

In IS-IS view:

set-overload [**on-startup** [[**start-from-nbr** *system-id* [*timeout1* [*nbr-timeout*]]] | *timeout2* | **wait-for-bgp** [*timeout3*]]] [**allow** { **external** | **interlevel** } *]

undo set-overload

In IS-IS IPv6 unicast address family view:

set-overload [**on-startup** [[**start-from-nbr** *system-id* [*timeout1* [*nbr-timeout*]]] | *timeout2* | **wait-for-bgp4+** [*timeout3*]]] [**allow** { **external** | **interlevel** } *]

undo set-overload

Default

The overload bit is not set.

Views

IS-IS view

IS-IS IPv6 unicast address family view

Predefined user roles

network-admin

context-admin

Parameters

on-startup: Sets the overload bit upon system startup.

start-from-nbr *system-id* [*timeout1* [*nbr-timeout*]]: Starts the *nbr-timeout* timer when the router begins to establish the neighbor relationship with the neighbor after system startup. If the neighbor relationship is formed within the *nbr-timeout* interval, IS-IS keeps the overload bit set. If not, the bit is cleared. IS-IS keeps the overload bit set within the *timeout1* interval after the neighbor relationship is formed within the *nbr-timeout* interval.

- *system-id*—Specifies the neighbor.
- *timeout1*—The *timeout1* interval is in the range of 5 to 86400 seconds, and the default is 600 seconds.
- *nbr-timeout*—The timer has an interval from 5 to 86400 seconds. The default is 1200 seconds.

timeout2: Sets the overload bit within the *timeout2* interval after system startup. The interval is in the range of 5 to 86400 seconds, and the default is 600 seconds.

wait-for-bgp [*timeout3*]: Starts the *timeout3* timer for BGP convergence after system startup. If BGP is not converged within the *timeout3* interval, IS-IS clears the overload bit. The value range for the *timeout3* argument is 5 to 86400 seconds, and the default is 600 seconds.

wait-for-bgp4+ [*timeout3*]: Starts the *timeout3* timer for IPv6 BGP convergence after system startup. If IPv6 BGP is not converged within the *timeout3* interval, IPv6 IS-IS clears the overload bit. The value range for the *timeout3* argument is 5 to 86400 seconds, and the default is 600 seconds.

allow: Allows advertising address prefixes. By default, no address prefixes are allowed to be advertised when the overload bit is set.

external: Allows advertising IP address prefixes redistributed from other routing protocols with the **allow** keyword specified.

interlevel: Allows advertising IP address prefixes learned from different IS-IS levels with the **allow** keyword specified.

Usage guidelines

If the **on-startup** keyword is not specified, the command sets the overload bit immediately until the **undo set-overload** command is executed.

If the **on-startup** keyword is specified, IS-IS sets the overload bit upon system startup and keeps it set within the *timeout2* interval.

Examples

Set overload flag on the current router.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] set-overload
```

snmp context-name

Use **snmp context-name** to set the context name for the SNMP object for managing IS-IS.

Use **undo snmp context-name** to restore the default.

Syntax

snmp context-name *context-name*

undo snmp context-name

Default

No context name is set for the SNMP object for managing IS-IS.

Views

IS-IS view

Predefined user roles

network-admin

context-admin

Parameters

context-name: Specifies a context name, a case-sensitive string of 1 to 32 characters.

Examples

Configure the context name as **isis** for the SNMP object for managing IS-IS process 1.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] snmp context-name isis
```

snmp-agent trap enable isis

Use **snmp-agent trap enable isis** to enable IS-IS SNMP notifications.

Use **undo snmp-agent trap enable isis** to disable IS-IS SNMP notifications.

Syntax

snmp-agent trap enable isis [**adjacency-state-change** | **area-mismatch** | **authentication** | **authentication-type** | **buffsize-mismatch** | **id-length-mismatch** | **lsdboverload-state-change** | **lsp-corrupt** | **lsp-parse-error** | **lsp-size-exceeded** | **manual-address-drop** | **max-seq-exceeded** | **maxarea-mismatch** | **own-lsp-purge** | **protocol-support** | **rejected-adjacency** | **skip-sequence-number** | **version-skew**] *

undo snmp-agent trap enable isis [**adjacency-state-change** | **area-mismatch** | **authentication** | **authentication-type** | **buffsize-mismatch** | **id-length-mismatch** | **lsdboverload-state-change** | **lsp-corrupt** | **lsp-parse-error** | **lsp-size-exceeded** | **manual-address-drop** | **max-seq-exceeded** | **maxarea-mismatch** | **own-lsp-purge** | **protocol-support** | **rejected-adjacency** | **skip-sequence-number** | **version-skew**] *

Default

IS-IS SNMP notifications are enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

adjacency-state-change: Specifies notifications about IS-IS adjacency status changes.

area-mismatch: Specifies notifications about area address mismatches between hello packets.

authentication: Specifies notifications about authentication failures of IS-IS packets.

authentication-type: Specifies notifications about authentication type errors of IS-IS packets.

buffsize-mismatch: Specifies notifications about buffer size mismatches for LSPs.

id-length-mismatch: Specifies notifications about system ID length mismatches of IS-IS packets.

lsdboverload-state-change: Specifies notifications about LSDB overload state changes.

lsp-corrupt: Specifies notifications about LSP checksum errors in the LSDB.

lsp-parse-error: Specifies notifications about LSP packet parse failures.

lsp-size-exceeded: Specifies notifications about propagation failures caused by oversized LSPs.

manual-address-drop: Specifies notifications about manually configured area addresses that have been dropped.

max-seq-exceeded: Specifies notifications about attempts to exceed the maximum LSP sequence number.

maxarea-mismatch: Specifies notifications about maximum area address mismatches of hello packets.

own-lsp-purge: Specifies notifications about attempts to remove the local LSP.

protocol-support: Specifies notifications about supported-protocol mismatches.

rejected-adjacency: Specifies notifications about adjacency creation failures.

skip-sequence-number: Specifies notifications about LSP sequence number duplications.

version-skew: Specifies notifications about hello packet version mismatches.

Usage guidelines

If you do not specify a notification, this command enables all IS-IS SNMP notifications.

If no IS-IS process exists, the configuration is not allowed.

This function does not take effect if all configured IS-IS processes are deleted.

Examples

Disable IS-IS SNMP notifications.

```
<Sysname> system-view
[Sysname] undo snmp-agent trap enable isis
```

summary

Use **summary** to configure a summary route.

Use **undo summary** to remove a summary route.

Syntax

In IS-IS IPv4 unicast address family view:

summary *ip-address* { *mask-length* | *mask* } [**avoid-feedback** | **generate_null0_route** | [**level-1** | **level-1-2** | **level-2**] | **tag** *tag*] *

undo summary *ip-address* { *mask-length* | *mask* } [**level-1** | **level-1-2** | **level-2**]

In IS-IS IPv6 unicast address family view:

summary *ipv6-prefix prefix-length* [**avoid-feedback** | **generate_null0_route** | [**level-1** | **level-1-2** | **level-2**] | **tag** *tag*] *

undo summary *ipv6-prefix prefix-length* [**level-1** | **level-1-2** | **level-2**]

Default

No summary route is configured.

Views

IS-IS IPv4 unicast address family view

IS-IS IPv6 unicast address family view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the destination IP address of the summary route.

mask-length: Specifies the mask length of the summary route, in the range of 0 to 32.

mask: Specifies the mask of the destination IP address, in dotted decimal notation.

ipv6-prefix: Specifies an IPv6 prefix for the summary route.

prefix-length: Specifies the length of the IPv6 prefix, in the range of 0 to 128.

avoid-feedback: Avoids learning summary routes by route calculation.

generate_null0_route: Generates the Null 0 route to avoid routing loops.

level-1: Summarizes only the routes redistributed to Level-1.

level-1-2: Summarizes the routes redistributed to both Level-1 and Level-2.

level-2: Summarizes only the routes redistributed to Level-2.

tag *tag*: Specifies a management tag in the range of 1 to 4294967295.

Usage guidelines

To reduce the size of the routing table, as well as the size of LSP and LSDB generated by the router, summarize multiple contiguous networks into a single network. You can summarize native IS-IS routes and redistributed routes. After summarization, the cost of the summary route is the smallest cost of the summarized routes.

If no level is specified, only **level-2** routes are summarized.

The router summarizes only routes generated from local LSPs.

Examples

Configure a summary route of 202.0.0.0/8.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] address-family ipv4
[Sysname-isis-1-ipv4] summary 202.0.0.0 255.0.0.0
```

timer lsp-generation

Use **timer lsp-generation** to set the LSP generation interval.

Use **undo timer lsp-generation** to remove the configuration.

Syntax

timer lsp-generation *maximum-interval* [*minimum-interval* [*incremental-interval*]] [**level-1** | **level-2**]

undo timer lsp-generation [**level-1** | **level-2**]

Default

The maximum interval is 5 seconds, the minimum interval is 50 milliseconds, and the incremental interval is 200 milliseconds.

Views

IS-IS view

Predefined user roles

network-admin

context-admin

Parameters

maximum-interval: Specifies the maximum interval in the range of 1 to 120 seconds.

minimum-interval: Specifies the minimum interval in the range of 10 to 60000 milliseconds.

incremental-interval: Specifies the incremental interval in the range of 10 to 60000 milliseconds.

level-1: Applies the intervals to Level-1.

level-2: Applies the intervals to Level-2. If no level is specified, the specified intervals apply to both Level-1 and Level-2.

Usage guidelines

By adjusting the LSP generation interval, you can prevent bandwidth and router resources from being over consumed due to frequent topology changes.

If you specify only the *maximum-interval* argument, the LSP generation interval is *maximum-interval*.

If you do not specify the *incremental-interval* argument, the LSP generation interval is in the range of *minimum-interval* to *maximum-interval*.

If you specify the *incremental-interval* argument, the LSP generation interval is as follows:

- When network changes are not frequent, the *minimum-interval* is adopted.
- If network changes are frequent, the LSP generation interval increases by *incremental-interval* × 2^{n-2} (n is the number of calculation times) each time a generation occurs until the *maximum-interval* is reached.

The minimum interval and the incremental interval cannot be greater than the maximum interval.

Examples

Set the maximum interval, minimum interval, and incremental interval to 10 seconds, 100 milliseconds, and 200 milliseconds, respectively.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1]timer lsp-generation 10 100 200
```

timer lsp-max-age

Use **timer lsp-max-age** to set the LSP maximum age in the LSDB.

Use **undo timer lsp-max-age** to restore the default.

Syntax

timer lsp-max-age *seconds*

undo timer lsp-max-age

Default

The LSP maximum age is 1200 seconds.

Views

IS-IS view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies the LSP maximum aging time in the range of 1 to 65535 seconds.

Usage guidelines

Each LSP has an age that decreases in the LSDB. Any LSP with an age of 0 is deleted from the LSDB. You can adjust the age value based on the scale of a network.

Examples

Set the maximum LSP age to 1500 seconds.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] timer lsp-max-age 1500
```

Related commands

timer lsp-refresh

timer lsp-refresh

Use **timer lsp-refresh** to set the LSP refresh interval.

Use **undo timer lsp-refresh** to restore the default.

Syntax

timer lsp-refresh *second*s

undo timer lsp-refresh

Default

The default LSP refresh interval is 900 seconds.

Views

IS-IS view

Predefined user roles

network-admin

context-admin

Parameters

*second*s: Specifies the LSP refresh interval in the range of 1 to 65534 seconds.

Usage guidelines

Each router refreshes its LSPs at a configurable interval and sends them to other routers to achieve the following purposes:

- Prevent valid routes from aging out.
- Synchronize LSPs in the network.

A smaller refresh interval speeds up network convergence but consumes more bandwidth.

To refresh LSPs before they are aged out, the interval configured by the **timer lsp-refresh** command must be smaller than that configured by the **timer lsp-max-age** command.

Examples

Set the LSP refresh interval to 1500 seconds.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] timer lsp-refresh 1500
```

Related commands

timer lsp-max-age

timer spf

Use **timer spf** to set the SPF calculation interval.

Use **undo timer spf** to restore the default.

Syntax

timer spf *maximum-interval* [*minimum-interval* [*incremental-interval*]]

undo timer spf

Default

The maximum interval is 5 seconds, the minimum interval is 50 milliseconds, and the incremental interval is 200 milliseconds.

Views

IS-IS view

IS-IS IPv6 unicast address family view

Predefined user roles

network-admin

context-admin

Parameters

maximum-interval: Specifies the maximum SPF calculation interval in the range of 1 to 120 seconds.

minimum-interval: Specifies the minimum SPF calculation interval in the range of 10 to 60000 milliseconds.

incremental-interval: Specifies the incremental SPF calculation interval in the range of 10 to 60000 milliseconds.

Usage guidelines

Based on the LSDB, an IS-IS router uses the SPF algorithm to calculate a shortest path tree with itself being the root, and uses the shortest path tree to determine the next hop to a destination network. By adjusting the SPF calculation interval, you can prevent bandwidth and router resources from being overused due to frequent topology changes.

When network changes are not frequent, the *minimum-interval is* adopted. If network changes become frequent, the SPF calculation interval increases by the *incremental-interval* each time a generation happens until the *maximum-interval* is reached.

The minimum interval and the incremental interval cannot be greater than the maximum interval.

Examples

Set the maximum interval to 10 seconds, the minimum interval to 100 milliseconds, and the incremental interval to 300 milliseconds, respectively.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] timer spf 10 100 300
```

virtual-system

Use **virtual-system** to configure a virtual system ID for the IS-IS process.

Use **undo virtual-system** to remove a virtual system ID.

Syntax

virtual-system *virtual-system-id*

undo virtual-system *virtual-system-id*

Default

No virtual system ID is configured.

Views

IS-IS view

Predefined user roles

network-admin

context-admin

Parameters

virtual-system-id: Specifies a virtual system ID for the IS-IS process.

Examples

Set a virtual system ID of 2222.2222.2222 for IS-IS process 1.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] virtual-system 2222.2222.2222
```

Contents

BGP commands

address-family ipv4

Use **address-family ipv4** to create the BGP IPv4 unicast address family, BGP-VPN IPv4 unicast address family, BGP IPv4 RT filter address family, or BGP IPv4 multicast address family, and enter its view, or enter the view of the existing address family.

Use **undo address-family ipv4** to remove the BGP IPv4 unicast address family, BGP-VPN IPv4 unicast address family, BGP IPv4 RT filter address family, or BGP IPv4 multicast address family, and all its configurations.

Syntax

In BGP instance view:

address-family ipv4 [**multicast** | **rtfilter** | **unicast**]

undo address-family ipv4 [**multicast** | **rtfilter** | **unicast**]

In BGP-VPN instance view:

address-family ipv4 [**unicast**]

undo address-family ipv4 [**unicast**]

Default

No BGP IPv4 unicast address family, BGP-VPN IPv4 unicast address family, BGP IPv4 RT filter address family, or BGP IPv4 multicast address family exists.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

context-admin

Parameters

multicast: Specifies the IPv4 multicast address family.

rtfilter: Specifies the BGP IPv4 RT filter address family.

The following compatibility matrixes show the support of hardware platforms for the **rtfilter** keyword:

Models	Parameter compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	No

unicast: Specifies the IPv4 unicast address family. If this command is executed with the **unicast** keyword in BGP instance view, it places you into BGP IPv4 unicast address family view. If this command is executed with the **unicast** keyword in BGP-VPN instance view, it places you into BGP-VPN IPv4 unicast address family view.

Usage guidelines

Configurations made in BGP IPv4 unicast address family view apply only to the BGP IPv4 unicast routes and peers of the public network.

Configurations made in BGP-VPN IPv4 unicast address family view apply only to the BGP IPv4 unicast routes and peers of the specified VPN instance.

Configurations made in BGP IPv4 multicast address family view apply only to the BGP IPv4 multicast routes and peers.

Configurations made in BGP IPv4 RT filter address family view apply only to the BGP IPv4 RT filter routes and peers.

By default, the **unicast** keyword is used if you do not specify the **multicast**, **rtfilter**, or **unicast** keyword.

Examples

In BGP instance view, create the BGP IPv4 unicast address family and enter its view.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4]
```

address-family ipv6

Use **address-family ipv6** to create the BGP IPv6 unicast address family, BGP-VPN IPv6 unicast address family, or BGP IPv6 multicast address family, and enter its view, or enter the view of the existing address family.

Use **undo address-family ipv6** to remove the BGP IPv6 unicast address family, BGP-VPN IPv6 unicast address family, or BGP IPv6 multicast address family, and all its configurations.

Syntax

In BGP instance view:

address-family ipv6 [**multicast** | **unicast**]

undo address-family ipv6 [**multicast** | **unicast**]

In BGP-VPN instance view:

address-family ipv6 [**unicast**]

undo address-family ipv6 [**unicast**]

Default

No BGP IPv6 unicast address family, BGP-VPN IPv6 unicast address family, or BGP IPv6 multicast address family exists.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

context-admin

Parameters

unicast: Specifies the IPv6 unicast address family. If this command is executed with the **unicast** keyword in BGP instance view, it places you into BGP IPv6 unicast address family view. If this command is executed with the **unicast** keyword in BGP-VPN instance view, it places you into BGP-VPN IPv6 unicast address family view.

multicast: Specifies the IPv6 multicast address family.

Usage guidelines

Configurations made in BGP IPv6 unicast address family view apply only to the BGP IPv6 unicast routes and peers of the public network.

Configurations made in BGP-VPN IPv6 unicast address family view apply only to the BGP IPv6 unicast routes and peers of the specified VPN instance.

Configurations made in BGP IPv6 multicast address family view apply only to the BGP IPv6 multicast routes and peers.

By default, the **unicast** keyword is used if neither the **multicast** keyword nor the **unicast** keyword is specified.

Examples

In BGP instance view, create the BGP IPv6 unicast address family and enter its view.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv6 unicast
[Sysname-bgp-default-ipv6]
```

address-family link-state

Use **address-family link-state** to create the BGP LS address family and enter its view, or enter the view of the existing address family.

Use **undo address-family link-state** to remove the BGP LS address family and all its configurations.

Syntax

address-family link-state

undo address-family link-state

Default

No BGP LS address family exists.

Views

BGP instance view

Predefined user roles

network-admin

context-admin

Usage guidelines

Configurations made in BGP LS address family view apply only to the BGP LS routes and peers of the public network.

Examples

In BGP instance view, create the BGP LS address family and enter its view.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family link-state
[Sysname-bgp-default-ls]
```

advertise-rib-active

Use **advertise-rib-active** to enable BGP to advertise only the optimal BGP routes in the IP routing table.

Use **undo advertise-rib-active** to restore the default.

Syntax

advertise-rib-active

undo advertise-rib-active

Default

In BGP instance view, BGP advertises optimal routes in the BGP routing table, regardless of whether they are optimal in the IP routing table. In other views, the setting is the same as that in BGP instance view.

Views

BGP instance view

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

Predefined user roles

network-admin

context-admin

Usage guidelines

The **advertise-rib-active** command does not apply to the following routes:

- Routes redistributed by the **import-route** command.
- Routes advertised by the **network** command.
- Default routes redistributed by the **default-route imported** command.
- VPNv4 routes.
- VPNv6 routes.

This command takes effect only on the routes generated after you execute this command. To apply this command to existing routes, use the **reset bgp** command to reset BGP sessions.

The setting in BGP unicast address family view applies when it is different from that in BGP instance view.

Examples

In BGP instance view, enable BGP to advertise optimal routes in the IP routing table.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] advertise-rib-active
```

aggregate

Use **aggregate** to create a summary route in the BGP routing table.

Use **undo aggregate** to remove a summary route.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view/BGP IPv4 multicast address family view:

aggregate *ipv4-address* { *mask-length* | *mask* } [**as-set** | **attribute-policy** *route-policy-name* | **detail-suppressed** | **origin-policy** *route-policy-name* | **suppress-policy** *route-policy-name*] *

undo aggregate ipv4-address { *mask-length* | *mask* }

Default

No summary routes are configured.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

BGP IPv4 multicast address family view

BGP IPv6 multicast address family view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-address: Specifies an IPv4 summary address.

mask-length: Specifies a mask length for the IPv4 summary address, in the range of 0 to 32.

mask: Specifies a mask for the IPv4 summary address, in dotted decimal notation.

ipv6-address: Specifies an IPv6 summary address.

prefix-length: Specifies a prefix length for the IPv6 summary address, in the range of 0 to 128.

as-set: Enables the AS_PATH attribute of the summary route to contain the AS path information for all summarized routes. The AS_PATH attribute is of the AS_SET type that requires no sequence when arranging AS numbers. If you do not specify this keyword, the AS_PATH attribute of the summary route contains only the AS number of the local router.

attribute-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to set attributes for the summary route.

detail-suppressed: Advertises only the summary route. If you do not specify this keyword, BGP advertises both the summary route and the more specific routes.

origin-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to select routes to be summarized.

suppress-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to filter more specific routes to be advertised. Routes

permitted by the specified routing policy are not advertised. Routes denied by the specified routing policy are advertised.

Usage guidelines

This command creates a summary route. If the BGP routing table has routes whose destination addresses fall within the specified network, the summary route is added to the BGP routing table. For example, if two routes 10.1.1.0/24 and 10.1.2.0/24 exist in the BGP routing table, configuring the **aggregate 10.1.0.0 16** command creates a summary route 10.1.0.0/16.

If the summarized routes have different ORIGIN attributes, the summary route selects the ORIGIN attribute in the sequence of INCOMPLETE, EGP, and IGP. For example, if the ORIGIN attributes of the summarized routes include INCOMPLETE and IGP, the ORIGIN attribute of the summary route is INCOMPLETE.

The COMMUNITY attribute of the summary route includes all the COMMUNITY (or extended community) attribute values if the routes have the following details:

- Summarized routes have different COMMUNITY (or extended community) attribute values.
- The summary route does not have the ATOMIC_AGGREGATE attribute.

Table 1 Functions of the keywords

Keywords	Function
as-set	Enables the summary route to carry the AS path information for all summarized routes. This feature can help avoid routing loops. However, if many routes are summarized and are changed frequently, do not specify this keyword. This configuration causes the summary route to flap with the more specific routes.
attribute-policy	Sets attributes except the AS-PATH attribute for the summary route. The **peer route-policy** command can achieve the same purpose.
detail-suppressed	Disables advertisement of all more specific routes. To disable advertisement of some more specific routes, use the **suppress-policy** keyword or the **peer filter-policy** command.
origin-policy	Summarizes only routes matching a routing policy. If the destination address of a route falls within the summary network but does not match the routing policy, the route is not summarized. It is not controlled by the **detail-suppressed** and **suppress-policy** keywords. There is no need to configure **apply** clauses for the routing policy applied by the **origin-policy** keyword because they do not take effect.
suppress-policy	Disables advertisement of some more specific routes filtered by a routing policy. The routing policy uses **if-match** clauses to filter routes. There is no need to configure **apply** clauses for the routing policy applied by the **suppress-policy** keyword because they do not take effect.

Examples

In BGP IPv4 unicast address family view, create summary route 1.1.0.0/16 in the BGP routing table.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4] aggregate 1.1.0.0 255.255.0.0
```

Related commands

display bgp routing-table ipv4 multicast

display bgp routing-table ipv4 unicast

display bgp routing-table ipv6 multicast

display bgp routing-table ipv6 unicast

summary automatic

balance

Use **balance** to enable load balancing and set the maximum number of BGP ECMP routes for load balancing.

Use **undo balance** to disable load balancing.

Syntax

balance [**ebgp** | **eibgp** | **ibgp**] *number*

undo balance [**ebgp** | **eibgp** | **ibgp**]

Default

Load balancing is disabled.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

BGP IPv4 multicast address family view

BGP IPv6 multicast address family view

Predefined user roles

network-admin

context-admin

Parameters

ebgp: Enables load balancing over EBGP routes.

eibgp: Enables load balancing between EBGP and IBGP routes.

ibgp: Enables load balancing over IBGP routes.

number: Specifies the maximum number of BGP ECMP routes for load balancing. When it is set to 1, load balancing is disabled.

Usage guidelines

Unlike IGP, BGP has no explicit metric for making load balancing decision. Instead, it implements load balancing by modifying route selection rules.

If multiple BGP routes destined for a network meet the following conditions, the device selects the specified number of routes for load balancing:

BGP uses the following load balancing criteria to determine load balanced routes:

- The routes have the same ORIGIN, LOCAL_PREF, and MED attributes.
- The routes meet the following requirements on the AS_PATH attribute:
  - If the **balance as-path-neglect** command is configured, the routes can have different AS_PATH attributes.

- If only the **balance as-path-relax** command is configured, the routes can have different AS_PATH attributes, but the length of the AS_PATH attributes must be the same.
- If neither the **balance as-path-neglect** nor the **balance as-path-relax** command is configured, the routes must have the same AS_PATH attribute.

- The next hops of the routes meet the following requirements on IGP metrics:
  - If the **bestroute igp-metric-ignore** command is not configured, the next hops of the routes must have the same IGP metric value.
  - If the **bestroute igp-metric-ignore** command is configured, the next hops of the routes can have different IGP metric values.

If you do not specify the **ibgp**, **eibgp**, or **ebgp** keyword, this command enables load balancing over EBGP routes and IBGP routes, but not between EBGP and IBGP routes.

You can remove the configuration of the **balance eibgp** *number* command only by executing the **undo balance eibgp** command.

After you execute the **balance eibgp** *number* command, the **balance** [**ebgp** | **ibgp**] *number* command cannot be executed; and vice versa.

Examples

In BGP IPv4 unicast address family view, enable load balancing and set the maximum number of BGP ECMP routes used for load balancing to 2.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4] balance 2
```

Related commands

balance as-path-neglect

balance as-path-relax

bestroute igp-metric-ignore

balance as-path-neglect

Use **balance as-path-neglect** to enable BGP to ignore the AS_PATH attribute when it implements load balancing.

Use **undo balance as-path-neglect** to restore the default.

Syntax

balance as-path-neglect

undo balance as-path-neglect

Default

BGP does not ignore the AS_PATH attribute when it implements load balancing.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

BGP IPv4 multicast address family view

BGP IPv6 multicast address family view

Predefined user roles

network-admin

context-admin

Usage guidelines

For BGP to implement load balancing over routes with different AS_PATH attributes, you must use this command together with the **balance** command.

After this command is executed, BGP ignores the AS_PATH attributes in the routes for load balancing and changes the attributes of the advertised routes to those of the optimal route. The operations might cause routing loops. In addition, this command might also affect the NetStream data. Therefore, use this command with caution.

Examples

In BGP IPv4 unicast address family view, enable BGP to ignore the AS_PATH attribute when it implements load balancing.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4] balance as-path-neglect
```

Related commands

balance

balance as-path-relax

Use **balance as-path-relax** to enable load balancing for routes that have different AS_PATH attributes of the same length.

Use **undo balance as-path-relax** to restore the default.

Syntax

balance as-path-relax

undo balance as-path-relax

Default

BGP cannot perform load balancing for routes that have different AS_PATH attributes of the same length.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

BGP IPv4 multicast address family view

BGP IPv6 multicast address family view

Predefined user roles

network-admin

context-admin

Usage guidelines

For BGP to perform load balancing for routes with different AS_PATH attributes of the same length, you must use this command together with the **balance** command.

If you configure both the **balance as-path-relax** and **balance as-path-neglect** commands, the **balance as-path-neglect** command takes effect.

After this command is executed, BGP ignores the AS_PATH attributes in the routes for load balancing and changes the attributes of the advertised routes to those of the optimal route. This might cause routing loops and affect NetStream statistics. Therefore, use this command with caution.

Examples

In BGP IPv4 unicast address family view, enable load balancing for routes that have different AS_PATH attributes of the same length.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4] balance as-path-relax
```

bestroute as-path-neglect

Use **bestroute as-path-neglect** to configure BGP to ignore the AS_PATH attribute during optimal route selection.

Use **undo bestroute as-path-neglect** to restore the default.

Syntax

In BGP instance view:

bestroute as-path-neglect [**all-instance**]

undo bestroute as-path-neglect [**all-instance**]

In BGP-VPN instance view:

bestroute as-path-neglect

undo bestroute as-path-neglect

Default

BGP considers the AS_PATH attribute during optimal route selection.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

context-admin

Parameters

all-instance: Enables this feature for the BGP instance and all BGP-VPN instances created in the BGP instance. If you do not specify this keyword, the command enables this feature for only the BGP instance or BGP-VPN instance.

Usage guidelines

If you do not specify the **all-instance** keyword for this command, this feature is enabled for only the current BGP instance or BGP-VPN instance.

After executing the **bestroute as-path-neglect all-instance** command in BGP instance view, you enable this feature for the BGP instance and all BGP-VPN instances in the BGP instance. Executing the **undo bestroute as-path-neglect** command in BGP instance view or BGP-VPN instance view cannot disable this feature. To enable this feature for a specific instance, execute the **bestroute as-path-neglect** command in BGP instance or BGP-VPN instance view and make sure the **bestroute as-path-neglect all-instance** command is not executed in BGP instance view.

Examples

In BGP instance view, ignore AS_PATH during optimal route selection.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] bestroute as-path-neglect
```

bestroute compare-med

Use **bestroute compare-med** to enable MED comparison for routes on a per-AS basis.

Use **undo bestroute compare-med** to restore the default.

Syntax

In BGP instance view:

bestroute compare-med [**all-instance**]

undo bestroute compare-med [**all-instance**]

In BGP-VPN instance view:

bestroute compare-med

undo bestroute compare-med

Default

MED comparison for routes on a per-AS basis is disabled.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

context-admin

Parameters

all-instance: Enables this feature for the BGP instance and all BGP-VPN instances created in the BGP instance. If you do not specify this keyword, the command enables this feature for only the BGP instance or BGP-VPN instance.

Usage guidelines

By default, BGP does not compare MEDs for routes from the same AS. When a router learns a new route, it compares the route with the optimal route in its BGP routing table. If the new route is more optimal, it becomes the optimal route in the BGP routing table. In this way, route learning sequence might affect optimal route selection.

To solve the selection problem, the router puts routes received from the same AS into a group when the **bestroute compare-med** command is configured. The router then selects the route with the lowest MED from the same group, and compares routes from different groups.

If you do not specify the **all-instance** keyword for this command, this feature is enabled for only the current BGP instance or BGP-VPN instance.

After executing the **bestroute compare-med all-instance** command in BGP instance view, you enable this feature for the BGP instance and all BGP-VPN instances in the BGP instance. Executing the **undo bestroute compare-med** command in BGP instance view or BGP-VPN instance view cannot disable this feature. To enable this feature for a specific instance, execute the **bestroute compare-med** command in BGP instance or BGP-VPN instance view and make sure the **bestroute compare-med all-instance** command is not executed in BGP instance view.

Examples

In BGP instance view, enable MED comparison for routes on a per-AS basis.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] bestroute compare-med
```

bestroute igp-metric-ignore

Use **bestroute igp-metric-ignore** to configure BGP to ignore IGP metrics during optimal route selection.

Use **undo bestroute igp-metric-ignore** to restore the default.

Syntax

In BGP instance view:

bestroute igp-metric-ignore [**all-instance**]

undo bestroute igp-metric-ignore [**all-instance**]

In BGP-VPN instance view:

bestroute igp-metric-ignore

undo bestroute igp-metric-ignore

Default

BGP considers IGP metrics during optimal route selection, and selects the route with the smallest IGP metric as the optimal route.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

context-admin

Parameters

all-instance: Enables this feature for the BGP instance and all BGP-VPN instances created in the BGP instance. If you do not specify this keyword, the command enables this feature for only the BGP instance or BGP-VPN instance.

Usage guidelines

After executing the **bestroute igp-metric-ignore all-instance** command in BGP instance view, you enable this feature for the BGP instance and all BGP-VPN instances in the BGP instance. Executing the **undo bestroute igp-metric-ignore** command in BGP instance view or BGP-VPN instance view cannot disable this feature. To enable this feature for a specific instance, execute the **bestroute igp-metric-ignore** command in BGP instance or BGP-VPN instance view and make sure the **bestroute igp-metric-ignore all-instance** command is not executed in BGP instance view.

Examples

In BGP instance view, ignore IGP metrics during optimal route selection.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] bestroute igp-metric-ignore
```

bestroute med-confederation

Use **bestroute med-confederation** to enable MED comparison for routes received from confederation peers.

Use **undo bestroute med-confederation** to restore the default.

Syntax

In BGP instance view:

bestroute med-confederation [**all-instance**]

undo bestroute med-confederation [**all-instance**]

In BGP-VPN instance view:

bestroute med-confederation

undo bestroute med-confederation

Default

MED comparison is disabled for routes received from confederation peers.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

context-admin

Parameters

all-instance: Enables this feature for the BGP instance and all BGP-VPN instances created in the BGP instance. If you do not specify this keyword, the command enables this feature for only the BGP instance or BGP-VPN instance.

Usage guidelines

This command enables BGP to compare the MEDs of routes received from confederation peers. However, if a route from a confederation peer has an AS number that does not belong to the confederation, BGP does not compare the route with other routes. For example, a confederation has three AS numbers 65006, 65007, and 65009. BGP receives three routes from different confederation peers. The AS_PATH attributes of these routes are 65006 65009, 65007 65009, and 65008 65009,

and the MED values of them are 2, 3, and 1. Because the third route's AS_PATH attribute contains AS number 65008, which does not belong to the confederation, BGP does not compare it with other routes. As a result, the first route becomes the optimal route.

After executing the **bestroute med-confederation all-instance** command in BGP instance view, you enable this feature for the BGP instance and all BGP-VPN instances in the BGP instance. Executing the **undo bestroute med-confederation** command in BGP instance view or BGP-VPN instance view cannot disable this feature. To enable this feature for a specific instance, execute the **bestroute med-confederation** command in BGP instance or BGP-VPN instance view and make sure the **bestroute med-confederation all-instance** command is not executed in BGP instance view.

Examples

In BGP instance view, enable MED comparison for routes received from confederation peers.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] bestroute med-confederation
```

bestroute router-id-ignore

Use **bestroute router-id-ignore** to enable BGP to ignore router IDs during optimal route selection.

Use **undo bestroute router-id-ignore** to restore the default.

Syntax

In BGP instance view:

bestroute router-id-ignore [**all-instance**]

undo bestroute router-id-ignore [**all-instance**]

In BGP-VPN instance view:

bestroute router-id-ignore

undo bestroute router-id-ignore

Default

BGP compares router IDs during optimal route selection. If multiple routes to the same destination are available, BGP selects the route with the smallest router ID as the optimal route.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

context-admin

Parameters

all-instance: Enables this feature for the BGP instance and all BGP-VPN instances created in the BGP instance. If you do not specify this keyword, the command enables this feature for only the BGP instance or BGP-VPN instance.

Usage guidelines

After executing the **bestroute router-id-ignore all-instance** command in BGP instance view, you enable this feature for the BGP instance and all BGP-VPN instances in the BGP

instance. Executing the **undo bestroute router-id-ignore** command in BGP instance view or BGP-VPN instance view cannot disable this feature. To enable this feature for a specific instance, execute the **bestroute router-id-ignore** command in BGP instance or BGP-VPN instance view and make sure the **bestroute router-id-ignore all-instance** command is not executed in BGP instance view.

Examples

In BGP instance view, enable BGP to ignore router IDs during optimal route selection.

```
<Sysname> system-view
[Sysname] bgp 1
[Sysname-bgp-default] bestroute router-id-ignore
```

bgp

Use **bgp** to enable a BGP instance and enter its view.

Use **undo bgp** to disable a BGP instance.

Syntax

bgp *as-number* [**instance** *instance-name*]

undo bgp [*as-number* [**instance** *instance-name*]]

Default

BGP is disabled and no BGP instances exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

as-number: Specifies a local AS by its number in the range of 1 to 4294967295.

instance *instance-name*: Specifies a BGP instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command enables the BGP instance **default**.

Usage guidelines

A router supports 4-byte AS number.

A BGP router can run multiple BGP processes. Each BGP process corresponds to a BGP instance. BGP maintains an independent routing table for each BGP instance.

You can create multiple public address families for a BGP instance. However, each public address family (except for public VPNv4 address family and public VPNv6 address family) can belong to only one BGP instance.

You can create multiple VPN instances for a BGP instance, and each VPN instance can have multiple address families. A VPN instance can belong to only one BGP instance.

You cannot specify the same peer for the same address family of different BGP instances.

The IPv4 and IPv6 multicast address families must belong to the same BGP instance.

Different BGP instances can have the same AS number but cannot have the same name.

Examples

Enable BGP instance **default**, set the local AS number to 100, and enter BGP instance view.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default]
```

bgp update-delay on-startup

Use **bgp update-delay on-startup** to configure BGP to delay sending route updates when it restores after a device reboot.

Use **undo bgp update-delay on-startup** to restore the default.

Syntax

bgp update-delay on-startup *seconds*

undo bgp update-delay on-startup

Default

BGP sends route updates immediately to BGP peers in established state when it restores after a device reboot.

Views

BGP instance view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies the delay time in the range of 0 to 3600 seconds. The value of 0 indicates that BGP sends route updates immediately when it restores after a device reboot.

Usage guidelines

With this feature enabled, BGP delays sending route updates when it restores after a device reboot. During the delay time, BGP learns all routes from other neighbors, and then selects the optimal route. After the delay time elapses, BGP will advertise the optimal route. Using this feature can reduce traffic loss caused by device reboot.

Examples

In BGP instance view, configure BGP to delay sending route updates when it restores after a device reboot, and set the delay time to 100 seconds.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] bgp update-delay on-startup 100
```

Related commands

bgp update-delay on-startup prefix-list

bgp update-delay on-startup prefix-list

Use **bgp update-delay on-startup prefix-list** to configure BGP to immediately send route updates for routes that match a prefix list.

Use **undo bgp update-delay on-startup prefix-list** to restore the default.

Syntax

bgp update-delay on-startup prefix-list *ipv4-prefix-list-name*

undo bgp update-delay on-startup prefix-list

Default

No prefix list is specified to filter routes.

Views

BGP instance view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-prefix-list-name: Specifies an IPv4 prefix list by its name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

After the **bgp update-delay on-startup** command is configured, BGP delays sending updates for all routes when it restores after a device reboot. For BGP to immediately send updates for the specified routes, execute the **bgp update-delay on-startup prefix-list** command.

This command is available only to IPv4 prefix lists.

Examples

In BGP instance view, configure BGP to send updates 100 seconds after it restores from a device reboot, and immediately send updates for routes that match prefix list **aaa**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] bgp update-delay on-startup 100
[Sysname-bgp-default] bgp update-delay on-startup prefix-list aaa
```

Related commands

bgp update-delay on-startup

compare-different-as-med

Use **compare-different-as-med** to enable MED comparison for routes from peers in different ASs.

Use **undo compare-different-as-med** to restore the default.

Syntax

compare-different-as-med

undo compare-different-as-med

Default

MED comparison is disabled for routes from peers in different ASs.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

context-admin

Usage guidelines

If multiple routes to a destination exist, the route with the smallest MED is selected.

Generally BGP only compares MEDs of routes received from the same AS. You can use the **compare-different-as-med** command to force BGP to compare MED values of routes received from different ASs.

Do not use this command unless relevant ASs adopt the same IGP protocol and routing selection method.

Examples

In BGP instance view, enable MED comparison for routes from peers in different ASs.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] compare-different-as-med
```

confederation id

Use **confederation id** to configure a confederation ID.

Use **undo confederation id** to restore the default.

Syntax

confederation id *as-number*

undo confederation id

Default

No confederation ID is configured.

Views

BGP instance view

Predefined user roles

network-admin

context-admin

Parameters

as-number: Specifies an AS number that identifies the confederation, in the range of 1 to 4294967295.

Usage guidelines

You can split an AS into several sub-ASs, and each sub-AS remains fully meshed. These sub-ASs form a confederation. Key path attributes of a route, such as the Next_HOP, MED, and LOCAL_PREF, are not discarded when crossing each sub-AS. The sub-ASs still look like one AS from the perspective of other ASs. The AS number is the confederation ID.

Confederation can ensure the integrity of the former AS, and solve the problem of too many IBGP connections in the AS.

Configure the same confederation ID for all routers in one confederation.

For a non-confederation BGP router that establishes a BGP connection to a router in a confederation, the confederation ID is the AS number of the router.

Examples

Confederation 9 consists of four sub-ASs numbered 38, 39, 40 and 41. Peer 10.1.1.1 is a member of sub-AS 38. Peer 200.1.1.1 is a member outside of confederation 9, which belongs to AS 98. Confederation 9 looks like one AS (with AS number 9) from the perspective of peer 200.1.1.1. This example uses a router in sub-AS 41.

```
<Sysname> system-view
[Sysname] bgp 41
[Sysname-bgp-default] confederation id 9
[Sysname-bgp-default] confederation peer-as 38 39 40
[Sysname-bgp-default] group Confed38 external
[Sysname-bgp-default] peer Confed38 as-number 38
[Sysname-bgp-default] peer 10.1.1.1 group Confed38
[Sysname-bgp-default] group Remote98 external
[Sysname-bgp-default] peer Remote98 as-number 98
[Sysname-bgp-default] peer 200.1.1.1 group Remote98
```

Related commands

confederation nonstandard

confederation peer-as

confederation nonstandard

Use **confederation nonstandard** to enable compatibility with routers not compliant with RFC 3065 in the confederation.

Use **undo confederation nonstandard** to restore the default.

Syntax

confederation nonstandard

undo confederation nonstandard

Default

The device is compatible with only routers compliant with RFC 3065 in the confederation.

Views

BGP instance view

Predefined user roles

network-admin

context-admin

Usage guidelines

Configure this command on all routers compliant with RFC 3065 to interact with those routers not compliant with RFC 3065 in the confederation.

Examples

Confederation 100 consists of two sub-ASs, 64000 and 65000, and contains routers not compliant with RFC 3065. Enable compatibility with routers not compliant with RFC 3065 in the confederation.

```
<Sysname> system-view
[Sysname] bgp 64000
[Sysname-bgp-default] confederation id 100
[Sysname-bgp-default] confederation peer-as 65000
```

```
[Sysname-bgp-default] confederation nonstandard
```

Related commands

confederation id

confederation peer-as

confederation peer-as

Use **confederation peer-as** to specify confederation peer sub-ASs.

Use **undo confederation peer-as** to remove the specified confederation peer sub-ASs.

Syntax

confederation peer-as *as-number-list*

undo confederation peer-as [*as-number-list*]

Default

No confederation peer sub-ASs are specified.

Views

BGP instance view

Predefined user roles

network-admin

context-admin

Parameters

as-number-list: Specifies a sub-AS number list. A maximum of 32 sub-ASs can be configured in one command line. The expression is *as-number-list = as-number* &<1-32>. The *as-number* argument specifies a sub-AS number in the range of 1 to 4294967295, and &<1-32> indicates that a maximum of 32 numbers can be specified.

Usage guidelines

Before this configuration, use the **confederation id** command to specify the confederation ID for the sub-ASs.

If the **undo confederation peer-as** command is executed without the *as-number-list* argument, all confederation peer sub-ASs are removed.

Examples

In BGP instance view, specify confederation peer sub-ASs 2000 and 2001.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] confederation id 10
[Sysname-bgp-default] confederation peer-as 2000 2001
```

Related commands

confederation id

confederation nonstandard

dampening

Use **dampening** to enable BGP route dampening.

Use **undo dampening** to restore the default.

Syntax

dampening [*half-life-reachable half-life-unreachable reuse suppress ceiling* | **route-policy** *route-policy-name*] *

undo dampening

Default

Route dampening is disabled.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

BGP IPv4 multicast address family view

BGP IPv6 multicast address family view

Predefined user roles

network-admin

context-admin

Parameters

half-life-reachable: Specifies a half-life for active routes, in the range of 1 to 45 minutes. By default, the value is 15 minutes.

half-life-unreachable: Specifies a half-life for suppressed routes, in the range of 1 to 45 minutes. By default, the value is 15 minutes.

reuse: Specifies a reuse threshold value for suppressed routes, in the range of 1 to 20000. A suppressed route whose penalty value decreases under the value is reused. By default, the reuse value is 750. The reuse threshold must be less than the suppression threshold.

suppress: Specifies a suppression threshold in the range of 1 to 20000. The route with a penalty value greater than the threshold is suppressed. The default value is 2000.

ceiling: Specifies a ceiling penalty value in the range of 1001 to 20000. The value must be greater than the *suppress* value. By default, the value is 16000.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

This command dampens only EBGP routes.

If an EBGP peer goes down after you configure this command, routes coming from the peer are dampened but not deleted.

Examples

In BGP IPv4 unicast address family view, configure BGP route dampening. Set the half-life for both active and suppressed routes to 10 minutes, the reuse threshold to 1000, the suppression threshold to 2000, and the ceiling penalty to 10000.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4] dampening 10 10 1000 2000 10000
```

Related commands

display bgp dampening parameter

default local-preference

Use **default local-preference** to configure a default local preference.

Use **undo default local-preference** to restore the default.

Syntax

default local-preference *value*

undo default local-preference

Default

The default local preference is 100.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

BGP IPv4 multicast address family view

BGP IPv6 multicast address family view

Predefined user roles

network-admin

context-admin

Parameters

value: Specifies a default local preference in the range of 0 to 4294967295. A larger value represents a higher preference.

Usage guidelines

You can also use the **apply local-preference** command in a routing policy to configure the local preference for BGP routes. If no routing policy is configured, all BGP routes use the local preference set by the **default local-preference** command. If a routing policy is configured, BGP routes matching the routing policy use the local preference set by the **apply local-preference** command. Other BGP routes use the local preference set by the **default local-preference** command.

Examples

In BGP IPv4 unicast address family view, set the default local preference to 180.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4] default local-preference 180
```

Related commands

apply local-preference

route-policy

default med

Use **default med** to specify a default MED value.

Use **undo default med** to restore the default.

Syntax

default med *med-value*

undo default med

Default

The default MED value is 0.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

BGP IPv4 multicast address family view

BGP IPv6 multicast address family view

Predefined user roles

network-admin

context-admin

Parameters

med-value: Specifies the default MED value in the range of 0 to 4294967295.

Usage guidelines

BGP selects a MED value in the following order:

1. MED set by the **apply cost** command.
2. MED set by the **med** keyword in the **import-route** command.
3. MED set by the **default med** command.
4. Original MED of a BGP route, or MED changed from the metric of a redistributed IGP route.

Examples

In BGP IPv4 unicast address family view, set the default MED to 25.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4] default med 25
```

Related commands

apply cost

import-route

route-policy

default-route imported

Use **default-route imported** to enable default route redistribution into the BGP routing table.

Use **undo default-route imported** to restore the default.

Syntax

default-route imported

undo default-route imported

Default

Default route redistribution into the BGP routing table is disabled.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

BGP IPv4 multicast address family view

BGP IPv6 multicast address family view

Predefined user roles

network-admin

context-admin

Usage guidelines

By default, BGP does not redistribute default IGP routes. To redistribute default IGP routes into the BGP routing table, you must use the **default-route imported** command together with the **import-route** command.

Examples

In BGP IPv4 unicast address family view, enable default route redistribution from OSPF process 1 into the BGP routing table.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4] default-route imported
[Sysname-bgp-default-ipv4] import-route ospf 1
```

Related commands

import-route

display bgp dampening parameter

Use **display bgp dampening parameter** to display BGP route dampening parameters.

Syntax

display bgp [**instance** *instance-name*] **dampening parameter** { **ipv4** | **ipv6** } [**multicast** | [**unicast**] [**vpn-instance** *vpn-instance-name*]]

display bgp [**instance** *instance-name*] **dampening parameter vpnv4**

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

instance *instance-name*: Specifies a BGP instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command displays BGP route dampening parameters for the default BGP instance.

ipv4: Displays BGP IPv4 route dampening parameters.

ipv6: Displays BGP IPv6 route dampening parameters.

multicast: Displays BGP multicast route dampening parameters.

unicast: Displays BGP unicast route dampening parameters.

vpnv4: Displays IBGP VPNv4 route dampening parameters.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays BGP route dampening parameters for the public network.

Usage guidelines

By default, the **unicast** keyword is used if neither the **multicast** keyword nor the **unicast** keyword is specified.

Examples

Display BGP IPv4 unicast route dampening parameters.

```
<Sysname> display bgp dampening parameter ipv4
Maximum suppression time (in seconds)              : 3973
Ceiling value                                      : 16000
Reuse value                                        : 750
Half-life time for reachable routes (in seconds)   : 900
Half-life time for unreachable routes (in seconds) : 900
Suppression threshold                              : 2000
```

Table 2 Command output

Field	Description
Maximum suppression time	Maximum time (in seconds) for the penalty value to decrease from the ceiling value to the reuse value.
Ceiling value	Penalty ceiling value.
Reuse value	Reuse threshold.

Related commands

dampening

display bgp group

Use **display bgp group** to display BGP peer group information.

Syntax

display bgp [**instance** *instance-name*] **group ipv4** [**mdt** | **multicast** | **mvpn** | **rtfilter** | [**flowspec** | **unicast**] [**vpn-instance** *vpn-instance-name*]] [**group-name** *group-name*]

display bgp [**instance** *instance-name*] **group ipv6** [**multicast** | [**unicast**] [**vpn-instance** *vpn-instance-name*]] [**group-name** *group-name*]

display bgp [**instance** *instance-name*] **group link-state** [**group-name** *group-name*]

display bgp [**instance** *instance-name*] **group vpnv4** [**vpn-instance** *vpn-instance-name*] [**group-name** *group-name*]

display bgp [**instance** *instance-name*] **group vpnv6** [**group-name** *group-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

instance *instance-name*: Specifies a BGP instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command displays BGP peer group information for the default BGP instance.

ipv4: Displays IPv4 BGP peer group information.

ipv6: Displays IPv6 BGP peer group information.

link-state: Displays BGP LS peer group information.

mdt: Displays BGP MDT peer group information.

multicast: Displays BGP multicast peer group information.

mvpn: Displays BGP IPv4 MVPN peer group information.

rtfilter: Displays BGP IPv4 RT filter peer group information.

The following compatibility matrixes show the support of hardware platforms for the **rtfilter** keyword:

Models	Parameter compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	No

flowspec: Displays BGP flowspec peer group information.

unicast: Displays BGP unicast peer group information.

vpnv4: Displays BGP VPNv4 peer group information.

vpnv6: Displays BGP VPNv6 peer group information.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays BGP peer group information for the public network.

group-name *group-name*: Specifies a BGP peer group by its name, a case-sensitive string of 1 to 47 characters. If you do not specify a group, this command displays brief information about all BGP peer groups for the specified address family.

Usage guidelines

By default, the **unicast** keyword is used if the **unicast**, **mdt**, **mvpn**, **rtfilter**, and **multicast** keywords are not specified.

Examples

Display brief information about all BGP IPv4 unicast peer groups.

```
<Sysname> display bgp group ipv4
 BGP peer group: group1
 Remote AS: 600
 Type: external
 Members:
  1.1.1.10

 BGP peer group: group2
 Remote AS number: not specified
 Type: external
 Members:
  2.2.2.2
```

Display detailed information about BGP IPv4 unicast peer group **group1**.

```
<Sysname> display bgp group ipv4 group-name group1
 BGP peer group: group1
 Remote AS: 600
 Type: external
 Maximum number of prefixes allowed: 4294967295
 Threshold: 75%
 Configured hold time: 180 seconds
 Keepalive time: 60 seconds
 Minimum time between advertisements: 30 seconds
 Peer preferred value: 0
 Site-of-Origin: Not specified

 Routing policy configured:
 No routing policy is configured

 Members:
* - Dynamically created peer
  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

  1.1.1.10               600        0        0    0       0 00:00:55 Established
```

Display detailed information about BGP IPv6 unicast peer group **group2**.

```
<Sysname> display bgp group ipv6 group-name group2
 BGP peer group: group2
 Remote AS: 600
 Type: external
 Maximum number of prefixes allowed: 4294967295
 Threshold: 75%
 Configured hold time: 180 seconds
 Keepalive time: 60 seconds
 Minimum time between advertisements: 30 seconds
 Peer preferred value: 0
 IPsec profile name: profile001
 Site-of-Origin: Not specified

 Routing policy configured:
 No routing policy is configured

 Members:
* - Dynamically created peer
  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

  2::2                   600        0        0    0       0 00:00:45 Established
  3::3                   600        0        0    0       0 00:00:40 Established
```

Table 3 Command output

Field	Description
BGP peer group	Name of the BGP peer group.
Remote AS	AS number of the peer group.
Type	Type of the peer groups: • **external**—EBGP peer group. • **internal**—IBGP peer group.
Maximum number of prefixes allowed	Maximum number of routes allowed to learn from the peer.
Threshold	Percentage of received routes from the peer to maximum routes allowed to learn from the peer. If the percentage is reached, the system generates a log message.
Configured hold time	Configured hold interval in seconds.
Keepalive time	Keepalive interval in seconds.
Minimum time between advertisements	Minimum route advertisement interval in seconds.
Peer preferred value	Preferred value specified for routes from the peer.
Site-of-Origin	SoO for the peer group.
Routing policy configured	Routing policy configured for the peer group. If you do not specify a routing policy, this field displays **No routing policy is configured**.
Members	Information about peers included in the peer group.

Field	Description
* - Dynamically created peer	An asterisk (*) before a peer address indicates that the peer is a dynamic peer.
Peer	IPv4 or IPv6 address of the peer.
AS	AS number of the peer.
MsgRcvd	Number of messages received.
MsgSent	Number of messages sent.
OutQ	Number of messages to be sent.
PrefRcv	For the IPv4, IPv6, VPNv4, and VPNv6 address families, this field displays the number of prefixes received from the peer. For the IPv4 flowspec address family, this field displays the number of IPv4 flowspec messages received from the peer. For the IPv4 MDT address family, this field displays the number of MDT messages received from the peer.
Up/Down	Lasting time of the current BGP session state.
State	Current state of the BGP session between the local router and the peer.
IPsec profile name	IPsec profile applied to the IPv6 BGP peer group.

display bgp instance-info

Use **display bgp instance-info** to display information about all BGP instances.

Syntax

display bgp instance-info

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display information about all BGP instances.

```
<Sysname> display bgp instance-info
Total BGP instances: 3
  BGP instance name               AS
  BGP1                            100
  BGP2                            200
  BGP3                            300
```

Table 4 Command output

Field	Description
Total BGP instances	Number of BGP instances.
BGP instance name	BGP instance name.
AS	AS number of the BGP instance.

display bgp link-state

Use **display bgp link-state** to display BGP LS information.

Syntax

display bgp [**instance** *instance-name*] **link-state** [*ls-prefix* [**advertise-info**] | **peer** { *ipv4-address* | *ipv6-address* } { **advertised** | **received** } [**statistics**] | **statistics**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

instance *instance-name*: Specifies a BGP instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command displays BGP LS information for the default BGP instance.

ls-prefix: Specifies an LS prefix. If you do not specify this argument, the command displays all BGP LS information.

advertise-info: Displays advertisement information for the specified LS prefix.

ipv4-address: Specifies a peer by its IPv4 address.

ipv6-address: Specifies a peer by its IPv6 address.

advertised: Displays advertised LS information.

received: Displays received LS information.

statistics: Displays statistics about LS messages.

Usage guidelines

If you do not specify any parameters, this command displays brief BGP LS information.

Examples

Display brief BGP LS information for the public network.

```
<Sysname> display bgp link-state

 Total number of routes: 2

 BGP local router ID is 1.1.2.1
```

```
 Status codes: * - valid, > - best, d – dampened, h – history
               s – suppressed, S – stale, i - internal, e - external
       Origin: i - IGP, e - EGP, ? - incomplete
 Prefix codes: E link, V node, T IP reachable route, u/U unknown,
               I Identifier, N local node, R remote node, L link, P prefix,
               L1/L2 ISIS level-1/level-2, O OSPF, D direct, S static,
               a area-ID, , l link-ID, t topology-ID, s ISO-ID,
               c confed-ID/ASN, b bgp-identifier, r router-ID,
               i if-address, n peer-address, o OSPF Route-type, p IP-prefix
               d designated router address
* >e Network : [V][O][I0x0][N[c20][b1.1.1.2][a0.0.0.0][r1.1.1.2]]/376
     NextHop : 1.1.1.2                                  LocPrf    :
     PrefVal : 0                                        OutLabel  : NULL
     MED     :
     Path/Ogn: 20i

* >e Network :
[T][O][I0x0][N[c20][b1.1.1.2][a0.0.0.0][r1.1.1.2]][P[o0x1][p1.1.1.0/24]]/480
     NextHop : 1.1.1.2                                  LocPrf    :
     PrefVal : 0                                        OutLabel  : NULL
     MED     :
     Path/Ogn: 20i
```

Table 5 Command output

Field	Description
Status codes	Status codes: • *** – valid**—Valid route. • **> – best**—Optimal route. • **d - dampened**—Dampened route. • **h – history**—History route. • **s – suppressed**—Suppressed route. • **S – stale**—Stale route. • **i – internal**—Internal route. • **e – external**—External route.

Field	Description
Prefix codes	Route status codes: • E – link. • V – node. • T – IP reachable route. • u/U – unknown. • I – Identifier. • N – local node. • R – remote node. • L – link. • P – prefix. • L1/L2 – ISIS level-1/level-2. • O – OSPF. • D – direct. • S – static. • a – area-ID. • l – link-ID. • t – topology-ID. • s – ISO-ID. • c – confed-ID/ASN. • b – bgp-identifier. • r – router-ID. • i – if-address. • n – peer-address. • o – OSPF Route-type. • p – IP-prefix. • d – designated router address.
Origin	Origin of the route: • **i – IGP**—Originated in the AS. The origin of routes advertised with the **network** command is IGP. • **e – EGP**—Learned through EGP. • **? – incomplete**—Unknown origin. The origin of routes redistributed from IGP protocols is INCOMPLETE.
Network	NLRI for the LS.
NextHop	Next hop IP address.
LocPrf	Local preference.
OutLabel	Outgoing label of the route.
MED	MED attribute.
Path/Ogn	AS_PATH and ORIGIN attributes of the route: • **AS_PATH**—Records the ASs the route has passed, which avoids routing loops. • **ORIGIN**—Identifies the origin of the route.

Display detailed BGP LS information with the specified LS prefix.

```
<Sysname> display bgp link-state [V][O][I0x0][N[c20][b1.1.1.2][a0.0.0.0][r1.1.1.2]]/376

 BGP local router ID: 1.1.1.2
 Local AS number: 20
```

```
Paths:   1 available, 1 best

BGP LS information of [V][O][I0x0][N[c20][b1.1.1.2][a0.0.0.0][r1.1.1.2]]/376:
Imported route.
Original nexthop: 0.0.0.0
OutLabel        : NULL
LS              : Node flag bits: 30[EA]
AS-path         : (null)
Origin          : igp
Attribute value : pref-val 32768
State           : valid, local, best
IP precedence   : N/A
QoS local ID    : N/A
Traffic index   : N/A
```

Table 6 Command output

Field	Description
Paths	Number of routes: • **available**—Number of valid routes. • **best**—Number of optimal routes.
BGP LS information of	NLRI prefix.
Original nexthop	Original next hop of the route. If the route was obtained from a BGP update message, the original next hop is the next hop IP address in the message.

LS	LS attribute:
	• **Node flag bits**—Node attribute in hexadecimal format:
	  ○ **10[A]**—OSPF ABR bit.
	  ○ **30[E]**—OSPF External bit.
	• **Metric**—Link or prefix cost.

AS-path	AS_PATH attribute of the route, which records the ASs the route has passed and avoids routing loops.
Attribute value	BGP path attributes: • **MED**—MED value. • **localpref**—Local preference value. • **pref-val**—Preferred value. • **pre**—Route preference.
State	Current state of the route: • valid. • internal. • external. • local. • synchronize. • best.
IP precedence	IP precedence in the range of 0 to 7. **N/A** indicates that the route does not support this field.
QoS local ID	QoS local ID in the range of 1 to 4095. **N/A** indicates that the route does not support this field.

Field	Description
Traffic index	Traffic index in the range of 1 to 64. **N/A** indicates that the route does not support this field.

Display advertisement information for the specified LS prefix.

```
<Sysname> display bgp link-state
[E][B][I0x0][N[r1.1.1.2]][c65008][R[r44.33.22.11]][c65009]][L[i2.1.1.3][n1.1.1.3]]/53
6 advertise-info
 BGP local router ID: 1.1.1.2
 Local AS number: 65008

 Paths:  1 best

 BGP LS information of
[E][B][I0x0][N[r1.1.1.2]][c65008][R[r44.33.22.11]][c65009]][L[i2.1.1.3][n1.1.1.3]]/53
6
(TxPathID:0):

 Advertised to peers (1 in total):
10.1.1.2
 LS attribute :
   Peer node segment identifier : Flag c0[VL], Metric 0, Label 23001
```

Table 7 Command output

Field	Description
Paths	Number of routes: • **available**—Number of valid routes. • **best**—Number of optimal routes.
BGP LS information of	NLRI prefix.
Advertised to peers (1 in total)	Peers to which the information has been advertised, and the total number of such peers.

Peer node segment identifier	Peer node SID:
	• **Flag c0[VL]**:
	  ◦ **V**—Value flag. If set, the SID carries a label value.
	  ◦ **L**—Local flag. If set, the SID has local significance.
	• **Metric**—Link cost.
	• **Label**—Label value.

TxPathID	Add-path ID of advertised routes.

display bgp network

Use **display bgp network** to display information about routes advertised by the **network** command and shortcut routes configured by the **network short-cut** command.

Syntax

display bgp [**instance** *instance-name*] **network** { **ipv4** | **ipv6** } [**multicast** | [**unicast**] [**vpn-instance** *vpn-instance-name*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

instance *instance-name*: Specifies a BGP instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command displays information for the default BGP instance.

ipv4: Displays IPv4 address family information.

ipv6: Displays IPv6 address family information.

multicast: Displays BGP multicast address family information.

unicast: Displays BGP unicast address family information.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays routing information for the public network.

Usage guidelines

By default, the **unicast** keyword is used if neither the **multicast** keyword nor the **unicast** keyword is specified.

Examples

Display information about routes advertised by the **network** command and shortcut routes configured by the **network short-cut** command in the IPv4 unicast address family.

```
<Sysname> display bgp network ipv4

  BGP local router ID: 192.168.1.135
  Local AS number: 100

  Network           Mask            Route-policy        Short-cut
  20.1.1.0          255.255.255.0                       No
  40.1.1.0          255.255.255.0   abc                 No
  30.1.1.0          255.255.255.0                       Yes
```

Display information about routes advertised by the **network** command and shortcut routes configured by the **network short-cut** command in the IPv6 unicast address family.

```
<Sysname> display bgp network ipv6

  BGP local router ID: 192.168.1.135
  Local AS number: 100

  Network           PrefixLen       Route-policy        Short-cut
  1::               24                                  No
  2::               24                                  No
  3::               64              policy1             No
```

```
2::                24                                      Yes
```

Table 8 Command output

Field	Description
Network	Destination network address of the routes advertised by the **network** command and the shortcut routes.
Mask	Mask of the destination network address.
PrefixLen	Prefix length of the destination network address.
Route-policy	Routing policy that is applied to the route.
Short-cut	Whether the route is a shortcut route: • Yes. • No.

display bgp non-stop-routing status

Use **display bgp non-stop-routing status** to display BGP NSR status information.

Syntax

display bgp [**instance** *instance-name*] **non-stop-routing status**

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

instance *instance-name*: Specifies a BGP instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command displays BGP NSR status information for the default BGP instance.

Examples

Display BGP NSR status information.

```
<Sysname> display bgp non-stop-routing status

BGP NSR status: Not ready
 Location of preferred standby process: -
 TCP NSR status: Not ready
```

Table 9 Command output

Field	Description
BGP NSR status	BGP NSR status: • **Ready**—BGP NSR has backed up BGP neighbor and routing information from the active process to the standby process. In this state, BGP NSR can ensure continuous routing when an active/standby process switchover occurs. • **Not ready**—BGP NSR is backing up BGP neighbor and routing information from the active process to the standby process. If an active/standby process switchover occurs in this state, traffic is interrupted and the BGP session will be re-established. • **Not configured**—BGP NSR is disabled.
Location of preferred standby process	ID of the IRF member device where the preferred standby process resides. This field displays **-** if no standby processes exist.
TCP NSR status	TCP NSR status: • **Ready**—TCP NSR has backed up TCP connection information from the active process to the standby process. • **Not ready**—TCP NSR is backing up TCP connection information from the active process to the standby process.

display bgp paths

Use **`display bgp paths`** to display BGP path attribute information.

Syntax

`display bgp` [**`instance`** *`instance-name`*] **`paths`** [*`as-regular-expression`*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

`instance` *`instance-name`*: Specifies a BGP instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command displays BGP path attribute information for the default BGP instance.

`as-regular-expression`: Displays information about BGP path attributes whose AS_PATH attribute matches the specified regular expression. The *`as-regular-expression`* argument is a string of 1 to 256 characters. If you do not specify this argument, the command displays information about all BGP path attributes.

Examples

Display information about all BGP path attributes.

```
<Sysname> display bgp paths

  RefCount    MED         Path/Origin
  3           0           ?
  2           0           100i
  3           0           100i
  1           0           ?
  1           0           ?
  1           0           ?
```

Table 10 Command output

Field	Description
RefCount	Number of BGP routes with these path attributes.
MED	MULTI_EXIT_DISC attribute.

Path/Origin	AS_PATH and ORIGIN attributes of the route:
	• **AS_PATH attribute**—Records the ASs the route has passed, which avoids routing loops.
	• **ORIGIN attribute**—Identifies the origin of the route:
	  ○ **i**—Originated in the AS. The origin of routes advertised with the **network** command is IGP.
	  ○ **e**—Learned through EGP.
	  ○ **?**—Unknown origin. The origin of routes redistributed from IGP protocols is INCOMPLETE.

display bgp peer

Use **display bgp peer** to display BGP peer or peer group information.

Syntax

display bgp [**instance** *instance-name*] **peer ipv4** [**mdt** | **multicast** | **mvpn** | **rtfilter** | [**flowspec** | **unicast**] [**vpn-instance** *vpn-instance-name*]] [*ipv4-address mask-length* | { *ipv4-address* | **group-name** *group-name* } **log-info** | [*ipv4-address*] **verbose**]

display bgp [**instance** *instance-name*] **peer ipv6** [**multicast** | [**unicast**] [**vpn-instance** *vpn-instance-name*]] [*ipv6-address prefix-length* | { *ipv6-address* | **group-name** *group-name* } **log-info** | [*ipv6-address*] **verbose**]

display bgp [**instance** *instance-name*] **peer ipv6** [**unicast**] [*ipv4-address mask-length* | *ipv4-address* **log-info** | [*ipv4-address*] **verbose**]

display bgp [**instance** *instance-name*] **peer link-state** [*ipv4-address mask-length* | *ipv6-address prefix-length* | { *ipv4-address* | *ipv6-address* | **group-name** *group-name* } **log-info** | [*ipv4-address* | *ipv6-address*] **verbose**]

display bgp [**instance** *instance-name*] **peer vpnv4** [**flowspec** | **vpn-instance** *vpn-instance-name*] [*ipv4-address mask-length* | { *ipv4-address* | **group-name** *group-name* } **log-info** | [*ipv4-address*] **verbose**]

display bgp [**instance** *instance-name*] **peer vpnv6** [*ipv4-address mask-length* | { *ipv4-address* | **group-name** *group-name* } **log-info** | [*ipv4-address*] **verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

instance *instance-name*: Specifies a BGP instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command displays BGP peer or peer group information for the default BGP instance.

flowspec: Displays BGP flowspec peer or peer group information.

ipv4: Displays IPv4 BGP peer or peer group information.

ipv6: Displays IPv6 BGP peer or peer group information.

link-state: Displays BGP LS peer or peer group information.

vpnv4: Displays BGP VPNv4 peer or peer group information.

vpnv6: Displays BGP VPNv6 peer or peer group information.

mdt: Displays BGP MDT peer or peer group information.

multicast: Displays BGP multicast peer or peer group information.

mvpn: Displays BGP IPv4 MVPN peer or peer group information.

rtfilter: Displays BGP IPv4 RT filter peer or peer group information.

The following compatibility matrixes show the support of hardware platforms for the **rtfilter** keyword:

Models	Parameter compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	No

unicast: Displays BGP unicast peer or peer group information.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays BGP peer or peer group information for the public network.

ipv4-address mask-length: Specifies a subnet. The value range for the mask length is 0 to 32. If you specify a subnet, this command displays information about all dynamic peers in the subnet.

ipv4-address: Specifies a peer by its IPv4 address.

ipv6-address prefix-length: Specifies a subnet. The value range for the prefix length is 0 to 128. If you specify a subnet, this command displays information about all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address.

group-name *group-name*: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters.

log-info: Displays log information.

verbose: Displays detailed information. If you do not specify this keyword, the command displays brief BGP peer or peer group information.

Usage guidelines

If you do not specify any parameters, this command displays brief information about all BGP peers for the specified address family.

By default, the **unicast** keyword is used if the **unicast**, **mdt**, **mvpn**, **rtfilter**, **flowspec**, and **multicast** keywords are not specified.

Examples

Display brief information about all BGP IPv4 unicast peers.

```
<Sysname> display bgp peer ipv4

 BGP local router ID: 192.168.100.1
 Local AS number: 100
 Total number of peers: 1                 Peers in established state: 1

  * - Dynamically created peer
  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

  10.2.1.2               200       13       16    0       0 00:10:34 Established
```

Table 11 Command output

Field	Description
* - Dynamically created peer	An asterisk (*) before a peer address indicates that the peer is a dynamic peer.
Peer	IPv4 or IPv6 address of the peer.
AS	AS number of the peer.
MsgRcvd	Number of messages received.
MsgSent	Number of messages sent.
OutQ	Number of messages to be sent.
PrefRcv	For the IPv4, IPv6, VPNv4, and VPNv6 address families, this field displays the number of prefixes that have been received from the peer and added into the local BGP routing table. For the IPv4 flowspec address family, this field displays the number of IPv4 flowspec messages received from the peer. For the VPNv4 flowspec address family, this field displays the number of VPNv4 flowspec messages received from the peer. For the IPv4 MDT address family, this field displays the number of MDT messages received from the peer. For IPv4 RT filter address family, this field displays the number of route targets received from the peer.
Up/Down	Lasting time of the current BGP session state.
State	Current state of the BGP session between the local router and the peer.

Display brief information about all dynamic peers in network 1.1.1.0/24.

```
<Sysname> display bgp peer ipv4 1.1.1.0 24

 Type: EBGP link
 Dynamic address range: 1.1.1.0 24
 Configured: Active Hold Time: 3 sec     Keepalive Time: 1 sec
 Address family IPv4 Unicast: Configured
 Address family IPv4 Multicast: Configured
 Address family IPv4 Label: Configured
 Address family VPNv4: Configured
 Address family IPv4 RT-Filter: Configured
 Address family IPv6 Unicast: Configured
 Address family VPNv6: Configured

 Maximum allowed prefix number: 100
 Threshold: 75%
 Minimum time between advertisements is 100 seconds
 Optional capabilities:
  Multi-protocol extended capability has been enabled
  Route refresh capability has been enabled
 Nexthop self has been configured
 Keep-all-routes has been configured
 Send community has been configured
 Send extend community has been configured
 Default route originating has been configured
 Multi-hop ebgp has been enabled
 Peer preferred value: 100
 BFD: Enabled
 Site-of-Origin: 1:1
 Routing policy configured:
 No import as-path-acl list
 Export as-path-acl list is: 22
 No import prefix list
 Export prefix list is: p1
 No import route policy
 Export route policy is: p1
 No import filter-policy
 No export filter-policy

 Dynamic peers:
  1.1.1.3
```

Display brief information about all dynamic peers in network 1::/64.

```
<Sysname> display bgp peer ipv6 1:: 64

 Type: IBGP link
 Dynamic address range: 1:: 64
 Configured: Active Hold Time: 180 sec   Keepalive Time: 60 sec
 Address family IPv6 Unicast: Configured
```

```
Maximum allowed prefix number: 4294967295
Threshold: 75%
Minimum time between advertisements is 15 seconds
Optional capabilities:
 Multi-protocol extended capability has been enabled
 Route refresh capability has been enabled
Send community has been configured
Peer preferred value: 0
Site-of-Origin: Not specified
Routing policy configured:
No routing policy is configured

Dynamic peers:
 1::1
```

Table 12 Command output

Field	Description
Type	BGP connection type between the local router and the dynamic peer: • **IBGP link**—IBGP connection. • **EBGP link**—EBGP connection.
Configured	Timers configured on the local router in seconds, including the hold time (Active Hold Time) and keepalive interval (Keepalive Time).
Address family IPv4 Unicast	IPv4 unicast address family capability.
Address family IPv4 Flowspec	IPv4 flowspec address family capability.
Address family link-state	LS address family capability.
Address family IPv6 Unicast	IPv6 unicast address family capability.
Address family IPv4 Multicast	IPv4 multicast address family capability.
Address family IPv6 Multicast	IPv6 multicast address family capability.
Address family MDT	IPv4 MDT address family capability.
Address family IPv4 RT-Filter	IPv4 RT filter address family capability.
Maximum allowed prefix number	Maximum number of routes allowed to learn from the peer.
Threshold	Percentage of received routes from the peer to maximum routes allowed to learn from the peer. If the percentage is reached, the system generates alarm messages.
Minimum time between advertisements	Minimum route advertisement interval in seconds.
Optional capabilities	Optional capabilities supported by the local end.
Peer Preferred Value	Preferred value specified for the routes from the peer.
BFD	Whether BFD is enabled to detect the link to the BGP peers.
IPsec profile name	IPsec profile applied to the IPv6 BGP peer. This field is available only for the IPv6 unicast and IPv6 multicast address families.

Field	Description
Routing policy configured	Routing policy configured for the peer. If you do not specify a routing policy, this field displays **No routing policy is configured**.
Dynamic peers	IP addresses of dynamic peers.

Display detailed information about BGP IPv4 unicast peer 10.2.1.2.

```
<Sysname> display bgp peer ipv4 10.2.1.2 verbose

         Peer: 10.2.1.2          Local: 192.168.100.1
         Type: EBGP link
         BGP version 4, remote router ID 192.168.100.2
         BGP current state: Established, Up for 00h11m10s
         BGP current event: RecvKeepalive
         BGP last state: OpenConfirm
         Port:  Local - 179      Remote - 60672
         Configured: Active Hold Time: 180 sec   Keepalive Time: 60 sec
         Received  : Active Hold Time: 180 sec
         Negotiated: Active Hold Time: 180 sec   Keepalive Time: 60 sec
         Peer optional capabilities:
         Peer supports BGP multi-protocol extension
         Peer supports BGP route refresh capability
         Peer supports BGP route AS4 capability
         Address family IPv4 Unicast: advertised and received

InQ updates: 0, OutQ updates: 0
 NLRI statistics:
         Rcvd:   UnReach NLRI          0,      Reach NLRI          0
         Sent:   UnReach NLRI          0,      Reach NLRI          0

 Message statistics:
 Msg type     Last rcvd time/      Current rcvd count/      History rcvd count/
              Last sent time       Current sent count       History sent count
 Open         10:38:50-2013.7.23   1                        1
              10:38:50-2013.7.23   1                        1
 Update       10:38:51-2013.7.23   1                        1
              10:38:51-2013.7.23   1                        1
 Notification -                    0                        0
              -                    0                        0
 Keepalive    10:38:50-2013.7.23   1                        1
              10:38:50-2013.7.23   1                        1
 RouteRefresh -                    0                        0
              -                    0                        0
 Total        -                    3                        3
              -                    3                        3

 Maximum allowed prefix number: 4294967295
 Threshold: 75%
```

```
 Minimum time between advertisements is 30 seconds
 Optional capabilities:
  Multi-protocol extended capability has been enabled
  Route refresh capability has been enabled
 Peer Preferred Value: 0
 GTSM has been enabled, and the maximum number of hops is 10
 BFD: Enabled
 Site-of-Origin: Not specified

 Routing policy configured:
 No routing policy is configured
```

Display detailed information about BGP IPv6 unicast peer 1::2.

```
<Sysname> display bgp peer ipv6 1::2 verbose

         Peer: 1::2      Local: 192.168.1.136
         Type: EBGP link
         BGP version 4, remote router ID 192.168.1.135
         BGP current state: Established, Up for 00h05m48s
         BGP current event: RecvKeepalive
         BGP last state: OpenConfirm
         Port:  Local - 13184    Remote - 179
         Configured: Active Hold Time: 180 sec   Keepalive Time: 60 sec
         Received  : Active Hold Time: 180 sec
         Negotiated: Active Hold Time: 180 sec   Keepalive Time: 60 sec
         Peer optional capabilities:
         Peer supports BGP multi-protocol extension
         Peer supports BGP route refresh capability
         Peer supports BGP route AS4 capability
         Address family IPv6 Unicast: advertised and received

 InQ updates: 0, OutQ updates: 0
 NLRI statistics:
         Rcvd:   UnReach NLRI          0,       Reach NLRI          0
         Sent:   UnReach NLRI          0,       Reach NLRI          3

 Message statistics:
 Msg type     Last rcvd time/      Current rcvd count/      History rcvd count/
              Last sent time       Current sent count       History sent count
 Open         18:59:15-2013.4.24   1                        1
              18:59:15-2013.4.24   1                        2
 Update       -                    0                        0
              18:59:16-2013.4.24   1                        1
 Notification -                    0                        0
              18:59:15-2013.4.24   0                        1
 Keepalive    18:59:15-2013.4.24   1                        1
              18:59:15-2013.4.24   1                        1
 RouteRefresh -                    0                        0
              -                    0                        0
```

```
Total        -                   2                     2
             -                   3                     5

Maximum allowed prefix number: 4294967295
Threshold: 75%
Minimum time between advertisements is 30 seconds
Optional capabilities:
 Multi-protocol extended capability has been enabled
 Route refresh capability has been enabled
Peer preferred value: 0
GTSM has been enabled, and the maximum number of hops is 10
BFD: Enabled
IPsec profile name: profile001
Site-of-Origin: Not specified

Routing policy configured:
No routing policy is configured
```

Table 13 Command output

Field	Description
Peer	IPv4 or IPv6 address of the peer.
Local	Local router ID.
Type	BGP connection type between the local router and the peer: • **IBGP link**—IBGP connection. • **EBGP link**—EBGP connection.
remote router ID	Router ID of the peer.
BGP current state	Current state of the BGP session between the local router and the peer.
Up for	Lasting time of the BGP session.
BGP current event	Current event of the BGP session between the local router and the peer.
BGP last state	Previous state of the BGP session.
Port	TCP port numbers of the local router and its peer.
Configured	Timers configured on the local router in seconds, including the hold time (Active Hold Time) and keepalive interval (Keepalive Time).
Received	Received timer (configured on the peer) in seconds, including the hold time (Active Hold Time).
Negotiated	Negotiated timers in seconds, including the hold time (Active Hold Time) and keepalive interval (Keepalive Time).
Peer optional capabilities	Optional capabilities supported by the peer.
Peer supports BGP route AS4 capability	The peer supports 4-byte AS number.
Address family IPv4 Unicast	IPv4 unicast address family capability: routes of the address family can be advertised and received.
Address family IPv4 Flowspec	IPv4 flowspec address family capability: routes of the address family can be advertised and received.

Field	Description
Address family LS	LS address family capability: routes of the address family can be advertised and received.
Address family IPv6 Unicast	IPv6 unicast address family capability: routes of the address family can be advertised and received.
Address family IPv4 Multicast	IPv4 multicast address family capability: routes of the address family can be advertised and received.
Address family IPv6 Multicast	IPv6 multicast address family capability: routes of the address family can be advertised and received.
Address family MDT	IPv4 MDT address family capability: routes of the address family can be advertised and received.
Address family IPv4 RT-Filter	IPv4 RT filter address family capability: route target filter information can be advertised and received.
InQ updates	Number of received updates to be processed.
OutQ updates	Number of updates to be sent to the peer.
NLRI statistics	Number of the reachable and unreachable routes received from and sent to the peer after the BGP session is established.
Message statistics	BGP message statistics.
Msg type	BGP message type.
Last rcvd time/Last sent time	Time when the most recent BGP message was received from or sent to the peer.
Current rcvd count/Current sent count	Number of BGP messages received from or sent to the peer on the current BGP session.
History rcvd count/History sent count	Number of BGP messages received from or sent to the peer since the BGP peer relationship was established.
Total	Total number of received and sent messages.
Maximum allowed prefix number	Maximum number of routes allowed to learn from the peer.
Threshold	Percentage of received routes from the peer to maximum routes allowed to learn from the peer. If the percentage is reached, the system generates alarm messages.
Minimum time between advertisements	Minimum route advertisement interval in seconds.
Optional capabilities	Optional capabilities supported by the local end.
Peer Preferred Value	Preferred value specified for the routes from the peer.
GTSM has been enabled	GTSM is supported.
the maximum number of hops	Maximum number of hops to the specified peer.
BFD	Whether BFD is enabled to detect the link to the BGP peer.
IPsec profile name	IPsec profile applied to the IPv6 BGP peer. This field is available only for the IPv6 unicast address families.
Routing policy configured	Routing policy configured for the peer. If you do not specify a routing policy, this field displays **No routing policy is configured**.

Display log information for BGP IPv4 unicast peer 1.1.1.1.

```
<Sysname> display bgp peer ipv4 1.1.1.1 log-info
```

```
Peer : 1.1.1.1

    Date      Time    State Notification
                            Error/SubError

 06-Feb-2013 22:54:42 Down  Send notification with error 6/4
                            Cease/Administrative Reset
                            <administrative reset>
```

Table 14 Command output

Field	Description
Peer	IPv4 or IPv6 address of the peer.
Date	Date on which the Notification was sent or received.
Time	Time at which the Notification was sent or received.
State	BGP session state: • **Up**—The BGP session is in Established state. • **Down**—The BGP session is down.
Notification Error/SubError	Error code of the Notification, indicating the cause of why the BGP session was down. • **Error**—Refers to the error code, which identifies the type of the Notification. • **SubError**—Refers to the error subcode of the Notification, which identifies the specific information about the reported error.

display bgp routing-table dampened

Use **display bgp routing-table dampened** to display dampened BGP routes.

Syntax

display bgp [**instance** *instance-name*] **routing-table dampened** { **ipv4** | **ipv6** } [**multicast** | [**unicast**] [**vpn-instance** *vpn-instance-name*]]

display bgp [**instance** *instance-name*] **routing-table dampened vpnv4**

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

instance *instance-name*: Specifies a BGP instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command displays dampened BGP routes for the default BGP instance.

ipv4: Displays dampened BGP IPv4 routes.

ipv6: Displays dampened BGP IPv6 routes.

vpnv4: Displays dampened IBGP VPNv4 routes.

multicast: Displays dampened BGP multicast routes.

unicast: Displays dampened BGP unicast routes.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays dampened BGP routes for the public network.

Usage guidelines

By default, the **unicast** keyword is used if neither the **multicast** keyword nor the **unicast** keyword is specified.

Examples

Display dampened BGP IPv4 unicast routes.

```
<Sysname> display bgp routing-table dampened ipv4

 Total number of routes: 1

 BGP local router ID is 192.168.1.135
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e - external
       Origin: i - IGP, e - EGP, ? - incomplete

     Network            From            Reuse                         Path/Ogn

  de 20.1.1.0/24        10.1.1.2        00:56:27                      100i
```

Display dampened BGP IPv6 unicast routes.

```
<Sysname> display bgp routing-table dampened ipv6

 Total number of routes: 2

 BGP local router ID is 192.168.1.135
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e - external
       Origin: i - IGP, e - EGP, ? - incomplete

  de Network : 2::                                  PrefixLen : 64
     From    : 10.1.1.1                             Reuse     : 00:39:49
     Path/Ogn: 100i

  de Network : 2::                                  PrefixLen : 64
     From    : 1::1                                 Reuse     : 00:39:49
     Path/Ogn: 100i
```

Table 15 Command output

Field	Description
Status codes	Status codes: • *** – valid**—Valid route. • **> – best**—Optimal route. • **d – dampened**—Dampened route. • **h – history**—History route. • **s – suppressed**—Suppressed route. • **S – stale**—Stale route. • **i – internal**—Internal route. • **e – external**—External route.
Origin	Origin of the route: • **i – IGP**—Originated in the AS. The origin of routes advertised with the **network** command is IGP. • **e – EGP**—Learned through EGP. • **?– incomplete**—Unknown origin. The origin of routes redistributed from IGP protocols is INCOMPLETE.
Network	Destination network address.
From	IP address from which the route was received.
Reuse	Reuse time of the route.
Path/Ogn	AS_PATH and ORIGIN attributes of the route: • **AS_PATH attribute**—Records the ASs the route has passed, which avoids routing loops. • **ORIGIN attribute**—Identifies the origin of the route.

Related commands

dampening

reset bgp dampening

display bgp routing-table flap-info

Use **display bgp routing-table flap-info** to display BGP route flap statistics.

Syntax

display bgp [**instance** *instance-name*] **routing-table flap-info ipv4** [**multicast** | [**unicast**] [**vpn-instance** *vpn-instance-name*]] [*ipv4-address* [{ *mask-length* | *mask* } [**longest-match**]] | **as-path-acl** *as-path-acl-number*]

display bgp [**instance** *instance-name*] **routing-table flap-info ipv6** [**multicast** | [**unicast**] [**vpn-instance** *vpn-instance-name*]] [*ipv6-address prefix-length* | **as-path-acl** *as-path-acl-number*]

display bgp [**instance** *instance-name*] **routing-table flap-info vpnv4** [*ipv4-address* [{ *mask* | *mask-length* } [**longest-match**]] | **as-path-acl** *as-path-acl-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

instance *instance-name*: Specifies a BGP instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command displays BGP route flap statistics for the default BGP instance.

ipv4: Displays BGP IPv4 route flap statistics.

ipv6: Displays BGP IPv6 route flap statistics.

vpnv4: Displays IBGP VPNv4 route flap statistics.

multicast: Displays BGP multicast route flap statistics.

unicast: Displays BGP unicast route flap statistics.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays BGP route flap statistics for the public network.

ipv4-address: Specifies a destination network address.

mask-length: Specifies a mask length in the range of 0 to 32.

mask: Specifies a network mask in dotted decimal notation.

longest-match: Specifies longest match mode, which selects the longest matching route through the following steps:

1. ANDs the specified network address with the mask of each route.
2. Matches a route if the AND result is the same as the network address of the route and the mask of the route is shorter than or equal to the specified mask.
3. Selects the route with the longest mask among the matching routes.

ipv6-address prefix-length: Displays route flap statistics for BGP IPv6 routes that match the specified network address, and match the prefix length in the range of 0 to 128.

as-path-acl *as-path-acl-number*: Displays route flap statistics for BGP routes that match the AS path list specified by its number in the range of 1 to 256.

Usage guidelines

If you specify only the *ipv4-address* argument, the system ANDs the network address with the mask of a route. If the result matches the network address of the route, the command displays flap statistics of the route.

If you specify the *ipv4-address mask* or *ipv4-address mask-length* argument, and do not specify the **longest-match** keyword, the command displays flap statistics of the BGP IPv4 unicast or multicast route that matches both the specified destination network address and the mask (or mask length).

By default, the **unicast** keyword is used if neither the **multicast** keyword nor the **unicast** keyword is specified.

Examples

Display BGP IPv4 unicast route flap statistics.

```
<Sysname> display bgp routing-table flap-info ipv4
```

```
 Total number of routes: 1

 BGP local router ID is 192.168.1.135
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e - external
       Origin: i - IGP, e - EGP, ? - incomplete

     Network            From            Flaps  Duration  Reuse        Path/Ogn

  de 20.1.1.0/24        10.1.1.2        1      00:02:36  00:53:58     100i
```

Display BGP IPv6 unicast route flap statistics.

```
<Sysname> display bgp routing-table flap-info ipv6

 Total number of routes: 2

 BGP local router ID is 192.168.1.135
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e - external
       Origin: i - IGP, e - EGP, ? - incomplete

  de Network : 2::                                    PrefixLen : 64
     From    : 10.1.1.1                               Flaps     : 5
     Duration: 00:03:25                               Reuse     : 00:39:28
     Path/Ogn: 100i

  de Network : 2::                                    PrefixLen : 64
     From    : 1::1                                   Flaps     : 5
     Duration: 00:03:25                               Reuse     : 00:39:28
     Path/Ogn: 100i
```

Table 16 Command output

Field	Description
Status codes	Status codes: • *** – valid**—Valid route. • **> – best**—Optimal route. • **d – dampened**—Dampened route. • **h – history**—History route. • **s – suppressed**—Suppressed route. • **S – stale**—Stale route. • **i – internal**—Internal route. • **e – external**—External route.
Origin	Origin of the route: • **i – IGP**—Originated in the AS. The origin of routes advertised with the **network** command is IGP. • **e – EGP**—Learned through EGP. • **?– incomplete**—Unknown origin. The origin of routes redistributed from IGP protocols is INCOMPLETE.

Field	Description
Network	Destination network address.
From	Source IP address of the route.
Flaps	Number of routing flaps.
Duration	Duration time of the flap route.
Reuse	Reuse time of the route.
Path/Ogn	AS_PATH and ORIGIN attributes of the route: • **AS_PATH attribute**—Records the ASs the route has passed, which avoids routing loops. • **ORIGIN attribute**—Identifies the origin of the route.

Related commands

dampening

reset bgp flap-info

display bgp routing-table ipv4 multicast

Use **display bgp routing-table ipv4 multicast** to display BGP IPv4 multicast routing information.

Syntax

display bgp [**instance** *instance-name*] **routing-table ipv4 multicast** [*ipv4-address* [{ *mask-length* | *mask* } [**longest-match**]] | *ipv4-address* [*mask-length* | *mask*] **advertise-info** | **as-path-acl** *as-path-acl-number* | **community-list** { { *basic-community-list-number* | *comm-list-name* } [**whole-match**] | *adv-community-list-number* } | **peer** *ipv4-address* { **advertised-routes** | **received-routes** } [*ipv4-address* [*mask-length* | *mask*] | **statistics**] | **statistics**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

instance *instance-name*: Specifies a BGP instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command displays BGP IPv4 multicast routing information for the default BGP instance.

ipv4-address: Specifies a destination network address.

mask-length: Specifies a mask length in the range of 0 to 32.

mask: Specifies a network mask in dotted decimal notation.

longest-match: Specifies longest match mode, which selects the longest matching route through the following steps:

1. ANDs the specified network address with the mask of each route.
2. Matches a route if the AND result is the same as the network address of the route and the mask of the route is shorter than or equal to the specified mask.
3. Selects the route with the longest mask among the matching routes.

advertise-info: Displays advertisement information for BGP IPv4 multicast routes.

as-path-acl *as-path-acl-number*: Displays BGP IPv4 multicast routes that match the AS path list specified by its number in the range of 1 to 256.

community-list: Displays BGP IPv4 multicast routes that match a community list.

basic-community-list-number: Specifies a basic community list by its number in the range of 1 to 99.

comm-list-name: Specifies a community list by its name, a case-sensitive string of 1 to 63 characters.

whole-match: Displays BGP IPv4 multicast routes exactly matching the specified community list. If you do not specify this keyword, the command displays BGP IPv4 multicast routes whose COMMUNITY attributes include the specified community list.

adv-community-list-number: Specifies an advanced community list by its number in the range of 100 to 199.

peer *ipv4-address*: Displays BGP IPv4 multicast routing information advertised to or received from the specified peer.

advertised-routes: Displays BGP IPv4 multicast routing information advertised to the specified peer.

received-routes: Displays BGP IPv4 multicast routing information received from the specified peer.

statistics: Displays routing statistics.

Usage guidelines

If you do not specify any parameters, this command displays brief information about all BGP IPv4 multicast routes.

If you specify only the *ipv4-address* argument, the system ANDs the network address with the mask of a route. If the result matches the network address of the route, the command displays information about the route.

If you specify the *ipv4-address mask* or *ipv4-address mask-length* argument and do not specify the **longest-match** keyword, this command displays information about the BGP IPv4 multicast route that matches both the specified destination network address and the mask (or mask length).

Examples

Display brief information about all BGP IPv4 multicast routes.

```
<Sysname> display bgp routing-table ipv4 multicast

 Total number of routes: 3

 BGP local router ID is 192.168.1.62
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e - external
       Origin: i - IGP, e - EGP, ? - incomplete

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn
```

```
* >  5.5.5.5/32         127.0.0.1       0                    32768   ?
* >  192.168.1.0        192.168.1.62    0                    32768   ?
* >  192.168.1.62/32    127.0.0.1       0                    32768   ?
```

Display information about BGP IPv4 multicast routes that match AS path list 20.

```
<Sysname> display bgp routing-table ipv4 multicast as-path-acl 20

 Total number of routes: 3

 BGP local router ID is 192.168.1.62
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e - external
       Origin: i - IGP, e - EGP, ? - incomplete

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

* >  5.5.5.5/32         127.0.0.1       0                    32768   ?
* >  192.168.1.0        192.168.1.62    0                    32768   ?
* >  192.168.1.62/32    127.0.0.1       0                    32768   ?
```

Display information about BGP IPv4 multicast routes that match BGP community list 100.

```
<Sysname> display bgp routing-table ipv4 multicast community-list 100

 Total number of routes: 3

 BGP local router ID is 192.168.1.62
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e - external
       Origin: i - IGP, e - EGP, ? - incomplete

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

* >  5.5.5.5/32         127.0.0.1       0                    32768   ?
* >  192.168.1.0        192.168.1.62    0                    32768   ?
* >  192.168.1.62/32    127.0.0.1       0                    32768   ?
```

Display information about all BGP IPv4 multicast routes advertised to peer 192.168.1.139.

```
<Sysname> display bgp routing-table ipv4 multicast peer 192.168.1.139 advertised-routes

 Total number of routes: 2

 BGP local router ID is 192.168.1.62
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e - external
       Origin: i - IGP, e - EGP, ? - incomplete

     Network            NextHop         MED        LocPrf             Path/Ogn

* >  5.5.5.5/32         127.0.0.1       0          100                ?
* >  192.168.1.0        192.168.1.62    0          100                ?
```

Display information about all BGP IPv4 multicast routes received from peer 192.168.1.139.

```
<Sysname> display bgp routing-table ipv4 multicast peer 192.168.1.139 received-routes

 Total number of routes: 2

 BGP local router ID is 192.168.1.62
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e - external
       Origin: i - IGP, e - EGP, ? - incomplete

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

* >i 8.8.8.8/32         192.168.1.139   0          100        0       ?
*  i 192.168.1.0        192.168.1.139   0          100        0       ?
```

Table 17 Command output

Field	Description
Status codes	Status codes: • *** – valid**—Valid route. • **> – best**—Optimal route. • **d – dampened**—Dampened route. • **h – history**—History route. • **s – suppressed**—Suppressed route. • **S – stale**—Stale route. • **i – internal**—Internal route. • **e – external**—External route.
Origin	Origin of the route: • **i – IGP**—Originated in the AS. The origin of routes advertised with the **network** command is IGP. • **e – EGP**—Learned through EGP. • **?– incomplete**—Unknown origin. The origin of routes redistributed from IGP protocols is INCOMPLETE.
Network	Destination network address.
NextHop	Next hop IP address.
MED	MULTI_EXIT_DISC attribute.
LocPrf	Local preference value.
PrefVal	Preferred value of the route.
Path/Ogn	AS_PATH and ORIGIN attributes of the route: • **AS_PATH**—Records the ASs the route has passed. • **ORIGIN**—Identifies the origin of the route.

Display detailed information about BGP IPv4 multicast routes destined to network 5.5.5.5/32.

```
<Sysname> display bgp routing-table ipv4 multicast 5.5.5.5 32

 BGP local router ID: 192.168.1.139
 Local AS number: 100

 Paths:   1 available, 1 best
```

```
BGP routing table information of 5.5.5.5/32:
From            : 192.168.1.62 (192.168.1.62)
Rely nexthop    : 192.168.1.62
Original nexthop: 192.168.1.62
OutLabel        : NULL
AS-path         : (null)
Origin          : incomplete
Attribute value : MED 0, localpref 100, pref-val 0
State           : valid, internal, best
Originator      : 176.1.1.2
Cluster list    : 80
IP precedence   : N/A
QoS local ID    : N/A
Traffic index   : N/A
VPN-Peer UserID : N/A
DSCP            : N/A
EXP             : N/A
```

Table 18 Command output

Field	Description
Paths	Number of routes: • **available**—Number of valid routes. • **best**—Number of optimal routes.
From	IP address of BGP peer that advertised the route.
Rely Nexthop	Next hop found by route recursion. If no next hop is found, this field displays **not resolved**.
Original nexthop	Original next hop of the route. If the route was obtained from a BGP update message, the original next hop is the next hop IP address in the message.
OutLabel	Outgoing label of the route.
AS-path	AS_PATH attribute of the route.
Origin	Origin of the route: • **igp**—Originated in the AS. The origin of routes advertised with the **network** command is IGP. • **egp**—Learned through EGP. • **incomplete**—Unknown origin. The origin of routes redistributed from IGP protocols is INCOMPLETE.
Attribute value	BGP path attributes: • **MED**—MED value. • **localpref**—Local preference value. • **pref-val**—Preferred value. • **pre**—Route preference.

Field	Description
State	Current state of the route: • valid. • internal. • external. • local. • synchronize. • best.
Originator	Router ID of the peer that advertised the route to the reflector.
IP precedence	IP precedence in the range of 0 to 7. **N/A** indicates that the route does not support this field.
QoS local ID	QoS local ID in the range of 1 to 4095. **N/A** indicates that the route does not support this field.
Traffic index	Traffic index in the range of 1 to 64. **N/A** indicates that the route does not support this field.
VPN-Peer UserID	VPN peer ID in the range of 1 to 134217727. **N/A** indicates that the route does not support this field.
DSCP	DSCP value in the range of 0 to 63. **N/A** indicates that the route does not support this field.
EXP	MPLS EXP value of the route. **N/A** indicates that the route does not support this field.

Display statistics for BGP IPv4 multicast routes advertised to peer 192.168.1.62.

```
<Sysname> display bgp routing-table ipv4 multicast peer 192.168.1.62 advertised-routes
statistics

 Advertised routes total: 2
```

Display statistics for BGP IPv4 multicast routes received from peer 192.168.1.62.

```
<Sysname> display bgp routing-table ipv4 multicast peer 192.168.1.62 received-routes
statistics

 Received routes total: 2
```

Table 19 Command output

Field	Description
Advertised routes total	Total number of advertised routes.
Received routes total	Total number of received routes.

Display BGP IPv4 multicast route statistics.

```
<Sysname> display bgp routing-table ipv4 multicast statistics

 Total number of routes: 5
```

Table 20 Command output

Field	Description
Total number of routes	Total number of routes.

Display advertisement information for the BGP IPv4 multicast route destined to network 8.8.8.8/32.

```
<Sysname> display bgp routing-table ipv4 multicast 8.8.8.8 32 advertise-info

 BGP local router ID: 192.168.1.139
 Local AS number: 100

 Paths:   1 best

 BGP routing table information of 8.8.8.8/32:
 Advertised to peers (1 in total):
    192.168.1.62
```

Table 21 Command output

Field	Description
BGP local router ID	Local BGP router ID.
Local AS number	Local AS number.
Paths	Number of optimal routes to the destination.
BGP routing table information of 8.8.8.8/32	Advertisement information for network 8.8.8.8/32.
Advertised to peers (1 in total)	Peers to which the network has been advertised.

Related commands

ip as-path

ip community-list

display bgp routing-table ipv4 rtfilter

Use **display bgp routing-table ipv4 rtfilter** to display BGP IPv4 RT filter routing information.

Syntax

display bgp [**instance** *instance-name*] **routing-table ipv4 rtfilter** [**default-rt** [**advertise-info**] | [**origin-as** *as-number*] [*route-target* [**advertise-info**]] | **peer** *ipv4-address* { **advertised-routes** | **received-routes** } [**default-rt** | [**origin-as** *as-number*] [*route-target*] | **statistics**] | **statistics**]

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	No

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

instance *instance-name*: Specifies a BGP instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command displays BGP IPv4 RT filter routing information for the default BGP instance.

default-rt: Displays BGP IPv4 RT filter routing information for an all-zero RT.

origin-as *as-number*: Specifies an origin AS by its number.

route-target: Specifies an RT, a string of 3 to 21 characters.

An RT has the following formats:

- *16-bit AS number:32-bit user-defined number*. For example, 101:3.
- *32-bit IP address:16-bit user-defined number*. For example, 192.168.122.15:1.
- *32-bit AS number:16-bit user-defined number*, where the minimum value of the AS number is 65536. For example, 65536:1.

advertise-info: Displays advertisement information for BGP IPv4 RT filter routes.

peer *ipv4-address*: Displays BGP IPv4 RT filter routing information advertised to or received from the specified peer.

advertised-routes: Displays BGP IPv4 RT filter routing information advertised to the specified peer.

received-routes: Displays BGP IPv4 RT filter routing information received from the specified peer.

statistics: Displays routing statistics.

Usage guidelines

If you do not specify any parameters, this command displays brief information about all BGP IPv4 RT filter routes.

Examples

Display brief information about all BGP IPv4 RT filter routes.

```
<Sysname> display bgp routing-table ipv4 rtfilter

BGP local router ID is 192.168.1.136
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e - external
       Origin: i - IGP, e - EGP, ? - incomplete

Total number of routes from all PEs: 2

Origin AS: 100
Total number of routes: 2

* >e Network : <100:1>                                PrefixLen : 96
     NextHop : 1.1.1.2                                LocPrf    :
```

```
     PrefVal : 0
     MED     :
     Path/Ogn: 100i

* >e Network : <1.1.1.1:1>                              PrefixLen : 96
     NextHop : 1.1.1.2                                 LocPrf    :
     PrefVal : 0
     MED     :
     Path/Ogn: 100i
```

Display information about BGP IPv4 RT filter routes that match origin AS 100.

```
<Sysname> display bgp routing-table ipv4 rtfilter origin-as 100

BGP local router ID is 192.168.1.136
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e - external
       Origin: i - IGP, e - EGP, ? - incomplete

Origin AS: 100
 Total number of routes: 2

* >e Network : <100:1>                                 PrefixLen : 96
     NextHop : 1.1.1.2                                 LocPrf    :
     PrefVal : 0
     MED     :
     Path/Ogn: 100i

* >e Network : <1.1.1.1:1>                              PrefixLen : 96
     NextHop : 1.1.1.2                                 LocPrf    :
     PrefVal : 0
     MED     :
     Path/Ogn: 100i
```

Display information about all public BGP IPv4 RT filter routes advertised to peer 10.2.1.2.

```
<Sysname> display bgp routing-table ipv4 rtfilter peer 10.2.1.2 advertised-routes

Total number of routes: 1

 BGP local router ID is 192.168.1.136
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e - external
       Origin: i - IGP, e - EGP, ? - incomplete

Origin AS: 100
 Total number of routes: 1

* >  Network : <100:1>                                 PrefixLen : 96
     NextHop : 1.1.1.2                                 LocPrf    :
     MED     : 0
     Path/Ogn: i
```

Display information about all public BGP IPv4 RT filter routes received from peer 10.2.1.2.

```
<Sysname> display bgp routing-table ipv4 rtfilter peer 10.2.1.2 received-routes

Total number of routes: 1

 BGP local router ID is 192.168.1.135
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e - external
       Origin: i - IGP, e - EGP, ? - incomplete

Origin AS: 100
 Total number of routes: 1

* >e Network : <100:1>                                PrefixLen : 96
     NextHop : 10.1.1.1                               LocPrf    :
     PrefVal : 0
     MED     : 0
     Path/Ogn: 100i
```

Table 22 Command output

Field	Description
Origin AS	Origin AS of the RT filter routes.
Status codes	Status codes: • *** – valid**—Valid route. • **> – best**—Optimal route. • **d – dampened**—Dampened route. • **h – history**—History route. • **s – suppressed**—Suppressed route. • **S – stale**—Stale route. • **i – internal**—Internal route. • **e – external**—External route.
Origin	Origin of the route: • **i – IGP**—Originated in the AS. The origin of routes advertised with the **network** command is IGP. • **e – EGP**—Learned through EGP. • **?– incomplete**—Unknown origin. The origin of routes redistributed from IGP protocols is INCOMPLETE.
Network	Destination network address.
NextHop	Next hop IP address.
MED	MULTI_EXIT_DISC attribute.
LocPrf	Local preference value.
PrefVal	Preferred value of the route.
Path/Ogn	AS_PATH and ORIGIN attributes of the route: • **AS_PATH**—Records the ASs the route has passed. • **ORIGIN**—Identifies the origin of the route.

Display detailed information about BGP IPv4 RT filter route 100:1.

```
<Sysname> display bgp routing-table ipv4 rtfilter 100:1

 BGP local router ID: 192.168.100.1
 Local AS number: 100

 Origin AS: 100
Total number of routes: 1
Paths:   1 available, 1 best

 BGP routing table information of <100:1>/96:
 Imported route.
 Original nexthop: 10.2.1.1
 OutLabel        : NULL
 AS-path         : (null)
 Origin          : igp
 Attribute value : MED 0, pref-val 32768, pre 0
 State           : valid, local, best
 IP precedence   : N/A
 QoS local ID    : N/A
 Traffic index   : N/A
 VPN-Peer UserID : N/A
 DSCP            : N/A
```

Table 23 Command output

Field	Description
Paths	Number of routes: • **available**—Number of valid routes. • **best**—Number of optimal routes.
Imported route	The BGP RT filter route is locally generated.
Original nexthop	Original next hop of the route. If the route was obtained from a BGP update message, the original next hop is the next hop IP address in the message.
OutLabel	Outgoing label of the route.
AS-path	AS_PATH attribute of the route.
Origin	Origin of the route: • **igp**—Originated in the AS. The origin of routes advertised with the **network** command is IGP. • **egp**—Learned through EGP. • **incomplete**—Unknown origin. The origin of routes redistributed from IGP protocols is INCOMPLETE.
Attribute value	BGP path attributes: • **MED**—MED value. • **localpref**—Local preference value. • **pref-val**—Preferred value. • **pre**—Route preference.
State	Current state of the route: • valid. • internal.

	• external. • local. • synchronize. • best.
From	IP address of BGP peer that advertised the route.
Rely Nexthop	Next hop found by route recursion. If no next hop is found, this field displays **not resolved**.
IP precedence	IP precedence in the range of 0 to 7. **N/A** indicates that the route does not support this field.
QoS local ID	QoS local ID in the range of 1 to 4095. **N/A** indicates that the route does not support this field.
Traffic index	Traffic index in the range of 1 to 64. **N/A** indicates that the route does not support this field.
VPN-Peer UserID	VPN peer ID in the range of 1 to 134217727. **N/A** indicates that the route does not support this field.
DSCP	DSCP value in the range of 0 to 63. **N/A** indicates that the route does not support this field.
Backup route	The route is a backup route.

Display statistics for BGP IPv4 RT filter routes advertised to peer 10.2.1.2.

```
<Sysname> display bgp routing-table ipv4 rtfilter peer 10.2.1.2 advertised-routes
statistics

 Advertised routes total: 2
```

Display statistics for BGP IPv4 RT filter routes received from peer 10.2.1.2.

```
<Sysname> display bgp routing-table ipv4 rtfilter peer 10.2.1.2 received-routes statistics

 Received routes total: 2
```

Table 24 Command output

Field	Description
Advertised routes total	Total number of advertised routes.
Received routes total	Total number of received routes.

Display BGP IPv4 RT filter route statistics.

```
<Sysname> display bgp routing-table ipv4 rtfilter statistics
 Total number of routes from all PEs: 6

Origin AS: 100
 Total number of routes: 2

 Origin AS: 200
 Total number of routes: 4
```

Display advertisement information for the BGP IPv4 RT filter route 1.1.1.1:1/96.

```
<Sysname> display bgp routing-table ipv4 rtfilter 1.1.1.1:1 advertise-info

 BGP local router ID: 192.168.100.1
```

```
 Local AS number: 100

 Paths:   1 best

Origin AS: 100
 Total number of routes: 1
 Paths:   1 best

 BGP route-target filter information of <1.1.1.1:1>/96:
 Advertised to VPN peers (1 in total):
1.1.1.2


 Origin AS: 200
 Total number of routes: 1
 Paths:   1 best

 BGP route-target filter information of <1.1.1.1:1>/96:
 Advertised to VPN peers (1 in total):
    1.1.1.2
```

Table 25 Command output

Field	Description
Paths	Number of optimal routes to the destination.
BGP route-target filter information of <1.1.1.1:1>/96	Information about BGP IPv4 RT filter route 1.1.1.1:1/96.
Advertised to VPN peers (1 in total)	Peers to which the network has been advertised.

display bgp routing-table ipv4 unicast

Use **display bgp routing-table ipv4 unicast** to display BGP IPv4 unicast routing information.

Syntax

display bgp [**instance** *instance-name*] **routing-table ipv4** [**unicast**] [**vpn-instance** *vpn-instance-name*] [*ipv4-address* [{ *mask-length* | *mask* } [**longest-match**]] | *ipv4-address* [*mask-length* | *mask*] **advertise-info** | **as-path-acl** *as-path-acl-number* | **community-list** { { *basic-community-list-number* | *comm-list-name* } [**whole-match**] | *adv-community-list-number* } | **peer** *ipv4-address* { **advertised-routes** | **received-routes** } [*ipv4-address* [*mask-length* | *mask*] | **statistics**] | **statistics**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

instance *instance-name*: Specifies a BGP instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command displays BGP IPv4 unicast routing information for the default BGP instance.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays the BGP IPv4 unicast routing information for the public network.

ipv4-address: Specifies a destination network address.

mask-length: Specifies a mask length in the range of 0 to 32.

mask: Specifies a network mask in dotted decimal notation.

longest-match: Specifies longest match mode, which selects the longest matching route through the following steps:

1. ANDs the specified network address with the mask of each route.
2. Matches a route if the AND result is the same as the network address of the route and the mask of the route is shorter than or equal to the specified mask.
3. Selects the route with the longest mask among the matching routes.

advertise-info: Displays advertisement information for BGP IPv4 unicast routes.

as-path-acl *as-path-acl-number*: Displays BGP IPv4 unicast routes that match the AS path list specified by its number in the range of 1 to 256.

community-list: Displays BGP IPv4 unicast routes that match a community list.

basic-community-list-number: Specifies a basic community list by its number in the range of 1 to 99.

comm-list-name: Specifies a community list by its name, a case-sensitive string of 1 to 63 characters.

whole-match: Displays routes exactly matching the specified community list. If you do not specify this keyword, the command displays routes whose COMMUNITY attributes include the specified community list.

adv-community-list-number: Specifies an advanced community list by its number in the range of 100 to 199.

peer *ipv4-address*: Displays BGP IPv4 unicast routing information advertised to or received from the specified peer.

advertised-routes: Displays routing information advertised to the specified peer.

received-routes: Displays routing information received from the specified peer.

statistics: Displays routing statistics.

Usage guidelines

If you do not specify any parameters, this command displays brief information about all BGP IPv4 unicast routes.

If you specify only the *ipv4-address* argument, the system ANDs the network address with the mask of a route. If the result matches the network address of the route, the command displays information about the route.

If you specify the *ipv4-address mask* or *ipv4-address mask-length* argument and do not specify the **longest-match** keyword, this command displays information about the BGP IPv4

unicast route that matches both the specified destination network address and the mask (or mask length).

This command displays BGP IPv4 unicast routing information regardless of whether the **unicast** keyword is specified.

Examples

Display brief information about all BGP IPv4 unicast routes.

```
<Sysname> display bgp routing-table ipv4

 Total number of routes: 4

 BGP local router ID is 192.168.100.1
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e - external
       Origin: i - IGP, e - EGP, ? - incomplete

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

* >  10.2.1.0/24        10.2.1.1        0                     0       i
   e                    10.2.1.2        0                     0       4294967295
 4294967294 4294967293 4294967292 4294967291 4294967290 4294967215 4294967225 4294967235
4294967245 4294967295 4294967294 4294967293 4294967292 4294967291 4294967290 i
* >  192.168.1.0        192.168.1.135   0                     0       i
*  e                    10.2.1.2        0                     0       200i
```

Display information about BGP IPv4 unicast routes that match AS path list 1.

```
<Sysname> display bgp routing-table ipv4 as-path-acl 1

 Total number of routes: 1

 BGP local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e - external
       Origin: i - IGP, e - EGP, ? - incomplete

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

* >e 30.1.1.0/24        20.1.1.1                              0       200i
```

Display information about all public BGP IPv4 unicast routes advertised to peer 10.2.1.2.

```
<Sysname> display bgp routing-table ipv4 peer 10.2.1.2 advertised-routes

 Total number of routes: 2

 BGP local router ID is 192.168.100.1
 Status codes: * - valid, > - best, d - damped, h - history
               s - suppressed, S - Stale, i - internal, e - external
       Origin: i - IGP, e - EGP, ? - incomplete

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn
```

```
* >  10.2.1.0/24        10.2.1.1        0                    0       i
* >  192.168.1.0        192.168.1.135   0                    0       i
```

Display information about all public BGP IPv4 unicast routes received from peer 10.2.1.2.

```
<Sysname> display bgp routing-table ipv4 peer 10.2.1.2 received-routes

 Total number of routes: 2

 BGP local router ID is 192.168.100.1
 Status codes: * - valid, > - best, d - damped, h - history
               s - suppressed, S - Stale, i - internal, e - external
       Origin: i - IGP, e - EGP, ? - incomplete

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

   e 10.2.1.0/24        10.2.1.2        0                     0       200i
*  e 192.168.1.0        10.2.1.2        0                     0       200i
```

Table 26 Command output

Field	Description
Status codes	Status codes: • *** – valid**—Valid route. • **> – best**—Optimal route. • **d – dampened**—Dampened route. • **h – history**—History route. • **s – suppressed**—Suppressed route. • **S – stale**—Stale route. • **i – internal**—Internal route. • **e – external**—External route.
Origin	Origin of the route: • **i – IGP**—Originated in the AS. The origin of routes advertised with the **network** command is IGP. • **e – EGP**—Learned through EGP. • **?– incomplete**—Unknown origin. The origin of routes redistributed from IGP protocols is INCOMPLETE.
Network	Destination network address.
NextHop	Next hop IP address.
MED	MULTI_EXIT_DISC attribute.
LocPrf	Local preference value.
PrefVal	Preferred value of the route.
Path/Ogn	AS_PATH and ORIGIN attributes of the route: • **AS_PATH**—Records the ASs the route has passed, which avoids routing loops. This field can display a maximum of 16 AS numbers. More AS numbers are omitted and can be viewed in the detailed route information. • **ORIGIN**—Identifies the origin of the route.

Display detailed information about BGP IPv4 unicast routes destined to network 10.2.1.0/24.

```
<Sysname> display bgp routing-table ipv4 10.2.1.0 24
```

```
 BGP local router ID: 192.168.100.1
 Local AS number: 100

 Paths:   2 available, 1 best

 BGP routing table information of 10.2.1.0/24:
 Imported route.
 Original nexthop: 10.2.1.1
 OutLabel        : NULL
 AS-path         : (null)
 Origin          : igp
 Attribute value : MED 0, pref-val 0, pre 0
 State           : valid, local, best
 Originator      : 176.1.1.2
 Cluster list    : 80
 IP precedence   : N/A
 QoS local ID    : N/A
 Traffic index   : N/A
 VPN-Peer UserID : N/A
 DSCP            : N/A
 EXP             : N/A

 From            : 10.2.1.2 (192.168.100.2)
 Rely nexthop   : not resolved
 Original nexthop: 10.2.1.2
 OutLabel        : NULL
 AS-path         : 200
 Origin          : igp
 Attribute value : MED 0, pref-val 0, pre 255
 State           : external
 IP precedence   : N/A
 QoS local ID    : N/A
 Traffic index   : N/A
 VPN-Peer UserID : N/A
 DSCP            : N/A
 EXP             : N/A
```

Display detailed information about the BGP IPv4 unicast route destined to address 1.1.1.1/32.

```
<Sysname> display bgp routing-table ipv4 1.1.1.1 32

 BGP local router ID: 192.168.100.1
 Local AS number: 100

 Paths:   2 available, 1 best

 BGP routing table information of 1.1.1.1/32:
 From            : 10.2.1.1 (192.168.100.3)
 Rely nexthop    : 10.2.1.1
 Original nexthop: 10.2.1.1
```

```
OutLabel        : NULL
AS-path         : (null)
Origin          : igp
Attribute value : MED 0, pref-val 0, pre 0
State           : valid, local, best
IP precedence   : N/A
QoS local ID    : N/A
Traffic index   : N/A
VPN-Peer UserID : N/A
DSCP            : N/A
EXP             : N/A

Backup route.
From            : 10.2.1.2 (192.168.100.2)
Rely nexthop    : 10.2.1.2
Original nexthop: 10.2.1.2
OutLabel        : NULL
AS-path         : 200
Origin          : igp
Attribute value : MED 0, pref-val 0, pre 255
State           : external
IP precedence   : N/A
QoS local ID    : N/A
Traffic index   : N/A
VPN-Peer UserID : N/A
DSCP            : N/A
EXP             : N/A
```

Table 27 Command output

Field	Description
Paths	Number of routes: • **available**—Number of valid routes. • **best**—Number of optimal routes.
Original nexthop	Original next hop of the route. If the route was obtained from a BGP update message, the original next hop is the next hop IP address in the message.
OutLabel	Outgoing label of the route.
AS-path	AS_PATH attribute of the route, which records the ASs the route has passed and avoids routing loops.
Origin	Origin of the route: • **igp**—Originated in the AS. The origin of routes advertised with the **network** command is IGP. • **egp**—Learned through EGP. • **incomplete**—Unknown origin. The origin of routes redistributed from IGP protocols is INCOMPLETE.
PrefixSID	Prefix SID: • **Label index**—Label index. • **SRGB**—SRGB range.

Field	Description
Attribute value	BGP path attributes: • **MED**—MED value. • **localpref**—Local preference value. • **pref-val**—Preferred value. • **pre**—Route preference.
State	Current state of the route: • valid. • internal. • external. • local. • synchronize. • best.
Originator	Router ID of the peer that advertised the route to the reflector.
From	IP address of the BGP peer that advertised the route.
Rely Nexthop	Next hop found by route recursion. If no next hop is found, this field displays **not resolved**.
IP precedence	IP precedence in the range of 0 to 7. **N/A** indicates that the route does not support this field.
QoS local ID	QoS local ID in the range of 1 to 4095. **N/A** indicates that the route does not support this field.
Traffic index	Traffic index in the range of 1 to 64. **N/A** indicates that the route does not support this field.
VPN-Peer UserID	VPN peer ID in the range of 1 to 134217727. **N/A** indicates that the route does not support this field.
DSCP	DSCP value in the range of 0 to 63. **N/A** indicates that the route does not support this field.
Backup route	The route is a backup route.
EXP	MPLS EXP value of the route. **N/A** indicates that the route does not support this field.
Tunnel policy	Tunnel policy that takes effect. **NULL** indicates that no tunnel policy takes effect.
Rely Tunnel IDs	Tunnel index IDs after route recursion. This field displays multiple tunnel index IDs if ECMP tunnels exist and displays **N/A** if no tunnels are found by route recursion.

Display statistics for public BGP IPv4 unicast routes advertised to peer 10.2.1.2.

```
<Sysname> display bgp routing-table ipv4 peer 10.2.1.2 advertised-routes statistics

 Advertised routes total: 2
```

Display statistics for public BGP IPv4 unicast routes received from peer 10.2.1.2.

```
<Sysname> display bgp routing-table ipv4 peer 10.2.1.2 received-routes statistics

 Received routes total: 2
```

Table 28 Command output

Field	Description
Advertised routes total	Total number of advertised routes.
Received routes total	Total number of received routes.

Display BGP IPv4 unicast route statistics.

```
<Sysname> display bgp routing-table ipv4 statistics

 Total number of routes: 4
```

Table 29 Command output

Field	Description
Total number of routes	Total number of routes.

Display advertisement information for the BGP IPv4 unicast route destined to network 10.2.1.0/24.

```
<Sysname> display bgp routing-table ipv4 10.2.1.0 24 advertise-info

 BGP local router ID: 192.168.100.1
 Local AS number: 100

 Paths:   1 best

 BGP routing table information of 10.2.1.0/24:
 Advertised to peers (1 in total):
    10.2.1.2
```

Table 30 Command output

Field	Description
BGP local router ID	Local BGP router ID.
Local AS number	Local AS number.
Paths	Number of optimal routes to the destination.
BGP routing table information of 10.2.1.0/24	Advertisement information for network 10.2.1.0/24.
Advertised to peers (1 in total)	Peers to which the network has been advertised.

Related commands

`ip as-path`

`ip community-list`

display bgp routing-table ipv6 multicast

Use **`display bgp routing-table ipv6 multicast`** to display BGP IPv6 multicast routing information.

Syntax

display bgp [**instance** *instance-name*] **routing-table ipv6 multicast** [*ipv6-address prefix-length* [**advertise-info**] | **as-path-acl** *as-path-acl-number* | **community-list** { { *basic-community-list-number* | *comm-list-name* } [**whole-match**] | *adv-community-list-number* } | **peer** *ipv6-address* { **advertised-routes** | **received-routes** } [*ipv6-address prefix-length* | **statistics**] | **statistics**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

instance *instance-name*: Specifies a BGP instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command displays BGP IPv6 multicast routing information for the default BGP instance.

ipv6-address prefix-length: Specifies the destination network address and prefix length. The value range for the *prefix-length* argument is 0 to 128. If you do not specify this argument, the command displays brief information about all BGP IPv6 multicast routing information.

advertise-info: Displays advertisement information for BGP IPv6 multicast routes. If you do not specify this keyword, the command displays the BGP IPv6 multicast routing table.

as-path-acl *as-path-acl-number*: Displays BGP IPv6 multicast routes that match the AS path list specified by its number in the range of 1 to 256.

community-list: Displays BGP IPv6 multicast routes that match a community list.

basic-community-list-number: Specifies a basic community list by its number in the range of 1 to 99.

comm-list-name: Specifies a community list by its name, a case-sensitive string of 1 to 63 characters.

whole-match: Displays BGP IPv6 multicast routes exactly matching the specified community list. If you do not specify this keyword, the command displays BGP IPv6 multicast routes whose COMMUNITY attributes include the specified community list.

adv-community-list-number: Specifies an advanced community list by its number in the range of 100 to 199.

peer: Displays BGP IPv6 multicast routing information advertised to or received from the specified peer.

ipv6-address: Specifies the peer IPv6 address.

advertised-routes: Displays BGP IPv6 multicast routing information advertised to the specified peer.

received-routes: Displays BGP IPv6 multicast routing information received from the specified peer.

statistics: Displays routing statistics.

Examples

Display brief information about all BGP IPv6 multicast routes.

```
<Sysname> display bgp routing-table ipv6 multicast

 Total number of routes: 5

 BGP local router ID is 192.168.1.139
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e - external
       Origin: i - IGP, e - EGP, ? - incomplete

* >  Network : 1::                                    PrefixLen : 64
     NextHop : ::                                     LocPrf    :
     PrefVal : 32768                                  OutLabel  : NULL
     MED     : 0
     Path/Ogn: ?

*  i Network : 1::                                    PrefixLen : 64
     NextHop : 1::1                                   LocPrf    : 100
     PrefVal : 0                                      OutLabel  : NULL
     MED     : 0
     Path/Ogn: ?

* >  Network : 1::2                                   PrefixLen : 128
     NextHop : ::1                                    LocPrf    :
     PrefVal : 32768                                  OutLabel  : NULL
     MED     : 0
     Path/Ogn: ?

* >  Network : 2::2                                   PrefixLen : 128
     NextHop : ::1                                    LocPrf    :
     PrefVal : 32768                                  OutLabel  : NULL
     MED     : 0
     Path/Ogn: ?

* >i Network : 5::5                                   PrefixLen : 128
     NextHop : 1::1                                   LocPrf    : 100
     PrefVal : 0                                      OutLabel  : NULL
     MED     : 0
     Path/Ogn: ?
```

Display information about BGP IPv6 multicast routes that match AS path list 1.

```
<Sysname> display bgp routing-table ipv6 multicast as-path-acl 1

 Total number of routes: 5

 BGP local router ID is 192.168.1.139
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e - external
```

```
       Origin: i - IGP, e - EGP, ? - incomplete

* >  Network : 1::                                      PrefixLen : 64
     NextHop : ::                                       LocPrf    :
     PrefVal : 32768                                    OutLabel  : NULL
     MED     : 0
     Path/Ogn: ?

*  i Network : 1::                                      PrefixLen : 64
     NextHop : 1::1                                     LocPrf    : 100
     PrefVal : 0                                        OutLabel  : NULL
     MED     : 0
     Path/Ogn: ?

* >  Network : 1::2                                     PrefixLen : 128
     NextHop : ::1                                      LocPrf    :
     PrefVal : 32768                                    OutLabel  : NULL
     MED     : 0
     Path/Ogn: ?

* >  Network : 2::2                                     PrefixLen : 128
     NextHop : ::1                                      LocPrf    :
     PrefVal : 32768                                    OutLabel  : NULL
     MED     : 0
     Path/Ogn: ?

* >i Network : 5::5                                     PrefixLen : 128
     NextHop : 1::1                                     LocPrf    : 100
     PrefVal : 0                                        OutLabel  : NULL
     MED     : 0
     Path/Ogn: ?
```

Display information about BGP IPv6 multicast routes that match BGP community list 100.

```
<Sysname> display bgp routing-table ipv6 multicast community-list 100

 Total number of routes: 5

 BGP local router ID is 192.168.1.139
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e - external
       Origin: i - IGP, e - EGP, ? - incomplete

* >  Network : 1::                                      PrefixLen : 64
     NextHop : ::                                       LocPrf    :
     PrefVal : 32768                                    OutLabel  : NULL
     MED     : 0
     Path/Ogn: ?

*  i Network : 1::                                      PrefixLen : 64
```

```
     NextHop : 1::1                                  LocPrf    : 100
     PrefVal : 0                                     OutLabel  : NULL
     MED     : 0
     Path/Ogn: ?

* >  Network : 1::2                                  PrefixLen : 128
     NextHop : ::1                                   LocPrf    :
     PrefVal : 32768                                 OutLabel  : NULL
     MED     : 0
     Path/Ogn: ?

* >  Network : 2::2                                  PrefixLen : 128
     NextHop : ::1                                   LocPrf    :
     PrefVal : 32768                                 OutLabel  : NULL
     MED     : 0
     Path/Ogn: ?

* >i Network : 5::5                                  PrefixLen : 128
     NextHop : 1::1                                  LocPrf    : 100
     PrefVal : 0                                     OutLabel  : NULL
     MED     : 0
     Path/Ogn: ?
```

Display information about all BGP IPv6 multicast routes advertised to peer 1::1.

```
<Sysname> display bgp routing-table ipv6 multicast peer 1::1 advertised-routes

 Total number of routes: 2

 BGP local router ID is 192.168.1.139
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e - external
       Origin: i - IGP, e - EGP, ? - incomplete

* >  Network : 1::                                   PrefixLen : 64
     NextHop : ::                                    LocPrf    : 100
     MED     : 0                                     OutLabel  : NULL
     Path/Ogn: ?

* >  Network : 2::2                                  PrefixLen : 128
     NextHop : ::1                                   LocPrf    : 100
     MED     : 0                                     OutLabel  : NULL
     Path/Ogn: ?
```

Display information about all BGP IPv6 multicast routes received from peer 1::1.

```
<Sysname> display bgp routing-table ipv6 multicast peer 1::1 received-routes

 Total number of routes: 2

 BGP local router ID is 192.168.1.139
 Status codes: * - valid, > - best, d - dampened, h - history
```

```
                s - suppressed, S - stale, i - internal, e - external
       Origin: i - IGP, e - EGP, ? - incomplete

*  i Network : 1::                                    PrefixLen : 64
     NextHop : 1::1                                   LocPrf    : 100
     PrefVal : 0                                      OutLabel  : NULL
     MED     : 0
     Path/Ogn: ?

* >i Network : 5::5                                   PrefixLen : 128
     NextHop : 1::1                                   LocPrf    : 100
     PrefVal : 0                                      OutLabel  : NULL
     MED     : 0
     Path/Ogn: ?
```

Table 31 Command output

Field	Description
Status codes	Status codes: • *** – valid**—Valid route. • **> – best**—Optimal route. • **d – dampened**—Dampened route. • **h – history**—History route. • **s – suppressed**—Suppressed route. • **S – stale**—Stale route. • **i – internal**—Internal route. • **e – external**—External route.
Origin	Origin of the route: • **i – IGP**—Originated in the AS. The origin of routes advertised with the **`network`** command is IGP. • **e – EGP**—Learned through EGP. • **?– incomplete**—Unknown origin. The origin of routes redistributed from IGP protocols is INCOMPLETE.
Network	Destination network address.
PrefixLen	Prefix length of the destination network address.
NextHop	Next hop IP address.
LocPrf	Local preference value.
PrefVal	Preferred value of the route.
OutLabel	Outgoing label of the route.
MED	MULTI_EXIT_DISC attribute.
Path/Ogn	AS_PATH and ORIGIN attributes of the route: • **AS_PATH**—Records the ASs the route has passed, which avoids routing loops. • **ORIGIN**—Identifies the origin of the route.

Display detailed information about BGP IPv6 multicast routes destined to network 2::2/128.

```
<Sysname> display bgp routing-table ipv6 multicast 2::2 128
```

```
BGP local router ID: 192.168.1.139
Local AS number: 100

Paths:   1 available, 1 best

BGP routing table information of 2::2/128:
Imported route.
Original nexthop: ::1
OutLabel        : NULL
AS-path         : (null)
Origin          : incomplete
Attribute value : MED 0, pref-val 32768
State           : valid, local, best
Originator      : 176.1.1.2
Cluster list    : 80
IP precedence   : N/A
QoS local ID    : N/A
Traffic index   : N/A
VPN-Peer UserID : N/A
DSCP            : N/A
EXP             : N/A
```

Table 32 Command output

Field	Description
Paths	Number of routes: • **available**—Number of valid routes. • **best**—Number of optimal routes.
Original nexthop	Original next hop of the route. If the route was obtained from a BGP update message, the original next hop is the next hop IP address in the message.
OutLabel	Outgoing label of the route.
AS-path	AS_PATH attribute of the route, which records the ASs the route has passed and avoids routing loops.
Origin	Origin of the route: • **igp**—Originated in the AS. The origin of routes advertised with the **network** command is IGP. • **egp**—Learned through EGP. • **incomplete**—Unknown origin. The origin of routes redistributed from IGP protocols is INCOMPLETE.
Attribute value	BGP path attributes: • **MED**—MED value. • **localpref**—Local preference value. • **pref-val**—Preferred value. • **pre**—Route preference.

Field	Description
State	Current state of the route: • valid. • internal. • external. • local. • synchronize. • best.
Originator	Router ID of the peer that advertised the route to the reflector.
From	IP address of the BGP peer that advertised the route.
Rely Nexthop	Next hop found by route recursion. If no next hop is found, this field displays **not resolved**.
IP precedence	IP precedence in the range of 0 to 7. **N/A** indicates that the route does not support this field.
QoS local ID	QoS local ID in the range of 1 to 4095. **N/A** indicates that the route does not support this field.
Traffic index	Traffic index in the range of 1 to 64. **N/A** indicates that the route does not support this field.
VPN-Peer UserID	VPN peer ID in the range of 1 to 134217727. **N/A** indicates that the route does not support this field.
DSCP	DSCP value in the range of 0 to 63. **N/A** indicates that the route does not support this field.
EXP	MPLS EXP value of the route. **N/A** indicates that the route does not support this field.

Display advertisement information for BGP IPv6 multicast routes destined to network 2::2/128.

```
<Sysname> display bgp routing-table ipv6 multicast 2::2 128 advertise-info

 BGP local router ID: 192.168.1.139
 Local AS number: 100

 Paths:   1 best

 BGP routing table information of 2::2/128:
 Advertised to peers (1 in total):
    1::1
```

Table 33 Command output

Field	Description
BGP local router ID	Local BGP router ID.
Local AS number	Local AS number.
Paths	Number of optimal routes to the destination.
BGP routing table information of 2::2/128	Advertisement information for network 2::2/128.
Advertised to peers (1 in total)	Peers to which the network has been advertised.

Display statistics for BGP IPv6 multicast routes advertised to peer 1::1.

```
<Sysname> display bgp routing-table ipv6 multicast peer 1::1 advertised-routes statistics

 Advertised routes total: 2
```

Display statistics for BGP IPv6 multicast routes received from peer 1::1.

```
<Sysname> display bgp routing-table ipv6 multicast peer 1::1 received-routes statistics

 Received routes total: 2
```

Table 34 Command output

Field	Description
Advertised routes total	Total number of advertised routes.
Received routes total	Total number of received routes.

Display BGP IPv6 multicast route statistics.

```
<Sysname> display bgp routing-table ipv6 multicast statistics

 Total number of routes: 5
```

Table 35 Command output

Field	Description
Total number of routes	Total number of routes.

Related commands

ip as-path

ip community-list

display bgp routing-table ipv6 unicast

Use **display bgp routing-table ipv6 unicast** to display BGP IPv6 unicast routing information.

Syntax

display bgp [**instance** *instance-name*] **routing-table ipv6** [**unicast**] [**vpn-instance** *vpn-instance-name*] [*ipv6-address prefix-length* [**advertise-info**] | **as-path-acl** *as-path-acl-number* | **community-list** { { *basic-community-list-number* | *comm-list-name* } [**whole-match**] | *adv-community-list-number* } | **peer** *ipv6-address* { **advertised-routes** | **received-routes** } [*ipv6-address prefix-length* | **statistics**] | **statistics**]

display bgp [**instance** *instance-name*] **routing-table ipv6** [**unicast**] **peer** *ipv4-address* { **advertised-routes** | **received-routes** } [*ipv6-address prefix-length* | **statistics**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

instance *instance-name*: Specifies a BGP instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command displays BGP IPv6 unicast routing information for the default BGP instance.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays the BGP IPv6 unicast routing information for the public network.

ipv6-address prefix-length: Specifies the destination network address and prefix length. The value range for the *prefix-length* argument is 0 to 128. If you do not specify this argument, the command displays brief information about all BGP IPv6 unicast routing information.

advertise-info: Displays advertisement information for BGP IPv6 unicast routes. If you do not specify this keyword, the command displays the BGP IPv6 unicast routing table.

as-path-acl *as-path-acl-number*: Displays BGP IPv6 unicast routes that match the AS path list specified by its number in the range of 1 to 256.

community-list: Displays BGP IPv6 unicast routes that match a community list.

basic-community-list-number: Specifies a basic community list by its number in the range of 1 to 99.

comm-list-name: Specifies a community list by its name, a case-sensitive string of 1 to 63 characters.

whole-match: Displays routes exactly matching the specified community list. If you do not specify this keyword, the command displays routes whose COMMUNITY attributes include the specified community list.

adv-community-list-number: Specifies an advanced community list by its number in the range of 100 to 199.

peer: Displays BGP IPv6 unicast routing information advertised to or received from the specified peer.

ipv4-address: Specifies the peer IPv4 address.

ipv6-address: Specifies the peer IPv6 address.

advertised-routes: Displays routing information advertised to the specified peer.

received-routes: Displays routing information received from the specified peer.

statistics: Displays routing statistics.

Usage guidelines

This command displays BGP IPv6 unicast routing information regardless of whether the **unicast** keyword is specified.

Examples

Display brief information about all BGP IPv6 unicast routes.

```
<Sysname> display bgp routing-table ipv6

 Total number of routes: 1

 BGP local router ID is 192.168.1.136
```

```
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e - external
       Origin: i - IGP, e - EGP, ? - incomplete

* >e Network : 3::                                    PrefixLen : 64
     NextHop : 1::2                                   LocPrf    :
     PrefVal : 0                                      OutLabel  : NULL
     MED     :
     Path/Ogn: 4294967295 4294967294 4294967293 4294967292 4294967291 4294967290
4294967215 4294967225 4294967235 4294967245 4294967295 4294967294 4294967293 4294967292
4294967291 4294967290 i
```

Display information about BGP IPv6 unicast routes that match AS path list 1.

```
<Sysname> display bgp routing-table ipv6 as-path-acl 1

 Total number of routes: 2

 BGP local router ID is 192.168.1.136
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e - external
       Origin: i - IGP, e - EGP, ? - incomplete

* >e Network : 2::                                    PrefixLen : 64
     NextHop : 1::2                                   LocPrf    :
     PrefVal : 0                                      OutLabel  : NULL
     MED     :
     Path/Ogn: 100i

* >e Network : 3::                                    PrefixLen : 64
     NextHop : 1::2                                   LocPrf    :
     PrefVal : 0                                      OutLabel  : NULL
     MED     :
     Path/Ogn: 100i
```

Display information about BGP IPv6 unicast routes that match BGP community list 100.

```
<Sysname> display bgp routing-table ipv6 community-list 100

 Total number of routes: 2

 BGP local router ID is 192.168.1.136
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e - external
       Origin: i - IGP, e - EGP, ? - incomplete

* >e Network : 2::                                    PrefixLen : 64
     NextHop : 1::2                                   LocPrf    :
     PrefVal : 0                                      OutLabel  : NULL
     MED     :
     Path/Ogn: 100i
```

```
* >e Network : 3::                                    PrefixLen : 64
     NextHop : 1::2                                   LocPrf    :
     PrefVal : 0                                      OutLabel  : NULL
     MED     :
     Path/Ogn: 100i
```

Display information about all BGP IPv6 unicast routes advertised to peer 1::1.

```
<Sysname> display bgp routing-table ipv6 peer 1::1 advertised-routes

 Total number of routes: 1

 BGP local router ID is 192.168.1.136
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e - external
       Origin: i - IGP, e - EGP, ? - incomplete

* >  Network : 2::                                    PrefixLen : 64
     NextHop : ::                                     LocPrf    :
     MED     : 0                                      OutLabel  : NULL
     Path/Ogn: i
```

Display information about all BGP IPv6 unicast routes received from peer 1::1.

```
<Sysname> display bgp routing-table ipv6 peer 1::1 received-routes

 Total number of routes: 1

 BGP local router ID is 192.168.1.135
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e - external
       Origin: i - IGP, e - EGP, ? - incomplete

* >e Network : 2::                                    PrefixLen : 64
     NextHop : ::FFFF:10.1.1.1                        LocPrf    :
     PrefVal : 0                                      OutLabel  : NULL
     MED     : 0
     Path/Ogn: 100i
```

Table 36 Command output

Field	Description
Status codes	Status codes: • *** – valid**—Valid route. • **> – best**—Optimal route. • **d – dampened**—Dampened route. • **h – history**—History route. • **s – suppressed**—Suppressed route. • **S – stale**—Stale route. • **i – internal**—Internal route. • **e – external**—External route.

Field	Description
Origin	Origin of the route: • **i – IGP**—Originated in the AS. The origin of routes advertised with the **network** command is IGP. • **e – EGP**—Learned through EGP. • **?– incomplete**—Unknown origin. The origin of routes redistributed from IGP protocols is INCOMPLETE.
Network	Destination network address.
PrefixLen	Prefix length of the destination network address.
NextHop	Next hop IPv6 address.
LocPrf	Local preference value.
PrefVal	Preferred value of the route.
OutLabel	Outgoing label of the route.
MED	MULTI_EXIT_DISC attribute.
Path/Ogn	AS_PATH and ORIGIN attributes of the route: • **AS_PATH attribute**—Records the ASs the route has passed, which avoids routing loops. This field can display a maximum of 16 AS numbers. More AS numbers are omitted and can be viewed in the detailed route information. • **ORIGIN attribute**—Identifies the origin of the route.

Display detailed information about BGP IPv6 unicast routes destined to network 2::/64.

```
<Sysname> display bgp routing-table ipv6 2:: 64

 BGP local router ID: 192.168.1.135
 Local AS number: 200

 Paths:   2 available, 1 best

 BGP routing table information of 2::/64:
 From            : 10.1.1.1 (192.168.1.136)
 Relay nexthop   : ::FFFF:10.1.1.1
 Original nexthop: ::FFFF:10.1.1.1
 OutLabel        : NULL
 AS-path         : 100
 Origin          : igp
 Attribute value : MED 0, pref-val 0
 State           : valid, external, best
 Originator      : 176.1.1.2
 Cluster list    : 80
 IP precedence   : N/A
 QoS local ID    : N/A
 Traffic index   : N/A
 VPN-Peer UserID : N/A
 DSCP            : N/A
 EXP             : N/A
```

```
Backup route.
From            : 1::1 (192.168.1.136)
Relay nexthop   : 1::1
Original nexthop: 1::1
OutLabel        : NULL
AS-path         : 100
Origin          : igp
Attribute value : MED 0, pref-val 0
State           : valid, external
IP precedence   : N/A
QoS local ID    : N/A
Traffic index   : N/A
VPN-Peer UserID : N/A
DSCP            : N/A
EXP             : N/A
```

Table 37 Command output

Field	Description
Paths	Number of routes: • **available**—Number of valid routes. • **best**—Number of optimal routes.
Original nexthop	Original next hop of the route. If the route was obtained from a BGP update message, the original next hop is the next hop IP address in the message.
OutLabel	Outgoing label of the route.
AS-path	AS_PATH attribute of the route, which records the ASs the route has passed and avoids routing loops.
Origin	Origin of the route: • **igp**—Originated in the AS. The origin of routes advertised with the **network** command is IGP. • **egp**—Learned through EGP. • **incomplete**—Unknown origin. The origin of routes redistributed from IGP protocols is INCOMPLETE.
Attribute value	BGP path attributes: • **MED**—MED value. • **localpref**—Local preference value. • **pref-val**—Preferred value. • **pre**—Route preference.
State	Current state of the route: • valid. • internal. • external. • local. • best.
Originator	Router ID of the peer that advertised the route to the reflector.
From	IP address of the BGP peer that advertised the route.
Relay Nexthop	Next hop found by route recursion. If no next hop is found, this field displays **not resolved**.

Field	Description
IP precedence	IP precedence in the range of 0 to 7. **N/A** indicates that the route does not support this field.
QoS local ID	QoS local ID in the range of 1 to 4095. **N/A** indicates that the route does not support this field.
Traffic index	Traffic index in the range of 1 to 64. **N/A** indicates that the route does not support this field.
VPN-Peer UserID	VPN peer ID in the range of 1 to 134217727. **N/A** indicates that the route does not support this field.
DSCP	DSCP value in the range of 0 to 63. **N/A** indicates that the route does not support this field.
Backup route	The route is a backup route.
EXP	MPLS EXP value of the route. **N/A** indicates that the route does not support this field.
Tunnel policy	Tunnel policy that takes effect. **NULL** indicates that no tunnel policy takes effect.
Rely Tunnel IDs	Tunnel index IDs after route recursion. This field displays multiple tunnel index IDs if ECMP tunnels exist and displays **N/A** if no tunnels are found by route recursion.

Display advertisement information for BGP IPv6 unicast routes destined to network 2::/64.

```
<Sysname> display bgp routing-table ipv6 2:: 64 advertise-info

 BGP local router ID: 192.168.1.136
 Local AS number: 100

 Paths:   1 best

 BGP routing table information of 2::/64:
 Advertised to peers (2 in total):
    10.1.1.2
    1::2
```

Table 38 Command output

Field	Description
Paths	Number of optimal routes destined to the specified network.
BGP routing table information of 2::/64	Advertisement information for BGP routes destined to network 2::/64.
Advertised to peers (2 in total)	Peers to which the route has been advertised, and the number of peers.

Display statistics for BGP IPv6 unicast routes advertised to peer 1::1.

```
<Sysname> display bgp routing-table ipv6 peer 1::1 advertised-routes statistics

 Advertised routes total: 1
```

Display statistics for BGP IPv6 unicast routes received from peer 1::1.

```
<Sysname> display bgp routing-table ipv6 peer 1::1 received-routes statistics
```

```
Received routes total: 1
```

Table 39 Command output

Field	Description
Advertised routes total	Total number of advertised routes.
Received routes total	Total number of received routes.

Display BGP IPv6 unicast route statistics.

```
<Sysname> display bgp routing-table ipv6 statistics

Total number of routes: 4
```

Table 40 Command output

Field	Description
Total number of routes	Total number of routes.

Related commands

ip as-path

ip community-list

display bgp routing-table ipv6 unicast inlabel

Use **display bgp routing-table ipv6 unicast inlabel** to display incoming labels for BGP IPv6 unicast routes.

Syntax

display bgp [**instance** *instance-name*] **routing-table ipv6** [**unicast**] **inlabel**

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

instance *instance-name*: Specifies a BGP instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command displays incoming labels of BGP IPv6 unicast routes in the default BGP instance.

Usage guidelines

This command displays incoming labels for BGP IPv6 unicast routes regardless of whether the **unicast** keyword is specified.

Examples

Display incoming labels for all BGP IPv6 unicast routes.

```
<Sysname> display bgp routing-table ipv6 inlabel

 Total number of routes: 2

 BGP local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e - external
       Origin: i - IGP, e - EGP, ? - incomplete

* >  Network : 1::1                                    PrefixLen : 128
     NextHop : 10::1                                   OutLabel  : NULL
     InLabel : 1279

* >  Network : 10::                                    PrefixLen : 64
     NextHop : ::                                      OutLabel  : NULL
     InLabel : 1278
```

Table 41 Command output

Field	Description
Status codes	Status codes. For more information, see Table 36.
Origin	Origin of the route. For more information, see Table 36.
Network	Destination network address.
PrefixLen	Prefix length of the destination network address.
NextHop	Next hop IPv6 address.
OutLabel	Outgoing label of the IPv6 unicast route, which is assigned by the peer 6PE device.
InLabel	Incoming label of the IPv6 unicast route, which is assigned by the local 6PE device.

display bgp routing-table ipv6 unicast outlabel

Use **display bgp routing-table ipv6 unicast outlabel** to display outgoing labels for BGP IPv6 unicast routes.

Syntax

display bgp [**instance** *instance-name*] **routing-table ipv6** [**unicast**] **outlabel**

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

instance *instance-name*: Specifies a BGP instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command display outgoing labels of BGP IPv6 unicast routes in the default BGP instance.

Usage guidelines

This command displays outgoing labels for BGP IPv6 unicast routes regardless of whether the **unicast** keyword is specified.

Examples

Display outgoing labels for all BGP IPv6 unicast routes.

```
<Sysname> display bgp routing-table ipv6 outlabel

 Total number of routes: 2

 BGP local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e - external
       Origin: i - IGP, e - EGP, ? - incomplete

* >i Network : 4::4                                    PrefixLen : 128
     NextHop : ::FFFF:3.3.3.3                         OutLabel  : 1279

* >i Network : 20::                                    PrefixLen : 64
     NextHop : ::FFFF:3.3.3.3                         OutLabel  : 1278
```

Table 42 Command output

Field	Description
Status codes	Status codes. For more information, see Table 36.
Origin	Origin of the route. For more information, see Table 36.
Network	Destination network address.
PrefixLen	Prefix length of the destination network address.
NextHop	Next hop IPv6 address.
OutLabel	Outgoing label of the IPv6 unicast route, which is assigned by the peer 6PE device.

display bgp update-group

Use **display bgp update-group** to display information about BGP update groups.

Syntax

display bgp [**instance** *instance-name*] **update-group ipv4** [**mdt** | **multicast** | **mvpn** | **rtfilter** | [**flowspec** | **unicast**] [**vpn-instance** *vpn-instance-name*]] [*ipv4-address*]

display bgp [**instance** *instance-name*] **update-group ipv6** [**multicast** | [**unicast**] [**vpn-instance** *vpn-instance-name*]] [*ipv6-address*]

display bgp [**instance** *instance-name*] **update-group ipv6** [**unicast**] [*ipv4-address*]

display bgp [**instance** *instance-name*] **update-group link-state** [*ipv4-address* | *ipv6-address*]

display bgp [**instance** *instance-name*] **update-group vpnv4** [**flowspec** | **vpn-instance** *vpn-instance-name*] [*ipv4-address*]

display bgp [**instance** *instance-name*] **update-group vpnv6** [*ipv4-address*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

instance *instance-name*: Specifies a BGP instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command displays BGP update group information for the default BGP instance.

flowspec: Displays BGP update group information for flowspec address family.

ipv4: Displays BGP update group information for IPv4 address family.

ipv6: Displays BGP update group information for IPv6 address family.

link-state: Displays BGP update group information for LS address family.

vpnv4: Displays BGP update group information for VPNv4 address family.

vpnv6: Displays BGP update group information for VPNv6 address family.

mdt: Displays BGP update group information for MDT address family.

multicast: Displays BGP update group information for multicast address family.

mvpn: Displays BGP update group information for IPv4 MVPN address family.

rtfilter: Displays BGP update group information for BGP IPv4 RT filter address family.

The following compatibility matrixes show the support of hardware platforms for the **rtfilter** keyword:

Models	Parameter compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	No

unicast: Displays BGP update group information for unicast address family.

vpn-instance *vpn-instance-name*: Displays BGP update group information for the MPLS L3VPN instance specified by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays update group information for the public network.

ipv4-address: Displays BGP update group information for the specified BGP peer.

ipv6-address: Displays BGP update group information for the specified IPv6 BGP peer.

Usage guidelines

The update group feature classifies BGP peers that have the same export policy into an update group. When BGP advertises routes to the peers in the update group, it uses the export policy to filter the routes and generates route updates for all the peers only once.

With this feature, BGP performs one-time policy filtering and encapsulation for a prefix before advertising the prefix to all the peers in the update group. For example, BGP advertises 1000 prefixes to 1000 peers that have the same export policy (in data centers for example). Without the update group feature, BGP matches the export policy 1000 × 1000 times. With the update group feature, BGP matches the export policy only 1000 × 1 times, improving encapsulation efficiency 1000 times.

If you do not specify any parameters, this command displays all update groups for the specified address family on the public network.

By default, the **unicast** keyword is used if the **unicast**, **mdt**, **mvpn**, **rtfilter**, **multicast**, and **flowspec** keywords are not specified.

Examples

Display information about all BGP update groups for the IPv4 unicast address family.

```
<Sysname> display bgp update-group ipv4


  Update-group ID: 0
  Type: EBGP link
  4-byte AS number: Supported
  Site-of-Origin: Not specified
  Minimum time between advertisements: 30 seconds
  OutQ: 0
  Members: 1
    99.1.1.1
```

Table 43 Command output

Field	Description
Update-group ID	ID of the update group.
Type	BGP link type: • **IBGP link**. • **EBGP link**. • **Confed IBGP link**—Confederation IBGP link. • **Confed EBGP link**—Confederation EBGP link.
Label capability: Supported	This field is not supported in the current software version. The peers in the update group support labeled routes.
4-byte AS number: Supported	4-byte AS number suppression is disabled for the peers in the update group. The peers in the update group support 4-byte AS numbers.
4-byte AS number: Suppressed	4-byte AS number suppression is enabled for the peers in the update group.
Fake AS	A fake local AS number is configured for the peers in the update group.

Field	Description
Public-AS-Only: Yes	BGP route updates advertised to the peers in the update group only carry the public AS number without the private AS number. • **Yes**—If a peer uses a private AS number, the AS number is used as an update group classification criterion. If a peer uses a public AS number, the AS number is not used as an update group classification criterion. • **No**—The AS number is not used as an update group classification criterion.
Substitute-AS: Yes	AS number substitution is enabled.
Minimum time between advertisements: number seconds	Minimum time between advertisements.
Advertising community: Yes	Community advertisement to peers in the update group is enabled.
Route-reflect client: Yes	The peer is a client of the route reflector.
Advertising extended community: Yes	Extended community advertisement to peers in the update group is enabled.
Export AS-path-ACL	AS path ACL used to filter BGP routes advertised to peers in the update group.
Export prefix list	Prefix list used to filter BGP routes advertised to peers in the update group.
Export route policy	Routing policy used to filter BGP routes advertised to peers in the update group.
Export filter-policy	ACL used to filter BGP routes advertised to peers in the update group.
OutQ	Number of prefixes to be advertised to peers in the update group.
Members	Number and IP addresses of peers in the update group.
Nesting VPN	Peers in the update group support nesting VPN.
UPE: Yes	Peers in the update group are UPE devices.
UPE export route policy	An outgoing routing policy is applied to peers in the update group.

domain-distinguisher

Use **domain-distinguisher** to specify an AS number and a router ID for BGP LS messages.

Use **undo domain-distinguisher** to restore the default.

Syntax

domain-distinguisher *as-number:router-id*

undo domain-distinguisher

Default

The AS number and router ID of the current BGP process are used.

Views

BGP LS address family view

Predefined user roles

network-admin

context-admin

Parameters

as-number:router-id: Specifies the AS number and router ID. The value range for the *as-number* argument is 1 to 4294967295, and the router ID is in IP address format.

Examples

Set the AS number and router ID for BGP LS messages to 65009 and 1.1.1.1, respectively.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family link-state
[Sysname-bgp-default-ls] domain-distinguisher 65009:1.1.1.1
```

ebgp-interface-sensitive

Use **ebgp-interface-sensitive** to enable immediate re-establishment of direct EBGP sessions.

Use **undo ebgp-interface-sensitive** to disable immediate re-establishment of direct EBGP sessions.

Syntax

ebgp-interface-sensitive

undo ebgp-interface-sensitive

Default

Immediate re-establishment of direct EBGP sessions is enabled.

Views

BGP instance view

Predefined user roles

network-admin

context-admin

Usage guidelines

When a direct link to an EBGP peer fails, BGP tears down the session and re-establishes a session to the peer immediately. If the feature is not enabled, the router does not tear down the session until the hold time expires. However, disabling this feature can prevent routing flaps from affecting EBGP session state.

This command applies only to direct EBGP sessions.

Examples

Enable immediate re-establishment of direct EBGP sessions.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] ebgp-interface-sensitive
```

fast-reroute route-policy

Use **fast-reroute route-policy** to apply a routing policy to fast reroute (FRR) for a BGP address family.

Use **undo fast-reroute route-policy** to restore the default.

Syntax

fast-reroute route-policy *route-policy-name*

undo fast-reroute route-policy

Default

No routing policy is applied to FRR.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

Predefined user roles

network-admin

context-admin

Parameters

route-policy-name: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

You can use the following methods to configure BGP FRR:

- **Method 1**—Execute the **pic** command in BGP address family view. BGP calculates a backup next hop for a BGP route in the address family if there are two or more unequal-cost routes to reach the destination.
- **Method 2**—Execute the **fast-reroute route-policy** command to use a routing policy in which a backup next hop is specified by using the command **apply** [**ipv6**] **fast-reroute backup-nexthop**. For BGP to generate a backup next hop for the primary route, the backup next hop calculated by BGP must be the same as the specified backup next hop. You can also configure **if-match** clauses in the routing policy to identify the routes protected by FRR.

If both methods are configured, Method 2 takes precedence over Method 1.

Examples

Apply routing policy **frr-policy** to FRR in BGP IPv4 unicast address family view.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4
[Sysname-bgp-default-ipv4] fast-reroute route-policy frr-policy
```

Related commands

apply fast-reroute

apply ipv6 fast-reroute

pic

route-policy

filter-policy export

Use **filter-policy export** to filter advertised BGP routes.

Use **undo filter-policy export** to remove the route filter.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view/BGP VPNv4 address family view/BGP IPv4 multicast address family view:

filter-policy { *ipv4-acl-number* | **prefix-list** *ipv4-prefix-list-name* } **export** [**direct** | { **isis** | **ospf** | **rip** } *process-id* | **static**]

undo filter-policy export [**direct** | { **isis** | **ospf** | **rip** } *process-id* | **static**]

In BGP IPv6 unicast address family view/BGP-VPN IPv6 unicast address family view/BGP VPNv6 address family view/BGP IPv6 multicast address family view:

filter-policy { *ipv6-acl-number* | **prefix-list** *ipv6-prefix-list-name* } **export** [**direct** | { **isisv6** | **ospfv3** | **ripng** } *process-id* | **static**]

undo filter-policy export [**direct** | { **isisv6** | **ospfv3** | **ripng** } *process-id* | **static**]

Default

Advertised BGP routes are not filtered.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP VPNv4 address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

BGP VPNv6 address family view

BGP IPv4 multicast address family view

BGP IPv6 multicast address family view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-acl-number: Specifies an IPv4 ACL by its number in the range of 2000 to 3999, to match routes by destination.

ipv6-acl-number: Specifies an IPv6 ACL by its number in the range of 2000 to 3999, to match routes by destination.

prefix-list *ipv4-prefix-list-name*: Specifies an IPv4 prefix list by its name, a case-sensitive string of 1 to 63 characters, to match routes by destination.

prefix-list *ipv6-prefix-list-name*: Specifies an IPv6 prefix list by its name, a case-sensitive string of 1 to 63 characters, to match routes by destination.

direct: Filters direct routes.

isis: Filters IS-IS routes.

isisv6: Filters IPv6 IS-IS routes.

ospf: Filters OSPF routes.

ospfv3: Filters OSPFv3 routes.

rip: Filters RIP routes.

ripng: Filters RIPng routes.

static: Filters static routes.

process-id: Specifies a routing protocol by its ID in the range of 1 to 65535.

Usage guidelines

If you specify a protocol (such as **direct** and **isis**), this command filters only routes redistributed from the specified protocol. If you do not specify a protocol, this command filters all advertised routes, including the following routes:

- Redistributed from IGP.
- Injected by the **network** command.
- Learned from BGP peers.

If you use a basic ACL (with a number from 2000 to 2999) configured with the **rule** [*rule-id*] { **deny** | **permit** } **source** *source-address source-wildcard* command, the command matches routes whose destination network addresses match the *source-address source-wildcard* argument. However, it does not match the masks of the destination addresses.

To use an advanced ACL (with a number from 3000 to 3999) in the command, configure the ACL using one of the following steps:

- To deny/permit a route with the specified destination, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* command.
- To deny/permit a route with the specified destination and mask, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* **destination** *dest-addr dest-wildcard* command.

The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the subnet mask of the destination address. For the mask configuration to take effect, specify a contiguous subnet mask.

Examples

In BGP IPv4 unicast address family view, use IPv4 basic ACL 2000 to filter advertised BGP IPv4 routes.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4] filter-policy 2000 export
```

Related commands

filter-policy import

peer as-path-acl

peer filter-policy

peer prefix-list

peer route-policy

filter-policy import

Use **filter-policy import** to filter received BGP routes.

Use **undo filter-policy import** to restore the default.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view/BGP VPNv4 address family view/BGP IPv4 multicast address family view:

filter-policy { *ipv4-acl-number* | **prefix-list** *ipv4-prefix-list-name* } **import**

undo filter-policy import

In BGP IPv6 unicast address family view/BGP-VPN IPv6 unicast address family view/BGP VPNv6 address family view/BGP IPv6 multicast address family view:

filter-policy { *ipv6-acl-number* | **prefix-list** *ipv6-prefix-list-name* } **import**

undo filter-policy import

Default

Received BGP routes are not filtered.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP VPNv4 address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

BGP VPNv6 address family view

BGP IPv4 multicast address family view

BGP IPv6 multicast address family view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-acl-number: Specifies an IPv4 ACL by its number in the range of 2000 to 3999, to match routes by destination.

ipv6-acl-number: Specifies an IPv6 ACL by its number in the range of 2000 to 3999, to match routes by destination.

prefix-list *ipv4-prefix-list-name*: Specifies an IPv4 prefix list by its name, a case-sensitive string of 1 to 63 characters, to match routes by destination.

prefix-list *ipv6-prefix-list-name*: Specifies an IPv6 prefix list by its name, a case-sensitive string of 1 to 63 characters, to match routes by destination.

Usage guidelines

If you use a basic ACL (with a number from 2000 to 2999) configured with the **rule** [*rule-id*] { **deny** | **permit** } **source** *source-address source-wildcard* command, the command matches routes whose destination network addresses match the *source-address source-wildcard* argument. However, it does not match the masks of the destination addresses.

To use an advanced ACL (with a number from 3000 to 3999) in the command, configure the ACL using one of the following steps:

- To deny/permit a route with the specified destination, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* command.
- To deny/permit a route with the specified destination and mask, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* **destination** *dest-addr dest-wildcard* command.

The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the subnet mask of the destination address. For the mask configuration to take effect, specify a contiguous subnet mask.

Examples

In BGP IPv4 unicast address family view, use IPv4 basic ACL 2000 to filter received BGP routes.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4] filter-policy 2000 import
```

Related commands

filter-policy export

peer as-path-acl

peer filter-policy

peer prefix-list

peer route-policy

flush suboptimal-route

Use **flush suboptimal-route** to enable BGP to flush the suboptimal BGP route to the RIB.

Use **undo flush suboptimal-route** to disable BGP from flushing the suboptimal BGP route to the RIB.

Syntax

flush suboptimal-route

undo flush suboptimal-route

Default

BGP is disabled from flushing the suboptimal BGP route to the RIB. Only the optimal route is flushed to the RIB.

Views

BGP instance view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command flushes the suboptimal BGP route to the RIB when the following conditions are met:

- The optimal route is generated by the **network** command or is redistributed by the **import-route** command.
- The suboptimal route is received from a BGP peer.

After the suboptimal route is flushed to the RIB on a network, BGP immediately switches traffic to the suboptimal route when the optimal route fails.

For example, the device has a static route to the subnet 1.1.1.0/24 that has a higher priority than a BGP route. BGP redistributes the static route and receives a route to 1.1.1.0/24 from a peer. After the **flush suboptimal-route** command is executed, BGP flushes the received BGP route to the RIB as the suboptimal route. When the static route fails, BGP immediately switches traffic to the suboptimal route if inter-protocol FRR is enabled. For more information about inter-protocol FRR, see *Layer 3—IP Routing Configuration Guide*.

Examples

Enable BGP to flush the suboptimal BGP route to the RIB.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] flush suboptimal-route
```

graceful-restart

Use **graceful-restart** to enable BGP Graceful Restart (GR) capability.

Use **undo graceful-restart** to disable BGP GR capability.

Syntax

graceful-restart

undo graceful-restart

Default

BGP GR capability is disabled.

Views

BGP instance view

Predefined user roles

network-admin

context-admin

Usage guidelines

GR ensures continuous forwarding when BGP restarts or an active/standby switchover occurs.

BGP peers exchange Open messages containing GR information. If both parties have GR capability, they establish a GR-capable session.

After you execute this command, the device re-establishes BGP sessions.

Examples

Enable GR capability for BGP process 100.

```
<Sysname> system-view
[Sysname] bgp 100
```

```
[Sysname-bgp-default] graceful-restart
```

Related commands

graceful-restart timer purge-time

graceful-restart timer restart

graceful-restart timer wait-for-rib

graceful-restart timer purge-time

Use **graceful-restart timer purge-time** to set the Routing Information Base (RIB) purge timer.

Use **undo graceful-restart timer purge-time** to restore the default.

Syntax

graceful-restart timer purge-time *timer*

undo graceful-restart timer purge-time

Default

The RIB purge timer is 480 seconds.

Views

BGP instance view

Predefined user roles

network-admin

context-admin

Parameters

timer: Sets the RIB purge timer in the range of 1 to 6000 seconds.

Usage guidelines

BGP starts the RIB purge timer when an active/standby switchover occurs or BGP restarts. If BGP route exchange is not completed within the RIB purge timer, the GR restarter quits the GR process. It updates the RIB with the BGP routes already learned, and removes the stale routes from RIB.

Enable BGP GR before you execute this command.

Set the RIB purge timer to be long enough to complete GR, especially when large numbers of BGP routes exist.

As a best practice, set the RIB purge timer in the following way:

- Set the timer to be greater than the timer set by the **graceful-restart timer wait-for-rib** command
- Set the timer to be less than the timer set by the **protocol lifetime** command.

Examples

Set the RIB purge timer to 300 seconds.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] graceful-restart
[Sysname-bgp-default] graceful-restart timer purge-time 300
```

Related commands

graceful-restart

graceful-restart timer restart

graceful-restart timer wait-for-rib

protocol lifetime (*Layer 3—IP Routing Command Reference*)

graceful-restart timer restart

Use **graceful-restart timer restart** to configure the GR timer.

Use **undo graceful-restart timer restart** to restore the default.

Syntax

graceful-restart timer restart *timer*

undo graceful-restart timer restart

Default

The GR timer is 150 seconds.

Views

BGP instance view

Predefined user roles

network-admin

context-admin

Parameters

timer: Specifies the GR timer in the range of 3 to 600 seconds.

Usage guidelines

The GR restarter sends the GR timer to the GR helper in an Open message. When the GR helper detects that an active/standby switchover or a BGP restart occurred on the GR restarter, the GR helper performs the following operations:

1. Marks all routes learned from the GR restarter as stale.
2. Starts the GR timer.
3. If no BGP session is established before the GR timer expires, the GR helper removes the stale routes.

Before you configure this command, enable the BGP GR capability.

To apply a new GR timer, you must re-establish BGP sessions.

Examples

Set the GR timer to 300 seconds.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] graceful-restart
[Sysname-bgp-default] graceful-restart timer restart 300
```

Related commands

graceful-restart

graceful-restart timer purge-time

graceful-restart timer wait-for-rib

graceful-restart timer wait-for-rib

Use **graceful-restart timer wait-for-rib** to configure the time to wait for the End-of-RIB marker.

Use **undo graceful-restart timer wait-for-rib** to restore the default.

Syntax

graceful-restart timer wait-for-rib *timer*

undo graceful-restart timer wait-for-rib

Default

The time to wait for the End-of-RIB marker is 180 seconds.

Views

BGP instance view

Predefined user roles

network-admin

context-admin

Parameters

timer: Specifies the time to wait for the End-of-RIB marker, in the range of 3 to 3600 seconds.

Usage guidelines

BGP uses this timer to control the time to receive updates from the peer. The timer is not advertised to the peer.

After the GR restarter and GR helper re-establish a BGP session, they start this timer. If they do not complete route exchange within the time period, the GR restarter does not receive new routes. It updates its routing table and forwarding table with learned BGP routes, and the GR helper removes the stale routes. Set a large value for the maximum time to wait for the End-of-RIB marker when a large number of routes exist.

This command controls the routing convergence speed. A smaller timer value means faster routing convergence but possibly results in incomplete routing information.

Before configuring this command, you must enable the BGP GR capability.

Examples

Set the time to wait for the End-of-RIB marker on the local end to 100 seconds.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] graceful-restart
[Sysname-bgp-default] graceful-restart timer wait-for-rib 100
```

Related commands

graceful-restart

graceful-restart timer purge-time

graceful-restart timer restart

group

Use **group** to create a peer group.

Use **undo group** to delete a peer group.

Syntax

group *group-name* [**external** | **internal**]

undo group *group-name*

Default

No peer groups exist.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a name for the peer group, a case-sensitive string of 1 to 47 characters.

external: Creates an EBGP peer group.

internal: Creates an IBGP peer group.

Usage guidelines

In a large-scale network, many peers can use the same route selection policy. You can configure a peer group and add these peers into this group. In this way, peers can share the same policy as the peer group. When the policy of the group is modified, the modification also applies to peers in it.

If you do not specify the **internal** or **external** keyword, this command creates an IBGP peer group.

If you perform configurations on a peer group and peers of the peer group, the most recent configuration takes effect.

After you create a peer group, you must use the **peer enable** command to enable BGP to exchange routing information with the specified peer group.

Examples

In BGP instance view, create EBGP peer group **test** with AS number 200, and add EBGP peers 10.1.1.1 and 10.1.2.1 into the group.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] group test external
[Sysname-bgp-default] peer test as-number 200
[Sysname-bgp-default] peer 10.1.1.1 group test
[Sysname-bgp-default] peer 10.1.2.1 group test
```

Related commands

display bgp group

peer enable

ignore-first-as

Use **ignore-first-as** to configure BGP to ignore the first AS number of EBGP route updates.

Use **undo ignore-first-as** to restore the default.

Syntax

ignore-first-as

undo ignore-first-as

Default

BGP checks the first AS number of a received EBGP route update. If the first AS number is neither that of the BGP peer nor a private AS number, the BGP router disconnects the BGP session to the peer.

Views

BGP instance view

Predefined user roles

network-admin

context-admin

Examples

Configure BGP to ignore the first AS number of EBGP route updates.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] ignore-first-as
```

Related commands

peer ignore-first-as

import-route

Use **import-route** to enable BGP to redistribute routes from an IGP protocol.

Use **undo import-route** to disable route redistribution from an IGP protocol.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view/BGP IPv4 multicast address family view:

import-route { **isis** | **ospf** | **rip** } [{ *process-id* | **all-processes** } [**allow-direct** | **med** *med-value* | **route-policy** *route-policy-name*] *]

import-route { **direct** | **static** } [**med** *med-value* | **route-policy** *route-policy-name*] *

undo import-route { **direct** | { **isis** | **ospf** | **rip** } [*process-id* | **all-processes**] | **static** }

In BGP IPv6 unicast address family view/BGP-VPN IPv6 unicast address family view/BGP IPv6 multicast address family view:

import-route { **isisv6** | **ospfv3** | **ripng** } [{ *process-id* | **all-processes** } [**allow-direct** | **med** *med-value* | **route-policy** *route-policy-name*] *]

import-route { **direct** | **static** } [**med** *med-value* | **route-policy** *route-policy-name*] *

undo import-route { **direct** | { **isisv6** | **ospfv3** | **ripng** } [*process-id* | **all-processes**] | **static** }

Default

BGP does not redistribute IGP routes.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

BGP IPv4 multicast address family view

BGP IPv6 multicast address family view

Predefined user roles

network-admin

context-admin

Parameters

direct: Redistributes direct routes.

isis: Redistributes IS-IS routes.

ospf: Redistributes OSPF routes.

rip: Redistributes RIP routes.

static: Redistributes static routes.

process-id: Specifies a process by its ID in the range of 1 to 65535.

all-processes: Redistributes routes from all the processes of the specified IGP protocol.

allow-direct: Redistributes the networks of the local interfaces enabled with the specified routing protocol. By default, the networks of the local interfaces are not redistributed. If you specify both the **allow-direct** keyword and the **route-policy** *route-policy-name* option, make sure the **if-match** rule defined in the routing policy does not conflict with the **allow-direct** keyword. For example, if you specify the **allow-direct** keyword, do not configure the **if-match route-type** rule for the routing policy. Otherwise, the **allow-direct** keyword does not take effect.

med *med-value*: Specifies a MED value for redistributed routes, in the range of 0 to 4294967295. If you do not specify an MED, the metric of a redistributed route is used as its MED.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to filter redistributed routes or set route attributes for redistributed routes.

Usage guidelines

The **import-route** command cannot redistribute default IGP routes. To redistribute default IGP routes, use the **default-route imported** command together with the **import-route** command.

Only active routes can be redistributed. You can use the **display ip routing-table protocol** or **display ipv6 routing-table protocol** command to view route state information.

If you do not specify any parameters when redistributing IS-IS, IPv6 IS-IS, OSPF, OSPFv3, RIP, or RIPng routes, the command redistributes routes from process 1.

The ORIGIN attribute of routes redistributed by the **import-route** command is INCOMPLETE.

After you redistribute routes from all processes of a routing protocol by using the **all-processes** keyword, this command does not take effect on any processes of the protocol.

Examples

In BGP IPv4 unicast address family view, redistribute routes from RIP process 1, and set the MED value for redistributed routes to 100.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4] import-route rip 1 med 100
```

Related commands

display ip routing-table protocol

display ipv6 routing-table protocol

import-route-append

import-route-append

Use **import-route-append** to redistribute routes from an IGP without overwriting the routes redistributed by the **import-route** command.

Use **undo import-route-append** to remove the redistributed routes.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view/BGP IPv4 multicast address family view:

import-route-append { **isis** | **ospf** | **rip** } [{ *process-id* | **all-processes** } [**allow-direct** | **med** *med-value* | **route-policy** *route-policy-name*] *]

import-route-append { **direct** | **static** } [**med** *med-value* | **route-policy** *route-policy-name*] *

undo import-route-append { **direct** | { **isis** | **ospf** | **rip** } [*process-id* | **all-processes**] | **static** }

In BGP IPv6 unicast address family view/BGP-VPN IPv6 unicast address family view/BGP IPv6 multicast address family view:

import-route-append { **isisv6** | **ospfv3** | **ripng** } [{ *process-id* | **all-processes** } [**allow-direct** | **med** *med-value* | **route-policy** *route-policy-name*] *]

import-route-append { **direct** | **static** } [**med** *med-value* | **route-policy** *route-policy-name*] *

undo import-route-append { **direct** | { **isisv6** | **ospfv3** | **ripng** } [*process-id* | **all-processes**] | **static** }

Default

BGP does not redistribute IGP routes.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

BGP IPv4 multicast address family view

BGP IPv6 multicast address family view

Predefined user roles

network-admin

context-admin

Parameters

direct: Redistributes direct routes.

isis: Redistributes IS-IS routes.

isisv6: Redistributes IPv6 IS-IS routes.

ospf: Redistributes OSPF routes.

ospfv3: Redistributes OSPFv3 routes.

rip: Redistributes RIP routes.

ripng: Redistributes RIPng routes.

static: Redistributes static routes.

process-id: Specifies a process by its number in the range of 1 to 65535.

all-processes: Redistributes routes from all processes of the specified routing protocol.

allow-direct: Redistributes the networks of the local interfaces enabled with the specified routing protocol. By default, the networks of the local interfaces are not redistributed. If you specify both the **allow-direct** keyword and the **route-policy** *route-policy-name* option, make sure the **if-match** rule defined in the routing policy does not conflict with the **allow-direct** keyword. For example, if you specify the **allow-direct** keyword, do not configure the **if-match route-type** rule for the routing policy. Otherwise, the **allow-direct** keyword does not take effect.

med *med-value*: Specifies a MED value for redistributed routes, in the range of 0 to 4294967295. If you do not specify an MED, the metric of a redistributed route is used as its MED.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to filter redistributed routes or set route attributes for redistributed routes.

Usage guidelines

If you execute the **import-route-append** command without executing the **import-route** command, the **import-route-append** command has the same effect as the **import-route** command.

If you execute both the **import-route** and **import-route-append** commands for an IGP process, the commands take effect as follows:

- A route is redistributed as long as it matches the criteria of either command.
- If a route matches the criteria of both commands, the route is redistributed, and the apply clauses in the routing policies specified in the two commands take effect as follows:
  - If the apply clauses do not conflict, all apply clauses take effect.
  - If conflicts occur between the apply clauses, only the apply clauses in the **import-route-append** command take effect.
- The MED value specified by the **import-route-append** command takes precedence over that specified by the **import-route** command.

If you execute the **import-route-append** command multiple times for an IGP process, the most recent configuration takes effect.

After you redistribute routes from all processes of a routing protocol by using the **all-processes** keyword, this command does not take effect on any processes of the protocol.

Examples

In BGP IPv4 unicast address family view, redistribute routes matching routing policy **policy1** from IS-IS process 1 without overwriting the routes redistributed by the **import-route** command.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4] import-route isis 1
[Sysname-bgp-default-ipv4] import-route-append isis 1 route-policy policy1
```

Related commands

display ip routing-table protocol

display ipv6 routing-table protocol

import-route

ip vpn-instance (BGP instance view)

Use **ip vpn-instance** to create a BGP-VPN instance and enter its view, or enter the view of an existing BGP-VPN instance.

Use **undo ip vpn-instance** to remove a BGP-VPN instance and all its configurations.

Syntax

ip vpn-instance *vpn-instance-name*

undo ip vpn-instance *vpn-instance-name*

Default

No BGP-VPN instances exist.

Views

BGP instance view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance-name: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

After you create a BGP peer in BGP-VPN instance view, the BGP routes learned from the peer are added into the routing table of the specified VPN instance.

After entering BGP-VPN instance view, you can execute related commands to add routes learned from different sites into different VPN instances.

Before you execute this command, you must perform the following tasks:

- Use the **ip vpn-instance** command to create the VPN instance in system view.
- Use the **route-distinguisher** command to configure a route distinguisher (RD) for the VPN instance.

Examples

Create a BGP-VPN instance and enter its view.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] route-distinguisher 100:1
[Sysname-vpn-instance-vpn1] quit
[Sysname] bgp 100
[Sysname-bgp-default] ip vpn-instance vpn1
[Sysname-bgp-default-vpn1]
```

Related commands

ip vpn-instance (system view)(*VPN Instance Command Reference*)

route-distinguisher(*VPN Instance Command Reference*)

label-allocation-mode

Use **label-allocation-mode** to specify a label allocation mode.

Use **undo label-allocation-mode** to restore the default.

Syntax

label-allocation-mode { **per-prefix** | **per-vrf** }

undo label-allocation-mode

Default

BGP allocates labels on a per-next-hop basis.

Views

BGP instance view

Predefined user roles

network-admin

context-admin

Parameters

per-prefix: Allocates a label to each route prefix.

per-vrf: Allocates a label to each VPN instance.

Usage guidelines

CAUTION:

A change to the label allocation mode enables BGP to re-advertise all routes, which will cause temporary service interruption. Use this command with caution.

BGP supports the following label allocation modes:

- **Per-prefix**—Allocates a label to each route prefix.
- **Per-next-hop**—Allocates a label to each next hop. This mode is applicable when the number of labels required by the per-prefix mode exceeds the maximum number of labels supported by the device.
- **Per-VPN-instance**—Allocates a label to each VPN instance. This mode is applicable when the number of labels required by the per-next-hop mode exceeds the maximum number of labels supported by the device.

When you specify the per-prefix or per-next-hop label allocation mode, you can execute the **vpn popgo** command to specify the POPGO forwarding mode on an egress PE. The egress PE will pop the label for each packet and forward the packet out of the interface corresponding to the label.

When you specify the per-VPN instance label allocation mode, do not execute the **vpn popgo** command because it is mutually exclusive with the **label-allocation-mode per-vrf** command. The egress PE will pop the label for each packet and forward the packet through the FIB table.

Examples

Specify the per-prefix label allocation mode.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] label-allocation-mode per-prefix
```

Related commands

vpn popgo

log-peer-change

Use **log-peer-change** to enable logging for BGP session state changes globally.

Use **undo log-peer-change** to disable logging for BGP session state changes globally.

Syntax

log-peer-change

undo log-peer-change

Default

Logging for BGP session state changes is enabled globally.

Views

BGP instance view

Predefined user roles

network-admin

context-admin

Usage guidelines

After you execute both the **log-peer-change** and **peer log-change** commands, BGP logs session establishment and disconnection events for the peer or peer group. To display the log information, use the **display bgp peer ipv4 unicast log-info** command or the **display bgp peer ipv6 unicast log-info** command. The logs are sent to the information center of the device. The output rules of the logs (whether to output the logs and where to output) are determined by the information center configuration. For more information about information center configuration, see *Network Management and Monitoring Configuration Guide*.

If you disable logging for BGP session state changes globally or disable logging for a peer or peer group, BGP does not generate logs for session establishments and disconnections.

Examples

Enable logging for session state changes globally.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] log-peer-change
```

Related commands

display bgp peer

peer log-change

network

Use **network** to inject a network to the BGP routing table and configure BGP to advertise the network.

Use **undo network** to remove a local network.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view/BGP IPv4 multicast address family view:

network *ipv4-address* [*mask-length* | *mask*] [**route-policy** *route-policy-name*]

undo network *ipv4-address* [*mask-length* | *mask*]

In BGP IPv6 unicast address family view/BGP-VPN IPv6 unicast address family view/BGP IPv6 multicast address family view:

network *ipv6-address prefix-length* [**route-policy** *route-policy-name*]

undo network *ipv6-address prefix-length*

Default

BGP does not advertise local networks.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

BGP IPv4 multicast address family view

BGP IPv6 multicast address family view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-address: Specifies an IPv4 network address. If you do not specify the *mask* or *mask-length* argument, natural mask is used.

mask-length: Specifies a mask length in the range of 0 to 32.

mask: Specifies a mask in dotted decimal notation.

ipv6-address: Specifies an IPv6 network address.

prefix-length: Specifies a prefix length in the range of 0 to 128.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to filter routes or set the route attributes.

Usage guidelines

The network to be injected must be available and active in the local IP routing table.

The ORIGIN attribute of the route injected with the **network** command is IGP.

When you execute the **undo network** command, you must specify the same mask or mask length/prefix length that you specified for the **network** command. Otherwise, the configuration cannot be removed.

Examples

In BGP IPv4 unicast address family view, inject local network 10.0.0.0/16 to the BGP routing table.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4] network 10.0.0.0 255.255.0.0
```

network short-cut

Use **network short-cut** to increase the preference for a received EBGP route. This EBGP route is called a shortcut route.

Use **undo network short-cut** to remove the configuration.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view/BGP IPv4 multicast address family view:

network *ipv4-address* [*mask-length* | *mask*] **short-cut**

undo network *ipv4-address* [*mask-length* | *mask*] **short-cut**

In BGP IPv6 unicast address family view/BGP-VPN IPv6 unicast address family view/BGP IPv6 multicast address family view:

network *ipv6-address prefix-length* **short-cut**

undo network *ipv6-address prefix-length* **short-cut**

Default

A received EBGP route has a preference of 255.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

BGP IPv4 multicast address family view

BGP IPv6 multicast address family view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-address: Specifies an IPv4 network address. If you do not specify the *mask* or *mask-length* argument, natural mask is used.

mask-length: Specifies a mask length in the range of 0 to 32.

mask: Specifies a mask for the network address, in dotted decimal notation.

ipv6-address: Specifies an IPv6 network address.

prefix-length: Specifies a prefix length in the range of 0 to 128.

Usage guidelines

Different routing protocols might find different routes to the same destination. However, not all of those routes are optimal. For route selection, routing protocols, direct routes, and static routes are assigned different preferences. The route with the highest preference is preferred.

By default, the preference of an EBGP route is lower than a local route. If a device has an EBGP route and a local route to reach the same destination, the device does not select the EBGP route. You can use the **network shortcut** command to configure the EBGP route to have the same preference as the local route so the EBGP route is more likely to become the optimal route.

You can use the **preference** command to modify the preferences for external and local BGP routes.

Examples

In BGP IPv4 unicast address family view, increase the preference of EBGP route 10.0.0.0/16.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4] network 10.0.0.0 255.255.0.0 short-cut
```

Related commands

preference

non-stop-routing

Use **non-stop-routing** to enable BGP nonstop routing (NSR).

Use **undo non-stop-routing** to disable BGP NSR.

Syntax

non-stop-routing

undo non-stop-routing

Default

BGP NSR is disabled.

Views

BGP instance view

Predefined user roles

network-admin

context-admin

Usage guidelines

BGP NSR ensures continuous routing by synchronizing BGP state and data information from the active BGP process to the standby BGP process. The standby BGP process can seamlessly take over all services when the active process fails.

Examples

Enable BGP NSR.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] non-stop-routing
```

Related commands

display bgp non-stop-routing status

peer advertise-community

Use **peer advertise-community** to advertise the COMMUNITY attribute to a peer or peer group.

Use **undo peer advertise-community** to disable the COMMUNITY attribute advertisement to a peer or peer group.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view/BGP VPNv4 address family view/BGP VPNv6 address family view/BGP IPv4 multicast address family view/BGP IPv4 MVPN address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] } **advertise-community**

undo peer { *group-name* | *ipv4-address* [*mask-length*] } **advertise-community**

In BGP IPv6 unicast address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **advertise-community**

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **advertise-community**

In BGP IPv6 multicast address family view/BGP-VPN IPv6 unicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **advertise-community**

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **advertise-community**

Default

No COMMUNITY attribute is advertised to any peers or peer groups.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP VPNv4 address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

BGP VPNv6 address family view

BGP IPv4 multicast address family view

BGP IPv6 multicast address family view

BGP IPv4 MVPN address family view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command advertises the COMMUNITY attribute to all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command advertises the COMMUNITY attribute to all dynamic peers in the subnet.

Usage guidelines

The COMMUNITY attribute is a group of specific data carried in update messages. A route can carry one or more COMMUNITY attribute values (each is represented by a 4-byte integer). The receiving router processes the route (for example, determining whether to advertise the route and the scope for advertising the route) based on the COMMUNITY attribute values.

After you execute the **peer advertise-community** command, routing updates advertised to the peer carry the COMMUNITY attribute.

After you execute the **undo peer advertise-community** command, BGP, upon receiving a route with the COMMUNITY attribute, removes the COMMUNITY attribute before sending the route to the peer or peer group.

Examples

In BGP IPv4 unicast address family view, advertise the COMMUNITY attribute to peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4] peer test advertise-community
```

Related commands

apply community

if-match community

ip community-list

peer advertise-ext-community

Use **peer advertise-ext-community** to advertise the extended community attribute to a peer or peer group.

Use **undo peer advertise-ext-community** to disable the extended community attribute advertisement to a peer or peer group.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view/BGP IPv4 multicast address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] } **advertise-ext-community**

undo peer { *group-name* | *ipv4-address* [*mask-length*] } **advertise-ext-community**

In BGP IPv6 unicast address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **advertise-ext-community**

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **advertise-ext-community**

In BGP IPv6 multicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **advertise-ext-community**

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **advertise-ext-community**

Default

No extended community attribute is advertised to any peers or peer groups.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP IPv4 multicast address family view

BGP IPv6 multicast address family view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command advertises the extended community attribute to all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command advertises the extended community attribute to all dynamic peers in the subnet.

Usage guidelines

To meet increasing user demands, BGP defines a new attribute—extended community attribute. The extended community attribute has the following advantages over the COMMUNITY attribute:

- The extended community attribute has an 8-byte length.
- The extended community attribute supports various types. You can select an extended community attribute type as needed to implement route filtering and control. This simplifies configuration and management.

After you execute the **peer advertise-ext-community** command, route updates sent to the peer or peer group carry the extended community attribute.

After you execute the **undo peer advertise-ext-community** command, BGP, upon receiving a route with the extended community attribute, removes the extended community attribute before sending the route to the peer or peer group.

Examples

In BGP IPv4 unicast address family view, advertise the extended community attribute to peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4] peer test advertise-ext-community
```

Related commands

apply extcommunity

if-match extcommunity

ip extcommunity-list

peer advertise-policy exist-policy

Use **peer advertise-policy exist-policy** to specify an existent policy to control route advertisement.

Use **undo peer advertise-policy exist-policy** to remove the configuration.

Syntax

In BGP IPv4 unicast address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] } **advertise-policy** *advertise-policy-name* **exist-policy** *exist-policy-name*

undo peer { *group-name* | *ipv4-address* [*mask-length*] } **advertise-policy exist-policy**

In BGP IPv6 unicast address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **advertise-policy** *advertise-policy-name* **exist-policy** *exist-policy-name*

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **advertise-policy exist-policy**

Default

No existent policy is specified to control route advertisement.

Views

BGP IPv4 unicast address family view

BGP IPv6 unicast address family view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command specifies all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command specifies all dynamic peers in the subnet.

advertise-policy-name: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters. The routing policy is used as the route advertisement policy.

exist-policy *exist-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters. The routing policy is used as the existent policy.

Usage guidelines

After you configure this command, routes that match the route advertisement policy can be advertised only when the BGP routing table contains prefixes that match the existent policy.

The existent policy does not apply to routes that do not match the route advertisement policy.

Examples

In BGP IPv4 unicast address family view, configure BGP to advertise routes matching routing policy **adv-policy** to peer 1.1.1.1 only when the BGP routing table contains prefixes matching routing policy **ex-policy**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4] peer 1.1.1.1 advertise-policy adv-policy exist-policy
ex-policy
```

Related commands

filter-policy export

filter-policy import

peer as-path-acl

peer filter-policy

peer prefix-list

peer route-policy

peer advertise-policy non-exist-policy

route-policy

peer advertise-policy non-exist-policy

Use **peer advertise-policy non-exist-policy** to specify a nonexistent policy to control route advertisement.

Use **undo peer advertise-policy non-exist-policy** to remove the configuration.

Syntax

In BGP IPv4 unicast address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] } **advertise-policy** *advertise-policy-name* **non-exist-policy** *non-exist-policy-name*

undo peer { *group-name* | *ipv4-address* [*mask-length*] } **advertise-policy non-exist-policy**

In BGP IPv6 unicast address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **advertise-policy** *advertise-policy-name* **non-exist-policy** *non-exist-policy-name*

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **advertise-policy non-exist-policy**

Default

No nonexistent policy is specified to control route advertisement.

Views

BGP IPv4 unicast address family view

BGP IPv6 unicast address family view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command specifies all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command specifies all dynamic peers in the subnet.

advertise-policy-name: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters. The routing policy is used as the route advertisement policy.

non-exist-policy *non-exist-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters. The routing policy is used as the nonexistent policy.

Usage guidelines

After you configure this command, routes that match the route advertisement policy can be advertised only when the BGP routing table does not contain any prefixes that match the nonexistent policy.

The nonexistent policy does not apply to routes that do not match the route advertisement policy.

Examples

In BGP IPv4 unicast address family view, configure BGP to advertise routes matching routing policy **adv-policy** to peer 1.1.1.1 only when the BGP routing table does not contain any prefixes matching routing policy **n-ex-policy**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4] peer 1.1.1.1 advertise-policy adv-policy non-exist-policy
n-ex-policy
```

Related commands

filter-policy export

filter-policy import

peer as-path-acl

peer filter-policy

peer prefix-list

peer route-policy

peer advertise-policy exist-policy

route-policy

peer allow-as-loop

Use **peer allow-as-loop** to allow a local AS number to exist in the AS_PATH attribute of routes from a peer or peer group, and to set the number of times the local AS number can appear.

Use **undo peer allow-as-loop** to remove the configuration.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view/BGP VPNv4 address family view/BGP IPv4 multicast address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] } **allow-as-loop** [*number*]

undo peer { *group-name* | *ipv4-address* [*mask-length*] } **allow-as-loop**

In BGP IPv6 unicast address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **allow-as-loop** [*number*]

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **allow-as-loop**

In BGP-VPN IPv6 unicast address family view/BGP IPv6 multicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **allow-as-loop** [*number*]

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **allow-as-loop**

Default

The local AS number is not allowed to exist in the AS_PATH attribute of routes from a peer or peer group.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP VPNv4 address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

BGP IPv4 multicast address family view

BGP IPv6 multicast address family view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet in this command, BGP allows a local AS number to exist in the AS_PATH attribute of routes from all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet in this command, BGP allows a local AS number to exist in the AS_PATH attribute of routes from all dynamic peers in the subnet.

number: Specifies the number of times for which the local AS number can appear, in the range of 1 to 10. The default number is 1. If the number of times for which the local AS number appears in a route is more than the specified number, BGP considers that a routing loop occurs and discards the route.

Usage guidelines

By default, BGP does not receive routes that contain the local AS number in the AS_PATH attribute to avoid routing loops. However, in some network environments, the AS_PATH attribute of a route from a peer must be allowed to contain the local AS number. Otherwise, the route cannot be advertised correctly.

Examples

In BGP IPv4 unicast address family view, set the number of times the local AS number can appear in AS_PATH attribute of routes from peer group **test** to 2.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4] peer test allow-as-loop 2
```

peer as-number (for a BGP peer group)

Use **peer as-number** to specify an AS number for a peer group.

Use **undo peer as-number** to delete the AS number of a peer group.

Syntax

peer *group-name* **as-number** *as-number*

undo peer *group-name* **as-number**

Default

No AS number is specified for a peer group.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a name for a peer group, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

as-number: Specifies an AS number for a peer group, in the range of 1 to 4294967295.

Usage guidelines

This command applies only to a peer group with no peers in it.

When you specify an AS number for a peer group and want to add peers to it, make sure the AS number of the peers is the same as the peer group.

If you do not specify an AS number for a peer group, peers added to it can use their own AS numbers.

Examples

In BGP instance view, set the AS number for peer group **test** to 100.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] peer test as-number 100
```

Related commands

peer group

peer as-number (for a BGP peer)

Use **peer as-number** to create a BGP peer and specify its AS number.

Use **undo peer** to delete a BGP peer.

Syntax

peer { *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **as-number** *as-number*

undo peer { *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] }

Default

No BGP peers exist.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-address: Specifies the IPv4 address of a peer.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command enables BGP to establish dynamic peer relationships with all devices in the subnet.

ipv6-address: Specifies the IPv6 address of a peer.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command enables BGP to establish dynamic peer relationships with all devices in the subnet.

as-number: Specifies an AS number for the peer, in the range of 1 to 4294967295. If the AS numbers of the peer and the local router are the same, the peer is an IBGP peer. If they are different, the peer is an EBGP peer.

Usage guidelines

You can also create a peer and add it to a peer group by using the **peer group** command.

To modify the AS number of a peer, do not execute the **peer as-number** command repeatedly. Instead, you must first delete the peer and configure it again.

After you create a peer, you must use the **peer enable** command to enable BGP to exchange routing information with the specified peer.

For a remote device to establish a peer relationship with the local device, you must specify the IP address of the local device on the remote device.

Examples

In BGP instance view, create BGP peer 1.1.1.1 and set its AS number to 100.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] peer 1.1.1.1 as-number 100
```

Related commands

display bgp peer

peer enable

peer group

peer as-path-acl

Use **peer as-path-acl** to specify an AS path list to filter routes incoming from or outgoing to a peer or peer group.

Use **undo peer as-path-acl** to delete the AS path list specified to filter routes incoming from or outgoing to a peer or peer group.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view/BGP VPNv4 address family view/BGP IPv4 multicast address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] } **as-path-acl** as-*path-acl-number* { **export** | **import** }

undo peer { *group-name* | *ipv4-address* [*mask-length*] } **as-path-acl** { **export** | **import** }

In BGP IPv6 unicast address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **as-path-acl** *as-path-acl-number* { **export** | **import** }

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **as-path-acl** { **export** | **import** }

In BGP IPv6 multicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **as-path-acl** *as-path-acl-number* { **export** | **import** }

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **as-path-acl** { **export** | **import** }

Default

No AS path list is specified for filtering.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP VPNv4 address family view

BGP IPv6 unicast address family view

BGP IPv4 multicast address family view

BGP IPv6 multicast address family view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command specifies an AS path list to filter routes incoming from or outgoing to all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command specifies an AS path list to filter routes incoming from or outgoing to all dynamic peers in the subnet.

as-path-acl-number: Specifies an AS path list by its number in the range of 1 to 256.

export: Filters outgoing routes.

import: Filters incoming routes.

Usage guidelines

The specified AS path list must have been created with the **ip as-path** command in system view. If you specify a nonexistent AS path list, all routes can pass the AS path list.

Examples

In BGP IPv4 unicast address family view, specify AS path list 1 to filter routes outgoing to peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4] peer test as-path-acl 1 export
```

Related commands

filter-policy export

filter-policy import

ip as-path

peer filter-policy

peer prefix-list

peer route-policy

peer bfd

Use **peer bfd** to enable BFD for the link to a BGP peer or peer group.

Use **undo peer bfd** to remove the configuration.

Syntax

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **bfd** [**multi-hop** | **single-hop**]

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **bfd**

Default

BFD is disabled for the link to a BGP peer or peer group.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command enables BFD for links to all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command enables BFD for links to all dynamic peers in the subnet.

multi-hop: Enables multi-hop BFD.

single-hop: Enables single-hop BFD.

Usage guidelines

When you do not specify the **multi-hop** keyword or the **single-hop** keyword:

- If an IBGP peer or peer group is specified, this command enables multi-hop BFD for the IBGP peer or peer group.
- If a directly connected EBGP peer or peer group is specified and the **peer ebgp-max-hop** command is not configured, this command enables single-hop BFD for the EBGP peer or peer group. If the EBGP peer or peer group is not directly connected or the **peer ebgp-max-hop** command is configured, this command enables multi-hop BFD for the EBGP peer or peer group.

For more information about multi-hop and single-hop BFD, see BFD configuration in *Network Management and Monitoring Configuration Guide*.

BFD helps speed up BGP routing convergence upon link failures. However, if you have enabled GR, use BFD with caution. BFD might detect a failure before the system performs GR, resulting in GR failure. If you have enabled both BFD and GR for BGP, do not disable BFD during a GR process to avoid GR failure.

For BGP sessions established with link-local addresses, you can use only single-hop BFD to detect the link between BGP peers.

To establish a BFD session to a BGP peer, you must configure the same BFD detection mode (multi-hop or single-hop) on the local router and the BGP peer.

Examples

In BGP instance view, enable BFD for the link to BGP peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] peer test bfd
```

Related commands

display bfd session (*Network Management and Monitoring Command Reference*)

display bgp peer

peer capability-advertise conventional

Use **peer capability-advertise conventional** to disable the BGP multi-protocol extension, route refresh, and 4-byte AS number features for a peer or peer group.

Use **undo peer capability-advertise conventional** to enable the BGP multi-protocol extension, route refresh, and 4-byte AS number features for a peer or peer group.

Syntax

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **capability-advertise conventional**

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **capability-advertise conventional**

Default

The BGP multi-protocol extension, route refresh, and 4-byte AS number features are enabled.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command disables BGP multi-protocol extension and route refresh for all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command disables BGP multi-protocol extension and route refresh for all dynamic peers in the subnet.

Usage guidelines

The route refresh feature enables BGP to send and receive Route-refresh messages and implement BGP session soft-reset.

The multi-protocol extension feature enables BGP to advertise and receive routing information for various protocols (for example, IPv6 routing information).

The 4-byte AS number feature enables BGP to use 4-byte AS numbers in the range of 1 to 4294967295.

If both the **peer capability-advertise conventional** and **peer capability-advertise route-refresh** commands are executed, the most recent configuration takes effect.

Examples

In BGP instance view, disable the multi-protocol extension, route refresh, and 4-byte AS number features for peer 1.1.1.1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] peer 1.1.1.1 as-number 100
[Sysname-bgp-default] peer 1.1.1.1 capability-advertise conventional
```

Related commands

display bgp peer

peer capability-advertise route-refresh

peer capability-advertise route-refresh

Use **peer capability-advertise route-refresh** to enable BGP route refresh for a peer or peer group.

Use **undo peer capability-advertise route-refresh** to disable BGP route refresh for a peer or peer group.

Syntax

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **capability-advertise route-refresh**

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **capability-advertise route-refresh**

Default

BGP route refresh is enabled.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command enables BGP route refresh for all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command enables BGP route refresh for all dynamic peers in the subnet.

Usage guidelines

The route refresh feature enables BGP to send and receive Route-refresh messages.

BGP uses the route refresh feature to implement BGP session soft-reset. After a policy is modified, the router advertises a Route-refresh message to the peers. The peers resend their routing information to the router. After receiving the routing information, the router filters the routing information by using the new policy. This method allows you to refresh the BGP routing table and apply the new route selection policy without tearing down BGP sessions.

BGP route refresh requires that both the local router and the peer support route refresh.

If both the **peer capability-advertise route-refresh** and **peer capability-advertise conventional** commands are executed, the most recent configuration takes effect.

Examples

In BGP instance view, enable BGP route refresh for peer 1.1.1.1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] peer 1.1.1.1 as-number 100
[Sysname-bgp-default] peer 1.1.1.1 capability-advertise route-refresh
```

Related commands

display bgp peer

peer capability-advertise conventional

peer keep-all-routes

refresh bgp

peer capability-advertise suppress-4-byte-as

Use **peer capability-advertise suppress-4-byte-as** to enable 4-byte AS number suppression.

Use **undo peer capability-advertise suppress-4-byte-as** to disable 4-byte AS number suppression.

Syntax

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **capability-advertise suppress-4-byte-as**

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **capability-advertise suppress-4-byte-as**

Default

The 4-byte AS number suppression feature is disabled.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command enables 4-byte AS number suppression for all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command enables 4-byte AS number suppression for all dynamic peers in the subnet.

Usage guidelines

BGP supports 4-byte AS numbers. The 4-byte AS number occupies four bytes, in the range of 1 to 4294967295. By default, a device sends an Open message to the peer device for session

establishment. The Open message indicates that the device supports 4-byte AS numbers. If the peer device supports 2-byte AS numbers instead of 4-byte AS numbers, the session cannot be established. To resolve this issue, enable the 4-byte AS number suppression feature. The device then sends an Open message to inform the peer that it does not support 4-byte AS numbers, so the BGP session can be established.

If the peer device supports 4-byte AS numbers, do not enable the 4-byte AS number suppression feature. If this feature is enabled, the BGP session cannot be established.

Examples

In BGP instance view, enable 4-byte AS number suppression for peer 1.1.1.1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] peer 1.1.1.1 as-number 100
[Sysname-bgp-default] peer 1.1.1.1 capability-advertise suppress-4-byte-as
```

Related commands

display bgp peer

peer connect-interface

Use **peer connect-interface** to specify a source interface (IPv4 address/IPv6 address) for establishing TCP connections to a peer or peer group.

Use **undo peer connect-interface** to remove the configuration.

Syntax

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **connect-interface** *interface-type interface-number*

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **connect-interface**

Default

BGP uses the primary IPv4 or IPv6 address of the output interface in the optimal route destined for the BGP peer or peer group as the source address.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command specifies a source interface for establishing TCP connections to all dynamic peers in the network.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command specifies a source interface for establishing TCP connections to all dynamic peers in the subnet.

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

The **peer connect-interface** command and the **peer source-address** command can both change the source address for establishing TCP connections. If you execute both commands, the most recent configuration takes effect.

The **peer source-address** and **peer connect-interface** commands are applicable to the following scenarios:

- The peer's IPv4/IPv6 address does not belong to the interface directly connected to the local router. To ensure successful TCP connection establishment, use one of the following methods:
  - Specify the interface to which the IPv4/IPv6 address belongs as the source interface on the peer.
  - Specify the IPv4/IPv6 address of the interface directly connected to the local router as the source address on the peer.
- A BGP peer at an IPv6 link-local address must be directly connected to the local router. On the local router, you must use the **peer connect-interface** command to specify the interface directly connected to the BGP peer as the source interface of TCP connections.
- On a BGP router that has multiple links to a peer, the source interface for TCP connection changes because the primary source interface fails. To avoid this problem, specify a loopback interface as the source interface or specify the IP address of a loopback interface as the source address.
- You want to establish multiple BGP sessions to a router. In this case, BGP might fail to determine the source address for each TCP connection based on the optimal route to the peer. To prevent this problem, use one of the following methods:
  - If the BGP sessions use IP addresses of different interfaces, specify a source interface or source address for each session.
  - If the BGP sessions use different IP addresses of the same interface, specify a source address for each session.

The source interfaces on the local router and the peer must be reachable to each other.

To specify an indirectly connected interface on an EBGP peer as the source interface, use the **peer ebgp-max-hop** command. The command allows the establishment of an EBGP session to the indirectly connected peer.

If an interface has multiple IPv4 addresses, BGP uses the primary IPv4 address to establish TCP connections. If an interface has multiple IPv6 addresses, BGP selects a source IPv6 address. To use an IPv6 address as the source address, specify that IPv6 address by using the **peer source-address** command.

You cannot specify a virtual template (VT) interface as the source interface for establishing TCP connections because a VT interface cannot process services.

Examples

In BGP instance view, specify loopback 0 as the source interface for TCP connections to peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] peer test connect-interface loopback 0
```

Related commands

peer ebgp-max-hop

peer source-address

peer default-route-advertise

Use **peer default-route-advertise** to advertise a default route to a peer or peer group.

Use **undo peer default-route-advertise** to disable default route advertisement to a peer or peer group.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view/BGP IPv4 multicast address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] } **default-route-advertise** [**route-policy** *route-policy-name*]

undo peer { *group-name* | *ipv4-address* [*mask-length*] } **default-route-advertise**

In BGP VPNv4 address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] } **default-route-advertise vpn-instance** *vpn-instance-name*

undo peer { *group-name* | *ipv4-address* } **default-route-advertise vpn-instance** *vpn-instance-name*

In BGP IPv6 unicast address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **default-route-advertise** [**route-policy** *route-policy-name*]

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **default-route-advertise**

In BGP-VPN IPv6 unicast address family view/BGP IPv6 multicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **default-route-advertise** [**route-policy** *route-policy-name*]

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **default-route-advertise**

In BGP IPv4 RT filter address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] } **default-route-advertise** [**route-policy** *route-policy-name*]

undo peer { *group-name* | *ipv4-address* [*mask-length*] } **default-route-advertise**

Default

No default route is advertised to any peers or peer groups.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP VPNv4 address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

BGP IPv4 multicast address family view

BGP IPv6 multicast address family view

BGP IPv4 RT filter address family view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command advertises a default route to all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command advertises a default route to all dynamic peers in the subnet.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to modify the route attribute.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

This command enables the router to send a default route with the next hop being itself to the peer or peer group regardless of whether the default route exists in the routing table.

Examples

In BGP IPv4 unicast address family view, advertise a default route to peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4] peer test default-route-advertise
```

peer description

Use **peer description** to configure a description for a peer or peer group.

Use **undo peer description** to remove the description for a peer or peer group.

Syntax

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **description** *text*

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **description**

Default

No description information is configured for a peer or peer group.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command configures a description for all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command configures a description for all dynamic peers in the subnet.

text: Specifies a description for a peer or peer group, a case-sensitive string of 1 to 79 characters.

Examples

In BGP instance view, set the description for peer group **test** to **ISP1**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] peer test description ISP1
```

peer ebgp-max-hop

Use **peer ebgp-max-hop** to enable BGP to establish an EBGP session to an indirectly connected peer or peer group and specify the maximum hop count.

Use **undo peer ebgp-max-hop** to disable BGP from establishing an EBGP session to an indirectly connected peer or peer group.

Syntax

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **ebgp-max-hop** [*hop-count*]

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **ebgp-max-hop**

Default

BGP does not establish an EBGP session to an indirectly connected peer or peer group.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet in this command, BGP establishes EBGP sessions to all indirectly connected dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet in this command, BGP establishes EBGP sessions to all indirectly connected dynamic peers in the subnet.

hop-count: Specifies the maximum number of hop counts, in the range of 1 to 255. The default is 64.

Usage guidelines

To become EBGP peers, two routers must be directly connected and use directly connected interfaces to establish an EBGP session. If they are not directly connected, use the **peer ebgp-max-hop** command to establish an EBGP session over multiple hops between two peers.

This command takes effect only on routes received after you execute this command. To apply this command to existing routes, use the **refresh bgp** command to soft-reset BGP sessions.

When the BGP GTSM feature is enabled, two peers can establish an EBGP session after passing GTSM check, regardless of whether the maximum number of hops is reached.

Examples

In BGP instance view, enable BGP to establish EBGP sessions to indirectly connected EBGP peer group **test**, and set the maximum hop count to 64 (default).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] peer test ebgp-max-hop
```

Related commands

peer ttl-security

peer enable

Use **peer enable** to enable BGP to exchange routing information for an address family with a peer or peer group.

Use **undo peer enable** to disable BGP from exchanging routing information for an address family with a peer or peer group.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view/BGP VPNv4 address family view/BGP VPNv6 address family view/BGP IPv4 multicast address family view/BGP IPv4 MDT address family view/BGP IPv4 flowspec address family view/BGP-VPN IPv4 flowspec

address family view/BGP VPNv4 flowspec address family view/BGP IPv4 RT filter address family view/BGP IPv4 MVPN address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] } **enable**

undo peer { *group-name* | *ipv4-address* [*mask-length*] } **enable**

In BGP IPv6 unicast address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **enable**

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **enable**

In BGP LS address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **enable**

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **enable**

In BGP-VPN IPv6 unicast address family view/BGP IPv6 multicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **enable**

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **enable**

Default

BGP cannot exchange routing information with a peer or peer group.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP VPNv4 address family view

BGP IPv6 unicast address family view

BGP LS address family view

BGP-VPN IPv6 unicast address family view

BGP VPNv6 address family view

BGP IPv4 multicast address family view

BGP IPv6 multicast address family view

BGP IPv4 MDT address family view

BGP IPv4 flowspec address family view

BGP-VPN IPv4 flowspec address family view

BGP VPNv4 flowspec address family view

BGP IPv4 RT filter address family view

BGP IPv4 MVPN address family view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet in this command, BGP exchanges routing information for an address family with all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet in this command, BGP exchanges routing information for an address family with all dynamic peers in the subnet.

Usage guidelines

Executing the **peer enable** command in different views enables BGP to exchange routing information for the corresponding address families with the specified peer.

- In BGP IPv4 unicast address family view, the command enables the capability to exchange IPv4 unicast routing information. It also adds the learned routes to the BGP routing table of the public network.
- In BGP-VPN IPv4 unicast address family view, the command enables the capability to exchange IPv4 unicast routing information. It also adds the learned routes to the BGP routing table of the specified VPN instance.
- In BGP VPNv4 address family view, the command enables the capability to exchange VPNv4 routing information.
- In BGP IPv6 unicast address family view, the command enables the capability to exchange IPv6 unicast routing information. It also adds the learned routes to the IPv6 BGP routing table of the public network.
- In BGP-VPN IPv6 unicast address family view, the command enables the capability to exchange IPv6 unicast routing information. It also adds the learned routes to the IPv6 BGP routing table of the specified VPN instance.
- In BGP VPNv6 address family view, the command enables the capability to exchange VPNv6 routing information.
- In BGP IPv4 multicast address family view, the command enables the capability to exchange IPv4 unicast routes used for RPF check. For information about RPF check, see *IP Multicast Configuration Guide*.
- In BGP IPv6 multicast address family view, the command enables the capability to exchange IPv6 unicast routes used for RPF check.
- In BGP IPv4 flowspec address family view, the command enables the capability to exchange IPv4 flowspec routing information. It also adds the learned routes to the BGP IPv4 flowspec routing table.
- In BGP-VPN IPv4 flowspec address family view, the command enables the capability to exchange IPv4 flowspec routing information. It also adds the learned routes to the BGP IPv4 flowspec routing table of the VPN instance.
- In BGP VPNv4 flowspec address family view, the command enables the capability to exchange VPNv4 flowspec routing information. It also adds the learned routes to the BGP VPNv4 flowspec routing table of the VPN instance.
- In BGP IPv4 RT filter address family view, the command enables the capability to exchange IPv4 RT filter routing information.

The **undo peer enable** command disables BGP to exchange routing information for the corresponding address family with the peer.

Examples

In BGP IPv4 unicast address family view, enable BGP to exchange IPv4 unicast routing information with peer 1.1.1.1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4] peer 1.1.1.1 enable
```

Related commands

display bgp peer

peer fake-as

Use **peer fake-as** to advertise a fake AS number to a peer or peer group.

Use **undo peer fake-as** to remove the fake AS number advertised to a peer or peer group.

Syntax

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **fake-as** *as-number*

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **fake-as**

Default

No fake local AS number is advertised to a peer or peer group.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command advertises a fake AS number to all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command advertises a fake AS number to all dynamic peers in the subnet.

as-number: Specifies a fake AS number in the range of 1 to 4294967295.

Usage guidelines

After you move a BGP router from an AS to another AS (from AS 2 to AS 3 for example), you have to modify the AS number of the router on all its EBGP peers. To avoid such modifications, you can

configure the router to advertise a fake AS number 2 to its EBGP peers so that the EBGP peers still think that Router A is in AS 2.

The **peer fake-as** command is applicable only to EBGP peers or peer groups.

If you execute the **peer fake-as** command on the local router, specify the local router's AS number on the peer as the fake local AS number specified in the command.

Examples

In BGP instance view, advertise a fake AS number of 200 to peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] peer test fake-as 200
```

peer filter-policy

Use **peer filter-policy** to filter routes advertised to or received from a peer or peer group by using an ACL.

Use **undo peer filter-policy** to remove the ACL specified to filter routes advertised to or received from a peer or peer group.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view/BGP VPNv4 address family view/BGP IPv4 multicast address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] } **filter-policy** *ipv4-acl-number* { **export** | **import** }

undo peer { *group-name* | *ipv4-address* [*mask-length*] } **filter-policy** { **export** | **import** }

In BGP IPv6 unicast address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **filter-policy** *ipv6-acl-number* { **export** | **import** }

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **filter-policy** { **export** | **import** }

In BGP-VPN IPv6 unicast address family view/BGP IPv6 multicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **filter-policy** *ipv6-acl-number* { **export** | **import** }

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **filter-policy** { **export** | **import** }

In BGP VPNv6 address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] } **filter-policy** *ipv6-acl-number* { **export** | **import** }

undo peer { *group-name* | *ipv4-address* [*mask-length*] } **filter-policy** { **export** | **import** }

Default

No ACL-based filtering is configured.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP VPNv4 address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

BGP VPNv6 address family view

BGP IPv4 multicast address family view

BGP IPv6 multicast address family view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command filters routes advertised to or received from all dynamic peers in the subnet by using an ACL.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command filters routes advertised to or received from all dynamic peers in the subnet by using an ACL.

ipv4-acl-number: Specifies an ACL by its number in the range of 2000 to 3999.

ipv6-acl-number: Specifies an IPv6 ACL by its number in the range of 2000 to 3999.

export: Filters routes advertised to the peer/peer group.

import: Filters routes received from the peer/peer group.

Usage guidelines

The specified ACL used by the **peer filter-policy** command must have been created with the **acl** command in system view. Otherwise, all routes can pass the ACL.

If you use a basic ACL (with a number from 2000 to 2999) configured with the **rule** [*rule-id*] { **deny** | **permit** } **source** *source-address source-wildcard* command, the command matches routes whose destination network addresses match the *source-address source-wildcard* argument without matching the masks of the destination addresses.

To use an advanced ACL (with a number from 3000 to 3999) in the command, configure the ACL using one of the following steps:

- To deny/permit a route with the specified destination, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* command.
- To deny/permit a route with the specified destination and mask, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* **destination** *dest-addr dest-wildcard* command.

The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the subnet mask of the destination address. For the mask configuration to take effect, specify a contiguous subnet mask.

Examples

In BGP IPv4 unicast address family view, apply ACL 2000 to filter routes advertised to peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4] peer test filter-policy 2000 export
```

Related commands

acl (*ACL and QoS Command Reference*)

filter-policy export

filter-policy import

peer as-path-acl

peer prefix-list

peer route-policy

peer group

Use **peer group** to add a peer to a peer group.

Use **undo peer group** to delete a peer from a peer group.

Syntax

peer { *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **group** *group-name* [**as-number** *as-number*]

undo peer { *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **group** *group-name*

Default

No peers exist in a peer group.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-address: Specifies a peer by its IPv4 address.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command adds all dynamic peers in the subnet to a peer group.

ipv6-address: Specifies a peer by its IPv6 address.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command adds all dynamic peers in the subnet to a peer group.

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

as-number *as-number*: Specifies an AS for a peer by its number in the range of 1 to 4294967295.

Usage guidelines

You can add a peer to a peer group in the following ways:

- Use the **peer as-number** command to create a peer and specify its AS number, and then use the **peer group** command to add the peer to the peer group.
  - You can specify the **as-number** keyword for the **peer group** command. The AS number must be the same as the AS number specified in the **peer as-number** command.
  - If you have specified the AS number of the peer group with the **peer as-number** command, the peer to be added must have the same AS number as the peer group.
  - To add a peer to an IBGP peer group, the peer must be an IBGP peer.
- Use the **peer group** command to create a peer and add it to the peer group.
  - If you have specified the AS number of the peer group with the **peer as-number** command, you do not need to specify the **as-number** keyword when you execute the **peer group** command. This is because the AS number of the peer is the same as the peer group. To specify the **as-number** keyword for the **peer group** command, make sure the AS number is the same as the peer group.
  - If no AS number is specified for an EBGP peer group, specify the **as-number** keyword when you execute the **peer group** command.
  - If no AS number is specified for an IBGP peer group, you do not need to specify the **as-number** keyword when you execute the **peer group** command. This is because the AS number of the IBGP peer group is the local AS number. To specify the **as-number** keyword for the **peer group** command, make sure the AS number is the same as the local AS number.

If you have specified the AS number of a peer group with the **peer as-number** command, only the peers with the same AS number can be added to the peer group. All peers in the group share the same AS number. If you have not specified the AS number for a peer group, peers added to it can use their own AS numbers.

After you add a peer to a peer group, you must use the **peer enable** command to enable BGP to exchange routing information with the peer group.

Examples

In BGP instance view, add peer 10.1.1.1 to EBGP peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] group test external
[Sysname-bgp-default] peer 10.1.1.1 group test as-number 2004
```

Related commands

group

peer as-number

peer enable

peer ignore

Use **peer ignore** to disable BGP session establishment with a peer or peer group.

Use **undo peer ignore** to enable BGP session establishment with a peer or peer group.

Syntax

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **ignore**

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **ignore**

Default

BGP can establish a session to a peer or peer group.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet in this command, BGP tears down sessions to all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet in this command, BGP tears down sessions to all dynamic peers in the subnet.

Usage guidelines

CAUTION:

- If a session has been established to a peer, executing the **peer ignore** command for the peer tears down the session and clears all related routing information.
- If sessions have been established to a peer group, executing the **peer ignore** command for the peer group tears down the sessions to all peers in the group and clears all related routing information.

This command enables you to temporarily tear down the BGP session to a peer or peer group. You can perform network upgrade and maintenance without needing to delete and reconfigure the peer or peer group. To recover the session, execute the **undo peer ignore** command.

Examples

In BGP instance view, disable session establishment with peer 1.1.1.1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] peer 1.1.1.1 ignore
```

peer ignore-first-as

Use **peer ignore-first-as** to enable BGP to ignore the first AS number of EBGP route updates received from a peer or peer group.

Use **undo peer ignore-first-as** to remove the configuration.

Syntax

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **ignore-first-as**

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **ignore-first-as**

Default

BGP checks the first AS number of an EBGP-learned route update. If the first AS number is neither that of the BGP peer nor a private AS number, the BGP router disconnects the BGP session to the peer.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet in this command, BGP ignores the first AS number of EBGP route updates received from all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet in this command, BGP ignores the first AS number of EBGP route updates received from all dynamic peers in the subnet.

Usage guidelines

This command takes effect only on the EBGP routes received after you execute this command. If you execute the **peer ignore-first-as** and then the **undo peer ignore-first-as** commands, BGP advertises a ROUTE-REFRESH message to request the routing information from the EBGP peer or peer group.

Examples

In BGP instance view, enable BGP to ignore the first AS number of EBGP route updates received from peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] peer test ignore-first-as
```

Related commands

ignore-first-as

peer ignore-originatorid

Use **peer ignore-originatorid** to configure BGP to ignore the ORIGINATOR_ID attribute in BGP route updates.

Use **undo peer ignore-originatorid** to remove the configuration.

Syntax

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **ignore-originatorid**

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **ignore-originatorid**

Default

BGP does not ignore the ORIGINATOR_ID attribute in BGP route updates.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet in this command, BGP ignores the ORIGINATOR_ID attribute in BGP route updates from all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet in this command, BGP ignores the ORIGINATOR_ID attribute in BGP route updates from all dynamic peers in the subnet.

Usage guidelines

Before using this command, make sure it does not cause any routing loops to the network.

Before forwarding a route received from a client, the route reflector adds an ORIGINATOR_ID attribute (the router ID of the client) to the route. By default, BGP drops incoming route updates whose ORIGINATOR_ID attribute is the same as the local router ID.

Some networks such as firewall networks require BGP to accept such route updates. To meet the requirement, you must configure BGP to ignore the ORIGINATOR_ID attribute.

After you execute this command, BGP also ignores the CLUSTER_LIST attribute.

Examples

In BGP instance view, configure BGP to ignore the ORIGINATOR_ID attribute in BGP route updates from peer 1.1.1.1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] peer 1.1.1.1 ignore-originatorid
```

peer ipsec-profile

Use **peer ipsec-profile** to apply an IPsec profile to an IPv6 BGP peer or peer group.

Use **undo peer ipsec-profile** to remove the profile from an IPv6 BGP peer or peer group.

Syntax

peer { *group-name* | *ipv6-address* [*prefix-length*] } **ipsec-profile** *profile-name*

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **ipsec-profile**

Default

No IPsec profile is configured for any IPv6 BGP peers or peer groups.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command applies an IPsec profile to all dynamic peers in the subnet.

profile-name: Specifies an IPsec profile by its name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

IPsec can protect IPv6 BGP packets from data eavesdropping, tampering, and attacks caused by forged IPv6 BGP packets.

When two IPv6 BGP neighbor devices, for example Device A and Device B, are configured with IPsec, Device A encapsulates an IPv6 BGP packet with IPsec before sending it to Device B. If Device B successfully receives and decapsulates the packet, it establishes an IPv6 BGP peer relationship with Device A or learns IPv6 BGP routes to Device A. If Device B receives but fails to decapsulate the packet, or receives a packet not protected by IPsec, it discards the packet.

Configure IPsec to protect IPv6 BGP packets through the following steps:

1. Configure an IPsec transform set.
2. Configure a manual IPsec profile.
3. Execute this command to apply the IPsec profile to an IPv6 BGP peer or peer group.

For more information about IPsec transform sets and IPsec profiles, see *Security Configuration Guide*.

This command supports only IPsec profiles in manual mode.

If you configure IPsec on a device, you must configure IPsec on its IPv6 BGP peer. Otherwise, IPv6 BGP packets cannot be received.

Examples

In BGP instance view, apply IPsec profile **profile001** to peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] peer test ipsec-profile profile001
```

Related commands

display bgp group

display bgp peer

peer keep-all-routes

Use **peer keep-all-routes** to save all route updates from a peer or peer group, regardless of whether the routes have passed the configured routing policy.

Use **undo peer keep-all-routes** to remove the configuration.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view/BGP VPNv4 address family view/BGP IPv4 multicast address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] } **keep-all-routes**

undo peer { *group-name* | *ipv4-address* [*mask-length*] } **keep-all-routes**

In BGP IPv6 unicast address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **keep-all-routes**

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **keep-all-routes**

In BGP-VPN IPv6 unicast address family view/BGP IPv6 multicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **keep-all-routes**

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **keep-all-routes**

Default

Route updates from a peer or peer group are not saved.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP VPNv4 address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

BGP IPv4 multicast address family view

BGP IPv6 multicast address family view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command saves all route updates from all dynamic peers in the subnet, regardless of whether the routes have passed the configured routing policy.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command saves all route updates from all dynamic peers in the subnet, regardless of whether the routes have passed the configured routing policy.

Usage guidelines

To implement BGP session soft-reset when the local router and a peer or peer group do not support the route refresh feature, use the **peer keep-all-routes** command. The command saves all route updates received from the peer or peer group. After modifying the route selection policy, filter all saved routes with the new policy to refresh the routing table. This method avoids tearing down BGP sessions.

Examples

In BGP IPv4 unicast address family view, save all route updates from peer 1.1.1.1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4] peer 1.1.1.1 keep-all-routes
```

Related commands

peer capability-advertise route-refresh

refresh bgp

peer keychain

Use **peer keychain** to enable keychain authentication for a BGP peer or peer group.

Use **undo peer keychain** to remove keychain authentication for a BGP peer or peer group.

Syntax

peer { *group-name* | *ip-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **keychain** *keychain-name*

undo peer { *group-name* | *ip-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **keychain**

Default

Keychain authentication is disabled.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ip-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ip-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command enables keychain authentication for all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command enables keychain authentication for all dynamic peers in the subnet.

keychain-name: Specifies a keychain by its name, a case-sensitive string of 1 to 63 characters. The keychain must have been created.

Usage guidelines

Keychain authentication enhances the security of BGP in the following ways:

- BGP peers can establish TCP connections only when they are both enabled with keychain authentication.
- The keys used by the BGP peers at the same time must have the same ID.
- The keys with the same ID must use the same authentication algorithm and key string.

BGP supports the HMAC-MD5, HMAC-SHA-256, HMAC-SM3, SM3, and MD5 authentication algorithms. To specify an authentication algorithm for a key, use the **authentication-algorithm** command.

The IDs of keys used for authentication can only be in the range of 0 to 63. To create a key, use the **key** command.

The **peer keychain** and **peer password** commands are mutually exclusive.

Examples

In BGP instance view, configure peer 10.1.1.1 to use keychain **abc** for authentication.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] peer 10.1.1.1 as-number 100
[Sysname-bgp-default] peer 10.1.1.1 keychain abc
```

Related commands

authentication-algorithm (*Security Command Reference*)

key (*Security Command Reference*)

peer password

peer label-route-capability

Use **peer label-route-capability** to enable BGP to exchange labeled routes with a peer or peer group.

Use **undo peer label-route-capability** to disable BGP from exchanging labeled routes with a peer or peer group.

Syntax

peer { *group-name* | *ipv4-address* [*mask-length*] } **label-route-capability**

undo peer { *group-name* | *ipv4-address* [*mask-length*] } **label-route-capability**

Default

BGP cannot exchange labeled routes with a peer or peer group.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet in this command, BGP exchanges labeled routes with all dynamic peers in the subnet.

Usage guidelines

On an inter-AS option C network, use this command in BGP IPv4 unicast or BGP-VPN IPv4 unicast address family view to exchange labeled IPv4 unicast routes for inter-AS public LSP establishment.

Examples

In BGP IPv4 unicast address family view, enable BGP to exchange labeled IPv4 routes with peer 2.2.2.2.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4
[Sysname-bgp-default-ipv4] peer 2.2.2.2 label-route-capability
```

peer log-change

Use **peer log-change** to enable logging for BGP session state changes for a peer or peer group.

Use **undo peer log-change** to disable logging for BGP session state changes for a peer or peer group.

Syntax

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **log-change**

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **log-change**

Default

Logging for BGP session state changes is enabled for all peers or peer groups.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must already exist.

ipv4-address: Specifies the IPv4 address of a peer. The peer must already exist.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command enables the logging of BGP session state changes for all dynamic peers in the subnet.

ipv6-address: Specifies the IPv6 address of a peer. The peer must already exist.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command enables the logging of BGP session state changes for all dynamic peers in the subnet.

Usage guidelines

After you execute both the **log-peer-change** and **peer log-change** commands, BGP logs session establishment and disconnection events for the peer or peer group. To view the log information, use the **display bgp peer ipv4 unicast log-info** command or the **display bgp peer ipv6 unicast log-info** command. The logs are sent to the information center of the device. The output rules of the logs (whether to output the logs and where to output) are determined by the information center configuration. For more information about information center configuration, see *Network Management and Monitoring Configuration Guide*.

If you disable logging for BGP session state changes globally or disable logging for a peer or peer group, BGP does not generate logs for session establishments and disconnections.

Examples

In BGP instance view, enable logging for BGP session state changes for peer 1.1.1.1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] peer 1.1.1.1 as-number 200
[Sysname-bgp-default] peer 1.1.1.1 log-change
```

Related commands

display bgp peer

log-peer-change

peer low-memory-exempt

Use **peer low-memory-exempt** to configure BGP to protect EBGP peers or peer groups when the memory usage reaches level 2 threshold.

Use **undo peer low-memory-exempt** to remove the configuration.

Syntax

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **low-memory-exempt**

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **low-memory-exempt**

Default

When the memory usage reaches level 2 threshold, BGP tears down an EBGP session to release memory resources periodically.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet in this command, BGP protects all dynamic peers in the subnet when the memory usage reaches level 2 threshold.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet in this command, BGP protects all dynamic peers in the subnet when the memory usage reaches level 2 threshold.

Usage guidelines

When level 2 memory usage threshold is reached, BGP tears down an EBGP session to release memory resources periodically until the memory usage is exempt from level 2 threshold. You can use this command to avoid tearing down the BGP session to an EBGP peer when memory usage reaches level 2 threshold. For more information about thresholds, see *Fundamentals Configuration Guide*.

Examples

In BGP instance view, configure BGP to protect EBGP peer 1.1.1.1 when the memory usage reaches level 2 threshold.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] peer 1.1.1.1 as-number 200
[Sysname-bgp-default] peer 1.1.1.1 low-memory-exempt
```

peer next-hop-local

Use **peer next-hop-local** to set the local router as the next hop for routes sent to a peer or peer group.

Use **undo peer next-hop-local** to remove the configuration.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view/BGP VPNv4 address family view/ BGP IPv4 multicast address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] } **next-hop-local**

undo peer { *group-name* | *ipv4-address* [*mask-length*] } **next-hop-local**

In BGP IPv6 unicast address family view/BGP IPv6 multicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **next-hop-local**

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **next-hop-local**

Default

BGP sets the local router as the next hop for all routes sent to an EBGP peer or peer group.

BGP sets the local router as the next hop for EBGP routes sent to an IBGP peer or peer group for BGP VPNv4 and VPNv6 address families. It does not set the local router as the next hop for EBGP routes sent to an IBGP peer or peer group for other address families.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP VPNv4 address family view

BGP IPv6 unicast address family view

BGP IPv4 multicast address family view

BGP IPv6 multicast address family view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command sets the local router as the next hop for routes sent to all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command sets the local router as the next hop for routes sent to all dynamic peers in the subnet.

Usage guidelines

By default, BGP does not set the local router as the next hop for EBGP routes sent to an IBGP peer or peer group. To ensure that an IBGP peer can find the next hop, you can use this command to specify the router as the next hop for routes sent to the IBGP peer.

The **peer next-hop-local** command is mutually exclusive with the **peer next-hop-invariable** command. Follow these restrictions and guidelines when you configure the commands for a peer or peer group:

- After you configure the **peer next-hop-local** command for a peer group, you cannot configure the **peer next-hop-invariable** command for the peer group or any peers in the peer group.
- After you configure the **peer next-hop-local** command for a peer, do not configure the **peer next-hop-invariable** command for the peer group to which the peer belongs. The configuration on the peer group will overwrite the configuration on the peer.

Examples

In BGP IPv4 unicast address family view, specify the router as the next hop for routes sent to peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4] peer test next-hop-local
```

peer password

Use **peer password** to enable MD5 authentication for a BGP peer or peer group.

Use **undo peer password** to remove MD5 authentication for a BGP peer or peer group.

Syntax

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **password** { **cipher** | **simple** } *password*

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **password**

Default

MD5 authentication is disabled.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command enables MD5 authentication for all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command enables MD5 authentication for all dynamic peers in the subnet.

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

password: Specifies the password. Its encrypted form is a case-sensitive string of 33 to 137 characters. Its plaintext form is a case-sensitive string of 1 to 80 characters.

Usage guidelines

You can enable MD5 authentication to enhance security using the following methods:

- Perform MD5 authentication when establishing TCP connections. Only the two parties that have the same password configured can establish TCP connections.
- Perform MD5 calculation on TCP segments to avoid modification to the encapsulated BGP packets.

The **peer keychain** and **peer password** commands are mutually exclusive.

Examples

In BGP instance view, perform MD5 authentication on the TCP connection between local router 10.1.100.1 and peer router 10.1.100.2. Set the authentication password to **aabbcc** in plaintext form.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] peer 10.1.100.2 password simple aabbcc
```

Related commands

peer keychain

peer preferred-value

Use **peer preferred-value** to set a preferred value for routes received from a peer or peer group.

Use **undo peer preferred-value** to remove the configuration.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view/BGP VPNv4 address family view/BGP VPNv6 address family view/BGP IPv4 multicast address family view/BGP IPv4 RT filter address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] } **preferred-value** *value*

undo peer { *group-name* | *ipv4-address* [*mask-length*] } **preferred-value**

In BGP IPv6 unicast address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **preferred-value** *value*

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **preferred-value**

In BGP-VPN IPv6 unicast address family view/BGP IPv6 multicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **preferred-value** *value*

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **preferred-value**

Default

The preferred value is 0 for routes received from a peer or peer group.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP VPNv4 address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

BGP VPNv6 address family view

BGP IPv4 multicast address family view

BGP IPv6 multicast address family view

BGP IPv4 RT filter address family view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command specifies a preferred value for routes received from all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command specifies a preferred value for routes received from all dynamic peers in the subnet.

value: Specifies a preferred value in the range of 0 to 65535.

Usage guidelines

If multiple routes that have the same destination are learned from different peers, you can specify different preferred values for the routes as needed to control BGP path selection. The one with the greatest preferred value is selected as the optimal route to the destination.

The preferred value is used for route selection on the local router and is not advertised to the peer. It has only local significance.

You can also use the **apply preferred-value** command in a routing policy to configure the preferred value for BGP routes. If both the **peer preferred-value** and **apply preferred-value** commands are configured, the **apply preferred-value** command applies. If the preferred value is not set in the routing policy or no routing policy is configured, the **peer preferred-value** command applies.

Examples

In BGP IPv4 unicast address family view, set the preferred value to 50 for routes from peer 1.1.1.1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4] peer 1.1.1.1 preferred-value 50
```

Related commands

apply preferred-value

route-policy

peer prefix-list

Use **peer prefix-list** to specify a prefix list to filter routes received from or advertised to a peer or peer group.

Use **undo peer prefix-list** to remove the prefix list specified to filter routes received from or advertised to a peer or peer group.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view/BGP VPNv4 address family view/BGP IPv4 multicast address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] } **prefix-list** *ipv4-prefix-list-name* { **export** | **import** }

undo peer { *group-name* | *ipv4-address* [*mask-length*] } **prefix-list** { **export** | **import** }

In BGP IPv6 unicast address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **prefix-list** *ipv6-prefix-list-name* { **export** | **import** }

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **prefix-list** { **export** | **import** }

In BGP-VPN IPv6 unicast address family view/BGP IPv6 multicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **prefix-list** *ipv6-prefix-list-name* { **export** | **import** }

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **prefix-list** { **export** | **import** }

In BGP VPNv6 address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] } **prefix-list** *ipv6-prefix-list-name* { **export** | **import** }

undo peer { *group-name* | *ipv4-address* [*mask-length*] } **prefix-list** { **export** | **import** }

Default

No prefix list based filtering is configured.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP VPNv4 address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

BGP VPNv6 address family view

BGP IPv4 multicast address family view

BGP IPv6 multicast address family view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command uses a prefix list to filter routes received from or advertised to all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command uses a prefix list to filter routes received from or advertised to all dynamic peers in the subnet.

ipv4-prefix-list-name: Specifies an IPv4 prefix list by its name, a case-sensitive string of 1 to 63 characters.

ipv6-prefix-list-name: Specifies an IPv6 prefix list by its name, a case-sensitive string of 1 to 63 characters.

export: Applies the filter to routes advertised to the specified peer/peer group.

import: Applies the filter to routes received from the specified peer/peer group.

Usage guidelines

The specified prefix list must have been created with the **ip prefix-list** or **ipv6 prefix-list** command in system view. If you specify a nonexistent IPv4/IPv6 prefix list, all routes can pass the prefix list.

Examples

In BGP IPv4 unicast address family view, use IPv4 prefix list **list1** to filter routes advertised to peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4] peer test prefix-list list1 export
```

Related commands

filter-policy export

filter-policy import

ip prefix-list

ipv6 prefix-list

peer as-path-acl

peer filter-policy

peer route-policy

peer public-as-only

Use **peer public-as-only** to remove private AS numbers in BGP updates sent to an EBGP peer or peer group.

Use **undo peer public-as-only** to remove the configuration.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view/BGP VPNv4 address family view/BGP VPNv6 address family view/BGP IPv4 multicast address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] } **public-as-only**

undo peer { *group-name* | *ipv4-address* [*mask-length*] } **public-as-only**

In BGP IPv6 unicast address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **public-as-only**

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **public-as-only**

In BGP-VPN IPv6 unicast address family view/BGP IPv6 multicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **public-as-only**

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **public-as-only**

Default

BGP updates sent to an EBGP peer or peer group can carry both public and private AS numbers.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP VPNv4 address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

BGP VPNv6 address family view

BGP IPv4 multicast address family view

BGP IPv6 multicast address family view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command removes private AS numbers in BGP updates sent to all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command removes private AS numbers in BGP updates sent to all dynamic peers in the subnet.

Usage guidelines

Private AS numbers are typically used in test networks, and need not be transmitted in public networks. The range of private AS numbers is from 64512 to 65535.

After you execute the command, you can get the following results:

- If the AS_PATH attribute of a BGP update carries only private AS numbers, the device removes the AS numbers before sending the update to the EBGP peer or peer group.
- If the AS_PATH attribute carries both public and private AS numbers, the command does not take effect. The device sends the BGP update to the EBGP peer or peer group without removing the private AS numbers.
- If the AS_PATH attribute carries AS numbers of the peer or peer group, the command does not take effect. The device sends the BGP update to the peer or peer group without removing the private AS numbers.

This command is applicable only to EBGP peers and peer groups.

Examples

In BGP IPv4 unicast address family view, remove private AS numbers in BGP updates sent to EBGP peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4] peer test public-as-only
```

peer reflect-client

Use **peer reflect-client** to configure the device as a route reflector and specify a peer or peer group as a client.

Use **undo peer reflect-client** to remove the configuration.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view/BGP VPNv4 address family view/BGP VPNv6 address family view/BGP IPv4 multicast address family view/BGP IPv4 MDT address family view/BGP IPv4 RT filter address family view/BGP IPv4 MVPN address family view/BGP IPv4 flowspec address family view/BGP VPNv4 flowspec address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] } **reflect-client**

undo peer { *group-name* | *ipv4-address* [*mask-length*] } **reflect-client**

In BGP IPv6 unicast address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **reflect-client**

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **reflect-client**

In BGP LS address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **reflect-client**

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **reflect-client**

In BGP IPv6 multicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **reflect-client**

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **reflect-client**

Default

Neither the route reflector nor the client is configured.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP VPNv4 address family view

BGP IPv6 unicast address family view

BGP LS address family view

BGP VPNv6 address family view

BGP IPv4 multicast address family view

BGP IPv6 multicast address family view

BGP IPv4 MDT address family view

BGP IPv4 RT filter address family view

BGP IPv4 MVPN address family view

BGP IPv4 flowspec address family view

BGP-VPN IPv4 flowspec address family view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command configures the device as a route reflector and specifies all dynamic peers in the subnet as clients.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command configures the device as a route reflector and specifies all dynamic peers in the subnet as clients.

Usage guidelines

Using route reflectors can solve the issue brought by too many IBGP connections. After you configure a device as a route reflector in an AS, it advertises routes as follows:

- Advertises routes received from a non-client IBGP peer to all clients.
- Advertises routes received from an IBGP peer that acts as a client to all peers.
- Advertises routes received from an EBGP peer to all peers.

Examples

In BGP IPv4 unicast address family view, configure the local device as a route reflector and specify IBGP peer group **test** as a client.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4] peer test reflect-client
```

Related commands

reflect between-clients

reflector cluster-id

peer route-limit

Use **peer route-limit** to set the maximum number of routes that can be received from a peer or peer group.

Use **undo peer route-limit** to remove the configuration.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view/BGP VPNv4 address family view/BGP VPNv6 address family view/BGP IPv4 multicast address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] } **route-limit** *prefix-number* [{ **alert-only** | **discard** | **reconnect** *reconnect-time* } | *percentage-value*] *

undo peer { *group-name* | *ipv4-address* [*mask-length*] } **route-limit**

In BGP IPv6 unicast address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **route-limit** *prefix-number* [{ **alert-only** | **discard** | **reconnect** *reconnect-time* } | *percentage-value*] *

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **route-limit**

In BGP IPv6 multicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **route-limit** *prefix-number* [{ **alert-only** | **discard** | **reconnect** *reconnect-time* } | *percentage-value*] *

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **route-limit**

Default

The number of routes that can be received from a peer or peer group is not limited.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP VPNv4 address family view

BGP IPv6 unicast address family view

BGP VPNv6 address family view

BGP IPv4 multicast address family view

BGP IPv6 multicast address family view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command specifies the maximum number of routes that can be received from all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command specifies the maximum number of routes that can be received from all dynamic peers in the subnet.

prefix-number: Specifies the number of routes that can be received from the peer or peer group.The value range for this argument is 1 to 4294967295.The router will tear down the session to the peer or peer group if the following conditions exist:

- The **alert-only**, **discard**, and **reconnect** keywords are not specified.
- The number of routes received from the peer or peer group reaches the *prefix-number*.

The router will not attempt to re-establish the session to a dynamic BGP peer until the router receives a connection request from the peer. For other peers, you can use the **reset bgp** command to re-establish the sessions.

alert-only: If the number of routes received from the peer or peer group reaches the *prefix-number*, the router generates a log message instead of tearing down the session to the peer or peer group. The router can continue to receive routes from the peer or peer group.

discard: If the number of routes received from the peer or peer group reaches the *prefix-number*, the router retains the session to the peer or peer group. However, it discards excess routes and generates a log message. After the number of routes received from the peer or peer group falls below the *prefix-number*, the router can continue to receive routes from the peer or peer group. To restore the discarded routes, use the **refresh bgp import** command to request the peer or peer group to resend the routes.

reconnect *reconnect-time*: Specifies a reconnect time. After the specified time is reached, the router re-establishes a session to the peer or peer group when the number of routes received from the peer or peer group reaches the *prefix-number*. The value range for the *reconnect-time* argument is 1 to 65535 seconds. This option is not available for dynamic BGP peers.

percentage-value: Specifies the threshold value for the router to generate a log message (the router generates a log message when the ratio of the number of received routes to the

prefix-number exceeds the percentage value). The value range of this argument is 1 to 100, and the default is 75.

Usage guidelines

When the number of routes received from the specified peer or peer group reaches *prefix-number*, the **discard** keyword takes effect on the device as follows:

- The device retains the routes already received from the peer or peer group.
- If the device receives subsequent routes from the peer or peer group, it will discard these routes.

Examples

In BGP IPv4 unicast address family view, set the maximum number of routes that can be received from peer 1.1.1.1 to 10000. Configure the router to tear down the session to the peer if the number is exceeded.

```
<Sysname> system-view
[Sysname] bgp 109
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4] peer 1.1.1.1 route-limit 10000
```

peer route-policy

Use **peer route-policy** to apply a routing policy to routes incoming from or outgoing to a peer or peer group.

Use **undo peer route-policy** to remove the configuration.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view/BGP VPNv4 address family view/BGP VPNv6 address family view/BGP IPv4 multicast address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] } **route-policy** *route-policy-name* { **export** | **import** }

undo peer { *group-name* | *ipv4-address* [*mask-length*] } **route-policy** { **export** | **import** }

In BGP IPv6 unicast address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **route-policy** *route-policy-name* { **export** | **import** }

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **route-policy** { **export** | **import** }

In BGP-VPN IPv6 unicast address family view/BGP IPv6 multicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **route-policy** *route-policy-name* { **export** | **import** }

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **route-policy** { **export** | **import** }

Default

No routing policy is applied to routes incoming from or outgoing to a peer or peer group.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP VPNv4 address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

BGP VPNv6 address family view

BGP IPv4 multicast address family view

BGP IPv6 multicast address family view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command applies a routing policy to routes incoming from or outgoing to all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command applies a routing policy to routes incoming from or outgoing to all dynamic peers in the subnet.

route-policy-name: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters.

export: Applies the routing policy to routes outgoing to the peer or peer group.

import: Applies the routing policy to routes incoming from the peer or peer group.

Usage guidelines

The specified routing policy must have been configured with the **route-policy** command in system view. If you specify a nonexistent routing policy, all routes can pass the routing policy.

The **apply** clause that modifies the AS path does not take effect in a routing policy applied to routes outgoing to an IBGP peer or peer group.

The **if-match interface** command, if configured for the applied routing policy, does not take effect on routes.

Examples

In BGP IPv4 unicast address family view, apply routing policy **test-policy** to routes outgoing to peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4] peer test route-policy test-policy export
```

Related commands

filter-policy export

filter-policy import

peer as-path-acl

peer filter-policy

peer prefix-list

route-policy

peer route-update-interval

Use **peer route-update-interval** to specify an interval for sending the same update to a peer or peer group.

Use **undo peer route-update-interval** to remove the configuration.

Syntax

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **route-update-interval** *interval*

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **route-update-interval**

Default

The interval for sending the same update to an IBGP peer is 15 seconds and the interval for sending the same update to an EBGP peer is 30 seconds.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command specifies an interval for sending the same update to all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command specifies an interval for sending the same update to all dynamic peers in the subnet.

interval: Specifies a minimum interval for sending the same update message, in the range of 0 to 600 seconds.

Usage guidelines

A BGP router sends an update message to its peers when a route is changed. If the route changes frequently, the BGP router sends many updates for the route, resulting in routing flaps. By configuring the interval for sending the same update to a peer or peer group, you can avoid such routing flaps. This command does not take effect on withdrawn routes. For withdrawn routes, BGP sends the withdrawal messages immediately.

Examples

In BGP instance view, set the interval for sending the same update to peer group **test** to 10 seconds.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] peer test as-number 100
[Sysname-bgp-default] peer test route-update-interval 10
```

peer soo

Use **peer soo** to configure the Site of Origin (SoO) attribute for a BGP peer or peer group.

Use **undo peer soo** to remove the configuration.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view/BGP VPNv4 address family view/BGP VPNv6 address family view/BGP IPv4 multicast address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] } **soo** *site-of-origin*

undo peer { *group-name* | *ipv4-address* [*mask-length*] } **soo**

In BGP IPv6 unicast address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **soo** *site-of-origin*

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **soo**

In BGP-VPN IPv6 unicast address family view/BGP IPv6 multicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **soo** *site-of-origin*

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **soo**

Default

No SoO attribute is configured for a peer or peer group.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP VPNv4 address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

BGP VPNv6 address family view

BGP IPv4 multicast address family view

BGP IPv6 multicast address family view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command configures the SoO attribute for all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command configures the SoO attribute for all dynamic peers in the subnet.

site-of-origin: Specifies the SoO attribute, a string of 3 to 21 characters. The SoO attribute has the following formats:

- *16-bit AS number:32-bit user-defined number*. For example, 100:3.
- *32-bit IP address:16-bit user-defined number*. For example, 192.168.122.15:1.
- *32-bit AS number:16-bit user-defined number*, where the minimum value of the AS number is 65536. For example, 65536:1.

Usage guidelines

The SoO attribute specifies the site where the route was originated. It prevents advertising a route back to the originating site. If the AS-path attribute is lost, the router can use the SoO attribute to avoid routing loops.

After you configure the SoO attribute for a BGP peer or peer group, BGP adds the SoO attribute into the route updates received from the BGP peer or peer group. Before advertising route updates to the peer or peer group, BGP checks the SoO attribute of the route update against the configured SoO attribute. If they are the same, BGP does not advertise the route updates to the BGP peer or peer group to avoid loops.

Examples

In BGP IPv4 unicast address family view, set the SoO attribute to 100:1 for peer 1.1.1.1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4
[Sysname-bgp-default-ipv4] peer 1.1.1.1 soo 100:1
```

Related commands

peer substitute-as

peer source-address

Use **peer source-address** to specify a source IPv4 or IPv6 address for establishing TCP connections to a peer or peer group.

Use **undo peer source-address** to remove the configuration.

Syntax

peer *ipv4-address* [*mask-length*] **source-address** *source-ipv4-address*

peer *ipv6-address* [*prefix-length*] **source-address** *source-ipv6-address*

undo peer { *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **source-address**

peer *group-name* **source-address** { *source-ipv4-address* | *source-ipv6-address* } *

undo peer *group-name* **source-address** [*source-ipv4-address* | *source-ipv6-address*]

Default

BGP uses the primary IPv4 or IPv6 address of the output interface in the optimal route destined for the BGP peer or peer group as the source address for TCP connection establishment.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command specifies a source IP address for establishing TCP connections to all dynamic peers in the subnet.

source-ipv4-address: Specifies a source IPv4 address.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command specifies a source IPv6 address for establishing TCP connections to all dynamic peers in the subnet.

source-ipv6-address: Specifies a source IPv6 address.

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

Usage guidelines

The **peer connect-interface** command and the **peer source-address** command can both change the source address for establishing TCP connections. If you execute both commands, the most recent configuration takes effect.

The **peer source-address** and **peer connect-interface** commands are applicable to the following scenarios:

- The peer's IPv4/IPv6 address does not belong to the interface directly connected to the local router. To ensure successful TCP connection establishment, use one of the following methods:
  - Specify the interface to which the IPv4/IPv6 address belongs as the source interface on the peer.
  - Specify the IPv4/IPv6 address of the interface directly connected to the local router as the source address on the peer.
- A BGP peer at an IPv6 link-local address must be directly connected to the local router. On the local router, you must use the **peer connect-interface** command to specify the interface directly connected to the BGP peer as the source interface of TCP connections.
- On a BGP router that has multiple links to a peer, the source interface for TCP connection changes because the primary source interface fails. To avoid this problem, specify a loopback interface as the source interface or specify the IP address of a loopback interface as the source address.

- You want to establish multiple BGP sessions to a router. In this case, BGP might fail to determine the source address for each TCP connection based on the optimal route to the peer. To prevent this problem, use one of the following methods:
  - If the BGP sessions use IP addresses of different interfaces, specify a source interface or source address for each session.
  - If the BGP sessions use different IP addresses of the same interface, specify a source address for each session.

The source addresses on the local router and the peer must be reachable to each other.

To specify the address of an indirectly connected interface as the source address, use the **peer ebgp-max-hop** command. The command allows the establishment of an EBGP session to the indirectly connected peer.

You can specify both a source IPv4 address and a source IPv6 address for a peer group. BGP uses the source IPv4 address to establish TCP connections to IPv4 peers in the group. It also uses the source IPv6 address to establish TCP connections to IPv6 peers in the group.

Examples

In BGP instance view, specify source IPv4 address 1.1.1.1 for peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] peer test source-address 1.1.1.1
```

Related commands

peer connect-interface

peer ebgp-max-hop

peer substitute-as

Use **peer substitute-as** to replace the AS number of a peer or peer group in the AS_PATH attribute with the local AS number.

Use **undo peer substitute-as** to remove the configuration.

Syntax

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **substitute-as**

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **substitute-as**

Default

The AS number of a peer or peer group in the AS_PATH attribute is not replaced.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command replaces the AS number of all dynamic peers in the subnet in the AS_PATH attribute with the local AS number.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command replaces the AS number of all dynamic peers in the subnet in the AS_PATH attribute with the local AS number.

Usage guidelines

If different CEs use the same AS number, you must configure this feature on the PE attached to the peer CE. With the feature enabled, upon advertising a route to the peer, the PE uses its own AS number to replace the peer AS number if it is contained in the AS_PATH attribute of the route. This ensures correct advertisement of private network routes.

Examples

In BGP instance view, substitute the local AS number for the AS number of peer 1.1.1.1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] peer 1.1.1.1 substitute-as
```

Related commands

peer soo

peer timer

Use **peer timer** to set a keepalive interval and hold time for a peer or peer group.

Use **undo peer timer** to remove the configuration.

Syntax

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **timer keepalive** *keepalive* **hold** *holdtime*

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **timer**

Default

The keepalive interval is 60 seconds, and the hold time is 180 seconds.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command configures a keepalive interval and hold time for all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command configures a keepalive interval and hold time for all dynamic peers in the subnet.

keepalive *keepalive*: Sets a keepalive interval in the range of 0 to 21845 seconds.

hold *holdtime*: Sets a hold time in the range of 3 to 65535 seconds. The hold time must be at least three times the keepalive interval.

Usage guidelines

After establishing a BGP session, two routers send keepalive messages at the specified keepalive interval to each other to keep the session.

If a router receives no keepalive or update message from the peer within the hold time, it tears down the session.

The timers configured with this command are preferred to the timers configured with the **timer** command.

If the hold time settings on the local and peer routers are different, the smaller one is used.

If the hold time is set to 0, no keepalive message will be sent to the peer, and the peer session will never time out. If neither the hold time nor the keepalive interval is set to 0, the actual keepalive interval is the smaller one between one third of the hold time and the keepalive interval.

The timers configured with this command do not take effect until a session is re-established (for example, a session is reset).

Examples

In BGP instance view, set the keepalive interval and hold time for peer group **test** to 60 seconds and 180 seconds, respectively.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] peer test timer keepalive 60 hold 180
```

Related commands

display bgp peer

timer

peer timer connect-retry

Use **peer timer connect-retry** to set the session retry timer for a peer or peer group.

Use **undo peer timer connect-retry** to remove the configuration.

Syntax

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **timer connect-retry** *retry-time*

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **timer connect-retry**

Default

The session retry timer is 32 seconds a peer or peer group.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command sets a connection retry timer for all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command sets a connection retry timer for all dynamic peers in the subnet.

retry-time: Specifies a session retry timer in the range of 1 to 65535 seconds.

Usage guidelines

To speed up session establishment to a peer or peer group and route convergence, set a small session retry timer. If the BGP session flaps, you can set a large session retry timer to reduce the impact.

The timer set by the **peer timer connect-retry** command takes precedence over the timer set by the **timer connect-retry** command.

Examples

In BGP instance view, set the session retry timer to 30 seconds for peer 1.1.1.1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] peer 1.1.1.1 timer connect-retry 30
```

Related commands

timer connect-retry

peer ttl-security

Use **peer ttl-security** to configure Generalized TTL Security Mechanism (GTSM) for a BGP peer or peer group.

Use **undo peer ttl-security** to disable BGP GTSM for a peer or peer group.

Syntax

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **ttl-security hops** *hop-count*

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **ttl-security hops**

Default

GTSM is disabled for BGP.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

context-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command configures GTSM for all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command configures GTSM for all dynamic peers in the subnet.

hops *hop-count*: Specifies the maximum number of hops to the specified peer, in the range of 1 to 254.

Usage guidelines

GTSM protects a BGP session by comparing the TTL value of an incoming IP packet against the valid TTL range. If the TTL value is within the valid TTL range, the packet is accepted. If not, the packet is discarded.

The valid TTL range is from 255 – the configured hop count + 1 to 255.

When GTSM is configured, the BGP packets sent by the device have a TTL of 255.

When GTSM is configured, the local device can establish an EBGP session to the peer after they pass GTSM check, regardless of whether the maximum number of hops is reached.

To use GTSM, you must configure GTSM on both the local and peer devices. You can specify different *hop-count* values for them.

Examples

In BGP instance view, enable GTSM for BGP peer group **test** and set the maximum number of hops to the specified peer in the peer group to 1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] peer test ttl-security hops 1
```

Related commands

peer ebgp-max-hop

pic

Use **pic** to enable BGP FRR for a BGP address family.

Use **undo pic** to disable BGP FRR for a BGP address family.

Syntax

pic

undo pic

Default

BGP FRR is disabled.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

Predefined user roles

network-admin

context-admin

Usage guidelines

FRR is used in a dual-homing network to protect a primary route with a backup route. It uses ARP (for IPv4), ND (for IPv6), or echo-mode BFD (for IPv4) to detect the connectivity of the primary route. When the primary route fails, BGP directs packets to the backup route.

After you enable FRR, BGP calculates a backup route for each BGP route in the address family if there are two or more unequal-cost routes to reach the destination.

You can also configure BGP FRR by using the **fast-reroute route-policy** command, which takes precedence over the **pic** command. For more information about routing policies, see *Layer 3—IP Routing Configuration Guide*.

Use the **pic** command with caution because it might cause routing loops in specific scenarios.

Examples

Enable BGP FRR in BGP IPv4 unicast address family view.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4] pic
```

Related commands

fast-reroute route-policy

preference

Use **preference** to configure preferences for BGP routes.

Use **undo preference** to restore the default.

Syntax

preference { *external-preference internal-preference local-preference* | **route-policy** *route-policy-name* }

undo preference

Default

The preferences of external, internal, and local BGP routes are 255, 255, and 130, respectively.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

BGP IPv4 multicast address family view

BGP IPv6 multicast address family view

Predefined user roles

network-admin

context-admin

Parameters

external-preference: Specifies a preference for EBGP routes, in the range of 1 to 255.

internal-preference: Specifies a preference for IBGP routes, in the range of 1 to 255.

local-preference: Specifies a preference for local routes, in the range of 1 to 255.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to set the route preference for matching routes. Routes not matching the routing policy use the default preference.

Usage guidelines

Different routing protocols might find different routes to the same destination. However, not all of those routes are optimal. For route selection, routing protocols, direct routes, and static routes are assigned different preferences. The route with the highest preference is preferred.

Configuring the preferences for BGP routes changes the possibility for the routes to become the optimal route.

To use a routing policy to set the preference, you must configure the preference with the **apply preference** command in the routing policy in advance. Otherwise, all matching routes use the default preference.

Examples

In BGP IPv4 unicast address family view, set preferences for EBGP, IBGP, and local routes to 20, 20, and 200, respectively.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4] preference 20 20 200
```

primary-path-detect bfd

Use **primary-path-detect bfd** to configure BGP FRR to use BFD to detect next hop connectivity for the primary route.

Use **undo primary-path-detect bfd** to restore the default.

Syntax

primary-path-detect bfd echo

undo primary-path-detect bfd

Default

BGP FRR uses ARP to detect the connectivity to the next hop of the primary route.

Views

BGP instance view

Predefined user roles

network-admin

context-admin

Parameters

echo: Uses echo-mode BFD to detect the connectivity to the next hop of the primary route.

Usage guidelines

With this command configured, the device automatically creates a BFD session of the IP FRR type for detecting next hop of the primary route. Upon detecting a failure, traffic immediately switches over to the backup next hop to ensure fast convergence.

This command takes effect and automatically creates a BFD session only when a backup next hop is available for the primary route.

In the current software version, BGP does not support calculating next hops for ECMP routes. The command cannot detect next hop connectivity for an ECMP route used as the primary route.

If another protocol (for example, OSPF and IS-IS) also uses BFD to detect next hop connectivity for the primary route, the protocol automatically creates a BFD session. If the detected link is the same as the link attached to the next hop of the BGP primary route, BGP reuses the BFD session created by the protocol, instead of creating a BFD session.

Examples

In BGP instance view, configure BGP FRR to use echo-mode BFD to detect next hop connectivity for the primary route.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] primary-path-detect bfd echo
```

Related commands

fast-reroute route-policy

pic

reflect between-clients

Use **reflect between-clients** to enable route reflection between clients.

Use **undo reflect between-clients** to disable route reflection between clients.

Syntax

reflect between-clients

undo reflect between-clients

Default

Route reflection between clients is enabled.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP VPNv4 address family view

BGP IPv6 unicast address family view

BGP LS address family view

BGP VPNv6 address family view

BGP IPv4 multicast address family view

BGP IPv6 multicast address family view

BGP IPv4 MDT address family view

BGP IPv4 RT filter address family view

BGP IPv4 MVPN address family view

BGP IPv4 flowspec address family view

BGP VPNv4 flowspec address family view

Predefined user roles

network-admin

context-admin

Usage guidelines

When a route reflector is configured, and the clients of a route reflector are fully meshed, route reflection is unnecessary because it consumes more bandwidth resources. You can use the **undo reflect between-clients** command to disable route reflection instead of modifying network configuration or changing network topology.

After route reflection is disabled between clients, routes can still be reflected between a client and a non-client.

Examples

In BGP IPv4 unicast address family view, disable route reflection between clients.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4] undo reflect between-clients
```

Related commands

peer reflect-client

reflector cluster-id

reflector cluster-id

Use **reflector cluster-id** to configure the cluster ID for a route reflector.

Use **undo reflector cluster-id** to restore the default.

Syntax

reflector cluster-id { *cluster-id* | *ipv4-address* }

undo reflector cluster-id

Default

A route reflector uses its router ID as the cluster ID.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP VPNv4 address family view

BGP IPv6 unicast address family view

BGP LS address family view

BGP VPNv6 address family view

BGP IPv4 multicast address family view

BGP IPv6 multicast address family view

BGP IPv4 MDT address family view

BGP IPv4 RT filter address family view

BGP IPv4 MVPN address family view

BGP IPv4 flowspec address family view

BGP VPNv4 flowspec address family view

Predefined user roles

network-admin

context-admin

Parameters

cluster-id: Specifies the cluster ID in the format of an integer, in the range of 1 to 4294967295.

ipv4-address: Specifies the cluster ID in the format of an IPv4 address in dotted decimal notation.

Usage guidelines

The route reflector and clients form a cluster. Typically a cluster has one route reflector. The ID of the route reflector is the cluster ID.

You can configure more than one route reflector in a cluster to improve network reliability and prevent a single point of failure. Use this command to configure the same cluster ID for all route reflectors in the cluster to avoid routing loops.

Do not configure the router ID of a client as the cluster ID.

Examples

In BGP IPv4 unicast address family view, set the cluster ID on the local router (a reflector in the cluster) to 80.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4] reflector cluster-id 80
```

Related commands

peer reflect-client

reflect between-clients

refresh bgp

Use **refresh bgp** to manually soft-reset BGP sessions.

Syntax

refresh bgp [**instance** *instance-name*] { *ipv4-address* [*mask-length*] | **all** | **external** | **group** *group-name* | **internal** } { **export** | **import** } **ipv4** [**multicast** | **mvpn** | **rtfilter** | [**flowspec** | **unicast**] [**vpn-instance** *vpn-instance-name*]]

refresh bgp [**instance** *instance-name*] { *ipv6-address* [*prefix-length*] | **all** | **external** | **group** *group-name* | **internal** } { **export** | **import** } **ipv6** [**multicast** | [**unicast**] [**vpn-instance** *vpn-instance-name*]]

refresh bgp [**instance** *instance-name*] *ipv4-address* [*mask-length*] { **export** | **import** } **ipv6** [**unicast**]

refresh bgp [**instance** *instance-name*] { *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] | **all** | **external** | **group** *group-name* | **internal** } { **export** | **import** } **link-state**

refresh bgp [**instance** *instance-name*] { *ipv4-address* [*mask-length*] | **all** | **external** | **group** *group-name* | **internal** } { **export** | **import** } **vpnv4** [**flowspec** | **vpn-instance** *vpn-instance-name*]

refresh bgp [**instance** *instance-name*] { *ipv4-address* [*mask-length*] | **all** | **external** | **group** *group-name* | **internal** } { **export** | **import** } **vpnv6**

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

instance *instance-name*: Specifies a BGP instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command soft-resets BGP sessions for the default BGP instance.

ipv4-address: Soft-resets the BGP session to a peer specified by its IP address.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command soft-resets BGP sessions to all dynamic peers in the subnet.

ipv6-address: Soft-resets the BGP session to a peer specified by its IPv6 address.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command soft-resets BGP sessions to all dynamic peers in the subnet.

all: Soft-resets all BGP sessions.

external: Soft-resets all EBGP sessions.

group *group-name*: Soft-resets the BGP sessions to the peers of the specified peer group. The *group-name* argument refers to the name of a peer group, a case-sensitive string of 1 to 47 characters.

internal: Soft-resets all IBGP sessions.

export: Performs outbound soft-reset (filters routes advertised to the specified peer or peer group by using the new configuration).

import: Performs inbound soft-reset (filters routes received from the specified peer or peer group by using the new configuration).

ipv4: Soft-resets BGP sessions for IPv4 address family.

ipv6: Soft-resets BGP sessions for IPv6 address family.

link-state: Soft-resets BGP sessions for LS address family.

multicast: Soft-resets BGP sessions for multicast address family.

mvpn: Soft-resets BGP sessions for IPv4 MVPN address family.

rtfilter: Soft-resets BGP sessions for IPv4 RT filter address family.

The following compatibility matrixes show the support of hardware platforms for the **rtfilter** keyword:

Models	Parameter compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	No

unicast: Soft-resets BGP sessions for unicast address family.

vpnv4: Soft-resets BGP sessions for VPNv4 address family.

vpnv6: Soft-resets BGP sessions for VPNv6 address family.

flowspec: Soft-resets BGP sessions for flowspec address family.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command soft-resets BGP sessions for the specified address family on the public network.

Usage guidelines

A soft-reset operation enables the router to apply a new route selection policy without tearing down BGP connections.

To apply a new policy to outbound BGP sessions, execute this command with the **export** keyword. The router uses the new policy to filter routing information and sends the routing information that passes the filtering to the BGP peers.

To apply a new policy to inbound sessions, execute this command with the **import** keyword. The router advertises a route-refresh message to the peer and the peer resends its routing information to

the router. After receiving the routing information, the router uses the new policy to filter the routing information.

This command requires that both the local router and the peer support route refresh.

If the **peer keep-all-routes** command is configured, the **refresh bgp import** command does not take effect.

By default, the **unicast** keyword is used if the **multicast**, **unicast**, **rtfilter**, and **flowspec** keywords are not specified.

Examples

Soft-reset all inbound BGP sessions for the IPv4 unicast address family.

```
<Sysname> refresh bgp all import ipv4
```

Related commands

peer capability-advertise route-refresh

peer keep-all-routes

reset bgp

Use **reset bgp** to reset BGP sessions for the specified address family.

Syntax

reset bgp [**instance** *instance-name*] { *as-number* | *ipv4-address* [*mask-length*] | **all** | **external** | **group** *group-name* | **internal** } **ipv4** [**mdt** | **multicast** | **mvpn** | **rtfilter** | [**flowspec** | **unicast**] [**vpn-instance** *vpn-instance-name*]]

reset bgp [**instance** *instance-name*] { *as-number* | *ipv6-address* [*prefix-length*] | **all** | **external** | **group** *group-name* | **internal** } **ipv6** [**multicast** | [**unicast**] [**vpn-instance** *vpn-instance-name*]]

reset bgp [**instance** *instance-name*] *ipv4-address* [*mask-length*] **ipv6** [**unicast**]

reset bgp [**instance** *instance-name*] { *as-number* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] | **all** | **external** | **group** *group-name* | **internal** } **link-state**

reset bgp [**instance** *instance-name*] { *as-number* | *ipv4-address* [*mask-length*] | **all** | **external** | **group** *group-name* | **internal** } **vpnv4** [**flowspec** | **vpn-instance** *vpn-instance-name*]

reset bgp [**instance** *instance-name*] { *as-number* | *ipv4-address* [*mask-length*] | **all** | **external** | **group** *group-name* | **internal** } **vpnv6**

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

instance *instance-name*: Specifies a BGP instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command resets BGP sessions for the default BGP instance.

as-number: Resets BGP sessions to peers in the AS specified by its number in the range of 1 to 4294967295.

ipv4-address: Resets the BGP session to a peer specified by its IPv4 address.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command resets BGP sessions to all dynamic peers in the subnet.

ipv6-address: Resets the BGP session to a peer specified by its IPv6 address.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command resets BGP sessions to all dynamic peers in the subnet.

all: Resets all BGP sessions.

external: Resets all EBGP sessions.

group *group-name*: Resets the BGP sessions to the peers in the peer group specified by its name, a case-sensitive string of 1 to 47 characters.

internal: Resets all IBGP sessions.

ipv4: Resets BGP sessions for IPv4 address family.

ipv6: Resets BGP sessions for IPv6 address family.

link-state: Resets BGP sessions for LS address family.

mdt: Resets BGP sessions for MDT address family.

multicast: Resets BGP sessions for multicast address family.

mvpn: Resets BGP sessions for IPv4 MVPN address family.

rtfilter: Resets BGP sessions for IPv4 RT filter address family.

The following compatibility matrixes show the support of hardware platforms for the **rtfilter** keyword:

Models	Parameter compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	No

unicast: Resets BGP sessions for unicast address family.

vpnv4: Resets BGP sessions for VPNv4 address family.

vpnv6: Resets BGP sessions for VPNv6 address family.

flowspec: Resets BGP sessions for flowspec address family.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command resets BGP sessions for the specified address family on the public network.

Usage guidelines

CAUTION:

A reset operation tears down BGP sessions for a short period of time.

A reset operation enables the router to apply a new route selection policy by re-establishing BGP sessions.

By default, the **unicast** keyword is used if the **unicast**, **mdt**, **mvpn**, **rtfilter**, **flowspec**, and **multicast** keywords are not specified.

Examples

Reset all BGP sessions for the IPv4 unicast address family.

```
<Sysname> reset bgp all ipv4
```

reset bgp all

Use **reset bgp all** to reset all BGP sessions for all address families.

Syntax

reset bgp [**instance** *instance-name*] **all**

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

instance *instance-name*: Specifies a BGP instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command resets all BGP sessions for all address families of the default BGP instance.

Usage guidelines

CAUTION:

A reset operation tears down BGP sessions for a short period of time.

A reset operation enables the router to apply a new route selection policy by re-establishing BGP sessions.

Examples

Reset all BGP sessions.

```
<Sysname> reset bgp all
```

reset bgp dampening

Use **reset bgp dampening** to clear BGP route dampening information and release suppressed BGP routes.

Syntax

reset bgp [**instance** *instance-name*] **dampening ipv4** [**multicast** | [**unicast**] [**vpn-instance** *vpn-instance-name*]] [*ipv4-address* [*mask-length* | *mask*]]

reset bgp [**instance** *instance-name*] **dampening ipv6** [**multicast** | [**unicast**] [**vpn-instance** *vpn-instance-name*]] [*ipv6-address prefix-length*]

reset bgp [**instance** *instance-name*] **dampening vpnv4** [*ipv4-address* [*mask* | *mask-length*]]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

instance *instance-name*: Specifies a BGP instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command clears BGP route dampening information and releases suppressed BGP routes for the default BGP instance.

ipv4: Clears BGP IPv4 route dampening information and releases suppressed BGP IPv4 routes.

ipv6: Clears BGP IPv6 route dampening information and releases suppressed BGP IPv6 routes.

vpnv4: Clears IBGP VPNv4 route dampening information and releases suppressed IBGP VPNv4 routes.

multicast: Clears BGP multicast route dampening information and releases suppressed BGP multicast routes.

unicast: Clears BGP unicast route dampening information and releases suppressed BGP unicast routes.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears BGP route dampening information for the public network, and releases suppressed BGP routes.

ipv4-address: Specifies an IPv4 destination network address. If you do not specify a network address, this command clears all BGP route dampening information, and releases all suppressed BGP routes.

mask-length: Specifies a mask length in the range of 0 to 32.

mask: Specifies a network mask in dotted decimal notation.

ipv6-address: Specifies an IPv6 destination network address. If you do not specify a network address, this command clears all BGP route dampening information, and releases all suppressed BGP routes.

prefix-length: Specifies a prefix length in the range of 0 to 128.

Usage guidelines

When you execute the **reset bgp dampening ipv4** command:

- If you specify only the *ipv4-address* argument, the system ANDs the network address with the mask of a route. If the result matches the network address of the route, the command clears dampening information for the route, and releases the suppressed route.
- If you specify the *ipv4-address mask* or *ipv4-address mask-length* argument, this command does the following:
  - Clears dampening information for the route that matches both the specified destination network address and the mask (or mask length).
  - Releases the suppressed route.

By default, the **unicast** keyword is used if neither the **unicast** keyword nor the **multicast** keyword is specified.

Examples

Clear dampening information for the BGP IPv4 unicast route to network 20.1.0.0/16 and release the suppressed route.

```
<Sysname> reset bgp dampening ipv4 20.1.0.0 255.255.0.0
```

Related commands

dampening

display bgp routing-table dampened

reset bgp flap-info

Use **reset bgp flap-info** to clear flap statistics for BGP routes.

Syntax

reset bgp [**instance** *instance-name*] **flap-info ipv4** [**multicast** | [**unicast**] [**vpn-instance** *vpn-instance-name*]] [*ipv4-address* [*mask-length* | *mask*] | **as-path-acl** *as-path-acl-number* | **peer** *ipv4-address* [*mask-length*]]

reset bgp [**instance** *instance-name*] **flap-info ipv6** [**multicast** | [**unicast**] [**vpn-instance** *vpn-instance-name*]] [*ipv6-address prefix-length* | **as-path-acl** *as-path-acl-number* | **peer** *ipv6-address* [*prefix-length*]]

reset bgp [**instance** *instance-name*] **flap-info vpnv4** [*ipv4-address* [*mask* | *mask-length*] | **as-path-acl** *as-path-acl-number* | **peer** *ipv4-address* [*mask-length*]]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

instance *instance-name*: Specifies a BGP instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command clears flap statistics for the default BGP instance.

ipv4: Clears flap statistics for BGP IPv4 routes.

ipv6: Clears flap statistics for BGP IPv6 routes.

vpnv4: Clears flap statistics for IBGP VPNv4 routes.

multicast: Clears flap statistics for BGP multicast routes.

unicast: Clears flap statistics for BGP unicast routes.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears flap statistics for public BGP routes.

ipv4-address: Specifies an IPv4 destination network address.

mask-length: Specifies a mask length in the range of 0 to 32.

mask: Specifies a network mask in dotted decimal notation.

ipv6-address: Specifies an IPv6 destination network address.

prefix-length: Specifies a prefix length in the range of 0 to 128.

as-path-acl *as-path-acl-number*: Specifies an AS path list by its number in the range of 1 to 256, to filter BGP route flap statistics.

peer *ipv4-address* [*mask-length*]: Clears flap statistics for BGP routes learned from the specified IPv4 BGP peer. The *mask-length* argument specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command clears flap statistics for BGP routes learned from all dynamic peers in the subnet.

peer *ipv6-address* [*prefix-length*]: Clears flap statistics for BGP routes learned from the specified IPv6 BGP peer. The *prefix-length* argument specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command clears flap statistics for BGP routes learned from all dynamic peers in the subnet.

Usage guidelines

When you execute the **reset bgp flap-info ipv4** command:

- If you specify only the *ipv4-address* argument, the system ANDs the IPv4 network address with the mask of a route. If the result matches the IPv4 network address of the route, this command clears the flap statistics of the route.
- If you specify the *ipv4-address mask* or *ipv4-address mask-length* argument, this command clears the flap statistics of the route that matches both the specified IPv4 destination network address and the mask (or mask length).

By default, the **unicast** keyword is used if neither the **unicast** keyword nor the **multicast** keyword is specified.

Examples

Clear flap statistics for the BGP IPv4 unicast route to network 20.1.0.0/16.

```
<Sysname> reset bgp flap-info ipv4 20.1.0.0 16
```

Related commands

dampening

display bgp routing-table flap-info

router id

Use **router id** to configure a global router ID.

Use **undo router id** to restore the default.

Syntax

router id *router-id*

undo router id

Default

No global router ID is configured.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

router-id: Specifies a router ID in IP address format.

Usage guidelines

Some routing protocols use a router ID to identify a device. You can configure a global router ID, which is used by routing protocols that have no router ID configured.

If no global router ID is configured, the highest loopback address, if any, is used as the router ID. If no loopback address is available, the highest physical interface IP address is used, regardless of the interface status. If no IP address is configured for any interface, the router ID is 0.0.0.0.

During an active/standby switchover, the standby main processing unit (MPU) checks the validity of the previous router ID backed up before switchover. If it is not valid, it selects a new router ID.

If the interface IP address that is selected as the router ID is removed or modified, a new router ID is selected. The following events will not trigger a router ID re-selection:

- The interface goes down.
- After a physical interface address is selected as the router ID, an IP address is configured for a loopback interface.
- A higher interface IP address is configured.

After you modify the global router ID and reset BGP sessions, the modification does not take effect for a BGP instance that uses the global router ID. To modify the router ID for the BGP instance, use the **router-id** command in BGP instance view.

Examples

Configure a global router ID as 1.1.1.1.

```
<Sysname> system-view
[Sysname] router id 1.1.1.1
```

Related commands

router-id (BGP instance view)

router-id (BGP instance view)

Use **router-id** to configure a router ID for a BGP instance.

Use **undo router-id** to restore the default.

Syntax

router-id *router-id*

undo router-id

Default

No router ID is configured for a BGP instance, and the BGP instance uses the global router ID configured by the **router id** command in system view.

Views

BGP instance view

Predefined user roles

network-admin

context-admin

Parameters

router-id: Specifies a router ID for BGP, in IP address format.

Usage guidelines

To run BGP, a BGP instance must have a router ID, which is an unsigned 32-bit integer that uniquely identifies the router in the AS.

To modify a non-zero router ID for BGP, execute the **router-id** command in BGP instance view.

To improve availability, specify the IP address of a loopback interface as the router ID for BGP.

If you execute this command in the same BGP instance view multiple times, the most recent configuration takes effect.

You can configure the same router ID for different BGP instances.

Examples

In BGP instance view, set the router ID for BGP to 1.1.1.1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] router-id 1.1.1.1
```

Related commands

router id

router-id (BGP-VPN instance view)

Use **router-id** to configure a router ID for a BGP VPN instance.

Use **undo router-id** to restore the default.

Syntax

router-id { *router-id* | **auto-select** }

undo router-id

Default

No router ID is configured for a BGP VPN instance, and the BGP VPN instance uses the router ID configured in BGP instance view. If no router ID is configured in BGP instance view, the BGP VPN instance uses the global router ID configured in system view.

Views

BGP-VPN instance view

Predefined user roles

network-admin

context-admin

Parameters

router-id: Specifies a router ID in IP address format.

auto-select: Automatically selects a router ID for the BGP VPN instance.

Usage guidelines

To run BGP, a VPN instance of a BGP instance must have a router ID, which is an unsigned 32-bit integer that uniquely identifies the BGP VPN router in the AS.

If the **auto-select** keyword is specified, the system selects a router ID for the BGP VPN instance in the following order:

1. The highest loopback address in the BGP VPN instance as the router ID.

2. The highest physical interface address in the BGP VPN instance as the router ID, regardless of the interface status.
3. 0.0.0.0 as the router ID.

If a non-zero router ID is selected for the BGP VPN instance, the router ID will not change when a more preferable router ID is available in the BGP VPN instance.

To improve availability, specify the IP address of a loopback interface as the router ID.

You can specify a different router ID for each VPN instance on a device.

If you execute this command in the same BGP-VPN instance view multiple times, the most recent configuration takes effect.

Examples

In BGP-VPN instance view, set the router ID to 1.1.1.1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] ip vpn-instance vpn1
[Sysname-bgp-default-vpn1] router-id 1.1.1.1
```

Related commands

router id

router-id (BGP instance view)

snmp context-name

Use **snmp context-name** to configure an SNMP context for a BGP instance.

Use **undo snmp context-name** to restore the default.

Syntax

snmp context-name *context-name*

undo snmp context-name

Default

No SNMP context is configured for a BGP instance.

Views

BGP instance view

Predefined user roles

network-admin

context-admin

Parameters

context-name: Specifies an SNMP context by its name, a case-sensitive string of 1 to 32 characters.

Usage guidelines

BGP does not know the BGP instance to which a managed MIB node belongs. To resolve this issue, configure different SNMP contexts for different BGP instances.

The device selects a MIB for an SNMP packet according to the context (for SNMPv3) or community name (for SNMPv1/v2c) in the following ways:

- For an SNMPv3 packet:

- The device selects the MIB of the BGP instance **default** if the packet does not carry a context and no SNMP context was configured for the BGP instance **default**.
- The device selects the MIB of a BGP instance if the packet meets the following conditions:
  - Carries a context that was configured with the **snmp-agent context** command in system view.
  - Matches the context of the BGP instance.
- The device does not process any MIBs in other situations.

- For an SNMPv1/v2c packet:
  - The device selects the MIB of the BGP instance **default** if the following conditions are met:
    - No SNMP community to SNMP context mapping was configured with the **snmp-agent community-map** command in system view.
    - No SNMP context was configured for the BGP instance **default**.
  - The device selects the MIB of a BGP instance if the SNMP community is mapped to an SNMP context and the context matches the context of the BGP instance.
  - The device does not process any MIBs in other situations.

For more information about SNMP contexts and community names, see *Network Management and Monitoring Configuration Guide*.

Do not configure the same SNMP context for different BGP instances.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure SNMP context **bgp-abc** for BGP instance **abc**.

```
<Sysname> system-view
[Sysname] bgp 100 instance abc
[Sysname-bgp-abc] snmp context-name bgp-abc
```

Related commands

snmp-agent community-map (*Network Management and Monitoring Command Reference*)

snmp-agent context (*Network Management and Monitoring Command Reference*)

snmp-agent trap enable bgp

Use **snmp-agent trap enable bgp** to enable SNMP notifications for BGP.

Use **undo snmp-agent trap enable bgp** to disable SNMP notifications for BGP.

Syntax

snmp-agent trap enable bgp [**instance** *instance-name*]

undo snmp-agent trap enable bgp [**instance** *instance-name*]

Default

SNMP notifications for BGP are enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

instance *instance-name*: Specifies a BGP instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command enables SNMP notifications for the default BGP instance.

Usage guidelines

After you enable SNMP notifications for BGP, the device generates a notification when a BGP neighbor state change occurs. The notification includes the neighbor address, the error code and subcode of the most recent error, and the current neighbor state.

For BGP notifications to be sent correctly, you must also configure SNMP on the device. For more information about SNMP configuration, see the network management and monitoring configuration guide for the device.

Examples

Enable SNMP notifications for BGP.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable bgp
```

summary automatic

Use **summary automatic** to configure automatic route summarization for redistributed IGP subnet routes.

Use **undo summary automatic** to restore the default.

Syntax

summary automatic

undo summary automatic

Default

Automatic route summarization is not performed for redistributed IGP subnet routes.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv4 multicast address family view

Predefined user roles

network-admin

context-admin

Usage guidelines

After the **summary automatic** command is configured, BGP summarizes IGP subnets redistributed by the **import-route** command.

Automatic summary routes can be manually summarized, but cannot be added to the IP routing table.

Examples

In BGP IPv4 unicast address family view, configure automatic route summarization for redistributed IGP subnet routes.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 unicast
```

```
[Sysname-bgp-default-ipv4] summary automatic
```

Related commands

aggregate

import-route

timer

Use **timer** to configure a BGP keepalive interval and hold time.

Use **undo timer** to restore the default.

Syntax

timer keepalive *keepalive* **hold** *holdtime*

undo timer

Default

The BGP keepalive interval and the hold time are 60 seconds and 180 seconds, respectively.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

context-admin

Parameters

keepalive *keepalive*: Configures a keepalive interval in the range of 0 to 21845 seconds.

hold *holdtime*: Configures a hold time in seconds, whose value is 0 or in the range of 3 to 65535. The hold time must be at least three times the keepalive interval.

Usage guidelines

After establishing a BGP session, two routers send keepalive messages at the specified keepalive interval to each other to keep the session.

If a router receives no keepalive or update message from the peer within the hold time, it tears down the session.

Use the **timer** command to configure the keepalive interval and hold time for all BGP peers. Use the **peer timer** command to configure the keepalive interval and hold time for a peer or peer group. If both commands are configured, the intervals configured by the **peer timer** command have higher priority.

If the hold time settings on the local and peer routers are different, the smaller one is used.

If the hold time is set to 0, no keepalive message will be sent to the peer, and the peer session will never time out. If neither the hold time nor the keepalive interval is set to 0, the actual keepalive interval is the smaller one between one third of the hold time and the keepalive interval.

The **timer** command affects only new BGP sessions.

After the **timer** command is executed, no peer session is closed at once. The configured hold time is used for negotiation in session re-establishment (for example, when you reset the BGP session).

Examples

In BGP instance view, set the keepalive interval and hold time to 60 seconds and 180 seconds, respectively.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] timer keepalive 60 hold 180
```

Related commands

display bgp peer

peer timer

timer connect-retry

Use **timer connect-retry** to set the session retry timer for all peers and peer groups.

Use **undo timer connect-retry** to restore the default.

Syntax

timer connect-retry *retry-time*

undo timer connect-retry

Default

The session retry timer is 32 seconds for all peers and peer groups.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

context-admin

Parameters

retry-time: Specifies a session retry timer in the range of 1 to 65535 seconds.

Usage guidelines

To speed up session establishment to a peer or peer group and route convergence, set a small session retry timer. If the BGP session flaps, you can set a large session retry timer to reduce the impact.

The timer set by the **peer timer connect-retry** command takes precedence over the timer set by the **timer connect-retry** command.

Examples

In BGP instance view, set the session retry timer to 30 seconds for all peers.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] timer connect-retry 30
```

Related commands

peer timer connect-retry

unicast-route recursive-lookup tunnel

Use **unicast-route recursive-lookup tunnel** to recurse unlabeled public BGP routes to LSPs.

Use **undo unicast-route recursive-lookup tunnel** to restore the default.

Syntax

In BGP IPv4 unicast address family view:

unicast-route recursive-lookup tunnel [**prefix-list** *ipv4-prefix-list-name*] [**tunnel-policy** *tunnel-policy-name*]

undo unicast-route recursive-lookup tunnel

In BGP IPv6 unicast address family view:

unicast-route recursive-lookup tunnel [**prefix-list** *ipv6-prefix-list-name*] [**tunnel-policy** *tunnel-policy-name*]

undo unicast-route recursive-lookup tunnel

Default

Unlabeled public BGP routes cannot be recursed to LSPs.

Views

BGP IPv4 unicast address family view

BGP IPv6 unicast address family view

Predefined user roles

network-admin

context-admin

Parameters

prefix-list *ipv4-prefix-list-name*: Recurses only unlabeled public BGP routes that match an IPv4 prefix list to LSPs. The *ipv4-prefix-list-name* argument specifies an IPv4 prefix list by its name, a case-sensitive string of 1 to 63 characters. If you do not specify this option, all unlabeled public BGP routes can be recursed to LSPs.

prefix-list *ipv6-prefix-list-name*: Recurses only unlabeled public BGP routes that match an IPv6 prefix list to LSPs. The *ipv6-prefix-list-name* argument specifies an IPv6 prefix list by its name, a case-sensitive string of 1 to 63 characters. If you do not specify this option, all unlabeled public BGP routes can be recursed to LSPs.

tunnel-policy *tunnel-policy-name*: Recurses unlabeled public BGP routes to only LSPs that match a tunnel policy. The *tunnel-policy-name* argument specifies a tunnel policy by its name, a case-sensitive string of 1 to 19 characters. If you do not specify this option, an unlabeled public BGP route can be recursed to any LSPs.

Usage guidelines

After you configure this command, unlabeled public BGP routes will be preferentially recursed to LSPs. If a route fails to be recursed to an LSP, the route will be recursed to the IP next hop.

If you execute this command multiple times for an address family, the most recent configuration takes effect.

Examples

In BGP IPv4 unicast address family view, recurse unlabeled public BGP routes to LSPs.

```
<Sysname> system-view
```

```
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4] unicast-route recursive-lookup tunnel
```

Contents

Policy-based routing commands

apply access-vpn

Use **apply access-vpn** to specify the forwarding tables that can be used for the matching packets.

Use **undo apply access-vpn** to remove the specified forwarding tables.

Syntax

apply access-vpn { **public** | **vpn-instance** *vpn-instance-name*&<1-4> }

undo apply access-vpn { **public** | **vpn-instance** [*vpn-instance-name*&<1-4>] }

Default

The device forwards matching packets by using the forwarding table for the network from which the packets are received.

Views

Policy node view

Predefined user roles

network-admin

context-admin

Parameters

public: Specifies the forwarding table for the public network.

vpn-instance: Specifies the forwarding table for the specified MPLS L3VPN instances.

vpn-instance-name&<1-4>: Specifies a space-separated list of up to n VPN instance names. A VPN instance name is a case-sensitive string of 1 to 31 characters. The specified VPN instance must already exist. The value for n is 4.

Usage guidelines

Use this command only in special scenarios that require sending packets received from one network to another network, for example, from a VPN to the public network, or from one VPN to another VPN.

You can repeat this command to specify the forwarding tables for the public network and VPN instances. The device forwards the matching packets by using the first available forwarding table selected in the order in which they are specified.

If you specify the **vpn-instance** keyword without specifying any VPN instances when you execute the **undo** form of this command, all the VPN instances are removed from the policy node.

After all the forwarding tables on the policy node are removed, the default forwarding behavior restores.

Examples

Specify the VPN 1 and VPN 2 forwarding tables on node 10. In this example, VPN 1 and VPN 2 already exist.

```
<Sysname> system-view
[Sysname] policy-based-route policy1 permit node 10
[Sysname-pbr-policy1-10] apply access-vpn vpn-instance vpn1 vpn2
```

Specify the public network forwarding table on node 10.

```
<Sysname> system-view
[Sysname] policy-based-route policy1 permit node 10
[Sysname-pbr-policy1-10] apply access-vpn public
```

Related commands

apply remark-vpn

apply continue

Use **apply continue** to compare packets with the next policy node upon failure on the current node.

Use **undo apply continue** to restore the default.

Syntax

apply continue

undo apply continue

Default

PBR does not compare packets with the next policy node upon failure on the current node.

Views

Policy node view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command takes effect only when the match mode of the node is **permit**.

This command applies when either of the following conditions exist:

- None of the following clauses is configured for packet forwarding:
  - **apply access-vpn**
  - **apply next-hop**
  - **apply output-interface**
  - **apply default-next-hop**
  - **apply default-output-interface**
- A clause listed above is configured, but it has become invalid. Then, a routing table lookup also fails for the matching packet.

NOTE:

A clause might become invalid because the specified next hop is unreachable, packets cannot be forwarded in the specified VPN instance, or the specified output interface is down.

Examples

Compare with the next policy node upon failure on the current node.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] apply continue
```

apply default-next-hop

Use **apply default-next-hop** to set default next hops.

Use **undo apply default-next-hop** to remove default next hops.

Syntax

apply default-next-hop [**vpn-instance** *vpn-instance-name* | **inbound-vpn**] { *ip-address* [**direct**] [**track** *track-entry-number*] }&<1-4>

undo apply default-next-hop [[**vpn-instance** *vpn-instance-name* | **inbound-vpn**] *ip-address*&<1-4>]

Default

No default next hops are set.

Views

Policy node view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. The specified VPN instance must already exist.

inbound-vpn: Specifies the VPN instance where the inbound interface belongs.

ip-address: Specifies the IP address of a default next hop. If you do not specify the **vpn-instance** *vpn-instance-name* option or the **inbound-vpn** keyword, the default next hop belongs to the public network.

direct: Specifies a directly connected default next hop.

track *track-entry-number*: Specifies a track entry by its number in the range of 1 to 1024.

&<1-4>: Indicates that you can specify up to four default next hops, each of which can be associated with a track entry.

Usage guidelines

You can specify multiple default next hops for backup or load sharing in one command line or by executing this command multiple times.

With a default next hop specified, the **undo apply default-next-hop** command removes the default next hop.

Without any default next hop specified, the **undo apply default-next-hop** command removes all default next hops.

Examples

Set a directly-connected default next hop of 1.1.1.1.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] apply default-next-hop 1.1.1.1 direct
```

Related commands

apply loadshare

apply default-output-interface

Use **apply default-output-interface** to set default output interfaces.

Use **undo apply default-output-interface** to remove default output interfaces.

Syntax

apply default-output-interface { *interface-type interface-number* [**track** *track-entry-number*] }&<1-4>

undo apply default-output-interface [{ *interface-type interface-number* }&<1-4>]

Default

No default output interfaces are set.

Views

Policy node view

Predefined user roles

network-admin

context-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

track *track-entry-number*: Specifies a track entry by its number in the range of 1 to 1024.

&<1-4>: Indicates that you can specify up to four interfaces, each of which can be associated with a track entry.

Usage guidelines

You can specify multiple default output interfaces for backup or load sharing in one command line or by executing this command multiple times.

The default output interface must be P2P type. Using a non-P2P default output interface can result in forwarding failures when the interface has multiple next hops. Non-P2P interfaces include broadcast interfaces such as Ethernet interfaces.

With a default output interface specified, the **undo apply default-output-interface** command removes the default output interface.

Without any default output interface specified, the **undo apply default-output-interface** command removes all default output interfaces.

Examples

Specify GigabitEthernet 1/0/1 as the default output interface for IP packets.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] apply default-output-interface gigabitethernet 1/0/1
```

Related commands

apply loadshare

apply ip-df

Use **apply ip-df** to set the Don't Fragment (DF) bit in the IP header of matching packets.

Use **undo apply ip-df** to restore the default.

Syntax

apply ip-df *df-value*

undo apply ip-df

Default

The DF bit is not set.

Views

Policy node view

Predefined user roles

network-admin

context-admin

Parameters

df-value: Sets the DF bit in the IP header of matching packets. The value can be 0 or 1.

Usage guidelines

Setting the DF bit to 0 allows packet fragmentation.

Setting the DF bit to 1 prohibits packet fragmentation.

Examples

Set the DF bit in the IP header of matching packets to 0.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] apply ip-df 0
```

apply loadshare

Use **apply loadshare** to enable load sharing among multiple next hops, output interfaces, default next hops, or default output interfaces.

Use **undo apply loadshare** to restore the default.

Syntax

apply loadshare { **default-next-hop** | **default-output-interface** | **next-hop** | **output-interface** }

undo apply loadshare { **default-next-hop** | **default-output-interface** | **next-hop** | **output-interface** }

Default

Multiple next hops, output interfaces, default next hops, or default output interfaces operate in primary/backup mode.

Views

Policy node view

Predefined user roles

network-admin

context-admin

Parameters

`default-next-hop`: Enables load sharing among multiple default next hops.

`default-output-interface`: Enables load sharing among multiple default output interfaces.

`next-hop`: Enables load sharing among multiple next hops.

`output-interface`: Enables load sharing among multiple output interfaces.

Usage guidelines

Multiple next hop, output interface, default next hop, or default output interface options operate in either primary/backup or load sharing mode.

- **Primary/backup mode**—One option is selected from all options in configuration order for packet forwarding, with all remaining options as backups. For example, if multiple output interfaces are configured, the first configured output interface is selected. When the selected output interface fails, the next available output interface takes over.
- **Load sharing mode**—Matching traffic is distributed across the available options, as follows:
  - **Multiple output interface, default next hop, or default output interface options**—Load share traffic in round robin manner, starting from the first configured option. They perform per-packet load sharing for traffic that does not match any fast forwarding entry, and perform per-flow load sharing for traffic that matches a fast forwarding entry.
  - **Multiple next hops**—Load share traffic in proportion to their weight. By default, all next hops have the same weight and traffic is evenly distributed among them.

Examples

Enable load sharing among multiple next hops.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] apply next-hop 1.1.1.1 2.2.2.2
[Sysname-pbr-aa-11] apply loadshare next-hop
```

Enable load sharing among multiple output interfaces.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] apply output-interface gigabitethernet 1/0/1 gigabitethernet 1/0/2
[Sysname-pbr-aa-11] apply loadshare output-interface
```

Enable load sharing among multiple default next hops.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] apply default-next-hop 1.1.1.1 2.2.2.2
[Sysname-pbr-aa-11] apply loadshare default-next-hop
```

Enable load sharing among multiple default output interfaces.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] apply default-output-interface gigabitethernet 1/0/1 gigabitethernet
1/0/2
[Sysname-pbr-aa-11] apply loadshare default-output-interface
```

Related commands

`apply default-next-hop`

`apply default-output-interface`

`apply next-hop`

apply output-interface

apply next-hop

Use **apply next-hop** to set next hops.

Use **undo apply next-hop** to remove next hops.

Syntax

apply next-hop [**vpn-instance** *vpn-instance-name* | **inbound-vpn**] { *ip-address* [**direct**] [**track** *track-entry-number*] [**weight** *weight-value*] }&<1-4>

undo apply next-hop [[**vpn-instance** *vpn-instance-name* | **inbound-vpn**] *ip-address*&<1-4>]

Default

No next hops are set.

Views

Policy node view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. The specified VPN instance must already exist.

inbound-vpn: Specifies the VPN instance where the inbound interface belongs.

ip-address: Specifies the IP address of a next hop. If you do not specify the **vpn-instance** *vpn-instance-name* option or the **inbound-vpn** keyword, the next hop belongs to the public network.

direct: Specifies that the next hop must be directly connected to take effect.

track *track-entry-number*: Specifies a track entry by its number in the range of 1 to 1024.

weight *weight-value*: Specifies a load sharing weight for the next hop, in the range of 1 to 100. The default is 10. If you specify weights 1, 1, and 2 for three next hops, they share 1/4, 1/4, and 1/2 of the whole traffic, respectively.

&<1-4>: Indicates that you can specify up to four next hops, each of which can be associated with a track entry.

Usage guidelines

You can specify multiple next hops for backup or load sharing in one command line or by executing this command multiple times.

With a next hop specified, the **undo apply next-hop** command removes the next hop.

Without any next hop specified, the **undo apply next-hop** command removes all next hops.

Examples

Set a directly-connected next hop of 1.1.1.1.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] apply next-hop 1.1.1.1 direct
```

Related commands

apply loadshare

apply output-interface

Use **apply output-interface** to set output interfaces.

Use **undo apply output-interface** to remove output interfaces.

Syntax

apply output-interface { *interface-type interface-number* [**track** *track-entry-number*] }&<1-4>

undo apply output-interface [{ *interface-type interface-number* }&<1-4>]

Default

No output interfaces are set.

Views

Policy node view

Predefined user roles

network-admin

context-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

track *track-entry-number*: Specifies a track entry by its number in the range of 1 to 1024.

&<1-4>: Indicates that you can specify up to four interfaces, each of which can be associated with a track entry.

Usage guidelines

You can specify multiple output interfaces for backup or load sharing in one command line or by executing this command multiple times.

The output interface must be P2P type. Using a non-P2P output interface can result in forwarding failures when the interface has multiple next hops. Non-P2P interfaces include broadcast interfaces such as Ethernet interfaces.

With an output interface specified, the **undo apply output-interface** command removes the output interface.

Without any output interface specified, the **undo apply output-interface** command removes all output interfaces.

Examples

Specify GigabitEthernet 1/0/1 as the output interface for IP packets.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] apply output-interface gigabitethernet 1/0/1
```

Related commands

apply loadshare

apply precedence

Use **apply precedence** to set a precedence for IP packets.

Use **undo apply precedence** to restore the default.

Syntax

apply precedence { *type* | *value* }

undo apply precedence

Default

No precedence is set for IP packets.

Views

Policy node view

Predefined user roles

network-admin

context-admin

Parameters

type: Specifies the precedence type for IP packets.

value: Specifies the precedence for IP packets. Eight precedence values (0 to 7) are available. Each precedence value corresponds to a precedence type, as shown in Table 1. You can set either a precedence value or a precedence type for IP packets.

Table 1 IP precedences and corresponding types

Precedence value	Precedence type
0	routine
1	priority
2	immediate
3	flash
4	flash-override
5	critical
6	internet
7	network

Examples

Set the precedence to 5 (critical) for IP packets.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] apply precedence critical
```

apply remark-vpn

Use **apply remark-vpn** to enable VPN remark action.

Use **undo apply remark-vpn** to restore the default.

Syntax

apply remark-vpn

undo apply remark-vpn

Default

VPN remark action is not configured.

Views

Policy node view

Predefined user roles

network-admin

context-admin

Usage guidelines

VPN remark action marks the matching packets as belonging to the VPN instance to which they are forwarded based on the **apply access-vpn vpn-instance** command. All subsequent service modules of PBR handle the packets as belonging to the re-marked VPN instance.

If the VPN remark action is not enabled, the forwarded matching packets are marked as belonging to the VPN instance or the public network from which they were received.

VPN remark action applies only to packets that have been successfully forwarded based on the **apply access-vpn vpn-instance** command.

Examples

Forward packets that match ACL 3000 based on the forwarding table of VPN instance **vpn1** and perform VPN remark action on the successfully forwarded packets.

```
<Sysname> system-view
[Sysname] policy-based-route aaa permit node 10
[Sysname-pbr-aaa-10] if-match acl 3000
[Sysname-pbr-aaa-10] apply access-vpn vpn-instance vpn1
[Sysname-pbr-aaa-10] apply remark-vpn
```

Related commands

apply access-vpn vpn-instance

display ip policy-based-route

Use **display ip policy-based-route** to display PBR policy information.

Syntax

display ip policy-based-route [**policy** *policy-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

policy *policy-name*: Specifies a policy by its name, a case-sensitive string of 1 to 19 characters. If you do not specify a policy, this command displays information for all PBR policies.

Examples

Display all policy information.

```
<Sysname> display ip policy-based-route
Policy name: aaa
  node 1 permit:
    if-match acl 2000
    apply next-hop 1.1.1.1
```

Table 2 Command output

Field	Description
node 1 permit	The match mode of Node 1 is **permit**.
if-match acl	Compares packets with the ACL.
apply next-hop	Specifies a next hop for permitted packets.

Related commands

policy-based-route

display ip policy-based-route interface

Use **display ip policy-based-route interface** to display interface PBR configuration and statistics.

Syntax

display ip policy-based-route interface *interface-type interface-number* [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information on the master device.

Examples

Display PBR configuration and statistics on GigabitEthernet 1/0/1.

```
<Sysname> display ip policy-based-route interface gigabitethernet 1/0/1
Policy based routing information for interface GigabitEthernet1/0/1(failed):
Policy name: aaa
```

```
  node 0 deny:
  Matched: 0
  node 1 permit:
    if-match acl 3999
  Matched: 0
  node 2 permit:
    if-match acl 2000
    apply next-hop 2.2.2.2
  Matched: 0
  node 5 permit:
    if-match acl 3101
    apply next-hop 1.1.1.1
    apply output-interface GigabitEthernet1/0/2 track 1 (down)
    apply output-interface GigabitEthernet1/0/3 track 2 (inactive)
  Matched: 0
Total matched: 0
```

Table 3 Command output

Field	Description
Policy based routing information for interface *XXXX*	PBR configuration and statistics on the interface. This field displays **failed** in brackets if none of the nodes in the policy has been successfully issued to the driver. To issue the policy, you must remove the policy from the interface and then apply it on the interface again. **NOTE:** The **failed** status is available on a per-slot basis. To obtain this information, you must specify a slot number when you execute the command. • For a global interface (for example, a VLAN interface), which might have member physical interfaces on multiple slots, specify a slot that contains its member interfaces. • For a physical interface, specify its slot number.
node 0 deny node 2 permit	Match mode of the node, **permit** or **deny**. If a node fails to be issued to the driver, the command displays the cause in brackets, which include: • **not support**—The device does not support the match criteria configured on the node. • **no resource**—No sufficient resources (for example, ACLs) are available for the node. **NOTE:** The cause is available only on a per-slot basis. To obtain this information, you must specify a slot number when you execute the command. • For a global interface (for example, a VLAN interface), which might have member physical interfaces on multiple slots, specify a slot that contains its member interfaces. • For a physical interface, specify its slot number.
if-match acl	Compares packets with the ACL.
apply next-hop	Specifies a next hop for permitted packets.
apply output-interface track 1	Specifies an output interface and its associated track entry for permitted packets.

Field	Description
	This field displays the interface status in brackets. • **down**—The interface is down at network layer. • **inactive**—The card that hosts the interface is not in position.
Matched	Number of successful matches on the node. If the device does not have sufficient resources to count matches, this field displays **no statistics resource** in brackets. **NOTE:** The statistics collection failure cause is available only on a per-slot basis. To obtain this information, you must specify a slot number when you execute the command. • For a global interface (for example, a VLAN interface), which might have member physical interfaces on multiple slots, specify a slot that contains its member interfaces. • For a physical interface, specify its slot number.
Total matched	Total number of successful matches on all nodes.

Related commands

ip policy-based-route

display ip policy-based-route local

Use **display ip policy-based-route local** to display local PBR configuration and statistics.

Syntax

display ip policy-based-route local [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays local PBR configuration and statistics for the master device.

Examples

Display local PBR configuration and statistics.

```
<Sysname> display ip policy-based-route local
Policy based routing information for local:
Policy name: aaa
  node 0 deny:
  Matched: 0
  node 1 permit:
    if-match acl 3999
```

```
  Matched: 0
  node 2 permit:
    if-match acl 2000
    apply next-hop 2.2.2.2
  Matched: 0
  node 5 permit:
    if-match acl 3101
    apply next-hop 1.1.1.1
  Matched: 0
Total matched: 0
```

Table 4 Command output

Field	Description
Policy based routing information for local	Local PBR configuration and statistics.
node 0 deny/node 2 permit	Match mode of the node: permit or deny.
if-match acl	Compares packets with the ACL.
apply next-hop	Specifies a next hop for permitted packets.
Matched	Number of successful matches on the node.
Total matched	Total number of successful matches on all nodes.

Related commands

`ip local policy-based-route`

display ip policy-based-route setup

Use **`display ip policy-based-route setup`** to display PBR configuration.

Syntax

`display ip policy-based-route setup`

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display PBR configuration.

```
Policy name              Type     Interface
aaa                      Forward  GigabitEthernet1/0/1
aaa                      Forward  GigabitEthernet1/0/2
aaa                      Local    N/A
```

Table 5 Command output

Field	Description
Type	Type of the PBR: • **Forward**—Interface PBR. • **Local**—Local PBR.
Interface	Interface where the policy is applied. This field displays **N/A** for a local PBR policy.

if-match acl

Use **if-match acl** to set an ACL match criterion.

Use **undo if-match acl** to restore the default.

Syntax

if-match acl { *acl-number* | **name** *acl-name* }

undo if-match acl

Default

No ACL match criterion is set.

Views

Policy node view

Predefined user roles

network-admin

context-admin

Parameters

acl-number: Specifies an ACL by its number in the range of 2000 to 2999 for a basic ACL, and in the range of 3000 to 3999 for an advanced ACL.

name *acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters starting with letter *a* to *z* or *A* to *Z*. The ACL name cannot be **all**. For the command to take effect, make sure the specified ACL is a basic or advanced ACL.

Usage guidelines

If the specified ACL does not exist or has no rules configured, no packets will match the ACL.

If the **vpn-instance** keyword is specified for an ACL rule, the rule applies to only VPN packets. If the **vpn-instance** keyword is not specified, the rule applies to only public network packets.

Examples

Configure Node 11 of policy **aa** to permit the packets matching ACL 2011.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] if-match acl 2011
```

Configure Node 11 of policy **aa** to permit the packets matching ACL **aaa**.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] if-match acl name aaa
```

if-match app-group

Use **if-match app-group** to set application group match criteria.

Use **undo if-match app-group** to delete application group match criteria.

Syntax

if-match app-group *app-group-name*&<1-6>

undo if-match app-group [*app-group-name*&<1-6>]

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB1180, NFNX3-HDB1480	No

Default

No application group match criteria are set.

Views

Policy node view

Predefined user roles

network-admin

context-admin

Parameters

app-group-name&<1-6>: Specifies up to six application groups by their names. An application group name is a case-insensitive string of 1 to 63 characters, which can contain letters, digits, underscores (_), and hyphens (-). The application group name cannot be **Invalid**, **other**, or any application group name predefined by the system.

Usage guidelines

The application match criteria apply only to interface PBR.

If you specify an application group, the **undo if-match app-group** command deletes the application group match criterion.

If you do not specify an application group, the **undo if-match app-group** command deletes all application group match criteria.

Examples

Specify the application group **test** as a match criterion.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] if-match app-group test
```

if-match object-group

Use **if-match object-group** to set service object group match criteria.

Use **undo if-match object-group** to delete service object group match criteria.

Syntax

if-match object-group service *object-group-name*&<1-6>

undo if-match object-group service [*object-group-name*&<1-6>]

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB1180, NFNX3-HDB1480	No

Default

No service object group match criteria are set.

Views

Policy node view

Predefined user roles

network-admin

context-admin

Parameters

object-group-name&<1-6>: Specifies up to six service object groups by their names. A service object group name is a case-insensitive string of 1 to 63 characters, which can contain letters, digits, underscores (_), and hyphens (-).

Usage guidelines

If you specify a service object group, the **undo if-match object-group** command deletes the service object group match criterion.

If you do not specify a service object group, the **undo if-match object-group** command deletes all service object group match criteria.

Examples

Specify the service object group **test** as a match criterion.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] if-match object-group service test
```

if-match packet-length

Use **if-match packet-length** to set a packet length match criterion.

Use **undo if-match packet-length** to restore the default.

Syntax

if-match packet-length *min-len max-len*

undo if-match packet-length

Default

No packet length match criterion is set.

Views

Policy node view

Predefined user roles

network-admin

context-admin

Parameters

min-len: Specifies the minimum IP packet length in the range of 1 to 65535 bytes.

max-len: Specifies the maximum IP packet length in the range of 1 to 65535 bytes. The maximum length must be no less than the minimum length.

Usage guidelines

Use this command to set a criterion to match the total length of data packets.

The packet length range includes boundary values. For example, if you set the *min-len* and *max-len* arguments to 100 and 200, respectively, packets with lengths of 100 bytes and 200 bytes are also matched.

Examples

Match packets with a length from 100 to 200 bytes.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] if-match packet-length 100 200
```

if-match source-ip

Use **if-match source-ip** to set a source IP address match criterion to match locally generated packets.

Use **undo if-match source-ip** to delete the source IP address match criterion to match locally generated packets.

Syntax

if-match source-ip { **interface** *interface-type interface-number* | [**vpn-instance** *vpn-instance-name*] *ip-address* }

undo if-match source-ip

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	No

Default

No source IP address match criterion is set.

Views

Policy node view

Predefined user roles

network-admin

context-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. The primary IP address of the interface will be used to match packets.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the specified IP address belongs to the public network.

ip-address: Specifies an IP address in dotted decimal notation.

Usage guidelines

This command matches locally generated packets sent out with the specified IP address or the primary IP address of the specified interface.

Typically, you use this command to make sure local tunneled or VPN traffic (for example, IPsec packets) is sent towards the correct ISP when the device is dual- or multi-homed to different ISPs. This command helps you avoid packet drops that might occur when packets are sent to an incorrect ISP.

For the matching traffic, use the **apply next-hop** or **apply output-interface** command to specify the next hop or the output interface. As a best practice, specify the output interface in the **apply** clause if you specify the source interface in the **if-match** clause.

If you execute this command multiple times on a policy node, the most recent configuration takes effect.

Examples

Match locally generated packets with source IP address 1.1.1.1.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] if-match source-ip 1.1.1.1
```

ip local policy-based-route

Use **ip local policy-based-route** to specify a policy for local PBR.

Use **undo ip local policy-based-route** to restore the default.

Syntax

ip local policy-based-route *policy-name*

undo ip local policy-based-route

Default

No policy is specified for local PBR.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies a policy by its name, a case-sensitive string of 1 to 19 characters. The specified policy must already exist.

Usage guidelines

Local PBR guides the forwarding of locally generated packets, such as ICMP packets generated by using the **ping** command.

Local PBR might affect local services, such as ping and Telnet. When you use local PBR, make sure you fully understand its impact on local services of the device.

You can specify only one policy for local PBR and must make sure the specified policy already exists.

Before you apply a new policy, you must first remove the current policy.

Examples

Configure local PBR based on policy **aaa**.

```
<Sysname> system-view
[Sysname] ip local policy-based-route aaa
```

Related commands

display ip policy-based-route local

ip policy-based-route

Use **ip policy-based-route** to specify a policy for interface PBR on an interface.

Use **undo ip policy-based-route** to restore the default.

Syntax

ip policy-based-route *policy-name*

undo ip policy-based-route

Default

No policy is applied to an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies a policy by its name, a case-sensitive string of 1 to 19 characters. The specified policy must already exist.

Examples

Apply policy **aaa** to GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip policy-based-route aaa
```

Related commands

display ip policy-based-route interface

policy-based-route

Use **policy-based-route** to create a policy node and enter its view, or enter the view of an existing policy node.

Use **undo policy-based-route** to delete a policy or policy node.

Syntax

policy-based-route *policy-name* [**deny** | **permit**] **node** *node-number*

undo policy-based-route *policy-name* [**deny** | **node** *node-number* | **permit**]

Default

No policy nodes exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies a policy by its name, a case-sensitive string of 1 to 19 characters.

deny: Specifies the match mode for the policy node as **deny**.

permit: Specifies the match mode for the policy node as **permit** (default mode).

node *node-number*: Specifies a policy node by its number. A smaller number has a higher priority. The value range for the *node-number* argument is 0 to 65535.

Usage guidelines

A policy that has been applied to an interface or locally cannot be deleted. To delete it, you must first cancel the application.

- If a policy node is specified, the **undo policy-based-route** command deletes the specified policy node.
- If a match mode is specified, the command deletes all nodes configured with the match mode.
- If no policy node or match mode is specified, the command deletes the whole policy.

Examples

Create permit-mode of Node 10 for policy **policy1** and enter its view.

```
<Sysname> system-view
[Sysname] policy-based-route policy1 permit node 10
[Sysname-pbr-policy1-10]
```

Related commands

display ip policy-based-route

reset ip policy-based-route statistics

Use **reset ip policy-based-route statistics** to clear PBR statistics.

Syntax

reset ip policy-based-route statistics [**policy** *policy-name*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

policy *policy-name*: Specifies a policy by its name, a case-sensitive string of 1 to 19 characters. If you do not specify a policy, this command clears PBR statistics for all policies.

Examples

Clear all PBR statistics.

```
<Sysname> reset ip policy-based-route statistics
```

Contents

IPv6 policy-based routing commands

apply access-vpn

Use **apply access-vpn** to specify the forwarding tables that can be used for the matching packets.

Use **undo apply access-vpn** to remove the specified forwarding tables.

Syntax

apply access-vpn { **public** | **vpn-instance** *vpn-instance-name*&<1-4> }

undo apply access-vpn { **public** | **vpn-instance** [*vpn-instance-name*&<1-4>] }

Default

The device forwards matching packets by using the forwarding table for the network from which the packets are received.

Views

IPv6 policy node view

Predefined user roles

network-admin

context-admin

Parameters

public: Specifies the forwarding table for the public network.

vpn-instance: Specifies the forwarding table for the specified MPLS L3VPN instances.

vpn-instance-name&<1-4>: Specifies a space-separated list of up to four VPN instance names. A VPN instance name is a case-sensitive string of 1 to 31 characters. The specified VPN instance must already exist. Specifies a space-separated list of up to four VPN instance names. A VPN instance name is a case-sensitive string of 1 to 31 characters. The specified VPN instance must already exist.

Usage guidelines

Use this command only in special scenarios that require sending packets received from one network to another network, for example, from a VPN to the public network, or from one VPN to another VPN.

You can repeat this command to specify the forwarding tables for the public network and VPN instances. The device forwards the matching packets by using the first available forwarding table selected in the order in which they are specified.

If you specify the **vpn-instance** keyword without specifying any VPN instances when you execute the **undo** form of this command, all the VPN instances are removed from the IPv6 policy node.

After all the forwarding tables on the IPv6 policy node are removed, the default forwarding behavior restores.

Examples

Specify the VPN 1 and VPN 2 forwarding tables on node 10. In this example, VPN 1 and VPN 2 already exist.

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route policy1 permit node 10
```

```
[Sysname-pbr6-policy1-10] apply access-vpn vpn-instance vpn1 vpn2
```

Specify the public network forwarding table on node 10.

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route policy1 permit node 10
[Sysname-pbr6-policy1-10] apply access-vpn public
```

Related commands

apply remark-vpn

apply continue

Use **apply continue** to compare packets with the next policy node upon failure on the current node.

Use **undo apply continue** to restore the default.

Syntax

apply continue

undo apply continue

Default

IPv6 PBR does not compare packets with the next policy node upon failure on the current node.

Views

IPv6 policy node view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command takes effect only when the mode of the node is **permit**.

This command applies when either of the following conditions exist:

- **apply access-vpn**
- **apply next-hop**
- **apply output-interface**
- **apply default-next-hop**
- **apply default-output-interface**

- A clause listed above is configured, but it has become invalid. Then, a routing table lookup also fails for the matching packet.

NOTE:

A clause might become invalid because the specified next hop is unreachable, packets cannot be forwarded in the specified VPN instance, or the specified output interface is down.

Examples

Compare with the next policy node upon failure on the current node.

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route aa permit node 11
[Sysname-pbr6-aa-11] apply continue
```

apply default-next-hop

Use **apply default-next-hop** to set default next hops.

Use **undo apply default-next-hop** to remove default next hops.

Syntax

apply default-next-hop [**vpn-instance** *vpn-instance-name* | **inbound-vpn**] { *ipv6-address* [**direct**] [**track** *track-entry-number*] }&<1-4>

undo apply default-next-hop [[**vpn-instance** *vpn-instance-name* | **inbound-vpn**] *ipv6-address*&<1-4>]

Default

No default next hops are set.

Views

IPv6 policy node view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. The specified VPN instance must already exist.

inbound-vpn: Specifies the VPN instance where the inbound interface belongs.

ipv6-address: Specifies the IPv6 address of a default next hop. If you do not specify the **vpn-instance** *vpn-instance-name* option or the **inbound-vpn** keyword, the default next hop belongs to the public network.

direct: Specifies a directly connected default next hop.

track *track-entry-number*: Specifies a track entry by its number in the range of 1 to 1024.

&<1-4>: Indicates that you can specify up to four default next hops, each of which can be associated with a track entry.

Usage guidelines

You can specify multiple default next hops for backup or load sharing in one command line or by executing this command multiple times.

With a default next hop specified, the **undo apply default-next-hop** command removes the default next hop.

Without any default next hop specified, the **undo apply default-next-hop** command removes all default next hops.

Examples

Set a directly-connected default next hop of 1:1::1:1.

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route aa permit node 11
[Sysname-pbr6-aa-11] apply default-next-hop 1:1::1:1 direct
```

Related commands

apply loadshare

apply default-output-interface

Use **apply default-output-interface** to set default output interfaces.

Use **undo apply default-output-interface** to remove default output interfaces.

Syntax

apply default-output-interface { *interface-type interface-number* [**track** *track-entry-number*] }&<1-4>

undo apply default-output-interface [{ *interface-type interface-number* }&<1-4>]

Default

No default output interfaces are set.

Views

IPv6 policy node view

Predefined user roles

network-admin

context-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

track *track-entry-number*: Specifies a track entry by its number in the range of 1 to 1024.

&<1-4>: Indicates that you can specify up to four interfaces, each of which can be associated with a track entry.

Usage guidelines

You can specify multiple default output interfaces for backup or load sharing in one command line or by executing this command multiple times.

The default output interface must be P2P type. Using a non-P2P default output interface can result in forwarding failures when the interface has multiple next hops. Non-P2P interfaces include broadcast interfaces such as Ethernet interfaces.

With a default output interface specified, the **undo apply default-output-interface** command removes the default output interface.

Without any default output interface specified, the **undo apply default-output-interface** command removes all default output interfaces.

Examples

Specify GigabitEthernet 1/0/1 as the default output interface for IPv6 packets.

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route aa permit node 11
[Sysname-pbr6-aa-11] apply default-output-interface gigabitethernet 1/0/1
```

Related commands

apply loadshare

apply loadshare

Use **apply loadshare** to enable load sharing among multiple next hops, output interfaces, default next hops, or default output interfaces.

Use **undo apply loadshare** to restore the default.

Syntax

apply loadshare { **default-next-hop** | **default-output-interface** | **next-hop** | **output-interface** }

undo apply loadshare { **default-next-hop** | **default-output-interface** | **next-hop** | **output-interface** }

Default

Multiple next hops, output interfaces, default next hops, or default output interfaces operate in primary/backup mode.

Views

IPv6 policy node view

Predefined user roles

network-admin

context-admin

Parameters

default-next-hop: Enables load sharing among multiple default next hops.

default-output-interface: Enables load sharing among multiple default output interfaces.

next-hop: Enables load sharing among multiple next hops.

output-interface: Enables load sharing among multiple output interfaces.

Usage guidelines

Multiple next hop, output interface, default next hop, or default output interface options operate in either primary/backup or load sharing mode.

- **Primary/backup mode**—One option is selected from all options in configuration order for packet forwarding, with all remaining options as backups. For example, if multiple output interfaces are configured, the first configured output interface is selected. When the selected output interface fails, the next available output interface takes over.
- **Load sharing mode**—Matching traffic is distributed across the available options, as follows:
  - **Multiple output interface, default next hop, or default output interface options**—Load share traffic in round robin manner, starting from the first configured option. They perform per-packet load sharing for traffic that does not match any fast forwarding entry, and perform per-flow load sharing for traffic that matches a fast forwarding entry.
  - **Multiple next hops**—Load share traffic in proportion to their weight. By default, all next hops have the same weight and traffic is evenly distributed among them.

Examples

Enable load sharing among multiple next hops.

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route aa permit node 11
[Sysname-pbr6-aa-11] apply next-hop 1::1 2::2
[Sysname-pbr6-aa-11] apply loadshare next-hop
```

Enable load sharing among multiple output interfaces.

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route aa permit node 11
[Sysname-pbr6-aa-11] apply output-interface gigabitethernet 1/0/1 gigabitethernet 1/0/2
[Sysname-pbr6-aa-11] apply loadshare output-interface
```

Enable load sharing among multiple default next hops.

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route aa permit node 11
[Sysname-pbr6-aa-11] apply default-next-hop 1::1 2::2
[Sysname-pbr6-aa-11] apply loadshare default-next-hop
```

Enable load sharing among multiple default output interfaces.

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route aa permit node 11
[Sysname-pbr6-aa-11] apply default-output-interface gigabitethernet 1/0/1
gigabitethernet 1/0/2
[Sysname-pbr6-aa-11] apply loadshare default-output-interface
```

Related commands

apply default-next-hop

apply default-output-interface

apply next-hop

apply output-interface

apply next-hop

Use **apply next-hop** to set next hops.

Use **undo apply next-hop** to remove next hops.

Syntax

apply next-hop [**vpn-instance** *vpn-instance-name* | **inbound-vpn**] { *ipv6-address* [**direct**] [**track** *track-entry-number*] [**weight** *weight-value*] } &<1-4>

undo apply next-hop [[**vpn-instance** *vpn-instance-name* | **inbound-vpn**] *ipv6-address*&<1-4>]

Default

No next hops are set.

Views

IPv6 policy node view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. The specified VPN instance must already exist.

inbound-vpn: Specifies the VPN instance where the inbound interface belongs.

ipv6-address: Specifies the IPv6 address of a next hop. If you do not specify the **vpn-instance** *vpn-instance-name* option or the **inbound-vpn** keyword, the next hop belongs to the public network.

direct: Specifies that the next hop must be directly connected to take effect.

track *track-entry-number*: Specifies a track entry by its number in the range of 1 to 1024.

weight *weight-value*: Specifies a load sharing weight for the next hop, in the range of 1 to 100. The default is 10. If you specify weights 1, 1, and 2 for three next hops, they share 1/4, 1/4, and 1/2 of the whole traffic, respectively.

&<1-4>: Indicates that you can specify up to four next hops, each of which can be associated with a track entry.

Usage guidelines

You can specify multiple next hops for backup or load sharing in one command line or by executing this command multiple times.

With a next hop specified, the **undo apply next-hop** command removes the next hop.

Without any next hop specified, the **undo apply next-hop** command removes all next hops.

Examples

Set a directly-connected next hop of 1::1.

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route aa permit node 11
[Sysname-pbr6-aa-11] apply next-hop 1::1
```

Related commands

apply loadshare

apply output-interface

Use **apply output-interface** to set output interfaces.

Use **undo apply output-interface** to remove output interfaces.

Syntax

apply output-interface { *interface-type interface-number* [**track** *track-entry-number*] }&<1-4>

undo apply output-interface [{ *interface-type interface-number* }&<1-4>]

Default

No output interfaces are set.

Views

IPv6 policy node view

Predefined user roles

network-admin

context-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

track *track-entry-number*: Specifies a track entry by its number in the range of 1 to 1024.

&<1-4>: Indicates that you can specify up to four interfaces, each of which can be associated with a track entry.

Usage guidelines

You can specify multiple output interfaces for backup or load sharing in one command line or by executing this command multiple times.

The output interface must be P2P type. Using a non-P2P output interface can result in forwarding failures when the interface has multiple next hops. Non-P2P interfaces include broadcast interfaces such as Ethernet interfaces.

With an output interface specified, the **undo apply output-interface** command removes the output interface.

Without any output interface specified, the **undo apply output-interface** command removes all output interfaces.

Examples

Specify GigabitEthernet 1/0/1 as the output interface for IPv6 packets.

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route aa permit node 11
[Sysname-pbr6-aa-11] apply output-interface gigabitethernet 1/0/1
```

Related commands

apply loadshare

apply precedence

Use **apply precedence** to set a precedence for IPv6 packets.

Use **undo apply precedence** to restore the default.

Syntax

apply precedence { *type* | *value* }

undo apply precedence

Default

No precedence is set for IPv6 packets.

Views

IPv6 policy node view

Predefined user roles

network-admin

context-admin

Parameters

type: Specifies the precedence type for IPv6 packets.

value: Specifies the precedence for IPv6 packets. Eight precedence values (0 to 7) are available. Each precedence value corresponds to a precedence type, as shown in Table 1. You can set either a precedence value or a precedence type for IPv6 packets.

Table 1 IP precedences and the corresponding types

Precedence value	Precedence type
0	routine
1	priority
2	immediate
3	flash
4	flash-override

Precedence value	Precedence type
5	critical
6	internet
7	network

Examples

Set the precedence to 5 (critical) for IPv6 packets.

```
<Sysname> system-view
[Sysname]ipv6 policy-based-route aa permit node 11
[Sysname-pbr6-aa-11] apply precedence critical
```

apply remark-vpn

Use **apply remark-vpn** to enable VPN remark action.

Use **undo apply remark-vpn** to restore the default.

Syntax

apply remark-vpn

undo apply remark-vpn

Default

VPN remark action is not configured.

Views

IPv6 policy node view

Predefined user roles

network-admin

context-admin

Usage guidelines

VPN remark action marks the matching packets as belonging to the VPN instance to which they are forwarded based on the **apply access-vpn vpn-instance** command. All subsequent service modules of IPv6 PBR handle the packets as belonging to the re-marked VPN instance.

If the VPN remark action is not enabled, the forwarded matching packets are marked as belonging to the VPN instance or the public network from which they were received.

VPN remark action applies only to packets that have been successfully forwarded based on the **apply access-vpn vpn-instance** command.

Examples

Forward packets that match ACL 3000 based on the forwarding table of VPN instance **vpn1** and perform VPN remark action on the successfully forwarded packets.

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route aaa permit node 10
[Sysname-pbr6-aaa-10] if-match acl 3000
[Sysname-pbr6-aaa-10] apply access-vpn vpn-instance vpn1
[Sysname-pbr6-aaa-10] apply remark-vpn
```

Related commands

apply access-vpn vpn-instance

display ipv6 policy-based-route

Use **display ipv6 policy-based-route** to display IPv6 PBR policy information.

Syntax

display ipv6 policy-based-route [**policy** *policy-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

policy *policy-name*: Specifies a policy by its name, a case-sensitive string of 1 to 19 characters. If you do not specify a policy, this command displays information for all IPv6 PBR policies.

Examples

Display all IPv6 policy information.

```
<Sysname> display ipv6 policy-based-route
Policy name: aaa
  node 1 permit:
    if-match acl 2000
    apply next-hop 1000::1
```

Table 2 Command output

Field	Description
node 1 permit	The match mode of Node 1 is **permit**.
if-match acl	Compares IPv6 packets with IPv6 ACL.
apply next-hop	Specifies a next hop for permitted IPv6 packets.

Related commands

ipv6 policy-based-route (system view)

display ipv6 policy-based-route interface

Use **display ipv6 policy-based-route interface** to display IPv6 interface PBR configuration and statistics.

Syntax

display ipv6 policy-based-route interface *interface-type interface-number* [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv6 interface PBR configuration and statistics for the master device.

Examples

Display IPv6 PBR configuration and statistics on GigabitEthernet 1/0/1.

```
<Sysname> display ipv6 policy-based-route interface gigabitethernet 1/0/1
Policy based routing information for interface GigabitEthernet1/0/1(failed):
Policy name: aaa
  node 0 deny:
  Matched: 0
  node 1 permit:
    if-match acl 3999
  Matched: 0
  node 2 permit:
    if-match acl 2000
    apply next-hop 1000::1
    apply output-interface GigabitEthernet1/0/2 track 1 (down)
    apply output-interface GigabitEthernet1/0/3 track 2 (inactive)
  Matched: 0
  node 5 permit:
    if-match acl 3101
    apply next-hop 1000::1
  Matched: 0
Total matched: 0
```

Table 3 Command output

Field	Description
Policy based routing information for interface *XXXX*(failed)	IPv6 PBR configuration and statistics on the interface. This field displays **failed** in brackets if none of the nodes in the policy has been successfully issued to the driver. To issue the policy, you must remove the policy from the interface and then apply it on the interface again. **NOTE:** The **failed** status is available on a per-slot basis. To obtain this information, you must specify a slot number when you execute the command. • For a global interface (for example, a VLAN interface), which might have member physical interfaces on multiple slots, specify

Field	Description
	a slot that contains its member interfaces. • For a physical interface, specify its slot number.
node 0 deny(not support) node 2 permit(no resource)	Match mode of the node, **permit** or **deny**. If a node fails to be issued to the driver, the command displays the cause in brackets, which include: • **not support**—The device does not support the match criteria configured on the node. • **no resource**—No sufficient resources (for example, ACLs) are available for the node. **NOTE:** The cause is available only on a per-slot basis. To obtain this information, you must specify a slot number when you execute the command. • For a global interface (for example, a VLAN interface), which might have member physical interfaces on multiple slots, specify a slot that contains its member interfaces. • For a physical interface, specify its slot number.
if-match acl	Compares IPv6 packets with the IPv6 ACL.
apply next-hop	Specifies a next hop for permitted IPv6 packets.
apply output-interface track 1 (down)	Specifies an output interface for permitted packets. The interface status includes the following: • **down**—The interface is down at network layer. • **inactive**—The interface is not in position.
Matched: 0 (no statistics resource)	Number of successful matches on the node. If the device does not have sufficient resources to count matches, this field displays **no statistics resource** in brackets. **NOTE:** The statistics collection failure cause is available only on a per-slot basis. To obtain this information, you must specify a slot number when you execute the command. • For a global interface (for example, a VLAN interface), which might have member physical interfaces on multiple slots, specify a slot that contains its member interfaces. • For a physical interface, specify its slot number.
Total matched	Total number of successful matches on all nodes.

Related commands

`ipv6 policy-based-route` (interface view)

display ipv6 policy-based-route local

Use **`display ipv6 policy-based-route local`** to display IPv6 local PBR configuration and statistics.

Syntax

`display ipv6 policy-based-route local` [**`slot`** *`slot-number`*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv6 local PBR configuration and statistics for the master device.

Examples

Display IPv6 local PBR configuration and statistics.

```
<Sysname> display ipv6 policy-based-route local
Policy based routing information for local:
Policy name: aaa
  node 0 deny:
  Matched: 0
  node 1 permit:
    if-match acl 3999
  Matched: 0
  node 2 permit:
    if-match acl 2000
    apply next-hop 1::1
  Matched: 0
  node 5 permit:
    if-match acl 3101
    apply next-hop 2::2
  Matched: 0
Total matched: 0
```

Table 4 Command output

Field	Description
Policy based routing information for local	IPv6 local PBR configuration and statistics.
node 0 deny/node 2 permit	Match mode of the node, **permit** or **deny**.
if-match acl	Compares packets with the ACL.
apply next-hop	Specifies a next hop for permitted packets.
Matched: 0	Number of successful matches on the node.
Total matched	Total number of successful matches on all nodes.

Related commands

ipv6 local policy-based-route

display ipv6 policy-based-route setup

Use **display ipv6 policy-based-route setup** to display IPv6 PBR configuration.

Syntax

display ipv6 policy-based-route setup

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display IPv6 PBR configuration.

```
<Sysname> display ipv6 policy-based-route setup
Policy name             Type              Interface
pr01                    Forward           GigabitEthernet 1/0/1
pr02                    Local             N/A
```

Table 5 Command output

Field	Description
Policy name	IPv6 PBR policy name.
Type	Type of the IPv6 PBR: • **Forward**—IPv6 interface PBR. • **Local**—IPv6 local PBR.
Interface	Interface where the policy is applied. This field displays **N/A** for an IPv6 local PBR policy.

if-match acl

Use **if-match acl** to set an ACL match criterion.

Use **undo if-match acl** to restore the default.

Syntax

if-match acl { *ipv6-acl-number* | **name** *ipv6-acl-name* }

undo if-match acl

Default

No ACL match criterion is set.

Views

IPv6 policy node view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-acl-number: Specifies an IPv6 ACL by its number in the range of 2000 to 3999. The value range of a basic ACL is 2000 to 2999 and that of an advanced ACL is 3000 to 3999.

name *ipv6-acl-name*: Specifies an IPv6 ACL by its name, a case-insensitive string of 1 to 63 characters starting with a letter. The ACL name cannot be **all**. For the command to take effect, make sure the specified IPv6 ACL is a basic or advanced ACL.

Usage guidelines

If the specified ACL does not exist or has no rules configured, no packets will match the ACL.

If the **vpn-instance** keyword is specified for an ACL rule, the rule applies to only VPN packets. If the **vpn-instance** keyword is not specified, the rule applies to only public network packets.

Examples

Configure Node 10 of policy **aa** to permit the packets matching ACL 2000.

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route aa permit node 10
[Sysname-pbr6-aa-10] if-match acl 2000
```

Configure Node 10 of policy **aa** to permit the packets matching ACL **aaa**.

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route aa permit node 10
[Sysname-pbr6-aa-10] if-match acl name aaa
```

if-match packet-length

Use **if-match packet-length** to set an IPv6 packet length match criterion.

Use **undo if-match packet-length** to restore the default.

Syntax

if-match packet-length *min-len max-len*

undo if-match packet-length

Default

No packet length match criterion is set.

Views

IPv6 policy node view

Predefined user roles

network-admin

context-admin

Parameters

min-len: Specifies the minimum IPv6 packet length in the range of 1 to 65535 bytes.

max-len: Specifies the maximum IP packet length in the range of 1 to 65535 bytes. The maximum length must be no less than the minimum length.

Usage guidelines

The packet length range includes boundary values. For example, if you set the *min-len* and *max-len* arguments to 100 and 200, respectively, packets with lengths of 100 bytes and 200 bytes are also matched.

Examples

Match packets with a length from 100 to 200 bytes.

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route aa permit node 11
[Sysname-pbr6-aa-11] if-match packet-length 100 200
```

ipv6 local policy-based-route

Use **ipv6 local policy-based-route** to configure IPv6 local PBR based on a specified policy.

Use **undo ipv6 local policy-based-route** to restore the default.

Syntax

ipv6 local policy-based-route *policy-name*

undo ipv6 local policy-based-route

Default

No policy is specified for IPv6 local PBR.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies a policy by its name, a case-sensitive string of 1 to 19 characters. The specified IPv6 policy must already exist.

Usage guidelines

You can apply only one policy locally. Before you apply a new policy, you must first remove the current policy.

IPv6 local PBR is used to route locally generated packets except the packets destined for the sender. This feature might affect local services. Do not configure IPv6 local PBR unless doing so is required.

Examples

Configure IPv6 local PBR based on policy **aaa**.

```
<Sysname> system-view
[Sysname] ipv6 local policy-based-route aaa
```

Related commands

display ipv6 policy-based-route local

ipv6 policy-based-route (interface view)

Use **ipv6 policy-based-route** to configure IPv6 interface PBR by applying an IPv6 policy to an interface.

Use **undo ipv6 policy-based-route** to restore the default.

Syntax

ipv6 policy-based-route *policy-name*

undo ipv6 policy-based-route

Default

No IPv6 is applied to an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies a policy by its name, a case-sensitive string of 1 to 19 characters. The specified policy must already exist.

Examples

Apply policy **aaa** to GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 policy-based-route aaa
```

Related commands

display ipv6 policy-based-route interface

ipv6 policy-based-route (system view)

Use **ipv6 policy-based-route** to create an IPv6 policy node and enter its view, or enter the view of an existing IPv6 policy node.

Use **undo ipv6 policy-based-route** to delete an IPv6 policy or IPv6 policy node.

Syntax

ipv6 policy-based-route *policy-name* [**deny** | **permit**] **node** *node-number*

undo ipv6 policy-based-route *policy-name* [**deny** | **node** *node-number* | **permit**]

Default

No IPv6 policy nodes exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies a policy name, a case-sensitive string of 1 to 19 characters.

deny: Specifies the match mode for the policy node as **deny**.

permit: Specifies the match mode for the policy node as **permit** (default mode).

node *node-number*: Specifies the number of the IPv6 policy node. A smaller number has a higher priority. The value range for the *node-number* argument is 0 to 65535.

Usage guidelines

To delete an IPv6 policy that has already applied to an interface, you must delete the policy from the interface first.

If a policy node is specified, the **undo ipv6 policy-based-route** command deletes the specified policy node. If a match mode is specified, the command deletes all nodes configured with the match mode. If no node is specified, the command deletes the whole policy.

Examples

Create permit-mode Node 10 for IPv6 policy **aaa** and enter its view.

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route aaa permit node 10
[Sysname-pbr6-aaa-10]
```

Related commands

display ipv6 policy-based-route

reset ipv6 policy-based-route statistics

Use **reset ipv6 policy-based-route statistics** to clear IPv6 PBR statistics.

Syntax

reset ipv6 policy-based-route statistics [**policy** *policy-name*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

policy *policy-name*: Specifies a policy by its name, a case-sensitive string of 1 to 19 characters. If you do not specify a policy, this command clears IPv6 PBR statistics for all policies.

Examples

Clear all IPv6 PBR statistics.

```
<Sysname> reset ipv6 policy-based-route statistics
```

Contents

Routing policy commands

Common routing policy commands

apply as-path

Use **apply as-path** to set the AS_PATH attribute for BGP routes.

Use **undo apply as-path** to restore the default.

Syntax

apply as-path *as-number*&<1-32> [**replace**]

undo apply as-path

Default

No AS_PATH attribute is set.

Views

Routing policy node view

Predefined user roles

network-admin

context-admin

Parameters

as-number&<1-32>: Specifies an AS by its number in the range of 1 to 4294967295. &<1-32> indicates that you can specify a maximum of 32 AS numbers.

replace: Replaces the original AS numbers. If you do not specify this keyword, the command adds the specified AS numbers before the original AS_PATH attribute.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to add AS number 200 before the original AS_PATH attribute of BGP routes matching AS path list 1.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match as-path 1
[Sysname-route-policy-policy1-10] apply as-path 200
```

Related commands

display ip as-path

if-match as-path

ip as-path

apply comm-list delete

Use **apply comm-list delete** to delete the COMMUNITY attributes from BGP routes.

Use **undo apply comm-list** to restore the default.

Syntax

apply comm-list { *comm-list-number* | *comm-list-name* } **delete**

undo apply comm-list

Default

No COMMUNITY attributes are deleted from BGP routes.

Views

Routing policy node view

Predefined user roles

network-admin

context-admin

Parameters

comm-list-number: Specifies a basic community list by its number in the range of 1 to 99 or an advanced community list by its number in the range of 100 to 199.

comm-list-name: Specifies a community list by its name, a case-sensitive string of 1 to 63 characters that cannot contain only numbers.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to delete the COMMUNITY attributes specified in community list 1 from BGP routes.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] apply comm-list 1 delete
```

Related commands

ip community-list

apply community

Use **apply community** to set the COMMUNITY attribute for BGP routes.

Use **undo apply community** to remove the specified COMMUNITY attribute for BGP routes.

Syntax

apply community { **none** | **additive** | { *community-number*&<1-32> | *aa:nn*&<1-32> | **internet** | **no-advertise** | **no-export** | **no-export-subconfed** } * [**additive**] }

undo apply community [**none** | **additive** | { *community-number*&<1-32> | *aa:nn*&<1-32> | **internet** | **no-advertise** | **no-export** | **no-export-subconfed** } * [**additive**]]

Default

No COMMUNITY attribute is set for BGP routes.

Views

Routing policy node view

Predefined user roles

network-admin

context-admin

Parameters

none: Removes the COMMUNITY attributes of BGP routes.

community-number&<1-32>: Specifies a community sequence number in the range of 1 to 4294967295. &<1-32> indicates that you can specify a maximum of 32 community sequence numbers.

aa:nn&<1-32>: Specifies a community number. Both *aa* and *nn* are in the range of 0 to 65535. &<1-32> indicates that you can specify a maximum of 32 community numbers.

internet: Sets the INTERNET community attribute for BGP routes. Routes with this attribute can be advertised to all BGP peers. By default, all routes have this attribute.

no-advertise: Sets the NO_ADVERTISE community attribute for BGP routes. Routes with this attribute cannot be advertised to any peers.

no-export: Sets the NO_EXPORT community attribute for BGP routes. Routes with this attribute cannot be advertised out of the AS or confederation, but can be advertised to other sub-ASs in the confederation.

no-export-subconfed: Sets the NO_EXPORT_SUBCONFED community attribute for BGP routes. Routes with this attribute cannot be advertised out of the local AS or to other sub-ASs in the confederation.

additive: Adds the specified COMMUNITY attribute to the original COMMUNITY attribute of BGP routes.

Examples

Configure node 16 in **permit** mode for routing policy **setcommunity** to set the NO_EXPORT community attribute for BGP routes.

```
<Sysname> system-view
[Sysname] route-policy setcommunity permit node 16
[Sysname-route-policy-setcommunity-16] apply community no-export
```

Related commands

if-match community

ip community-list

apply cost

Use **apply cost** to set a cost for routes.

Use **undo apply cost** to restore the default.

Syntax

apply cost [**+** | **-**] *cost-value*

undo apply cost

Default

No cost is set for routes.

Views

Routing policy node view

Predefined user roles

network-admin

context-admin

Parameters

+: Increases a cost value.

-: Decreases a cost value.

cost-value: Specifies a cost in the range of 0 to 4294967295.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to set a cost of 120 for OSPF external routes.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match route-type external-type1or2
[Sysname-route-policy-policy1-10] apply cost 120
```

apply cost-type

Use **apply cost-type** to set a cost type for routes.

Use **undo apply cost-type** to restore the default.

Syntax

apply cost-type { **external** | **internal** | **type-1** | **type-2** }

undo apply cost-type

Default

No cost type is set for routes.

Views

Routing policy node view

Predefined user roles

network-admin

context-admin

Parameters

external: Sets the cost type to IS-IS external route.

internal: Sets the cost type to IS-IS internal route, or sets the MED value for a matching BGP route to the IGP metric of the route's next hop.

type-1: Sets the cost type to OSPF Type-1 external route.

type-2: Sets the cost type to OSPF Type-2 external route.

Usage guidelines

For IS-IS, the **apply cost-type internal** command sets the cost type for a matching IS-IS route to IS-IS internal route.

For BGP, the **apply cost-type internal** command sets the MED for a matching BGP route learned from an IBGP peer to the IGP metric of the route's next hop. The MED is modified when BGP advertises the route to an EBGP peer.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to set the cost type for routes that have a tag of 8 to OSPF Type-1 external routes.

```
<Sysname> system-view
```

```
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match tag 8
[Sysname-route-policy-policy1-10] apply cost-type type-1
```

apply extcommunity

Use **apply extcommunity** to set the extended community attribute for BGP routes.

Use **undo apply extcommunity** to remove the extended community attribute for BGP routes.

Syntax

apply extcommunity { **rt** *route-target* }&<1-32> [**additive**]

undo apply extcommunity [{ **rt** *route-target* }&<1-32>]

Default

No extended community attribute is set for BGP routes.

Views

Routing policy node view

Predefined user roles

network-admin

context-admin

Parameters

{ **rt** *route-target* }&<1-32>: Sets the RT extended community attribute, a string of 3 to 21 characters. &<1-32> indicates that you can specify a maximum of 32 RT extended community attributes.

An RT attribute has the following forms:

- *16-bit AS number*:*32-bit self-defined number*. For example, 101:3. The AS number is in the range of 0 to 65535, and the self-defined number is in the range of 0 to 4294967295.
- *32-bit IP address*:*16-bit self-defined number*. For example, 192.168.122.15:1. The self-defined number is in the range of 0 to 65535.
- *32-bit AS number*:*16-bit self-defined number*. For example, 70000:3. The AS number is in the range of 65536 to 4294967295, and the self-defined number is in the range of 0 to 65535.

additive: Adds the specified attribute to the original extended community attribute.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to add the RT extended community attribute 100:2 to BGP routes matching AS path list 1.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match as-path 1
[Sysname-route-policy-policy1-10] apply extcommunity rt 100:2 additive
```

apply ip-precedence

Use **apply ip-precedence** to set an IP precedence for matching routes.

Use **undo apply ip-precedence** to restore the default.

Syntax

apply ip-precedence { *value* | **clear** }

undo apply ip-precedence

Default

No IP precedence is set.

Views

Routing policy node view

Predefined user roles

network-admin

context-admin

Parameters

value: Specifies an IP precedence in the range of 0 to 7.

clear: Clears the IP precedence of matching routes.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to set an IP precedence of 3 for routes matching prefix list 100.

```
<Sysname> system-view
[Sysname] ip prefix-list 100 permit 192.168.10.1 24
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match ip address prefix-list 100
[Sysname-route-policy-policy1-10] apply ip-precedence 3
```

apply isis

Use **apply isis** to redistribute routes into the specified IS-IS level.

Use **undo apply isis** to restore the default.

Syntax

apply isis { **level-1** | **level-1-2** | **level-2** }

undo apply isis

Default

No IS-IS level is set.

Views

Routing policy node view

Predefined user roles

network-admin

context-admin

Parameters

level-1: Redistributes routes into IS-IS Level-1.

level-1-2: Redistributes routes into both IS-IS Level-1 and Level-2.

level-2: Redistributes routes into IS-IS Level-2.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to redistribute routes that have a tag of 8 to IS-IS level-2.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match tag 8
[Sysname-route-policy-policy1-10] apply isis level-2
```

apply local-preference

Use **apply local-preference** to set a local preference for BGP routes.

Use **undo apply local-preference** to restore the default.

Syntax

apply local-preference *preference*

undo apply local-preference

Default

No local preference is set for BGP routes.

Views

Routing policy node view

Predefined user roles

network-admin

context-admin

Parameters

preference: Specifies a local preference in the range of 0 to 4294967295.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to set a local preference of 130 for BGP routes matching AS path list 1.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match as-path 1
[Sysname-route-policy-policy1-10] apply local-preference 130
```

apply origin

Use **apply origin** to set the ORIGIN attribute for BGP routes.

Use **undo apply origin** to restore the default.

Syntax

apply origin { **egp** *as-number* | **igp** | **incomplete** }

undo apply origin

Default

No ORIGIN attribute is set for BGP routes.

Views

Routing policy node view

Predefined user roles

network-admin

context-admin

Parameters

egp *as-number*: Sets the ORIGIN attribute to EGP. The *as-number* argument specifies an AS number in the range 1 to 4294967295 for EGP routes.

igp: Sets the ORIGIN attribute to IGP.

incomplete: Sets the ORIGIN attribute to UNKNOWN.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to set the ORIGIN attribute to IGP for BGP routes matching AS path list 1.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match as-path 1
[Sysname-route-policy-policy1-10] apply origin igp
```

apply preference

Use **apply preference** to set a preference for a routing protocol.

Use **undo apply preference** to restore the default.

Syntax

apply preference *preference*

undo apply preference

Default

No preference is set for a routing protocol.

Views

Routing policy node view

Predefined user roles

network-admin

context-admin

Parameters

preference: Specifies a preference in the range of 1 to 255.

Usage guidelines

If you have set preferences for routing protocols by using the **preference** command, the **apply preference** command sets a new preference for the matching routing protocol. Unmatched routing protocols still use the preferences set by using the **preference** command.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to set the preference for OSPF external routes to 90.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match route-type external-type1or2
[Sysname-route-policy-policy1-10] apply preference 90
```

apply preferred-value

Use **apply preferred-value** to set a preferred value for BGP routes.

Use **undo apply preferred-value** to restore the default.

Syntax

apply preferred-value *preferred-value*

undo apply preferred-value

Default

No preferred value is set for BGP routes.

Views

Routing policy node view

Predefined user roles

network-admin

context-admin

Parameters

preferred-value: Specifies a preferred value in the range of 0 to 65535.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to set a preferred value of 66 for BGP routes matching AS path list 1.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match as-path 1
[Sysname-route-policy-policy1-10] apply preferred-value 66
```

apply prefix-priority

Use **apply prefix-priority** to set a prefix priority for routes.

Use **undo apply prefix-priority** to restore the default.

Syntax

apply prefix-priority { **critical** | **high** | **medium** }

undo apply prefix-priority

Default

No prefix priority is set, which means the prefix priority is low.

Views

Routing policy node view

Predefined user roles

network-admin

context-admin

Parameters

critical: Sets the critical prefix priority for routes.

high: Sets the high prefix priority for routes.

medium: Sets the medium prefix priority for routes.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to set prefix priority **critical** for routes matching prefix list **abc**.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match ip address prefix-list abc
[Sysname-route-policy-policy1-10] apply prefix-priority critical
```

apply qos-local-id

Use **apply qos-local-id** to set a local QoS ID for matching routes.

Use **undo apply qos-local-id** to restore the default.

Syntax

apply qos-local-id { *local-id-value* | **clear** }

undo apply qos-local-id

Default

No local QoS ID is set.

Views

Routing policy node view

Predefined user roles

network-admin

context-admin

Parameters

local-id-value: Specifies a local QoS ID in the range of 1 to 4095.

clear: Clears the local QoS ID of matching routes.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to set a local QoS ID of 100 for routes matching prefix list 100.

```
<Sysname> system-view
[Sysname] ip prefix-list 100 permit 192.168.10.1 24
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match ip address prefix-list 100
[Sysname-route-policy-policy1-10] apply qos-local-id 100
```

apply tag

Use **apply tag** to set a tag for IGP routes.

Use **undo apply tag** to restore the default.

Syntax

apply tag *tag-value*

undo apply tag

Default

No routing tag is set for IGP routes.

Views

Routing policy node view

Predefined user roles

network-admin

context-admin

Parameters

tag-value: Specifies the tag value in the range of 0 to 4294967295.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to set a tag of 100 for IGP routes.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] apply tag 100
```

apply traffic-index

Use **apply traffic-index** to set a traffic index for BGP routes.

Use **undo apply traffic-index** to restore the default.

Syntax

apply traffic-index { *value* | **clear** }

undo apply traffic-index

Default

No traffic index is set for BGP routes.

Views

Routing policy node view

Predefined user roles

network-admin

context-admin

Parameters

value: Specifies the traffic index in the range of 1 to 64.

clear: Clear the traffic index of BGP routes.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to set a traffic index of 6 for BGP routes matching extended community list 100.

```
<Sysname> system-view
```

```
[Sysname] ip extcommunity-list 100 permit rt 100:100
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match extcommunity 100
[Sysname-route-policy-policy1-10] apply traffic-index 6
```

continue

Use **continue** to specify the next node to be matched.

Use **undo continue** to restore the default.

Syntax

continue [*node-number*]

undo continue

Default

No next node is specified.

Views

Routing policy node view

Predefined user roles

network-admin

context-admin

Parameters

node-number: Specifies the routing policy node number in the range of 0 to 65535.

Usage guidelines

The specified next node must have a larger number than the current node.

Example

Specify the next node 20 for node 10 of the routing policy **policy1**.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] continue 20
```

description

Use **description** to configure a description for a routing policy node.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

No description is configured for a routing policy node.

Views

Routing policy node view

Predefined user roles

network-admin

context-admin

Parameters

text: Specifies a description for the routing policy node, a case-sensitive string of 1 to 80 characters.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** and configure **aa** as the description for the node.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] description aa
```

display ip as-path

Use **display ip as-path** to display BGP AS path list information.

Syntax

display ip as-path [*as-path-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

as-path-number: Specifies an AS path list by its number in the range of 1 to 256. If you do not specify this argument, the command displays information about all BGP AS path lists.

Examples

Display information about BGP AS path list 1.

```
<Sysname> display ip as-path 1
ListID    Mode      Expression
1         Permit    2
```

Table 1 Command output

Field	Description
ListID	AS path list ID.
Mode	Match mode: • **Permit**. • **Deny**.
Expression	Regular expression used to match routes.

display ip community-list

Use **display ip community-list** to display BGP community list information.

Syntax

display ip community-list [*basic-community-list-number* | *adv-community-list-number* | **name** *comm-list-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

basic-community-list-number: Specifies a basic community list by its number in the range of 1 to 99.

adv-community-list-number: Specifies an advanced community list by its number in the range of 100 to 199.

name *comm-list-name*: Specifies a community list by its name, a case-sensitive string of 1 to 63 characters that cannot contain only numbers.

Usage guidelines

If no community list is specified, this command displays information about all BGP community lists.

Examples

Display information about all BGP community lists.

```
<Sysname> display ip community-list
Community List Basic aaa
        Permit
Community List Advanced bbb
        Permit  3333
```

Table 2 Command output

Field	Description
Community List Basic	Basic community list.
Community List Advanced	Advanced community list.
permit	Match mode: • **Permit**. • **Deny**.

display ip extcommunity-list

Use **display ip extcommunity-list** to display BGP extended community list information.

Syntax

display ip extcommunity-list [*ext-comm-list-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ext-comm-list-number: Specifies an extended community list by its number in the range of 1 to 65535. If you do not specify this argument, the command displays information about all BGP extended community lists.

Examples

Display information about BGP extended community list 1.

```
<Sysname> display ip extcommunity-list 1
Extended Community List Number 1
        Index: 1          Mode:Permit RT: 3:1 SoO: 3:2
        Index: 2          Mode:Permit RT: 3:1 SoO: 3:2 SoO: 5:2
        Index: 3          Mode:Permit RT: 3:1 SoO: 3:2 RT: 6:7
```

Table 3 Command output

Field	Description
Extended Community List Number	Extended community list.
Index	Index of the extended community list entry.
Mode	Match mode: • Permit. • Deny.
rt	Route Target (RT) extended community attribute.
soo	Site of Origin (SoO) extended community attribute.

display ip rd-list

Use **display ip rd-list** to display route distinguisher (RD) list information.

Syntax

display ip rd-list [*rd-list-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

rd-list-number: Displays information about an RD list. The *rd-list-number* argument represents the number of the RD list, in the range of 1 to 65535. If you do not specify an RD list, this command displays information about all RD lists.

Examples

Display information about all RD lists.

```
<Sysname> display ip rd-list
Route Distinguisher List Number 1
        index: 1          Permit 1.1.1.1:1 2.2.2.2:* 100:1 200:*
Route Distinguisher List Number 2
        index: 2          Deny   1:1 2:2
```

Table 4 Command output

Field	Description
Route Distinguisher List Number	RD list number.
index	Index of the RD list item.
Permit	Match mode: • **Permit**. • **Deny**.

Related commands

ip rd-list

display route tag-list

Use **display route tag-list** to display tag list information.

Syntax

display route tag-list [*tag-list-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

tag-list-number: Specifies a tag list by its number in the range of 1 to 65535. If you do not specify this argument, the command displays information about all tag lists.

Examples

Display information about tag list 1.

```
<Sysname> display route tag-list 1
```

```
Tag list 1
        Index: 1          Mode: Permit  Tag value: 1 2 3
        Index: 2          Mode: Permit  Tag value: 6 7 8
```

Table 5 Command output

Field	Description
Tag list	Tag list number.
Index	Index of an item.
Mode	Match mode: • Permit. • Deny.
Tag value	Tag value.

Related commands

`route tag-list`

display route-policy

Use **`display route-policy`** to display routing policy information.

Syntax

`display route-policy` [**`name`** *`route-policy-name`*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

`name` *`route-policy-name`*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters. If you do not specify this option, the command displays information about all routing policies.

Examples

Display information about routing policy **policy1**.

```
<Sysname> display route-policy name policy1
Route-policy: policy1
  Permit : 1
          Description: policy1
          if-match cost 10
          continue: next node 11
          apply preference 10
```

Table 6 Command output

Field	Description
Route-policy	Routing policy name.
permit	Match mode: • **Permit**. • **Deny**.
Description	Routing policy description.
if-match	Match criterion.
continue	Specify the next node to be matched.
apply	Action.

if-match as-path

Use **if-match as-path** to match BGP routes whose AS_PATH attribute matches a specified AS path list.

Use **undo if-match as-path** to remove the specified AS path list match criterion.

Syntax

if-match as-path *as-path-number*&<1-32>

undo if-match as-path [*as-path-number*&<1-32>]

Default

No AS path list match criterion is configured.

Views

Routing policy node view

Predefined user roles

network-admin

context-admin

Parameters

as-path-number&<1-32>: Specifies an AS path list by its number in the range of 1 to 256. &<1-32> indicates that you can specify a maximum of 32 AS path lists.

Examples

Configure AS path list 2 to permit BGP routes containing AS number 200 or 300 to pass. Configure node 10 in **permit** mode for routing policy **test** to match AS path list 2.

```
<Sysname> system-view
[Sysname] ip as-path 2 permit _*200.*300
[Sysname] route-policy test permit node 10
[Sysname-route-policy-policy1-10] if-match as-path 2
```

Related commands

apply as-path

ip as-path

if-match community

Use **if-match community** to match BGP routes whose COMMUNITY attribute matches a specified community list.

Use **undo if-match community** to remove the specified community list match criterion.

Syntax

if-match community { { *basic-community-list-number* | **name** *comm-list-name* } [**whole-match**] | *adv-community-list-number* }&<1-32>

undo if-match community [{ *basic-community-list-number* | **name** *comm-list-name* } [**whole-match**] | *adv-community-list-number*]&<1-32>

Default

No community list match criterion is configured.

Views

Routing policy node view

Predefined user roles

network-admin

context-admin

Parameters

basic-community-list-number: Specifies a basic community list by its number in the range of 1 to 99.

adv-community-list-number: Specifies an advanced community list by its number in the range of 100 to 199.

comm-list-name: Specifies a community list by its name, a case-sensitive string of 1 to 63 characters that cannot contain only numbers.

whole-match: Exactly matches the specified community list. All of the communities and only those communities specified must be present.

&<1-32>: Indicates that you can specify a maximum of 32 community lists.

Examples

Configure community list 1 to permit BGP routes with community number 100 or 200. Then configure node 10 in **permit** mode for routing policy **test** to use community list 1 to match BGP routes.

```
<Sysname> system-view
[Sysname] ip community-list 1 permit 100 200
[Sysname] route-policy test permit node 10
[Sysname-route-policy-test-10] if-match community 1
```

Related commands

apply community

ip community-list

if-match cost

Use **if-match cost** to match routes that have the specified cost.

Use **undo if-match cost** to restore the default.

Syntax

if-match cost *cost-value*

undo if-match cost

Default

No cost match criterion is configured.

Views

Routing policy node view

Predefined user roles

network-admin

context-admin

Parameters

cost-value: Specifies a cost in the range of 0 to 4294967295.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to permit routes with a cost of 8.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match cost 8
```

if-match extcommunity

Use **if-match extcommunity** to match BGP routes whose extended community attribute matches a specified extended community list.

Use **undo if-match extcommunity** to remove the specified extended community list match criterion.

Syntax

if-match extcommunity *ext-comm-list-number*&<1-32>

undo if-match extcommunity [*ext-comm-list-number*&<1-32>]

Default

No extended community list match criterion is configured.

Views

Routing policy node view

Predefined user roles

network-admin

context-admin

Parameters

ext-comm-list-number&<1-32>: Specifies an extended community list by its number in the range of 1 to 65535. &<1-32> indicates that you can specify a maximum of 32 extended community lists.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to match BGP routes whose extended community attribute matches extended community lists 100 and 150.

```
<Sysname> system-view
[Sysname] ip extcommunity-list 100 permit rt 100:100
[Sysname] ip extcommunity-list 150 permit rt 150:150
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match extcommunity 100 150
```

Related commands

apply extcommunity

ip extcommunity-list

if-match interface

Use **if-match interface** to match routes that have the specified output interfaces.

Use **undo if-match interface** to remove the specified output interface match criterion.

Syntax

if-match interface { *interface-type interface-number* }&<1-16>

undo if-match interface [*interface-type interface-number*]&<1-16>

Default

No output interface match criterion is configured.

Views

Routing policy node view

Predefined user roles

network-admin

context-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

&<1-16>: Indicates that you can specify a maximum of 16 interfaces.

Usage guidelines

BGP does not support criteria for matching the output interfaces of routes.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to permit routes with the output interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match interface gigabitethernet 1/0/1
```

if-match local-preference

Use **if-match local-preference** to match BGP routes that have the specified local preference.

Use **undo if-match local-preference** to restore the default.

Syntax

if-match local-preference *preference*

undo if-match local-preference

Default

No local preference match criterion is configured.

Views

Routing policy node view

Predefined user roles

network-admin

context-admin

Parameters

preference: Specifies a local preference in the range of 0 to 4294967295.

Examples

Create node 10 in **permit** mode for routing policy **policy1** to match BGP routes that have a local preference of 2.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match local-preference 2
```

if-match rd-list

Use **if-match rd-list** to match routes whose RD matches the specified RD list.

Use **undo if-match rd-list** to remove the specified RD list match criterion.

Syntax

if-match rd-list *rd-list-number*

undo if-match rd-list

Default

No RD list match criterion is configured.

Views

Routing policy node view

Predefined user roles

network-admin

context-admin

Parameters

rd-list-number: Specifies an RD list by its number in the range of 1 to 65535.

Examples

Configure node 10 in **permit** mode for routing policy **rp1** to match routes whose RD matches RD list 1.

```
<Sysname> system-view
[Sysname] ip rd-list 1 permit 1:1
[Sysname] route-policy rp1 permit node 10
[Sysname-route-policy-rp1-10] if-match rd-list 1
```

Related commands

ip rd-list

if-match route-type

Use **if-match route-type** to set a route-type match criterion.

Use **undo if-match route-type** to remove the specified route-type match criterion.

Syntax

if-match route-type { **external-type1** | **external-type1or2** | **external-type2** | **internal** | **is-is-level-1** | **is-is-level-2** | **nssa-external-type1** | **nssa-external-type1or2** | **nssa-external-type2** } *

undo if-match route-type [**external-type1** | **external-type1or2** | **external-type2** | **internal** | **is-is-level-1** | **is-is-level-2** | **nssa-external-type1** | **nssa-external-type1or2** | **nssa-external-type2**] *

Default

No route-type match criterion is set.

Views

Routing policy node view

Predefined user roles

network-admin

context-admin

Parameters

external-type1: Matches OSPF Type 1 external routes.

external-type1or2: Matches OSPF Type 1 and Type 2 external routes.

external-type2: Matches OSPF Type 2 external routes.

internal: Matches OSPF internal routes (including OSPF intra-area and inter-area routes).

is-is-level-1: Matches IS-IS Level-1 routes.

is-is-level-2: Matches IS-IS Level-2 routes.

nssa-external-type1: Matches OSPF NSSA Type 1 external routes.

nssa-external-type1or2: Matches OSPF NSSA Type 1 and 2 external routes.

nssa-external-type2: Matches OSPF NSSA Type 2 external routes.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to match OSPF internal routes.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match route-type internal
```

if-match tag

Use **if-match tag** to match IGP routes that have the specified tag.

Use **undo if-match tag** to restore the default.

Syntax

if-match tag *tag-value*

undo if-match tag

Default

No tag match criterion is configured.

Views

Routing policy node view

Predefined user roles

network-admin

context-admin

Parameters

tag-value: Specifies a tag in the range of 0 to 4294967295.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to match IGP routes that have a tag of 8.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match tag 8
```

if-match tag-list

Use **if-match tag-list** to match IGP routes whose tag matches the specified tag list.

Use **undo if-match tag-list** to restore the default.

Syntax

if-match tag-list *tag-list-number*

undo if-match tag-list

Default

No tag list match criterion is configured.

Views

Routing policy node view

Predefined user roles

network-admin

context-admin

Parameters

tag-list-number: Specifies a tag list by its number in the range of 1 to 65535.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to match IGP routes whose tag matches tag list 100.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match tag-list 100
```

Related commands

route tag-list

ip as-path

Use **ip as-path** to configure an AS path list.

Use **undo ip as-path** to remove an AS path list.

Syntax

ip as-path *as-path-number* { **deny** | **permit** } *regular-expression*

undo ip as-path *as-path-number* [*regular-expression* | **deny** | **permit**]

Default

No AS path lists exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

as-path-number: Specifies an AS path list number in the range of 1 to 256.

deny: Specifies the match mode for the AS path list as **deny**.

permit: Specifies the match mode for the AS path list as **permit**.

regular-expression: Specifies an AS path regular expression, a string of 1 to 63 characters.

Usage guidelines

BGP routing updates contain an AS_PATH attribute field that identifies the ASs through which the routes have passed. An AS path regular expression, for example, ^200.*100$, matches the AS_PATH attribute that starts with AS 200 and ends with AS 100. For more information about regular expressions, see *Layer 3—IP Routing Configuration Guide*.

Examples

Configure AS path list 1 to permit routes whose AS_PATH attribute starts with 10.

```
<Sysname> system-view
[Sysname] ip as-path 1 permit ^10
```

Related commands

apply as-path

display ip as-path

if-match as-path

ip community-list

Use **ip community-list** to configure a community list.

Use **undo ip community-list** to remove a community list.

Syntax

ip community-list { *basic-comm-list-num* | **basic** *basic-comm-list-name* } { **deny** | **permit** } [*community-number*&<1-32> | *aa:nn*&<1-32>] [**internet** | **no-advertise** | **no-export** | **no-export-subconfed**] *

undo ip community-list { *basic-comm-list-num* | **basic** *basic-comm-list-name* } [**deny** | **permit**] [*community-number*&<1-32> | *aa:nn*&<1-32>] [**internet** | **no-advertise** | **no-export** | **no-export-subconfed**] *

ip community-list { *adv-comm-list-num* | **advanced** *adv-comm-list-name* } { **deny** | **permit** } *regular-expression*

undo ip community-list { *adv-comm-list-num* | **advanced** *adv-comm-list-name* } [**deny** | **permit**] [*regular-expression*]

Default

No community lists exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

basic-comm-list-num: Specifies a basic community list number in the range of 1 to 99.

basic *basic-comm-list-name*: Specifies a basic community list name, a case-sensitive string of 1 to 63 characters that cannot contain only numbers.

advanced *adv-comm-list-name*: Specifies an advanced community list name, a case-sensitive string of 1 to 63 characters that cannot contain only numbers.

adv-comm-list-num: Specifies an advanced community list number in the range of 100 to 199.

regular-expression: Specifies a regular expression for the advanced community list, a string of 1 to 63 characters. For more information about regular expressions, see routing policy configuration in *Layer 3—IP Routing Configuration Guide*.

deny: Specifies the match mode for the community list as **deny**.

permit: Specifies the match mode for the community list as **permit**.

community-number&<1-32>: Specifies a community sequence number in the range of 1 to 4294967295. &<1-32> indicates that you can specify a maximum of 32 community sequence numbers.

aa:nn&<1-32>: Specifies a community number. Both *aa* and *nn* are in the range of 0 to 65535. &<1-32> indicates that you can specify a maximum of 32 community numbers.

internet: Specifies the INTERNET community attribute. Routes with this attribute can be advertised to all BGP peers. By default, all routes have this attribute.

no-advertise: Specifies the NO_ADVERTISE community attribute. Routes with this attribute cannot be advertised to other BGP peers.

no-export: Specifies the NO_EXPORT community attribute. Routes with this attribute cannot be advertised out of the local AS or the local confederation but can be advertised to other ASs in the confederation.

no-export-subconfed: Specifies the NO_EXPORT_SUBCONFED community attribute. Routes with this attribute cannot be advertised out of the local AS, or to other sub-ASs in the local confederation.

Examples

Configure basic community list 1 to permit routes with the INTERNET community attribute.

```
<Sysname> system-view
[Sysname] ip community-list 1 permit internet
```

Configure advanced community list 100 to permit routes with the COMMUNITY attribute starting with 10.

```
<Sysname> system-view
[Sysname] ip community-list 100 permit ^10
```

Related commands

apply comm-list delete

apply community

display ip community-list

if-match community

ip extcommunity-list

Use **ip extcommunity-list** to configure an extended community list.

Use **undo ip extcommunity-list** to remove an extended community list.

Syntax

ip extcommunity-list *ext-comm-list-number* [**index** *index-number*] { **deny** | **permit** } { **rt** *route-target* | **soo** *site-of-origin* }&<1-32>

undo ip extcommunity-list *ext-comm-list-number* [**index** *index-number* | { **deny** | **permit** } [**rt** *route-target* | **soo** *site-of-origin*]&<1-32>]

Default

No extended community lists exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ext-comm-list-number: Specifies an extended community list number in the range of 1 to 65535.

index *index-number*: Specifies an index for the extended community list entry, in the range of 1 to 4294967295. An extended community list entry with a smaller index number is matched first. If you do not specify this option, the index number starts from 1 and increases by 1 for each of the consecutive extended community list entries.

deny: Specifies the match mode for the extended community list as **deny**.

permit: Specifies the match mode for the extended community list as **permit**.

rt *route-target*: Specifies a space-separated list of up to 32 RT extended community attribute items. Each item is a string of 3 to 21 characters.

soo *site-of-origin*: Specifies a space-separated list of up to 32 SoO extended community attribute items. Each item is a string of 3 to 21 characters.

An RT or SoO attribute has the following forms:

- *16-bit AS number*:*32-bit self-defined number*. For example, 101:3. The AS number is in the range of 0 to 65535, and the self-defined number is in the range of 0 to 4294967295.
- *32-bit IP address*:*16-bit self-defined number*. For example, 192.168.122.15:1. The self-defined number is in the range of 0 to 65535.
- *32-bit AS number*:*16-bit self-defined number*. For example, 70000:3. The AS number is in the range of 65536 to 4294967295, and the self-defined number is in the range of 0 to 65535.

Usage guidelines

If you execute this command multiple times for an extended community list entry, the most recent configuration takes effect.

Examples

Configure extended community list 1 to permit routes with RT 200:200 to pass.

```
<Sysname> system-view
[Sysname] ip extcommunity-list 1 permit rt 200:200
```

Configure extended community list 2 to permit routes with SoO 100:100 to pass.

```
<Sysname> system-view
[Sysname] ip extcommunity-list 2 permit soo 100:100
```

Related commands

apply extcommunity

display ip extcommunity-list

if-match extcommunity

ip rd-list

Use **ip rd-list** configure an RD list.

Use **undo ip rd-list** to remove an RD list.

Syntax

ip rd-list *rd-list-number* [**index** *index-number*] { **deny** | **permit** } *route-distinguisher*&<1-10>

undo ip rd-list *rd-list-number* [**index** *index-number*] [{ **deny** | **permit** } *route-distinguisher*&<1-10>]

Default

No RD lists exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

rd-list-number: Specifies an RD list by its number in the range of 1 to 65535.

index *index-number*: Specifies an index number for an RD list item, in the range of 1 to 4294967295. An item with a smaller index number is matched first. If you do not specify this option, the index number starts from 10 and increases by 10 for each of the consecutive RD list items.

deny: Specifies the deny mode. If a route matches the item, the route is denied without being compared with the next item. If a route does not match the item, the route is compared with the next item.

permit: Specifies the permit mode. If a route matches the item, it passes the RD list. If a route does not match the item, the route is compared with the next item.

route-distinguisher&<1-10>: Specifies a list of up to 10 RD list items. Each item is a string of 3 to 21 characters.

An RD has the following forms:

- *16-bit AS number*:*32-bit self-defined number*. For example, 101:3.
- *16-bit AS number*:*wildcard character*. For example, 101:*.
- *32-bit IP address*:*16-bit self-defined number*. For example, 192.168.122.15:1.
- *32-bit IP address*:*wildcard character*. For example, 192.168.122.15:*.
- *32-bit AS number*:*16-bit self-defined number*. For example, 65536:1. The minimum AS number is 65536.
- *32-bit AS number*:*wildcard character*. For example, 65536:*. The minimum AS number is 65536.

Usage guidelines

An RD list matches the RDs of BGP routes. An RD list is identified by an RD list number and can contain multiple items that specify RD ranges. The relationship between the items is logical OR. A route matches the RD list if it matches one item in the list. A route does not match the RD list if it does not match any items in the list.

To filter routes by RD, use the **ip rd-list** command together with the **if-match rd-list** command. If you specify a nonexistent RD list for the **if-match rd-list** command, all routes pass the RD match criterion.

Examples

Configure RD list 1 to permit routes with RD 100: 1.

```
<Sysname> system-view
[Sysname] ip rd-list 1 permit 100:1
```

Related commands

display ip rd-list

if-match rd-list

route tag-list

Use **route tag-list** to configure a tag list.

Use **undo route tag-list** to delete a tag list or a tag list entry.

Syntax

route tag-list *tag-list-number* [**index** *index-number*] { **deny** | **permit** } *tag-value*&<1-32>

undo route tag-list *tag-list-number* [**index** *index-number* [{ **deny** | **permit** } *tag-value*&<1-32>]]

Default

No tag lists exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

tag-list-number: Specifies a tag list by its number in the range of 1 to 65535.

index *index-number*: Specifies an index for the tag list entry, in the range of 1 to 4294967295. A tag list entry with a smaller index number is matched first. If you do not specify this option, the index number starts from 1 and increases by 1 for each of the consecutive tag list entries.

deny: Specifies the match mode for the tag list as **deny**.

permit: Specifies the match mode for the tag list as **permit**.

tag-value: Specifies a tag value in the range of 0 to 4294967295. &<1-32> indicates that the argument before it can be entered up to 32 times.

Usage guidelines

If you execute this command multiple times for a tag list entry, all tag values take effect. A tag list entry can contain up to 32 tag values.

Examples

Configure tag list 1 and create tag list entry 10 to permit IGP routes with tag value 100 to pass.

```
<Sysname> system-view
[Sysname] route tag-list 1 index 10 permit 100
```

Related commands

display route tag-list

if-match tag-list

route-policy

Use **route-policy** to create a routing policy and a node and enter routing policy node view, or enter the view of an existing routing policy node.

Use **undo route-policy** to remove a routing policy or a node of it.

Syntax

route-policy *route-policy-name* { **deny** | **permit** } **node** *node-number*

undo route-policy *route-policy-name* [**deny** | **permit**] [**node** *node-number*]

Default

No routing policies exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

route-policy-name: Specifies a routing policy name, a case-sensitive string of 1 to 63 characters.

deny: Specifies the deny match mode for the routing policy node. If a route matches all the **if-match** clauses of the node, it is denied without being compared with the next node. If a route does not match any **if-match** clauses of the node, the route is compared with the next node.

permit: Specifies the permit match mode for the routing policy node. If a route matches all the **if-match** clauses of the node, it is handled by the **apply** clauses of the node. If a route does not match any **if-match** clauses of the node, the route is compared with the next node.

node *node-number*: Specifies a node number in the range of 0 to 65535. A node with a smaller number is matched first.

Usage guidelines

Use a routing policy to filter routing information. A routing policy can contain several nodes and each node contains a set of **if-match** and **apply** clauses. The **if-match** clauses define the match criteria of the node and the **apply** clauses define the actions to be taken on packets matching the criteria. The relation between the **if-match** clauses of different types is logical AND and the relation between the **if-match** clauses of the same type is logical OR. **if-match** clauses of all types must be met. The relation between nodes is logical OR. A packet passing a node passes the routing policy. If a packet does not pass any nodes, the packet does not pass the routing policy.

Examples

Create node 10 in **permit** mode for routing policy **policy1** and enter routing policy node view.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10]
```

Related commands

display route-policy

IPv4 routing policy commands

apply fast-reroute

Use **apply fast-reroute** to set a backup link for fast route (FRR).

Use **undo apply fast-reroute** to restore the default.

Syntax

apply fast-reroute { **backup-interface** *interface-type interface-number* [**backup-nexthop** *ip-address*] | **backup-nexthop** *ip-address* }

undo apply fast-reroute

Default

No backup link for FRR is configured.

Views

Routing policy node view

Predefined user roles

network-admin

context-admin

Parameters

backup-interface *interface-type interface-number*: Specifies a backup output interface by its type and number. If the specified interface is a non-P2P interface, you must also specify a backup next hop. Non-P2P interfaces include NBMA and broadcast interfaces.

backup-nexthop *ip-address*: Specifies a backup next hop.

Usage guidelines

This command sets a backup link in the routing policy for FRR.

Using the routing policy, a routing protocol can designate a backup link for specific routes to implement FRR. When the primary link fails, FRR immediately directs packets to the backup link to minimize interruption time.

Examples

Configure node 10 of routing policy **policy1** to set the backup output interface GigabitEthernet 1/0/1 and backup next hop 193.1.1.8 for the route destined for 100.1.1.0/24.

```
<Sysname> system-view
[Sysname] ip prefix-list abc index 10 permit 100.1.1.0 24
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match ip address prefix-list abc
[Sysname-route-policy-policy1-10] apply fast-reroute backup-interface gigabitethernet
1/0/1 backup-nexthop 193.1.1.8
```

apply ip-address next-hop

Use **apply ip-address next-hop** to set a next hop for IPv4 routes.

Use **undo apply ip-address next-hop** to restore the default.

Syntax

apply ip-address next-hop *ip-address* [**public** | **vpn-instance** *vpn-instance-name*]

undo apply ip-address next-hop

Default

No next hop is set for IPv4 routes.

Views

Routing policy node view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the next hop IP address.

public: Specifies the public network.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

If you use this command to set a next hop for redistributed routes, the configuration does not take effect.

If you do not specify the **public** keyword and the **vpn-instance** *vpn-instance-name* option, the next hop belongs to the public network.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to set next hop 193.1.1.8 for routes matching prefix list 100.

```
<Sysname> system-view
[Sysname] ip prefix-list 100 permit 192.168.10.1 24
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match ip address prefix-list 100
[Sysname-route-policy-policy1-10] apply ip-address next-hop 193.1.1.8
```

display ip prefix-list

Use **display ip prefix-list** to display IPv4 prefix list statistics.

Syntax

display ip prefix-list [**name** *prefix-list-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

name *prefix-list-name*: Specifies an IP prefix list by its name, a case-sensitive string of 1 to 63 characters. If you do not specify this option, the command displays statistics for all IPv4 prefix lists.

Examples

Display the statistics for IPv4 prefix list **abc**.

```
<Sysname> display ip prefix-list name abc
Prefix-list: abc
 Permitted 0
 Denied 0
        index: 10        Deny   6.6.6.0/24              ge  26  le  28
```

Table 7 Command output

Field	Description
Prefix-list	Name of the IPv4 prefix list.

Permitted	Number of routes matching the criterion.
Denied	Number of routes not matching the criterion.
index	Index of an item.
deny	Match mode of the item: • **Permit**. • **Deny**.
6.6.6.0/24	IP address and mask.
ge	Greater-equal, the lower mask length limit.
le	Less-equal, the upper mask length limit.

Related commands

ip prefix-list

reset ip prefix-list

if-match ip

Use **if-match ip** to match IPv4 routes whose destination, next hop, or source address matches an ACL or IPv4 prefix list.

Use **undo if-match ip** to remove the specified ACL or IPv4 prefix list match criterion.

Syntax

if-match ip { **address** | **next-hop** | **route-source** } { **acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **prefix-list** *prefix-list-name* }

undo if-match ip { **address** | **next-hop** | **route-source** } [**acl** | **prefix-list**]

Default

No ACL or IPv4 prefix list match criterion is configured.

Views

Routing policy node view

Predefined user roles

network-admin

context-admin

Parameters

address: Matches the destination address of IPv4 routes.

next-hop: Matches the next hop of IPv4 routes.

route-source: Matches the source address of BGP routes. This keyword corresponds to the **Neighbor** field in the output from the **display ip routing-table verbose** command.

acl *ipv4-acl-number*: Specifies an ACL by its number. The value range for the *ipv4-acl-number* argument is 2000 to 3999 for the **address** keyword, and 2000 to 2999 for the **next-hop** keyword and **route-source** keyword.

acl name *ipv4-acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters. The ACL name must start with a letter and cannot be **all**.

prefix-list *prefix-list-name*: Specifies an IP prefix list by its name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

Follow these restrictions and guidelines to use an IPv4 advanced ACL rule to configure an ACL match criterion:

- To match the destination address of IPv4 routes, execute the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* command to create the rule.
- To match the destination address mask of IPv4 routes, execute the **rule** [*rule-id*] { **deny** | **permit** } **ip destination** *dest-addr dest-wildcard* command to create the rule. Make sure the wildcard mask specified by the *dest-wildcard* argument is consecutive. If the wildcard mask is nonconsecutive, the rule is not applicable to the **if-match ip** command.

Examples

Configure node 10 of routing policy **policy1** to match IPv4 routes whose next hop matches IP prefix list **p1**.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match ip next-hop prefix-list p1
```

ip prefix-list

Use **ip prefix-list** to configure an IPv4 prefix list or an item for the list.

Use **undo ip prefix-list** to remove an IPv4 prefix list or an item of it.

Syntax

ip prefix-list *prefix-list-name* [**index** *index-number*] { **deny** | **permit** } *ip-address mask-length* [**greater-equal** *min-mask-length*] [**less-equal** *max-mask-length*]

undo ip prefix-list *prefix-list-name* [**index** *index-number*]

Default

No IPv4 prefix lists exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

prefix-list-name: Specifies an IPv4 prefix list name, a case-sensitive string of 1 to 63 characters.

index *index-number*: Specifies an index number for an IPv4 prefix list item, in the range of 1 to 65535. An item with a smaller index number is matched first. If you do not specify this option, the index number starts from 10 and increases by 10 for each of the consecutive prefix list items.

deny: Specifies the deny mode. If a route matches the item, the route is denied without being compared with the next item. If a route does not match the item, the route is compared with the next item.

permit: Specifies the permit mode. If a route matches the item, it passes the IPv4 prefix list. If a route does not match the item, the route is compared with the next item.

ip-address mask-length: Specifies an IPv4 prefix and mask length. The value range for the *mask-length* argument is 0 to 32.

greater-equal *min-mask-length*, **less-equal** *max-mask-length*: Specifies a prefix length range. The **greater-equal** keyword means "greater than or equal to" and the **less-equal** keyword means "less than or equal to." The prefix length range relation is *mask-length* <= *min-mask-length* <= *max-mask-length* <= 32.

- If only the *min-mask-length* argument is specified, the prefix length range is [*min-mask-length*, 32].
- If only the *max-mask-length* argument is specified, the prefix length range is [*mask-length*, *max-mask-length*].
- If both the *min-mask-length* and *max-mask-length* arguments are specified, the prefix length range is [*min-mask-length*, *max-mask-length*].

Usage guidelines

An IPv4 prefix list is used to filter IPv4 addresses. It can contain multiple items, each of which specifies a range of IPv4 prefixes. The relation between the items is logical OR. If an item is passed, the IPv4 prefix list is passed. If no item is passed, the IP prefix list cannot be passed.

If both the *ip-address* and *mask-length* arguments are specified as 0.0.0.0 0, only the default route will be matched.

To match all routes, use 0.0.0.0 0 **less-equal** 32.

Examples

Configure IP prefix list **p1** to permit routes destined for network 10.0.0.0/8 and with mask length 17 or 18.

```
<Sysname> system-view
[Sysname] ip prefix-list p1 permit 10.0.0.0 8 greater-equal 17 less-equal 18
```

Related commands

display ip prefix-list

reset ip prefix-list

reset ip prefix-list

Use **reset ip prefix-list** to clear IPv4 prefix list statistics.

Syntax

reset ip prefix-list [*prefix-list-name*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

prefix-list-name: Specifies an IP prefix list by its name, a case-sensitive string of 1 to 63 characters. If you do not specify this argument, the command clears statistics for all IPv4 prefix lists.

Examples

Clear the statistics for IPv4 prefix list **abc**.

```
<Sysname> reset ip prefix-list abc
```

Related commands

display ip prefix-list

ip prefix-list

IPv6 routing policy commands

apply ipv6 fast-reroute

Use **apply ipv6 fast-reroute** to set a backup link for fast route (FRR).

Use **undo apply ipv6 fast-reroute** to restore the default.

Syntax

apply ipv6 fast-reroute { **backup-interface** *interface-type interface-number* [**backup-nexthop** *ipv6-address*] | **backup-nexthop** *ipv6-address* }

undo apply ipv6 fast-reroute

Default

No backup link for FRR is configured.

Views

Routing policy node view

Predefined user roles

network-admin

context-admin

Parameters

backup-interface *interface-type interface-number*: Specifies a backup output interface by its type and number. If the specified interface is a non-P2P interface, you must also specify a backup next hop. Non-P2P interfaces include NBMA and broadcast interfaces.

backup-nexthop *ipv6-address*: Specifies an IPv6 backup next hop.

Usage guidelines

This command sets a backup link in the routing policy for FRR.

Using the routing policy, a routing protocol can designate a backup link for specific routes to implement FRR. When the primary link fails, FRR immediately directs packets to the backup link to minimize interruption time.

Examples

Configure node 10 of routing policy **policy1** to set the backup next hop 1::1/64 for the route destined for 100::1/64.

```
<Sysname> system-view
[Sysname] ipv6 prefix-list abc index 10 permit 100::1 64
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match ipv6 address prefix-list abc
[Sysname-route-policy-policy1-10] apply ipv6 fast-reroute backup-nexthop 1::1
```

apply ipv6 next-hop

Use **apply ipv6 next-hop** to set a next hop for IPv6 routes.

Use **undo apply ipv6 next-hop** to restore the default.

Syntax

apply ipv6 next-hop *ipv6-address*

undo apply ipv6 next-hop

Default

No next hop is set for IPv6 routes.

Views

Routing policy node view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address: Specifies the next hop IPv6 address.

Usage guidelines

If you use this command to set a next hop for redistributed routes, the configuration does not take effect.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to set next hop 3ffe:506::1 for IPv6 routes matching prefix list 100.

```
<Sysname> system-view
[Sysname] ipv6 prefix-list 100 permit 2::2 64
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match ipv6 address prefix-list 100
[Sysname-route-policy-policy1-10] apply ipv6 next-hop 3ffe:506::1
```

display ipv6 prefix-list

Use **display ipv6 prefix-list** to display IPv6 prefix list statistics.

Syntax

display ipv6 prefix-list [**name** *prefix-list-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

name *prefix-list-name*: Specifies an IPv6 prefix list by its name, a case-sensitive string of 1 to 63 characters. If you do not specify this option, the command displays statistics for all IPv6 prefix lists.

Examples

Display the statistics for all IPv6 prefix lists.

```
<Sysname> display ipv6 prefix-list
Prefix-list6: 666
 Permitted 0
 Denied 0
        index: 10        Permit 6::/64                 ge  66  le  88
```

Table 8 Command output

Field	Description
Prefix-list6	Name of the IPv6 prefix list.
Permitted	Number of routes matching the criterion.
Denied	Number of routes not matching the criterion.
index	Index number of an item.
permit	Match mode of the item: • **Permit**. • **Deny**.
6::/64	IPv6 address and prefix length for matching.
ge	Greater-equal, the lower prefix length limit.
le	Less-equal, the upper prefix length limit.

Related commands

ipv6 prefix-list

reset ipv6 prefix-list

if-match ipv6

Use **if-match ipv6** to match IPv6 routes whose destination, next hop, or source address matches an ACL or IPv6 prefix list.

Use **undo if-match ipv6** to remove the specified ACL or IPv6 prefix list match criterion.

Syntax

if-match ipv6 { **address** | **next-hop** | **route-source** } { **acl** { *ipv6-acl-number* | **name** *ipv6-acl-name* } | **prefix-list** *prefix-list-name*

undo if-match ipv6 { **address** | **next-hop** | **route-source** } [**acl** | **prefix-list**]

Default

No ACL or IPv6 prefix list match criterion is configured.

Views

Routing policy node view

Predefined user roles

network-admin

context-admin

Parameters

address: Matches the destination address of IPv6 routes.

next-hop: Matches the next hop of IPv6 routes.

route-source: Matches the source address of IPv6 routes.

acl *ipv6-acl-number*: Specifies an IPv6 ACL by its number. The value range for the *ipv6-acl-number* argument is 2000 to 3999 for the **address** keyword, and 2000 to 2999 for the **next-hop** and **route-source** keywords.

acl name *ipv6-acl-name*: Specifies an IPv6 ACL by its name, a case-insensitive string of 1 to 63 characters. The ACL name must start with a letter and cannot be **all**.

prefix-list *prefix-list-name*: Specifies an IPv6 prefix list by its name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

Follow these restrictions and guidelines to use an IPv6 advanced ACL rule to configure an ACL match criterion:

- To match the destination address of IPv6 routes, execute the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* command to create the rule.
- To match the destination address prefix of IPv6 routes, execute the **rule** [*rule-id*] { **deny** | **permit** } **ip destination** *dest-addr dest-wildcard* command to create the rule. Make sure the address prefix specified by the *dest-wildcard* argument is consecutive. If the address prefix is nonconsecutive, the rule is not applicable to the **if-match ipv6** command.

Examples

Configure node 10 of routing policy **policy1** to permit routes whose next hop matches IPv6 prefix list **p1**.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match ipv6 next-hop prefix-list p1
```

ipv6 prefix-list

Use **ipv6 prefix-list** to configure an IPv6 prefix list or an item for it.

Use **undo ipv6 prefix-list** to remove an IPv6 prefix list or an item.

Syntax

ipv6 prefix-list *prefix-list-name* [**index** *index-number*] { **deny** | **permit** } *ipv6-address* { *prefix-length* [**greater-equal** *min-prefix-length*] [**less-equal** *max-prefix-length*] | **inverse** *inverse-prefix-length* }

undo ipv6 prefix-list *prefix-list-name* [**index** *index-number*]

Default

No IPv6 prefix lists exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

prefix-list-name: Specifies an IPv6 prefix list name, a case-sensitive string of 1 to 63 characters.

index *index-number*: Specifies an index number for an IPv6 prefix list item, in the range of 1 to 65535. An item with a smaller index number is matched first. If you do not specify this option, the index number starts from 10 and increases by 10 for each of the consecutive IPv6 prefix list items.

deny: Specifies the deny mode. If a route matches the item, the route is denied without being compared with the next item. If a route does not match the item, the route is compared with the next item.

permit: Specifies the permit mode. If a route matches the item, it passes the IPv6 prefix list. If a route does not match the item, the route is compared with the next item.

ipv6-address: Specifies an IPv6 address.

prefix-length: Specifies the IPv6 prefix length. The value range for the *prefix-length* argument is 0 to 128.

greater-equal *min-mask-length*, **less-equal** *max-mask-length*: Specifies a prefix length range. The **greater-equal** keyword means "greater than or equal to" and the **less-equal** keyword means "less than or equal to."

The prefix length range relation is *mask-length* <= *min-mask-length* <= *max-mask-length* <= 128.

- If only the *min-prefix-length* argument is specified, the prefix length range is [*min-prefix-length*, 128].
- If only the *max-prefix-length* argument is specified, the prefix length range is [*prefix-length*, *max-prefix-length*].
- If both the *min-prefix-length* and *max-prefix-length* arguments are specified, the prefix length range is [*min-prefix-length*, *max-prefix-length*].

inverse *inverse-prefix-length*: Matches IPv6 addresses from the least significant bit to the specified length. The value range for the *inverse-prefix-length* argument is 1 to 128.

Usage guidelines

An IPv6 prefix list is used to filter IPv6 addresses. An IPv6 prefix list can have multiple items, and each of them specifies a range of IPv6 prefixes. The relation between the items is logical OR. A route passing an item passes the IPv6 prefix list. A route passing no item does not pass the IPv6 prefix list.

If the *ipv6-address prefix-length* argument is specified as :: 0, only the default route matches.

To match all routes, configure :: 0 **less-equal** 128.

Examples

Permit IPv6 addresses with a mask length between 32 bits and 64 bits.

```
<Sysname> system-view
[Sysname] ipv6 prefix-list abc permit :: 0 greater-equal 32 less-equal 64
```

Deny IPv6 addresses with a prefix 3FFE:D00::/32 and a prefix length greater than or equal to 32 bits.

```
<Sysname> system-view
[Sysname] ipv6 prefix-list abc deny 3FFE:D00:: 32 less-equal 128
```

Related commands

display ipv6 prefix-list

reset ipv6 prefix-list

reset ipv6 prefix-list

Use **reset ipv6 prefix-list** to clear IPv6 prefix list statistics.

Syntax

reset ipv6 prefix-list [*prefix-list-name*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

prefix-list-name: Specifies an IPv6 prefix list by its name, a case-sensitive string of 1 to 63 characters. If you do not specify this argument, the command clears statistics for all IPv6 prefix lists.

Examples

Clear the statistics for IPv6 prefix list **abc**.

```
<Sysname> reset ipv6 prefix-list abc
```

Related commands

display ipv6 prefix-list

ipv6 prefix-list

Contents

Guard route commands

ip route-guard

Use **ip route-guard** to configure an IPv4 guard route.

Use **undo ip route-guard** to delete an IPv4 guard route.

Syntax

ip route-guard *ip-address* { *mask-length* | *mask* }

undo ip route-guard *ip-address* { *mask-length* | *mask* }

Default

No IPv4 guard route is configured.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the destination IP address in dotted decimal format.

mask-length: Specifies a mask length in the range of 0 to 32.

mask: Specifies a mask in dotted decimal format.

Usage guidelines

A guard route directs traffic to the guard device for filtering and cleaning. You can manually configure a guard route on the guard device, or use a script to automatically configure a guard route upon receipt of a notification.

Guard routes have the following characteristics:

- Guard routes use Null 0 as the outgoing interface.
- Guard routes are inactive routes and will not be installed into the FIB.
- You must configure a routing protocol, such as BGP or OSPF, to redistribute and advertise guard routes for directing traffic to the guard device.

Examples

Configure a guard route destined to 11.11.11.11/32.

```
<Sysname> system-view
[Sysname] ip route-guard 11.11.11.11 255.255.255.255
```

Related commands

display ip routing-table protocol

ipv6 route-guard

Use **ipv6 route-guard** to configure an IPv6 guard route.

Use **undo ipv6 route-guard** to delete an IPv6 guard route.

Syntax

ipv6 route-guard *ipv6-address prefix-length*

undo ipv6 route-guard *ipv6-address prefix-length*

Default

No IPv6 guard route is configured.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address: Specifies the destination IPv6 address.

prefix-length: Specifies a prefix length in the range of 0 to 128.

Usage guidelines

A guard route directs traffic to the guard device for filtering and cleaning. You can manually configure a guard route on the guard device, or use a script to automatically configure a guard route upon receipt of a notification.

Guard routes have the following characteristics:

- Guard routes use Null 0 as the outgoing interface.
- Guard routes are inactive routes and will not be installed into the FIB.
- You must configure a routing protocol, such as BGP or OSPFv3, to redistribute and advertise guard routes for directing traffic to the guard device.

Examples

Configure a guard route destined to 1:1:2::/64.

```
<Sysname> system-view
[Sysname] ipv6 route-guard 1:1:2:: 64
```

Related commands

display ipv6 routing-table protocol

Contents

RIR commands

The following compatibility matrixes show the support of hardware platforms for RIR:

Models	RIR compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB1180, NFNX3-HDB1480	No

client enable

Use **client enable** to enable the RIR client globally.

Use **undo client enable** to disable the RIR client globally.

Syntax

client enable

undo client enable

Default

The RIR client is disabled globally.

Views

RIR view

Predefined user roles

network-admin

context-admin

Usage guidelines

To avoid NQA probes from occupying too many resources on a hub in a hub-spoke network, configure the hub as an RIR server and configure the spokes as RIR clients.

You can enable the RIR client globally or on an interface.

- Enabling the RIR client globally also enables the RIR client for all interfaces on the device. The interfaces can send link quality probe results for the RIR client.
- Enabling the RIR client on an interface allows only that interface to send link quality probe results for the RIR client.

When you enable the RIR client, follow these restrictions and guidelines:

- In a VXLAN network, only tunnel interfaces support enabling the RIR client. The RIR client uses the tunnel interfaces to send link quality probe results.
- The RIR server and RIR client cannot be both enabled on the same interface.
- If the enabled role (RIR server or client) on an interface is different from the globally enabled role, the interface-specific role takes effect on that interface.

Examples

Enable the RIR client globally.

```
<Sysname> system-view
[Sysname] rir
```

```
[Sysname-rir] client enable
```

Related commands

probe connect

probe sync-port

server enable

collaboration peer local

Use **collaboration peer local** to enable the local device to establish RIR collaboration relationship with a peer device.

Use **undo collaboration peer local** to restore the default.

Syntax

collaboration peer [**vpn-instance** *vpn-instance-name*] *peer-ipv4-address* **local** *local-ipv4-address* **sync-port** *port-number*

undo collaboration peer [**vpn-instance** *vpn-instance-name*] *peer-ipv4-address* **local**

Default

The local device does not establish RIR collaboration relationship with any device.

Views

RIR view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance on which the local and peer devices establish RIR collaboration relationship. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. The specified VPN instance must exist. If the local and peer IP addresses belong to the public network, do not specify this option.

peer-ipv4-address: Specifies an RIR collaboration peer by its IPv4 address.

local-ipv4-address: Specifies the IPv4 address of the local device. The local and peer devices must both belong to the public network or the same VPN instance.

sync-port *port-number*: Specifies the TCP port number used by the local and peer devices to synchronize link data. The value range for the *port-number* argument is 1024 to 65535. Make sure the port number is not used by any other service on the device.

Usage guidelines

Each pair of devices in an RIR collaboration device group must establish RIR collaboration relationship. You must configure this command on both the local and peer devices.

In a pair of devices with RIR collaboration relationship, the device with a lower IP address is the client. The client uses the port number specified by using this command to initiate a TCP connection request to its peer. Through the TCP connection, the local device can synchronize the configuration and status data of links that meet the service requirements to the peer device. The data does not include link data synchronized from other devices in the same RIR collaboration device group.

For the local device to select links from a peer device, you must execute the **collaboration peer redirect** command on both the local and peer devices.

The local and peer devices must use the same TCP port number for link data synchronization. A device can use the same or different TCP port numbers to synchronize data to different peers.

If you execute this command multiple times for the same pair of devices in the public network or a VPN instance, the most recent configuration takes effect.

Examples

Establish RIR collaboration relationship between local device 1.1.1.1 and peer device 1.1.1.2 on the public network. They use TCP port number 6000 for link data synchronization.

```
<Sysname> system-view
[Sysname] rir
[Sysname-rir] collaboration peer 1.1.1.2 local 1.1.1.1 sync-port 6000
```

Establish RIR collaboration relationship between local device 1.1.1.1 and peer device 1.1.1.2 in VPN instance **a**. They use TCP port number 6000 for link data synchronization.

```
<Sysname> system-view
[Sysname] rir
[Sysname-rir] collaboration peer vpn-instance a 1.1.1.2 local 1.1.1.1 sync-port 6000
```

Related commands

collaboration peer redirect

collaboration peer redirect

Use **collaboration peer redirect** to configure the redirect IP address of an RIR collaboration peer.

Use **undo collaboration peer redirect** to delete the redirect IP address of an RIR collaboration peer.

Syntax

collaboration peer [**vpn-instance** *vpn-instance-name*] *peer-ipv4-address* **redirect** [**vpn-instance** *redirect-vpn-instance-name*] *redirect-ipv4-address*

undo collaboration peer [**vpn-instance** *vpn-instance-name*] *peer-ipv4-address* **redirect** [**vpn-instance** *redirect-vpn-instance-name*]

Default

No redirect IP address is configured for an RIR collaboration peer.

Views

RIR view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance on which the local and peer devices establish RIR collaboration relationship. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the local and peer devices establish RIR collaboration relationship on the public network, do not specify this option.

peer-ipv4-address: Specifies an RIR collaboration peer by its IPv4 address.

vpn-instance *redirect-vpn-instance-name*: Specifies the MPLS L3VPN instance for the packets to be redirected to the redirect IPv4 address of the peer device. The

redirect-vpn-instance-name argument is a case-sensitive string of 1 to 31 characters. If the packets to be redirected belong to the public network, do not specify this option.

redirect-ipv4-address: Specifies the redirect IPv4 address of the peer device.

Usage guidelines

Use this command on both the local and peer devices that have established RIR collaboration relationship. This command specifies the redirect IP address for packets redirected to a peer device on the public network or a VPN instance. When the local device selects links from the peer device to forward packets on the public network or a VPN instance, it performs the following operations:

- Looks up the routing table of the public network or VPN instance based on the redirect IP address.
- Forwards the packets to the peer device through the RIR dedicated link.

If you execute the **undo** form of this command without the **vpn-instance** *redirect-vpn-instance-name* option for a peer, the redirect IPv4 address of the public network is deleted for the peer.

If you execute this command multiple times for the same peer on the public network or in the same redirect VPN instance, the most recent configuration takes effect.

Examples

Specify 2.1.1.1 as the redirect IP address in VPN instance **b** for peer device 1.1.1.2 in VPN instance **a**.

```
<Sysname> system-view
[Sysname] rir
[Sysname-rir] collaboration peer vpn-instance a 1.1.1.2 redirect vpn-instance b 2.1.1.1
```

Related commands

collaboration peer local

delay threshold

Use **delay threshold** to set the link delay threshold.

Use **undo delay threshold** to restore the default.

Syntax

delay threshold *threshold-value*

undo delay threshold

Default

The link delay threshold is 10 milliseconds.

Views

SLA view

Predefined user roles

network-admin

context-admin

Parameters

threshold-value: Sets the link delay threshold, in the range of 10 to 60000 milliseconds.

Usage guidelines

Link delay refers to the interval between the sending time and receiving time of a packet.

The shorter the delay time, the higher the link quality.

A flow template uses the link delay threshold in its associated SLA to filter links that meet the link delay requirement.

Examples

In SLA 1, set the link delay threshold to 1000 milliseconds.

```
<Sysname> system-view
[Sysname] sla 1
[Sysname-sla-1] delay threshold 1000
```

display tunnel flow-statistics

Use **display tunnel flow-statistics** to display flow ID-based traffic rate statistics for tunnels.

Syntax

display tunnel flow-statistics [**flow** *flow-id* [**interface tunnel** *number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

flow *flow-id*: Specifies a flow template by its flow ID, in the range of 1 to 65535. If you do not specify a flow ID, this command displays statistics for all flow templates.

interface tunnel *number*: Specifies a tunnel interface by its tunnel interface number. The value range for the *number* argument is 1 to 65535. If you do not specify a tunnel interface, this command displays statistics about the specified flow template for all tunnel interfaces.

Examples

Display flow ID-based traffic rate statistics for tunnels.

```
<Sysname> display tunnel flow-statistics

RIR flow 100:
  Interface    Out pps       Out bps
  Tunnel1      10            4800
  Tunnel2      20            9600

RIR flow 101:
  Interface    Out pps       Out bps
  Tunnel3      10            4800
  Tunnel4      20            9600
```

Table 1 Command output

Field	Description
RIR flow	Flow ID of an RIR flow template.
Interface	Tunnel interface name.
Out pps	Number of outgoing packets per second.
Out bps	Number of outgoing bits per second.

Related commands

`reset tunnel flow-statistics`

`tunnel flow-statistics enable`

expect-bandwidth

Use **`expect-bandwidth`** to specify the per-session expected bandwidth.

Use **`undo expect-bandwidth`** to restore the default.

Syntax

`expect-bandwidth` *`bandwidth`*

`undo expect-bandwidth`

Default

The per-session expected bandwidth is 0 kbps.

Views

Flow template view

Predefined user roles

network-admin

context-admin

Parameters

`bandwidth`: Specifies the bandwidth in kbps, in the range of 1 to 400000000.

Usage guidelines

The per-session expected bandwidth configured by using this command is not the actual bandwidth used by a session. It is only a value estimated based on user services.

When performing RIR link selection for a session, the device performs bandwidth detection based on the per-session expected bandwidth configured in the flow template to which the session belongs. If the used bandwidth plus the per-session expected bandwidth of a candidate link is less than 80% of its total bandwidth, the current available bandwidth of the candidate link meets the session bandwidth requirements. The link passes the bandwidth detection.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the per-session expected bandwidth to 10 kbps in flow template 1.

```
<Sysname> system-view
[Sysname] rir
[Sysname-rir] flow 1
[Sysname-rir-flow-1] expect-bandwidth 10
```

Related commands

flow

flow

Use **flow** to create a flow template and enter its view, or enter the view of an existing flow template.

Use **undo flow** to delete a flow template.

Syntax

flow *flow-id*

undo flow *flow-id*

Default

No flow templates exist.

Views

RIR view

Predefined user roles

network-admin

context-admin

Parameters

flow-id: Specifies a flow ID for the flow template. The flow ID is a hexadecimal string in the range of 0 to ffffff.

Usage guidelines

Use a flow template to define link selection policies (including the quality policy and link preference) that can filter qualified links for a type of service flow. After the device identifies the service of a packet based on the quintuple and DSCP of the packet, it assigns a flow ID to the packet according to the QoS policy applied to the service. Then, RIR selects a qualified link for the packet based on the link selection policies of the flow template that uses the flow ID.

Examples

Create flow template 1 and enter its view.

```
<Sysname> system-view
[Sysname] rir
[Sysname-rir] flow 1
[Sysname-rir-flow-1]
```

Related commands

remark flow-id (*ACL and QoS Command Reference*)

flow priority-based-schedule bandwidth-threshold

Use **flow priority-based-schedule bandwidth-threshold** to set the bandwidth usage thresholds for flow priority-based traffic scheduling.

Use **undo flow priority-based-schedule bandwidth-threshold** to restore the default.

Syntax

flow priority-based-schedule bandwidth-threshold upper *upper-threshold* **lower** *lower-threshold*

undo flow priority-based-schedule bandwidth-threshold

Default

The bandwidth usage upper threshold is 90% and the bandwidth usage lower threshold is 20%.

Views

RIR view

Predefined user roles

network-admin

context-admin

Parameters

upper *upper-threshold*: Sets the bandwidth usage upper threshold in percentage, in the range of 1 to 100. The upper threshold must be greater than or equal to the lower threshold.

lower *lower-threshold*: Sets the bandwidth usage lower threshold in percentage, in the range of 1 to 100.

Usage guidelines

If flow priority-based traffic scheduling is enabled, traffic scheduling is triggered when the bandwidth usage of a link exceeds the upper threshold. The scheduling might be last for several scheduling periods. Within each scheduling period, RIR redistributes the current lowest priority flow on this link to other links. The scheduling does not stop until the bandwidth usage of all links for the current lowest priority flow is below the lower threshold or only the highest priority flow is left on this link.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Enable flow priority-based traffic scheduling and set the bandwidth usage upper threshold and lower threshold to 80% and 30%, respectively.

```
<Sysname> system-view
[Sysname] rir
[Sysname-rir] flow priority-based-schedule enable
[Sysname-rir] flow priority-based-schedule bandwidth-threshold upper 80 lower 30
```

Related commands

flow priority-based-schedule enable

flow priority-based-schedule enable

Use **flow priority-based-schedule enable** to enable flow priority-based traffic scheduling.

Use **undo flow priority-based-schedule enable** to disable flow priority-based traffic scheduling.

Syntax

flow priority-based-schedule enable

undo flow priority-based-schedule enable

Default

Flow priority-based traffic scheduling is disabled.

Views

RIR view

Predefined user roles

network-admin

context-admin

Usage guidelines

To ensure that services with higher priority preferentially use link resources, enable flow priority-based traffic scheduling.

The priority of a flow that matches a flow template is determined by the ID of the SLA associated with that flow template. The greater the SLA ID, the higher the flow priority. To specify an SLA for a flow template, use the **quality-policy** command. If the command is not configured in a flow template, flows that match the flow template have the lowest priority.

If flow priority-based traffic scheduling is enabled, traffic scheduling is triggered when the bandwidth usage of a link exceeds the upper threshold. The scheduling might be last for several scheduling periods. Within each scheduling period, RIR redistributes the current lowest priority flow on this link to other links. The scheduling does not stop until the bandwidth usage of all links for the current lowest priority flow is below the lower threshold or only the highest priority flow is left on this link.

Examples

Enable flow priority-based traffic scheduling.

```
<Sysname> system-view
[Sysname] rir
[Sysname-rir] flow priority-based-schedule enable
```

Related commands

quality-policy

sla

flow priority-based-schedule schedule-period

Use **flow priority-based-schedule schedule-period** to set the scheduling period for flow priority-based traffic scheduling.

Use **undo flow priority-based-schedule schedule-period** to restore the default.

Syntax

flow priority-based-schedule schedule-period *schedule-period-value*

undo flow priority-based-schedule schedule-period

Default

The scheduling period for flow priority-based traffic scheduling is 30 seconds.

Views

RIR view

Predefined user roles

network-admin

context-admin

Parameters

schedule-period-value: Sets the scheduling period for flow priority-based traffic scheduling, in seconds. The value range for this argument is 15 to 65535.

Usage guidelines

If flow priority-based traffic scheduling is enabled, traffic scheduling is triggered when the bandwidth usage of a link exceeds the upper threshold. The scheduling might be last for several scheduling periods. Within each scheduling period (set by using this command), RIR redistributes the current lowest priority flow on this link to other links. The scheduling does not stop until the bandwidth usage of all links for the current lowest priority flow is below the lower threshold or only the highest priority flow is left on this link.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the scheduling period for flow priority-based traffic scheduling to 20 seconds.

```
<Sysname> system-view
[Sysname] rir
[Sysname-rir] flow priority-based-schedule enable
[Sysname-rir] flow priority-based-schedule schedule-period 20
```

jitter threshold

Use **jitter threshold** to set the link jitter threshold.

Use **undo jitter threshold** to restore the default.

Syntax

jitter threshold *threshold-value*

undo jitter threshold

Default

The link jitter threshold is 100 milliseconds.

Views

SLA view

Predefined user roles

network-admin

context-admin

Parameters

threshold-value: Sets the link jitter threshold, in the range of 0 to 3600000 milliseconds.

Usage guidelines

The jitter time equals the receiving time interval between two consecutive packets minus the sending time interval between the two consecutive packets. The shorter the jitter time, the higher the link quality. A flow template uses the jitter threshold in its associated SLA to filter links that meet the jitter requirement.

Examples

In SLA 1, set the link jitter threshold to 1000 milliseconds.

```
<Sysname> system-view
[Sysname] sla 1
[Sysname-sla-1] jitter threshold 1000
```

link-select delay

Use **link-select delay** to set the link selection delay.

Use **undo link-select delay** to restore the default.

Syntax

link-select delay *delay*

undo link-select delay

Default

The link selection delay is 60 seconds.

Views

RIR view

Predefined user roles

network-admin

context-admin

Parameters

delay: Sets the link selection delay in seconds, in the range of 1 to 65535.

Usage guidelines

To improve packet forwarding efficiency, the device does not repeatedly perform link selection for traffic of the same session. After the device performs link selection for traffic of a session, it forwards the subsequent traffic of that session according to the previous link selection result. Link reselection is triggered when any link in the session's flow template has one of the following changes:

- The quality of a link becomes qualified from unqualified or the quality of a link becomes unqualified from qualified.
- The bandwidth usage of a link has reached the maximum.

To avoid frequent link selection caused by link flapping, RIR defines a link selection delay and link selection suppression period.

After the device performs link selection, it starts the link selection suppression period if the period has been configured. Within the link selection suppression period, the device does not perform link reselection, but it maintains the link state data. When the link selection suppression period ends, the link selection delay timer starts. If the link state still meets the conditions that can trigger link reselection when the delay timer expires, the device performs link reselection. If the link state changes to not meet the conditions that can trigger link reselection within the delay time, the device does not perform link reselection.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the link selection delay to 30 seconds.

```
<Sysname> system-view
[Sysname] rir
[Sysname-rir] link-select delay 30
```

Related commands

link-select suppress-period

link-select suppress-period

Use **link-select suppress-period** to set the link selection suppression period.

Use **undo link-select suppress-period** to restore the default.

Syntax

link-select suppress-period *period-value*

undo link-select suppress-period

Default

No link selection suppression period is configured. The device does not start the link selection suppression period after a link selection.

Views

RIR view

Predefined user roles

network-admin

context-admin

Parameters

period-value: Sets the link selection suppression period in seconds, in the range of 1 to 131070.

Usage guidelines

To avoid frequent link selection caused by link flapping, configure a link selection suppression period. The device starts the link selection suppression period after it performs a link selection.

Within the link selection suppression period, the device does not perform link reselection, but it maintains the link state data. When the link selection suppression period ends, the link selection delay timer starts. If the link state still meets the conditions that can trigger link reselection when the delay timer expires, the device performs link reselection. If the link state changes to not meet the conditions that can trigger link reselection within the delay time, the device does not perform link reselection.

As a best practice, set the link selection suppression period to a multiple of the link selection delay time. Make sure the suppression period is at least double of the link selection delay time.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the link selection suppression period to 60 seconds.

```
<Sysname> system-view
[Sysname] rir
[Sysname-rir] link-select suppress-period 60
```

Related commands

link-select delay

load-balance per-packet enable

Use **load-balance per-packet enable** to enable per-packet load balancing.

Use **undo load-balance enable** to restore the default.

Syntax

load-balance per-packet enable

undo load-balance enable

Default

The RIR global link load balancing mode applies.

Views

Flow template view

Predefined user roles

network-admin

context-admin

Usage guidelines

Based on link bandwidth, RIR supports the following link load balancing modes:

- **Per-session weight-based link selection mode**—RIR global link load balancing mode that takes effect on all RIR flows. This mode can distribute the sessions that match the same flow template to different links according to the weights of the links. RIR selects only one link to transmit a session.
- **Per-session periodic link adjustment mode**—RIR global link load balancing mode that takes effect on all RIR flows. This mode not only can distribute the sessions that match the same flow template to different links, but also can periodically adjust links for the sessions. Within one adjustment period, RIR selects only one link to transmit a session.
- **Per-packet mode**—Flow-specific link load balancing mode that takes effect only on sessions that match the flow template where this mode is enabled. This mode can distribute the same session to different links for transmission.

The mechanisms of the per-packet mode are as follows:

- **For preference-based primary link selection, preference-based backup link selection, and quality tolerant link selection**—If multiple links with the same preference meet the requirements of a session, all these links are candidate optimal links for this session. When forwarding traffic for the session, the device distributes the traffic to these links packet by packet according to the remaining bandwidth weight of each link.

  For example, the device needs 10 Mbps of bandwidth to transmit traffic for a session with flow ID 1. Links 1 and 2 are available to transmit traffic for this session. The remaining bandwidth of link 1 is 20 Mbps and the remaining bandwidth of link 2 is 30 Mbps. Finally, the traffic of this session uses 4 Mbps of bandwidth on link 1 and 6 Mbps of bandwidth on link 2.
- **For bandwidth tolerant link selection**—If multiple links meet the requirements of a session, all these links are candidate optimal links for this session. When forwarding traffic for the session, the device distributes the traffic to these links packet by packet. Each link has the same probability to be selected.

Because packets of the same session are distributed to multiple links, the receiver might receive out-of-order packets. As a best practice, do not enable per-packet load balancing for order-sensitive services (except the services that use protocols to maintain a correct packet order, for example, TCP).

Examples

Enable per-packet load balancing mode in flow template with flow ID 1.

```
<Sysname> system-view
[Sysname] rir
[Sysname-rir] flow 1
[Sysname-rir-flow-1] load-balance per-packet enable
```

load-balance per-session periodic-adjust adjust-interval

Use **load-balance per-session periodic-adjust adjust-interval** to set the adjustment interval for per-session periodic link adjustment mode.

Use **undo load-balance per-session periodic-adjust adjust-interval** to restore the default.

Syntax

load-balance per-session periodic-adjust adjust-interval *interval-value*

undo load-balance per-session periodic-adjust adjust-interval

Default

The adjustment interval for per-session periodic link adjustment mode is 30 seconds.

Views

RIR view

Predefined user roles

network-admin

context-admin

Parameters

interval-value: Sets the adjustment interval for per-session periodic link adjustment mode, in the range of 15 to 65535 seconds.

Usage guidelines

In per-session periodic link adjustment mode, the device periodically detects the bandwidth usage of all links that have RIR sessions at intervals configured by using this command. RIR reselect links for sessions that match a flow template if the links in the flow template meets the following requirements: The difference between the largest remaining bandwidth ratio and the smallest remaining bandwidth ratio becomes larger than or equal to the periodic adjustment upper threshold. The link adjustment might be last for several adjustment intervals. RIR stops link adjustment if one of the following requirements is met:

- The difference between the largest remaining bandwidth ratio and the smallest remaining bandwidth ratio of the links becomes smaller than the periodic adjustment lower threshold.
- The adjustment interval is the 20th interval after link reselection is triggered.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the adjustment interval for per-session periodic link adjustment mode to 20 seconds.

```
<Sysname> system-view
[Sysname] rir
[Sysname-rir] load-balance per-session periodic-adjust adjust-interval 20
```

Related commands

load-balance per-session periodic-adjust enable

load-balance per-session periodic-adjust threshold

load-balance per-session periodic-adjust enable

Use **load-balance per-session periodic-adjust enable** to enable per-session periodic link adjustment mode.

Use **undo load-balance per-session periodic-adjust enable** to restore the default.

Syntax

load-balance per-session periodic-adjust enable

undo load-balance per-session periodic-adjust enable

Default

The per-session weight-based link selection mode is used.

Views

RIR view

Predefined user roles

network-admin

context-admin

Usage guidelines

Based on link bandwidth, RIR supports the following link load balancing modes:

- **Per-session weight-based link selection mode**—RIR global link load balancing mode that takes effect on all RIR flows. This mode can distribute the sessions that match the same flow template to different links according to the weights of the links. RIR selects only one link to transmit a session.
- **Per-session periodic link adjustment mode**—RIR global link load balancing mode that takes effect on all RIR flows. This mode not only can distribute the sessions that match the same flow template to different links, but also can periodically adjust links for the sessions. Within one adjustment period, RIR selects only one link to transmit a session.
- **Per-packet mode**—Flow-specific link load balancing mode that takes effect only on traffic that matches the flow template where this mode is enabled. This mode can distribute the same session to different links for transmission.

The mechanisms of the per-session periodic link adjustment mode are as follows:

- **For preference-based primary link selection, preference-based backup link selection, and quality tolerant link selection**—If multiple links with the same preference meet the requirements of a flow template, RIR selects one optimal link for each session of the flow template from these links. RIR preferentially selects the link with the lowest bandwidth usage for a session. The bandwidth usage adopted by RIR is the actual bandwidth usage plus the per-session expected bandwidth.
- **For bandwidth tolerant link selection**—If multiple links meet the requirements of a flow template, RIR selects one optimal link for each session of the flow template from these links. The link selected the last time for a session takes precedence over the other links for that session. If RIR performs link selection for a session for the first time, it selects a link based on the remaining bandwidth weights of the available links.

In per-session periodic link adjustment mode, the device periodically detects the bandwidth usage of all links that have RIR sessions at the configured adjustment intervals. RIR reselect links for sessions that match a flow template if the links in the flow template meets the following requirements: The difference between the largest remaining bandwidth ratio and the smallest remaining bandwidth ratio becomes larger than or equal to the periodic adjustment upper threshold. The link adjustment might be last for several adjustment intervals. RIR stops link adjustment if one of the following requirements is met:

- The difference between the largest remaining bandwidth ratio and the smallest remaining bandwidth ratio of the links becomes smaller than the periodic adjustment lower threshold.
- The adjustment interval is the 20th interval after link reselection is triggered.

For a flow template, the per-packet load balancing mode takes precedence over the global per-session periodic link adjustment mode. If the per-packet load balancing mode is not enabled for a flow template, the flow template uses the global link load balancing mode.

Examples

Enable per-session periodic link adjustment mode.

```
<Sysname> system-view
[Sysname] rir
[Sysname-rir] load-balance per-session periodic-adjust enable
```

Related commands

load-balance per-session periodic-adjust adjust-interval

load-balance per-session periodic-adjust threshold

load-balance per-session periodic-adjust threshold

Use **load-balance per-session periodic-adjust threshold** to set the periodic adjustment thresholds in per-session periodic link adjustment mode.

Use **undo load-balance per-session periodic-adjust threshold** to restore the default.

Syntax

load-balance per-session periodic-adjust threshold upper *upper-threshold-value* **lower** *lower-threshold-value*

undo load-balance per-session periodic-adjust threshold

Default

The periodic adjustment upper threshold is 50% and the periodic adjustment lower threshold is 20%.

Views

RIR view

Predefined user roles

network-admin

context-admin

Parameters

upper *upper-threshold-value*: Sets the periodic adjustment upper threshold, in the range of 1 to 100. The *upper-threshold-value* argument specifies the largest difference allowed between the largest remaining bandwidth ratio and the smallest remaining bandwidth ratio of all available links.

lower *lower-threshold-value*: Sets the periodic adjustment lower threshold, in the range of 1 to 100. After the difference between the largest remaining bandwidth ratio and the smallest remaining bandwidth ratio becomes smaller than this threshold, RIR stops link adjustment.

Usage guidelines

In per-session periodic link adjustment mode, the device periodically detects the bandwidth usage of all links that have RIR sessions at the configured adjustment intervals. RIR reselect links for sessions that match a flow template if the links in the flow template meets the following requirements: The difference between the largest remaining bandwidth ratio and the smallest remaining bandwidth ratio becomes larger than or equal to the periodic adjustment upper threshold. The link adjustment might be last for several adjustment intervals. RIR stops link adjustment if one of the following requirements is met:

- The difference between the largest remaining bandwidth ratio and the smallest remaining bandwidth ratio of the links becomes smaller than the periodic adjustment lower threshold.
- The adjustment interval is the 20th interval after link reselection is triggered.

The periodic adjustment upper threshold must be greater than or equal to the periodic adjustment lower threshold.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the periodic adjustment upper threshold and the periodic adjustment lower threshold to 60% and 30%, respectively.

```
<Sysname> system-view
[Sysname] rir
[Sysname-rir] load-balance per-session periodic-adjust threshold upper 60 lower 30
```

Related commands

load-balance per-session periodic-adjust enable

load-balance per-session periodic-adjust adjust-interval

log enable

Use **log enable** to enable RIR logging.

Use **undo log enable** to disable RIR logging.

Syntax

log enable

undo log enable

Default

RIR logging is disabled.

Views

RIR view

Predefined user roles

network-admin

context-admin

Usage guidelines

RIR logs record events occurred during the RIR process, such as link selection and reselection, quality change, bandwidth change, configuration change, and link fault events. The logs help the administrator analyze, maintain, and adjust the RIR network.

RIR logs are flow logs. To output RIR logs, you must also configure flow log features. For more information about flow logs, see *Network Management and Monitoring Configuration Guide*.

Examples

Enable RIR logging.

```
<Sysname> system-view
[Sysname] rir
[Sysname-rir] log enable
```

Related commands

`userlog flow export host` (*Network Management and Monitoring Command Reference*)

`userlog flow syslog` (*Network Management and Monitoring Command Reference*)

nqa

Use **nqa** to create an NQA link quality operation and enter its view, or enter the view of an existing NQA link quality operation.

Use **undo nqa** to delete an NQA link quality operation.

Syntax

nqa *`nqa-id`*

undo nqa *`nqa-id`*

Default

No NQA link quality operations exist.

Views

RIR view

Predefined user roles

network-admin

context-admin

Parameters

`nqa-id`: Specifies an NQA link quality operation by its ID, in the range of 0 to 128.

Usage guidelines

An NQA link quality operation allows a flow template to start UDP jitter probes based on the probe parameters in the operation in order to detect the quality of links.

You can configure a quality policy for a flow template to associate the flow template with an SLA and an NQA link quality operation. The device monitors the quality of links in the flow template based on the NQA link quality operation and compares the NQA probe results with the thresholds in the SLA. If all parameter values in the probe results of a link are lower than or equal to the thresholds in the SLA, the link is qualified for the flow.

To differentiate service flows that have different link quality requirements, associate the flow templates with NQA link quality operations that contain different probe parameter values. Two NQA link quality operations with different probe parameter values might offer different probe results for the same link.

In a VXLAN network, the NQA link quality probe targets are VXLAN tunnel interfaces enabled with the RIR client.

The device supports a maximum of 129 NQA link quality operations.

Examples

Create NQA link quality operation 1 and enter its view.

```
<Sysname> system-view
[Sysname] rir
[Sysname-rir] nqa 1
[Sysname-rir-nqa-1]
```

Related commands

nqa agent enable (*Network Management and Monitoring Command Reference*)

quality-policy

packet-loss threshold

Use **packet-loss threshold** to set the packet loss threshold.

Use **undo packet-loss threshold** to restore the default.

Syntax

packet-loss threshold *threshold-value*

undo packet-loss threshold

Default

The packet loss threshold is 100‰.

Views

SLA view

Predefined user roles

network-admin

context-admin

Parameters

threshold-value: Sets the packet loss threshold, in the range of 0 to 1000 in permillage.

Usage guidelines

The packet loss ratio is the number of lost packets to the total number of sent packets. The lower the packet loss ratio, the higher the link quality. A flow template uses the packet loss threshold in its associated SLA to filter links that meet the packet loss requirement.

Examples

In SLA 1, set the packet loss threshold to 500‰.

```
<Sysname> system-view
[Sysname] sla 1
[Sysname-sla-1] packet-loss threshold 500
```

Related commands

sla

path link-type index preference

Use **path link-type index preference** to specify a link preference for a type of links with a specific link index in a flow template.

Use **undo path link-type index preference** to restore the default.

Syntax

path link-type { **4g** | **internet** | **mpls** | **mstp** } **index** *link-index* **preference** *preference*

undo path link-type { **4g** | **internet** | **mpls** | **mstp** } **index** *link-index*

Default

No link preference is specified for a type of links with a specific link index in a flow template.

Views

Flow template view

Predefined user roles

network-admin

context-admin

Parameters

4g: Specifies the 4G type.

internet: Specifies the Internet type.

mpls: Specifies the MPLS type.

mstp: Specifies the MSTP type.

index *link-index*: Specifies a link index in the range of 1 to 65535.

preference *preference*: Specifies a link preference in the range of 1 to 255. The lower the value, the higher the priority.

Usage guidelines

RIR preferentially selects links with higher preference.

The link type and link index specified in this command identify links on a VSI interface. .Because a VSI interface can have only one VXLAN tunnel between a hub and spoke, this command sets the link preference for a specific VXLAN tunnel.

You can assign the same link preference value to different links in the same flow template.

Examples

In flow template 1, set the preference of MPLS link 1 to 100.

```
<Sysname> system-view
[Sysname] rir
[Sysname-rir] flow 1
[Sysname-flow-1] path link-type mpls index 1 preference 100
```

Related commands

rir link-type

probe connect

Use **probe connect** to configure NQA link connectivity probe parameters.

Use **undo probe connect** to restore the default.

Syntax

probe connect interval *interval* **timeout** *timeout*

undo probe connect

Default

The NQA link connectivity probe interval is 100 milliseconds. The timeout time is 3000 milliseconds for waiting for a response to a link connectivity probe packet.

Views

RIR view

Predefined user roles

network-admin

context-admin

Parameters

interval *interval*: Sets the NQA link connectivity probe interval in milliseconds. The value range for the *interval* argument is 0 to 604800000. The value of 0 represents that only one probe is performed.

timeout *timeout*: Sets the timeout time for waiting for a response to a link connectivity probe packet. The value range for the *timeout* argument is 10 to 3600000 milliseconds.

Usage guidelines

The device starts to detect the connectivity of all links in flow templates after RIR is enabled. Spokes (RIR clients) performs consecutive probes at the configured intervals and wait for responses for the probe packets. If an RIR client has not received any responses on a link when the probe packet timeout timer expires, the client determines that the link has connectivity issues.

Setting a shorter probe interval obtains more precise probe results but requires more system resources.

Set a shorter probe packet timeout time if the requirement for link quality is high.

In a VXLAN network, the probe targets are VXLAN tunnel interfaces enabled with the RIR client.

Examples

Set the NQA link connectivity probe interval to 30 milliseconds, and set the timeout time to 20 milliseconds for waiting for a response to a link connectivity probe packet.

```
<Sysname> system-view
[Sysname] rir
[Sysname-rir] probe connect interval 30 timeout 20
```

Related commands

client enable

probe sync-port

server enable

probe interval

Use **probe interval** to set the NQA link quality probe interval.

Use **undo probe interval** to restore the default.

Syntax

probe interval *interval*

undo probe interval

Default

The NQA link quality probe interval is 100 milliseconds.

Views

NQA link quality operation view

Predefined user roles

network-admin

context-admin

Parameters

interval: Sets the NQA link quality probe interval, in the range of 0 to 604800000 milliseconds.

Usage guidelines

Use this command to specify the intervals at which the NQA client performs consecutive probes.

Examples

In NQA link quality operation 1, set the probe interval to 60 milliseconds.

```
<Sysname> system-view
[Sysname] rir
[Sysname-rir] nqa 1
[Sysname-rir-nqa-1] probe interval 60
```

Related commands

nqa

probe packet-dscp

Use **probe packet-dscp** to set the DSCP value of NQA link quality probe packets.

Use **undo probe packet-dscp** to restore the default.

Syntax

probe packet-dscp *dscp-value*

undo probe packet-dscp

Default

The DSCP value of NQA link quality probe packets is 63.

Views

NQA link quality operation view

Predefined user roles

network-admin

context-admin

Parameters

dscp-value: Sets the DSCP value of NQA link quality probe packets, in the range of 0 to 63. The larger the value, the higher the priority.

Usage guidelines

Assign different DSCP values to the probe packets of different NQA link quality operations to affect the priority of links in the flow templates associated with the operations.

Examples

In NQA link quality operation 1, set the DSCP value of probe packets to 10.

```
<Sysname> system-view
[Sysname] rir
[Sysname-rir] nqa 1
```

```
[Sysname-rir-nqa-1] probe packet-dscp 10
```

Related commands

nqa

probe packet-interval

Use **probe packet-interval** to set the intervals at which NQA link quality probe packets are sent.

Use **undo probe packet-interval** to restore the default.

Syntax

probe packet-interval *interval*

undo probe packet-interval

Default

NQA link quality probe packets are sent at intervals of 20 milliseconds.

Views

NQA link quality operation view

Predefined user roles

network-admin

context-admin

Parameters

interval: Sets the probe packet sending interval, in the range of 10 to 60000 milliseconds.

Usage guidelines

The device performs consecutive NQA link quality probes at intervals set by using the **probe interval** command and it sends multiple probe packets at each probe. The **probe packet-interval** command sets the probe packet sending interval within a probe.

Examples

In NQA link quality operation 1, set the probe packet sending interval to 10 milliseconds.

```
<Sysname> system-view
[Sysname] rir
[Sysname-rir] nqa 1
[Sysname-rir-nqa-1] probe packet-interval 10
```

Related commands

nqa

probe packet-number

Use **probe packet-number** to set the number of NQA link quality probe packets sent per probe.

Use **undo probe packet-number** to restore the default.

Syntax

probe packet-number *number*

undo probe packet-number

Default

An NQA client sends 100 NQA link quality probe packets per probe.

Views

NQA link quality operation view

Predefined user roles

network-admin

context-admin

Parameters

number: Sets the number of NQA link quality probe packets sent per probe, in the range of 10 to 1000.

Usage guidelines

The device performs consecutive NQA link quality probes at intervals set by using the **probe interval** command and it sends multiple probe packets at each probe. The **probe packet-number** command sets the number of probe packets sent at each probe.

Examples

In NQA link quality operation 1, set the number of link quality probe packets sent per probe to 100.

```
<Sysname> system-view
[Sysname] rir
[Sysname-rir] nqa 1
[Sysname-rir-nqa-1] probe packet-number 100
```

Related commands

nqa

probe packet-timeout

Use **probe packet-timeout** to set the timeout time for waiting for a response to an NQA link quality probe packet.

Use **undo probe packet-timeout** to restore the default.

Syntax

probe packet-timeout *packet-timeout*

undo probe packet-timeout

Default

The timeout time is 3000 milliseconds.

Views

NQA link quality operation view

Predefined user roles

network-admin

context-admin

Parameters

packet-timeout: Sets the timeout time for waiting for a response to an NQA link quality probe packet. The value range for this argument is 10 to 3600000 milliseconds.

Usage guidelines

A probe packet times out on an NQA client if the NQA client fails to receive any response to the probe packet when the probe packet timeout timer expires.

Examples

In NQA link quality operation 1, set the NQA link quality probe packet timeout time to 200 milliseconds.

```
<Sysname> system-view
[Sysname] rir
[Sysname-rir] nqa 1
[Sysname-rir-nqa-1] probe packet-timeout 200
```

Related commands

nqa

probe port

Use **probe port** to specify a destination port for NQA link quality probes.

Use **undo probe port** to restore the default.

Syntax

probe port *port-number*

undo probe port

Default

No destination port is specified for NQA link quality probes.

Views

NQA link quality operation view

Predefined user roles

network-admin

context-admin

Parameters

port-number: Specifies a destination port number in the range of 1024 to 65535.

Usage guidelines

Use this command for an NQA client. The destination port number must be the same as the listening port number on the NQA server.

Examples

In NQA link quality operation 1, set the NQA link quality probe destination port to 65500.

```
<Sysname> system-view
[Sysname] rir
[Sysname-rir] nqa 1
[Sysname-rir-nqa-1] probe port 65500
```

Related commands

nqa

probe sync-port

Use **probe sync-port** to specify a port for synchronizing probe information between the RIR client and the RIR server.

Use **undo probe sync-port** to restore the default.

Syntax

probe sync-port *port-number*

undo probe sync-port

Default

No port is specified for synchronizing probe information between the RIR client and the RIR server.

Views

RIR view

Predefined user roles

network-admin

context-admin

Parameters

port-number: Specifies a TCP port number in the range of 1024 to 65535.

Usage guidelines

Specify the same synchronization port on the RIR client and server for successful synchronization of link quality probe results.

Examples

Set the port to 65550 for synchronizing probe information between the RIR client and the RIR server.

```
<Sysname> system-view
[Sysname] rir
[Sysname-rir] probe sync-port 65550
```

Related commands

client enable

probe connect

server enable

quality-policy

Use **quality-policy** to configure a quality policy for a flow template.

Use **undo quality-policy** to restore the default.

Syntax

quality-policy sla *sla-id* **nqa** *nqa-id*

undo quality-policy

Default

No quality policy is configured for a flow template.

Views

Flow template view

Predefined user roles

network-admin

context-admin

Parameters

sla *sla-id*: Specifies an SLA by its ID, in the range of 0 to 128. The specified SLA must exist on the device.

nqa *nqa-id*: Specifies an NQA link quality operation by its ID, in the range of 0 to 128. The specified NQA link quality operation must exist.

Usage guidelines

Use this command to specify an SLA and an NQA link quality operation for a flow template. The device monitors the link quality based on the NQA link quality operation and compares the NQA probe results with the thresholds set in the SLA. The device selects only links that meet the quality requirements of the SLA for traffic that matches the flow template.

For flow priority-based traffic scheduling, the priority of a flow that matches a flow template is determined by the SLA ID specified in the quality policy of that flow template. The greater the SLA ID, the higher the flow priority. If no quality policy is configured for a flow template, flows that match the flow template have the lowest priority.

You can specify only one SLA and one NQA link quality operation for the quality policy of a flow template. However, you can specify the same SLA or NQA link quality operation for the quality policies of multiple flow templates.

If you execute this command multiple times for a flow template, the most recent configuration takes effect.

Examples

Configure the quality policy of flow template **1** to associate SLA 2 with NQA link quality operation 1.

```
<Sysname> system-view
[Sysname] rir
[Sysname-rir] flow 1
[Sysname-rir-flow-1] quality-policy sla 2 nqa 1
```

Related commands

flow priority-based-schedule enable

nqa

sla

reset tunnel flow-statistics

Use **reset tunnel flow-statistics** to clear flow ID-based traffic rate statistics for tunnels.

Syntax

reset tunnel flow-statistics [**flow** *flow-id* [**interface tunnel** *number*]]

Views

User view

Predefined user roles

network-admin

context-admin

context-operator

Parameters

flow *flow-id*: Specifies a flow template by its flow ID, in the range of 1 to 65535. If you do not specify a flow ID, this command clears statistics for all flow templates.

interface tunnel *number*: Specifies a tunnel interface by its tunnel interface number. If you do not specify a tunnel interface, this command clears statistics about the specified flow template for all tunnel interfaces.

Examples

Clear flow ID-based traffic rate statistics for tunnels.

```
<Sysname> reset tunnel flow-statistics
```

Related commands

display tunnel flow-statistics

tunnel flow-statistics enable

rir

Use **rir** to enable the RIR process and enter RIR view, or directly enter RIR view if the RIR process is already enabled.

Use **undo rir** to disable the RIR process.

Syntax

rir

undo rir

Default

The RIR process is not enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

In a hub-spoke network, you must enable the RIR process on all hubs and spokes.

Examples

Enable the RIR process and enter RIR view.

```
<Sysname> system-view
[Sysname] rir
[Sysname-rir]
```

rir backup

Use **rir backup** to configure a tunnel as an RIR backup tunnel.

Use **undo rir backup** to restore the default.

Syntax

rir backup

undo rir backup

Default

A tunnel is an RIR primary tunnel.

Views

VXLAN tunnel interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command enables the RIR process if the RIR process has not been enabled. The **undo** form of this command does not disable the RIR process.

RIR selects qualified primary links prior to qualified backup links.

A spoke is typically connected to both a primary hub and a backup hub. You can specify the tunnels connected to the backup hub as backup tunnels. If no suitable link is available to reach the primary hub, the spoke can forward traffic through the backup tunnels to the backup hub to ensure service continuity.

Examples

Configure VXLAN tunnel **Tunnel 1** as an RIR backup tunnel.

```
<Sysname> system-view
[Sysname] interface tunnel1 mode vxlan
[Sysname-Tunnel1] rir backup
```

rir collaboration-link-group

Use **rir collaboration-link-group** to assign a VXLAN tunnel to an RIR collaboration link group.

Use **undo rir collaboration-link-group** to restore the default.

Syntax

rir collaboration-link-group *group-id*

undo rir collaboration-link-group

Default

A VXLAN tunnel belongs to the RIR collaboration link group with a group ID of 0.

Views

VXLAN tunnel interface view

Predefined user roles

network-admin

context-admin

Parameters

group-id: Specifies an RIR collaboration link group by its group ID in the range of 1 to 65535.

Usage guidelines

In an RIR collaboration device group, make sure all links to the same device or RIR collaboration device group are assigned to the same RIR collaboration link group. A device in an RIR collaboration device group can select links for service packets from the following links:

- ECMP links configured in the matching flow template on the local device.
- Links configured in the same flow template on devices that belong to the same RIR collaboration device group as the local device. In addition, the links belong to the same RIR collaboration link group as the candidate links on the local device.

You can use this command when RIR is enabled or disabled. However, this command takes effect only when RIR is enabled.

To ensure correct link selection, use this command on each device that belongs to the same RIR collaboration device group. Make sure all links to the same device or RIR collaboration device group are assigned to the same RIR collaboration link group.

In an RIR collaboration device group, make sure the links to different devices or RIR collaboration device groups are assigned to different RIR collaboration link groups.

In different RIR collaboration device groups, the links to the same device or RIR collaboration device group can be assigned to the same RIR collaboration link group. As a best practice to identify links, assign the links to different RIR collaboration link groups.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Assign VXLAN tunnel 1 to RIR collaboration link group 1.

```
<Sysname> system-view
[Sysname] interface Tunnel 1
[Sysname-Tunnel1] rir collaboration-link-group 1
```

rir link-type index

Use **rir link-type** to assign a link type and link index to a VSI interface.

Use **undo rir link-type** to restore the default.

Syntax

rir link-type { **4g** | **internet** | **mpls** | **mstp** } **index** *link-index*

undo rir link-type { **4g** | **internet** | **mpls** | **mstp** } **index** *link-index*

Default

No link type or link index is assigned to a VSI interface.

Views

VSI interface view

Predefined user roles

network-admin

context-admin

Parameters

4g: Specifies the 4G type.

internet: Specifies the Internet type.

mpls: Specifies the MPLS type.

mstp: Specifies the MSTP type.

index *link-index*: Specifies a link index in the range of 1 to 65535.

Usage guidelines

This command enables the RIR process if the RIR process has not been enabled. The **undo** form of this command does not disable the RIR process.

The link type and link index together uniquely identify a link between a hub and a spoke. For a flow template to use a link, you must assign a link type and index to the link. Use this command to configure the link type as 4G, Internet, MPLS, or MSTP. The link type only marks the network type of the link and it does not affect packet encapsulation.

VXLAN-based RIR allows a hub and a spoke to have only one VXLAN tunnel for a VSI interface (a VXLAN). By assigning a link type and index to the VSI interface, RIR can identify the VXLAN tunnel between the hub and spoke.

A VSI interface on a hub (or spoke) can have a VXLAN tunnel to each spoke (or hub). The VXLAN tunnels of the same VSI interface are assigned the same link type and link index.

A VSI interface can be associated only with one link type.

You must assign different link indexes to the same type of links on different VSI interfaces.

Examples

Set the link type to MPLS and link index to 1 on VSI-interface 1.

```
<Sysname>system-view
[Sysname] interface vsi-interface 1
[Sysname-Vsi-interface1] rir link-type mpls index 1
```

rir role

Use **rir role** to enable the RIR client or the RIR server on a VXLAN tunnel interface.

Use **undo rir role** to restore the default.

Syntax

rir role { **client** | **server** }

undo rir role

Default

The default for this command depends on the configuration of the **client enable** and **server enable** commands.

Views

VXLAN tunnel interface view

Predefined user roles

network-admin

context-admin

Parameters

client: Specifies the RIR client.

server: Specifies the RIR server.

Usage guidelines

To avoid NQA probes from occupying too many resources on a hub in a hub-spoke network, configure the hub as an RIR server and configure the spokes as RIR clients.

You can enable the RIR client or server globally or on an interface.

- Enabling the RIR client or server globally also enables the RIR client or server for all interfaces on the device. The interfaces can send or receive link quality probe results.
- Enabling the RIR client or server on an interface allows only that interface to send or receive link quality probe results.

Enable the RIR server or RIR client, or use them in combination, depending on the role of the device in the network.

- If the device acts only as a hub, you can enable the RIR server globally.
- If the device acts only as a spoke, you can enable the RIR client globally.
- If the device acts as both a hub and a spoke, you can enable the RIR server and RIR client on the corresponding interfaces.

When you enable the RIR client or server, follow these restrictions and guidelines:

- In a VXLAN network, only tunnel interfaces support enabling the RIR client or server. The RIR server uses the tunnel interfaces to receive link quality probe results synchronized from RIR clients.
- The RIR client and RIR server cannot be both enabled on the same interface.
- If the enabled role (RIR server or client) on an interface is different from the globally enabled role, the interface-specific role takes effect on that interface.

To modify the role of an interface, you must first use the **undo rir role** command to remove the original role.

Examples

Enable the RIR server on tunnel interface **Tunnel 1**.

```
<Sysname> system-view
[Sysname] interface Tunnel 1 mode vxlan
[Sysname-tunnel1] rir role client
```

Related commands

client enable

server enable

server enable

Use **server enable** to enable the RIR server globally.

Use **undo server enable** to disable the RIR server globally.

Syntax

server enable

undo server enable

Default

The RIR server is disabled globally.

Views

RIR view

Predefined user roles

network-admin

context-admin

Usage guidelines

To avoid NQA probes from occupying too many resources on a hub in a hub-spoke network, configure the hub as an RIR server and configure the spokes as RIR clients.

You can enable the RIR server globally or on an interface.

- Enabling the RIR server globally also enables the RIR server for all interfaces on the device. The interfaces can receive link quality probe results synchronized from RIR clients.
- Enabling the RIR server on an interface allows only that interface to receive link quality probe results synchronized from RIR clients.

When you enable the RIR server, follow these restrictions and guidelines:

- In a VXLAN network, only tunnel interfaces support enabling the RIR server. The RIR server uses the tunnel interfaces to receive link quality probe results synchronized from RIR clients.
- The RIR server and RIR client cannot be both enabled on the same interface.
- If the enabled role (RIR server or client) on an interface is different from the globally enabled role, the interface-specific role takes effect on that interface.

Examples

Enable the RIR server globally.

```
<Sysname> system-view
[Sysname] rir
[Sysname-rir] server enable
```

Related commands

client enable

probe connect

probe sync-port

sla

Use **sla** to create an SLA and enter its view, or enter the view of an existing SLA.

Use **undo sla** to delete an SLA.

Syntax

sla *sla-id*

undo sla *sla-id*

Default

No SLAs exist.

Views

RIR view

Predefined user roles

network-admin

context-admin

Parameters

sla-id: Specifies an SLA ID in the range of 0 to 128.

Usage guidelines

To meet the differentiated requirements of services on link quality, configure a Service Level Agreement (SLA) for each service. An SLA contains a set of parameters to evaluate link quality, including the link delay, jitter, and packet loss thresholds.

The quality policy of a flow template contains an SLA and an NQA link quality operation. By comparing the NQA link quality probe results with the thresholds in the SLA, the device determines whether a link meets the quality requirements of the service. If all parameter values in the probe results of a link are lower than or equal to the thresholds in the SLA, the link is qualified for the service.

For flow priority-based traffic scheduling, the priority of a flow that matches a flow template is determined by the SLA ID specified in the quality policy of that flow template. The greater the SLA ID, the higher the flow priority. If no quality policy is configured for a flow template, flows that match the flow template have the lowest priority.

The device supports a maximum of 129 SLAs.

Examples

Create SLA 1 and enter its view.

```
<Sysname> system-view
[Sysname] rir
[Sysname-rir] sla 1
[Sysname-rir-sla-1]
```

Related commands

flow priority-based-schedule enable

quality-policy

tunnel flow-statistics enable

Use **tunnel flow-statistics enable** to enable flow ID-based traffic rate statistics for tunnels.

Use **undo tunnel flow-statistics enable** to disable flow ID-based traffic rate statistics for tunnels.

Syntax

tunnel flow-statistics enable

undo tunnel flow-statistics enable

Default

Flow ID-based traffic rate statistics for tunnels is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Examples

Enable flow ID-based traffic rate statistics for tunnels.

```
<Sysname> system-view
[Sysname] tunnel flow-statistics enable
```

Related commands

display tunnel flow-statistics

tunnel flow-statistics interval

tunnel flow-statistics interval

Use **tunnel flow-statistics interval** to set the intervals at which the device collects flow ID-based traffic rate statistics for tunnels.

Use **undo tunnel flow-statistics interval** to restore the default.

Syntax

tunnel flow-statistics interval *interval*

undo tunnel flow-statistics interval

Default

The device collects flow ID-based traffic rate statistics for tunnels at intervals of 300 seconds.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies an interval in the range of 5 to 300 seconds.

Examples

Enable the device to collect flow ID-based traffic rate statistics for tunnels at intervals of 100 seconds.

```
<Sysname> system-view
[Sysname] tunnel flow-statistics interval 100
```

Related commands

tunnel flow-statistics enable

NSFOCUS Firewall Series

NF ACL and QoS

Command Reference

NSFOCUS Technologies, Inc.

Document version: 6W600-20230221

Preface

This command reference describes the commands for configuring ACL and QoS features, including ACL, QoS, and time range.

This preface includes the following topics about the documentation:

- Audience.
- Conventions.

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators.

Conventions

The following information describes the conventions used in the documentation.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select a minimum of one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
CAUTION:	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Contents

ACL commands

accelerate

Use **accelerate** to enable ACL acceleration.

Use **undo accelerate** to restore the default.

Syntax

accelerate

undo accelerate

Default

ACL acceleration is disabled.

Views

IPv4 basic/advanced ACL view

IPv6 basic/advanced ACL view

Layer 2 ACL view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command does not take effect if the ACL resources are insufficient.

ACL acceleration can be successfully enabled only if all rules in an ACL support acceleration.

You can modify, add, or delete rules for an accelerated ACL. ACL acceleration might fail when the ACL resources are insufficient or the modified or added rule does not support acceleration.

ACL acceleration is delayed for a period after an ACL rule is added, deleted, or modified. If additional rule changes occur during the delay period, the delay period starts to count again. If an ACL contains 100 or less rules, the delay period is 2 seconds. If an ACL contains more than 100 rules, the delay period is 20 seconds.

Examples

Enable ACL acceleration for ACL 2000.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] accelerate
```

Related commands

display acl accelerate

acl

Use **acl** to create an ACL and enter its view, or enter the view of an existing ACL.

Use **undo acl** to delete the specified or all ACLs.

Syntax

acl [**ipv6**] { **name** *acl-name* | **number** *acl-number* [**name** *acl-name*] [**match-order** { **auto** | **config** }] }

undo acl [**ipv6**] { **all** | **name** *acl-name* | **number** *acl-number* }

acl [**ipv6**] { **advanced** | **basic** } { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }]

acl mac { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }]

undo acl [**ipv6**] { **all** | { **advanced** | **basic** } { *acl-number* | **name** *acl-name* } }

undo acl mac { **all** | *acl-number* | **name** *acl-name* }

Default

No ACLs exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ipv6: Specifies the IPv6 ACL type.

basic: Specifies the basic ACL type.

advanced: Specifies the advanced ACL type.

mac: Specifies the Layer 2 ACL type.

acl-number: Assigns a number to the ACL. The following are available value ranges:

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

name *acl-name*: Assigns a name to the ACL. The *acl-name* argument is a case-insensitive string of 1 to 63 characters. It must start with an English letter and to avoid confusion, it cannot be **all**.

match-order: Specifies the order in which ACL rules are compared against packets.

auto: Compares ACL rules in depth-first order.

config: Compares ACL rules in ascending order of rule ID. The rule with a smaller ID has a higher priority. If you do not specify a match order, the **config** order applies by default.

all: Specifies all ACLs of the specified type.

Usage guidelines

If you create a numbered ACL, you can enter the view of the ACL by using the following commands:

- **acl** [**ipv6**] **number** *acl-number*
- **acl** { [**ipv6**] { **advanced** | **basic** } | **mac** } *acl-number*

If you create a ACL by specifying both a number and a name, you can enter the view of the ACL by using the following commands:

- **acl** [**ipv6**] **number** *acl-number* (only for basic and advanced ACLs)

- **acl** [**ipv6**] **number** *acl-number* [**name** *acl-name*]
- **acl** { [**ipv6**] { **advanced** | **basic** } | **mac** } **name** *acl-name*

If you create a named ACL by using the **acl** { [**ipv6**] { **advanced** | **basic** } | **mac** } **name** *acl-name* command, you can enter the view of the ACL by using the following commands:

- **acl** [**ipv6**] **name** *acl-name*
- **acl** { [**ipv6**] { **advanced** | **basic** } | **mac** } **name** *acl-name*

You can change the match order only for ACLs that do not contain any rules.

Matching packets are forwarded through slow forwarding if an ACL rule contains match criteria or has functions enabled in addition to the following match criteria and functions:

- Source and destination IP addresses.
- Source and destination ports.
- Transport layer protocol.
- ICMP or ICMPv6 message type, message code, and message name.
- VPN instance.
- Logging.
- Time range.

Slow forwarding requires packets to be sent to the control plane for forwarding entry calculation, which affects the device forwarding performance.

Examples

Create IPv4 basic ACL 2000 and enter its view.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000]
```

Create IPv4 basic ACL **flow** and enter its view.

```
<Sysname> system-view
[Sysname] acl basic name flow
[Sysname-acl-ipv4-basic-flow]
```

Create IPv4 advanced ACL 3000 and enter its view.

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000]
```

Create IPv6 basic ACL 2000 and enter its view.

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2000
[Sysname-acl-ipv6-basic-2000]
```

Create IPv6 basic ACL **flow** and enter its view.

```
<Sysname> system-view
[Sysname] acl ipv6 basic name flow
[Sysname-acl-ipv6-basic-flow]
```

Create IPv6 advanced ACL **abc** and enter its view.

```
<Sysname> system-view
[Sysname] acl ipv6 advanced name abc
[Sysname-acl-ipv6-adv-abc]
```

Create Layer 2 ACL 4000 and enter its view.

```
<Sysname> system-view
[Sysname] acl mac 4000
[Sysname-acl-mac-4000]
```

Create Layer 2 ACL **flow** and enter its view.

```
<Sysname> system-view
[Sysname] acl mac name flow
[Sysname-acl-mac-flow]
```

Related commands

display acl

acl copy

Use **acl copy** to create an ACL by copying an ACL that already exists.

Syntax

acl [**ipv6** | **mac**] **copy** { *source-acl-number* | **name** *source-acl-name* } **to** { *dest-acl-number* | **name** *dest-acl-name* }

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

source-acl-number: Specifies an existing source ACL by its number. The following are available value ranges:

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

name *source-acl-name*: Specifies an existing source ACL by its name. The *source-acl-name* argument is a case-insensitive string of 1 to 63 characters.

dest-acl-number: Assigns a unique number to the new ACL. The following are available value ranges:

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

name *dest-acl-name*: Assigns a unique name to the new ACL. The *dest-acl-name* argument is a case-insensitive string of 1 to 63 characters. It must start with an English letter and to avoid confusion, it cannot be **all**.

Usage guidelines

The new ACL and the source ACL must be the same type.

The new ACL has the same properties and content as the source ACL, but uses a different number or name from the source ACL.

Examples

Create IPv4 basic ACL 2002 by copying IPv4 basic ACL 2001.

```
<Sysname> system-view
[Sysname] acl copy 2001 to 2002
```

Create IPv4 basic ACL **paste** by copying IPv4 basic ACL **test**.

```
<Sysname> system-view
[Sysname] acl copy name test to name paste
```

acl logging interval

Use **acl logging interval** to enable logging for packet filtering and set the interval.

Use **undo acl logging interval** to restore the default.

Syntax

acl logging interval *interval*

undo acl logging interval

Default

The interval is 0. The device does not generate log entries for packet filtering.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies the interval at which log entries are generated and output. It must be a multiple of 5, in the range of 0 to 1440 minutes. To disable the logging, set the value to 0.

Usage guidelines

The logging feature is available for IPv4 or IPv6 ACL rules that have the **logging** keyword.

You can configure the ACL module to generate log entries for packet filtering and output them to the information center at the output interval. The log entry records the number of matching packets and the matched ACL rules. When the first packet of a flow matches an ACL rule, the output interval starts, and the device immediately outputs a log entry for this packet. When the output interval ends, the device outputs a log entry for subsequent matching packets of the flow.

For more information about the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Configure the device to generate and output packet filtering log entries every 10 minutes.

```
<Sysname> system-view
[Sysname] acl logging interval 10
```

Related commands

rule (IPv4 advanced ACL view)

rule (IPv4 basic ACL view)

rule (IPv6 advanced ACL view)

rule (IPv6 basic ACL view)

acl trap interval

Use **acl trap interval** to enable SNMP notifications for packet filtering and set the interval.

Use **undo acl interval** to restore the default.

Syntax

acl trap interval *interval*

undo acl trap interval

Default

The interval is 0. The device does not generate SNMP notifications for packet filtering.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies the interval at which SNMP notifications are generated and output. It must be a multiple of 5, in the range of 0 to 1440 minutes. To disable SNMP notifications, set the value to 0.

Usage guidelines

The SNMP notifications feature is available for IPv4 or IPv6 ACL rules that have the **logging** keyword.

You can configure the ACL module to generate SNMP notifications for packet filtering and output them to the SNMP module at the output interval. The notification records the number of matching packets and the matched ACL rules. When the first packet of a flow matches an ACL rule, the output interval starts, and the device immediately outputs a notification for this packet. When the output interval ends, the device outputs a notification for subsequent matching packets of the flow. For more information about SNMP, see *Network Management and Monitoring Configuration Guide*.

Examples

Configure the device to generate and output packet filtering SNMP notifications every 10 minutes.

```
<Sysname> system-view
[Sysname] acl trap interval 10
```

Related commands

rule (IPv4 advanced ACL view)

rule (IPv4 basic ACL view)

rule (IPv6 advanced ACL view)

rule (IPv6 basic ACL view)

description

Use **description** to configure a description for an ACL.

Use **undo description** to delete an ACL description.

Syntax

description *text*

undo description

Default

An ACL does not have a description.

Views

IPv4 basic/advanced ACL view

IPv6 basic/advanced ACL view

Layer 2 ACL view

Predefined user roles

network-admin

context-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 127 characters.

Examples

Configure a description for IPv4 basic ACL 2000.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] description This is an IPv4 basic ACL.
```

Related commands

display acl

display acl

Use **display acl** to display ACL configuration and match statistics.

Syntax

display acl [**ipv6** | **mac**] { *acl-number* | **all** | **name** *acl-name* }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

acl-number: Specifies an ACL by its number. The following are available value ranges:

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.

- 4000 to 4999 for Layer 2 ACLs.

all: Specifies all ACLs of the specified type.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters.

Usage guidelines

This command displays ACL rules in **config** or **auto** order, whichever is configured.

Examples

Display configuration and match statistics for all IPv4 ACLs.

```
<Sysname> display acl all
Basic IPv4 ACL 2001, 2 rules, match-order is auto,
This is an IPv4 basic ACL.
ACL's step is 5
ACL accelerated
Rule insert-only enabled
 rule 5 permit source 1.1.1.1 0 (5 times matched)
 rule 5 comment This rule is used on GigabitEthernet1/0/1.
 rule 10 permit source object-group permit (5 times matched)
Advanced IPv4 ACL 3001, 1 rule,
ACL's step is 5
 rule 0 permit ip source 1.1.1.0 0.0.0.255 destination 3.3.3.0 0.0.0.255 (Dynamic)
```

Table 1 Command output

Field	Description
Basic IPv4 ACL 2001	Type and number of the ACL.
2 rules	The ACL contains two rules.
match-order is auto	The match order for the ACL is **auto**, which sorts ACL rules in depth-first order. This field is not displayed when the match order is **config**.
This is an IPv4 basic ACL.	Description of the ACL.
ACL's step is 5	The rule numbering step is 5.
ACL accelerated	ACL acceleration is enabled for the ACL.
Rule insert-only enabled	Rule ID preemption is enabled for the ACL.
rule 5 permit source 1.1.1.1 0	Content of rule 5. The rule permits packets sourced from the IP address 1.1.1.1.
rule 10 permit source object-group permit	Content of rule 10. The rule permits packets sourced from the object group **permit**.
5 times matched	The rule has been matched five times. Only matches performed in software are counted. This field is not displayed when no packets matched the rule.
rule 5 comment This rule is used on GigabitEthernet1/0/1.	Comment of rule 5.
Dynamic	A dynamic rule is added dynamically by an application module.

display acl accelerate

Use **display acl accelerate** to display ACL acceleration status.

Syntax

display acl accelerate { **summary** [**ipv6** | **mac**] | **verbose** [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* } **slot** *slot-number* }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

summary: Displays summary information about ACL acceleration status.

verbose: Displays detailed information about ACL acceleration status.

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

acl-number: Specifies an ACL by its number. The following are available value ranges:

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters.

slot *slot-number*: Specifies an IRF member device. The *slot-number* argument represents the ID of the IRF member device. The specified device must be the device where the acceleration chip resides.

Usage guidelines

If you specify the **verbose** keyword, this command displays the ACLs for which acceleration is successfully enabled and their rules. The ACLs for which acceleration is disabled or fails to be enabled are not displayed.

Examples

Display summary information about ACL acceleration status.

```
<Sysname> display acl accelerate summary
Basic IPv4 ACL 2000
```

display packet-filter

Use **display packet-filter** to display ACL application information for packet filtering.

Syntax

display packet-filter { **interface** [*interface-type interface-number*] [**inbound**] | **zone-pair security** [**source** *source-zone-name* **destination** *destination-zone-name*] } [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface [*interface-type interface-number*]: Specifies an interface by its type and number. If you do not specify an interface, this command displays ACL application information for packet filtering on all interfaces except VA interfaces. For information about VA interfaces, see PPP in *Layer 2—WAN Access Configuration Guide*. If you specify an Ethernet interface, you do not need to specify the **slot** *slot-number* option.

zone-pair security [**source** *source-zone-name* **destination** *destination-zone-name*]: Specifies a zone pair. The *source-zone-name* argument specifies a source security zone by its name. The *destination-zone-name* argument specifies a destination security zone by its name. The security zone name is a case-insensitive string of 1 to 31 characters.

inbound: Specifies the inbound direction.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays ACL application information for packet filtering for the master device.

Usage guidelines

Examples

Display ACL application information for inbound packet filtering on interface GigabitEthernet 1/0/1.

```
<Sysname> display packet-filter interface gigabitethernet 1/0/1 inbound
Interface: GigabitEthernet1/0/1
Inbound policy:
  IPv4 ACL 2001
  IPv6 ACL 2002 (Failed)
  MAC ACL 4003 (Failed)
  IPv4 default action: Deny
  IPv6 default action: Deny
  MAC default action: Deny
```

Display ACL application information for packet filtering from source security zone **office** to destination security zone **library**.

```
<Sysname> display packet-filter zone-pair security source office destination library
Zone-pair: source office destination library
  IPv4 ACL 2001
  IPv4 ACL 2002
```

Table 2 Command output

Field	Description
Interface	Interface to which the ACL applies.
Zone-pair	Zone pair to which the ACL applies.
Inbound policy	ACL used for filtering incoming traffic.
IPv4 ACL 2001	IPv4 basic ACL 2001 has been successfully applied.
IPv6 ACL 2002 (Failed)	The device has failed to apply IPv6 basic ACL 2002.
IPv4 default action	Packet filter default action for packets that do not match any IPv4 ACLs: • **Deny**—The default action **deny** has been successfully applied for packet filtering. • **Deny (Failed)**—The device has failed to apply the default action **deny** for packet filtering. The action **permit** still functions. • **Permit**—The default action **permit** has been successfully applied for packet filtering.
IPv6 default action	Packet filter default action for packets that do not match any IPv6 ACLs: • **Deny**—The default action **deny** has been successfully applied for packet filtering. • **Deny (Failed)**—The device has failed to apply the default action **deny** for packet filtering. The action **permit** still functions. • **Permit**—The default action **permit** has been successfully applied for packet filtering.
MAC default action	Packet filter default action for packets that do not match any Layer 2 ACLs: • **Deny**—The default action **deny** has been successfully applied for packet filtering. • **Deny (Failed)**—The device has failed to apply the default action **deny** for packet filtering. The action **permit** still functions. • **Permit**—The default action **permit** has been successfully applied for packet filtering.

display packet-filter statistics

Use **display packet-filter statistics** to display packet filtering statistics.

Syntax

display packet-filter statistics { **interface** *interface-type interface-number* **inbound** [**default** | [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* }] | **zone-pair security source** *source-zone-name* **destination** *destination-zone-name* [[**ipv6**] { *acl-number* | **name** *acl-name* }] } [**brief**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number.

zone-pair security source *source-zone-name* **destination** *destination-zone-name*: Specifies a zone pair. The *source-zone-name* argument specifies a source security zone by its name. The *destination-zone-name* argument specifies a destination security zone by its name. The security zone name is a case-insensitive string of 1 to 31 characters.

inbound: Specifies the inbound direction.

default: Displays the default action statistics for packet filtering.

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

acl-number: Specifies an ACL by its number. The following are available value ranges:

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters.

brief: Displays brief statistics.

Usage guidelines

If you do not specify any parameters, this command displays packet filtering statistics for all ACLs.

Examples

Display packet filtering statistics for all ACLs on incoming packets of GigabitEthernet 1/0/1.

```
<Sysname> display packet-filter statistics interface gigabitethernet 1/0/1 inbound
Interface: GigabitEthernet1/0/1
 Inbound policy:
  IPv4 ACL 2001
   From 2011-06-04 10:25:21 to 2011-06-04 10:35:57
   rule 0 permit source 2.2.2.2 0 counting (2 packets, 256 bytes)
   rule 5 permit source 1.1.1.1 0 counting (Failed)
   rule 10 permit vpn-instance test counting (No resource)
   Totally 2 packets 256 bytes permitted, 0 packets 0 bytes denied
   Totally 100% permitted, 0% denied

  IPv6 ACL 2000

  MAC ACL 4000
   rule 0 permit

  IPv4 default action: Deny
   From 2011-06-04 10:25:21 to 2011-06-04 10:35:57
   Totally 7 packets
```

```
  IPv6 default action: Deny
    From 2011-06-04 10:25:41 to 2011-06-04 10:35:57
    Totally 0 packets
  MAC default action: Deny
    From 2011-06-04 10:25:34 to 2011-06-04 10:35:57
    Totally 0 packets
```

Display packet filtering statistics for IPv4 advanced ACL 3001 on packets from source security zone **office** to destination security zone **library**.

```
<Sysname> display packet-filter statistics zone-pair security source office destination
library 3001
Zone-pair: source office destination library
IPv4 ACL 3001
   rule 0 permit source 2.2.2.2 0
   rule 5 permit source 1.1.1.1 0 counting (2 packets)
   rule 10 permit vpn-instance test (Failed)
   Totally 2 packets 256 bytes permitted, 0 packets 0 bytes denied
   Totally 100% permitted, 0% denied
```

Table 3 Command output

Field	Description
Interface	Interface to which the ACL applies.
Zone-pair	Zone pair to which the ACL applies.
Inbound policy	ACL used for filtering incoming traffic.
IPv4 ACL 2001	IPv4 basic ACL 2001 has been successfully applied.
IPv4 ACL 2002 (Failed)	The device has failed to apply IPv4 basic ACL 2002.
From 2011-06-04 10:25:21 to 2011-06-04 10:35:57	Start time and end time of the statistics. This field is not supported in the current software version.
2 packets	Two packets matched the rule. This field is not displayed when no packets matched the rule.
No resource	Resources are not enough for counting matches for the rule. In packet filtering statistics, this field is displayed for a rule when resources are not sufficient for rule match counting.
rule 5 permit source 1.1.1.1 0 (Failed)	The device has failed to apply rule 5.
Totally 2 packets permitted, 0 packets denied	Number of packets permitted and denied by the ACL.
Totally 100% permitted, 0% denied	Ratios of permitted and denied packets to all packets.
IPv4 default action	Packet filter default action for packets that do not match any IPv4 ACLs: • **Deny**—The default action **deny** has been successfully applied for packet filtering. • **Deny (Failed)**—The device has failed to apply the default action **deny** for packet filtering. The action **permit** still functions. • **Permit**—The default action **permit** has been successfully applied for packet filtering.

IPv6 default action	Packet filter default action for packets that do not match any IPv6 ACLs: • **Deny**—The default action **deny** has been successfully applied for packet filtering. • **Deny (Failed)**—The device has failed to apply the default action **deny** for packet filtering. The action **permit** still functions. • **Permit**—The default action **permit** has been successfully applied for packet filtering.
MAC default action	Packet filter default action for packets that do not match any Layer 2 ACLs: • **Deny**—The default action **deny** has been successfully applied for packet filtering. • **Deny (Failed)**—The device has failed to apply the default action **deny** for packet filtering. The action **permit** still functions. • **Permit**—The default action **permit** has been successfully applied for packet filtering.
Totally 7 packets	The default action has been executed on seven packets. This field is not supported in the current software version.

Related commands

reset packet-filter statistics

display packet-filter statistics sum

Use **display packet-filter statistics sum** to display accumulated packet filtering statistics for an ACL.

Syntax

display packet-filter statistics sum inbound [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* } [**brief**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

inbound: Specifies the inbound direction.

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

acl-number: Specifies an ACL by its number. The following are available value ranges:

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters.

brief: Displays brief statistics.

Examples

Display accumulated packet filtering statistics for IPv4 basic ACL 2001 on incoming packets.

```
<Sysname> display packet-filter statistics sum inbound 2001
Sum:
 Inbound policy:
  IPv4 ACL 2001
   rule 0 permit source 2.2.2.2 0 counting (2 packets, 256 bytes)
   rule 5 permit source 1.1.1.1 0
   rule 10 permit vpn-instance test
   Totally 2 packets 256 bytes permitted, 0 packets 0 bytes denied
   Totally 100% permitted, 0% denied
```

Display brief accumulated packet filtering statistics for IPv4 basic ACL 2000 on incoming packets.

```
<Sysname> display packet-filter statistics sum inbound 2000 brief
Sum:
 Inbound policy:
  IPv4 ACL 2000
   Totally 2 packets 256 bytes permitted, 0 packets 0 bytes denied
   Totally 100% permitted, 0% denied
```

Table 4 Command output

Field	Description
Sum	Accumulated packet filtering statistics.
Inbound policy	Accumulated packet filtering statistics in the inbound direction.
IPv4 ACL 2001	Accumulated packet filtering statistics of IPv4 basic ACL 2001.
2 packets, 256 bytes	Number of packets matched the rule and the size of the matching packets. In this example, 2 packets (256 bytes) matched the rule. This field is not displayed when no packets matched the rule.
Totally 2 packets 256 bytes permitted, 0 packets 0 bytes denied	Number of packets and number of bytes permitted and denied by the ACL.
Totally 100% permitted, 0% denied	Ratios of permitted and denied packets to all packets.

Related commands

reset packet-filter statistics

display packet-filter verbose

Use **display packet-filter verbose** to display ACL application details for packet filtering.

Syntax

display packet-filter verbose { **interface** *interface-type interface-number* **inbound** [[**ipv6** | **mac**] { *acl-number* | **name** *acl-name* }] | **zone-pair security source** *source-zone-name* **destination** *destination-zone-name* [[**ipv6**] { *acl-number* | **name** *acl-name* }] } [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. The **slot** *slot-number* option is not available for an Ethernet interface.

zone-pair security source *source-zone-name* **destination** *destination-zone-name*: Specifies a zone pair. The *source-zone-name* argument specifies a source security zone by its name. The *destination-zone-name* argument specifies a destination security zone by its name. The security zone name is a case-insensitive string of 1 to 31 characters.

inbound: Specifies the inbound direction.

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

acl-number: Specifies an ACL by its number. The following are available value ranges:

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays ACL application details for packet filtering for the master device.

Usage guidelines

If *acl-number*, **name** *acl-name*, **ipv6**, or **mac** is not specified, this command displays application details of all ACLs for packet filtering.

Examples

Display application details of all ACLs for inbound packet filtering on GigabitEthernet 1/0/1.

```
<Sysname> display packet-filter verbose interface gigabitethernet 1/0/1 inbound
Interface: GigabitEthernet1/0/1
 Inbound policy:
  IPv4 ACL 2001
   rule 0 permit
   rule 5 permit source 1.1.1.1 0 (Failed)
   rule 10 permit vpn-instance test (Failed)

  IPv6 ACL 2000
   rule 0 permit

  MAC ACL 4000

  IPv4 default action: Deny
```

```
  IPv6 default action: Deny

  MAC default action: Deny
```

Display application details of all ACLs for packet filtering from source security zone **office** to destination security zone **library**.

```
<Sysname> display packet-filter verbose zone-pair security source office destination
library
Zone-pair: source office destination library
  IPv4 ACL 2001
   rule 0 permit
   rule 5 permit source 1.1.1.1 0
   rule 10 permit vpn-instance test
```

Table 5 Command output

Field	Description
Interface	Interface to which the ACL applies.
Zone-pair	Zone pair to which the ACL applies.
Inbound policy	ACL used for filtering incoming traffic.
IPv4 ACL 2001	IPv4 basic ACL 2001 has been successfully applied.
IPv4 ACL 2002 (Failed)	The device has failed to apply IPv4 basic ACL 2002.
Hardware-count	ACL rule match counting in hardware has been successfully enabled.
Hardware-count (Failed)	The device has failed to enable counting ACL rule matches in hardware.
rule 5 permit source 1.1.1.1 0 (Failed)	The device has failed to apply rule 5.
IPv4 default action	Packet filter default action for packets that do not match any IPv4 ACLs: • **Deny**—The default action **deny** has been successfully applied for packet filtering. • **Deny (Failed)**—The device has failed to apply the default action **deny** for packet filtering. The action **permit** still functions. • **Permit**—The default action **permit** has been successfully applied for packet filtering.
IPv6 default action	Packet filter default action for packets that do not match any IPv6 ACLs: • **Deny**—The default action **deny** has been successfully applied for packet filtering. • **Deny (Failed)**—The device has failed to apply the default action **deny** for packet filtering. The action **permit** still functions. • **Permit**—The default action **permit** has been successfully applied for packet filtering.
MAC default action	Packet filter default action for packets that do not match any Layer 2 ACLs: • **Deny**—The default action **deny** has been successfully applied for packet filtering. • **Deny (Failed)**—The device has failed to apply the default action **deny** for packet filtering. The action **permit**

	still functions. • **Permit**—The default action **permit** has been successfully applied for packet filtering.

packet-filter (interface view)

Use **packet-filter** to apply an ACL to an interface to filter packets.

Use **undo packet-filter** to remove an ACL from an interface.

Syntax

packet-filter [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* } **inbound**

undo packet-filter [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* } **inbound**

Default

No ACL is applied to an interface to filter packets.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

acl-number: Specifies an ACL by its number. The following are available value ranges:

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters.

inbound: Filters incoming packets.

Usage guidelines

When you reference an ACL, follow these restrictions and guidelines:

- If the ACL does not exist or contains no rules, the ACL is not used to filter packets.
- If the **vpn-instance** *vpn-instance* option is specified in a rule, the rule takes effect only on VPN packets. If the **vpn-instance** *vpn-instance* option is not specified in a rule, the rule takes effect on both VPN packets and non-VPN packets.

This command does not take effect on member ports of an aggregation group.

Examples

Apply IPv4 basic ACL 2001 to filter incoming traffic on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] packet-filter 2001 inbound
```

Related commands

display packet-filter

display packet-filter statistics

display packet-filter verbose

packet-filter (zone pair view)

Use **packet-filter** to apply an ACL to a zone pair to filter packets.

Use **undo packet-filter** to remove an ACL from a zone pair.

Syntax

packet-filter [**ipv6**] { *acl-number* | **name** *acl-name* }

undo packet-filter [**ipv6**] { *acl-number* | **name** *acl-name* }

Default

No ACL is applied to a zone pair to filter packets.

Views

Zone pair view

Predefined user roles

network-admin

context-admin

Parameters

ipv6: Specifies the IPv6 ACL type. To specify the IPv4 ACL type, do not provide this keyword.

acl-number: Specifies an ACL by its number:

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters.

Usage guidelines

When you reference an ACL, follow these restrictions and guidelines:

- If the ACL does not exist or contains no rules, the ACL is not used to filter packets.
- If the **vpn-instance** *vpn-instance* option is specified in a rule, the rule takes effect only on VPN packets. If the **vpn-instance** *vpn-instance* option is not specified in a rule, the rule takes effect on both VPN packets and non-VPN packets.

Examples

Apply IPv4 basic ACL 2002 to filter traffic from source security zone **office** to destination security zone **library**.

```
<Sysname> system-view
[Sysname] zone-pair security source office destination library
[Sysname-zone-pair-security-office-library] packet-filter 2002
```

Related commands

display packet-filter

display packet-filter statistics

display packet-filter verbose

packet-filter default deny

Use **packet-filter default deny** to set the packet filtering default action to **deny**. The packet filter denies packets that do not match any ACL rule.

Use **undo packet-filter default deny** to restore the default.

Syntax

packet-filter default deny

undo packet-filter default deny

Default

The packet filtering default action is **permit**. The packet filter permits packets that do not match any ACL rule.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

The packet filter applies the default action to all ACL applications for packet filtering. The default action appears in the **display** command output for packet filtering.

Examples

Set the packet filter default action to **deny**.

```
<Sysname> system-view
[Sysname] packet-filter default deny
```

Related commands

display packet-filter

display packet-filter statistics

display packet-filter verbose

reset acl counter

Use **reset acl counter** to clear statistics for ACLs.

Syntax

reset acl [**ipv6** | **mac**] **counter** { *acl-number* | **all** | **name** *acl-name* }

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

acl-number: Specifies an ACL by its number. The following are available value ranges:

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

all: Clears statistics for all ACLs of the specified type.

name *acl-name*: Clears statistics of an ACL specified by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters.

Examples

Clear statistics for IPv4 basic ACL 2001.

```
<Sysname> reset acl counter 2001
```

Related commands

display acl

reset packet-filter statistics

Use **reset packet-filter statistics** to clear the packet filtering statistics.

Syntax

reset packet-filter statistics { **interface** [*interface-type interface-number*] **inbound** [**default** | [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* }] | **zone-pair security** [**source** *source-zone-name* **destination** *destination-zone-name*] [**ipv6**] { *acl-number* | **name** *acl-name* }] }

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

interface [*interface-type interface-number*]: Specifies an interface by its type and number. If you do not specify an interface, this command clears packet filtering statistics for all interfaces.

zone-pair security [**source** *source-zone-name* **destination** *destination-zone-name*]: Specifies a zone pair. The *source-zone-name* argument specifies a source security zone by its name. The *destination-zone-name* argument specifies a destination security zone by its name. The security zone name is a case-insensitive string of 1 to 31 characters.

inbound: Specifies the inbound direction.

default: Clears the default action statistics for packet filtering.

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

acl-number: Specifies an ACL by its number. The following are available value ranges:

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters.

Usage guidelines

If **default**, *acl-number*, **name** *acl-name*, **ipv6**, or **mac**is not specified, this command clears the packet filtering statistics for all ACLs.

Examples

Clear IPv4 basic ACL 2001 statistics for inbound packet filtering on GigabitEthernet 1/0/1.

```
<Sysname> reset packet-filter statistics interface gigabitethernet 1/0/1 inbound 2001
```

Clear IPv4 basic ACL 2001 statistics for packet filtering on the zone pair from source security zone **office** to destination security zone **library**.

```
<Sysname> reset packet-filter statistics zone-pair security source office destination
library 2001
```

Related commands

display packet-filter statistics

display packet-filter statistics sum

rule (IPv4 advanced ACL view)

Use **rule** to create or edit an IPv4 advanced ACL rule.

Use **undo rule** to delete an entire IPv4 advanced ACL rule or some attributes in the rule.

Syntax

rule [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **counting** | **destination** { **object-group** *address-group-name* | *dest-address dest-wildcard* | **any** } | **destination-port** { **object-group** *port-group-name* | *operator port1* [*port2*] } | { **dscp** *dscp* | { **precedence** *precedence* | **tos** *tos* } * } | **fragment** | **icmp-type** { *icmp-type* [*icmp-code*] | *icmp-message* } | **logging** | **source** { **object-group** *address-group-name* | *source-address source-wildcard* | **any** } | **source-port** { **object-group** *port-group-name* | *operator port1* [*port2*] } | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *

undo rule *rule-id* [{ { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **established** } | **counting** | **destination** | **destination-port** | { **dscp** | { **precedence** | **tos** } * } | **fragment** | **icmp-type** | **logging** | **source** | **source-port** | **time-range** | **vpn-instance**] *

undo rule [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **counting** | **destination** { **object-group** *address-group-name* | *dest-address dest-wildcard* | **any** } | **destination-port** { **object-group** *port-group-name* | *operator port1* [*port2*] } | { **dscp** *dscp* | { **precedence** *precedence* | **tos** *tos* } * } | **fragment** | **icmp-type** { *icmp-type* [*icmp-code*] | *icmp-message* } | **logging** | **source** { **object-group** *address-group-name* | *source-address source-wildcard* | **any** } | **source-port** { **object-group**

port-group-name | *operator port1* [*port2*] } | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *

Default

No IPv4 advanced ACL rules exist.

Views

IPv4 advanced ACL view

Predefined user roles

network-admin

context-admin

Parameters

rule-id: Specifies a rule ID in the range of 0 to 65534. If you do not specify a rule ID when creating an ACL rule, the system automatically assigns it a rule ID. This rule ID is the nearest higher multiple of the numbering step to the current highest rule ID, starting from the start rule ID. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the rule is numbered 30.

deny: Denies matching packets.

permit: Allows matching packets to pass.

protocol: Specifies one of the following values:

- A protocol number in the range of 0 to 255.
- A protocol by its name: **gre** (47), **icmp** (1), **igmp** (2), **ip**, **ipinip** (4), **ospf** (89), **tcp** (6), or **udp** (17). The **ip** keyword specifies all protocols.

Table 6 describes the parameters that you can specify regardless of the value for the *protocol* argument.

Table 6 Match criteria and other rule information for IPv4 advanced ACL rules

Parameters	Function	Description
source { **object-group** *address-group-name* | *source-address source-wildcard* | **any** }	Specifies a source address.	The *address-group-name* argument specifies an object group of source IP addresses. The *source-address source-wildcard* arguments specify a source IP address and a wildcard mask in dotted decimal notation. An all-zero wildcard represents a host address. The **any** keyword specifies any source IP address.
destination { **object-group** *address-group-name* | *dest-address dest-wildcard* | **any** }	Specifies a destination address.	The *address-group-name* argument specifies an object group of destination IP addresses. The *dest-address dest-wildcard* arguments specify a destination IP address and a wildcard mask in dotted decimal notation. An all-zero wildcard mask represents a host address. The **any** keyword represents any destination IP address.
counting	Enables rule match counting in software.	The **counting** keyword enables match counting specific to rules. If the **counting**

		keyword is not specified, matches for the rule are not counted in software.
precedence *precedence*	Specifies an IP precedence value.	The *precedence* argument can be a number in the range of 0 to 7, or in words: **routine** (0), **priority** (1), **immediate** (2), **flash** (3), **flash-override** (4), **critical** (5), **internet** (6), or **network** (7).
tos *tos*	Specifies a ToS preference.	The *tos* argument can be a number in the range of 0 to 15, or in words: **max-reliability** (2), **max-throughput** (4), **min-delay** (8), **min-monetary-cost** (1), or **normal** (0).
dscp *dscp*	Specifies a DSCP priority.	The *dscp* argument can be a number in the range of 0 to 63, or in words: **af11** (10), **af12** (12), **af13** (14), **af21** (18), **af22** (20), **af23** (22), **af31** (26), **af32** (28), **af33** (30), **af41** (34), **af42** (36), **af43** (38), **cs1** (8), **cs2** (16), **cs3** (24), **cs4** (32), **cs5** (40), **cs6** (48), **cs7** (56), **default** (0), or **ef** (46).
fragment	Applies the rule only to non-first fragments.	If you do not specify this keyword, the rule applies to all fragments and non-fragments.
logging	Logs the number of matching packets.	This feature requires that the module (for example, packet filtering) that uses the ACL supports logging.
time-range *time-range-name*	Specifies a time range for the rule.	The *time-range-name* argument is a case-insensitive string of 1 to 32 characters. If the time range is not configured, the system creates the rule. However, the rule using the time range can take effect only after you configure the time range. For more information about time range, see *ACL and QoS Configuration Guide*.
vpn-instance *vpn-instance-name*	Applies the rule to an MPLS L3VPN instance.	The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. For an ACL used to filter packets, if you do not specify a VPN instance, the rule applies to only non-VPN packets. For an ACL used by other features, if you do not specify a VPN instance, the implementation varies by feature. For more information, see the configuration guide of the feature..

If the *protocol* argument is **tcp** (6) or **udp** (17), set the parameters shown in Table 7.

Table 7 TCP/UDP-specific parameters for IPv4 advanced ACL rules

Parameters	Function	Description
source-port { **object-group** *port-group-name* | *operator port1* [*port2*] }	Specifies one or more UDP or TCP source ports.	The *port-group-name* argument specifies an object group of ports. The *operator* argument can be **lt** (lower than), **gt** (greater than), **eq** (equal to), **neq** (not equal to), or **range** (inclusive range). The *port1* and *port2* arguments are TCP or UDP port numbers in the range of 0 to 65535. The *port2* argument is needed only when the *operator* argument is **range**.
destination-port	Specifies one or more	

{ **object-group** *port-group-name* | *operator port1* [*port2*] }	UDP or TCP destination ports.	TCP port numbers can be represented as: **chargen** (19), **bgp** (179), **cmd** (514), **daytime** (13), **discard** (9), **dns** (53), **domain** (53), **echo** (7), **exec** (512), **finger** (79), **ftp** (21), **ftp-data** (20), **gopher** (70), **hostname** (101), **irc** (194), **klogin** (543), **kshell** (544), **login** (513), **lpd** (515), **nntp** (119), **pop2** (109), **pop3** (110), **smtp** (25), **sunrpc** (111), **tacacs** (49), **talk** (517), **telnet** (23), **time** (37), **uucp** (540), **whois** (43), and **www** (80). UDP port numbers can be represented as: **biff** (512), **bootpc** (68), **bootps** (67), **discard** (9), **dns** (53), **dnsix** (90), **echo** (7), **mobilip-ag** (434), **mobilip-mn** (435), **nameserver** (42), **netbios-dgm** (138), **netbios-ns** (137), **netbios-ssn** (139), **ntp** (123), **rip** (520), **snmp** (161), **snmptrap** (162), **sunrpc** (111), **syslog** (514), **tacacs-ds** (65), **talk** (517), **tftp** (69), **time** (37), **who** (513), and **xdmcp** (177).
{ **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* }*	Specifies one or more TCP flags including ACK, FIN, PSH, RST, SYN, and URG.	Parameters specific to TCP. The value for each argument can be 0 (flag bit not set) or 1 (flag bit set). The TCP flags in a rule are ORed. For example, a rule configured with **ack** 0 **psh** 1 matches both packets that have the ACK flag bit not set and packets that have the PSH flag bit set.
established	Specifies the flags for indicating the established status of a TCP connection.	Parameter specific to TCP. The rule matches TCP connection packets with the ACK or RST flag bit set.

If the *protocol* argument is **icmp** (1), set the parameters shown in Table 8.

Table 8 ICMP-specific parameters for IPv4 advanced ACL rules

Parameters	Function	Description
icmp-type { *icmp-type icmp-code* | *icmp-message* }	Specifies the ICMP message type and code.	The *icmp-type* argument is in the range of 0 to 255. The *icmp-code* argument is in the range of 0 to 255. The *icmp-message* argument specifies a message name. Supported ICMP message names and their corresponding type and code values are listed in Table 9.

Table 9 ICMP message names supported in IPv4 advanced ACL rules

ICMP message name	ICMP message type	ICMP message code
echo	8	0
echo-reply	0	0
fragmentneed-DFset	3	4
host-redirect	5	1
host-tos-redirect	5	3
host-unreachable	3	1

information-reply	16	0
information-request	15	0
net-redirect	5	0
net-tos-redirect	5	2
net-unreachable	3	0
parameter-problem	12	0
port-unreachable	3	3
protocol-unreachable	3	2
reassembly-timeout	11	1
source-quench	4	0
source-route-failed	3	5
timestamp-reply	14	0
timestamp-request	13	0
ttl-exceeded	11	0

Usage guidelines

Within an ACL, the permit or deny statement of each rule must be unique. If the rule you are creating or editing has the same deny or permit statement as another manually added rule in the ACL, the rule will not be created or changed. If the rule you are creating or editing has the same deny or permit statement as a dynamically added rule in the ACL, the rule will overwrite the dynamically added rule.

The object group you specify when creating or editing a rule must already exist. Otherwise, the rule will not be created or changed.

You can edit ACL rules only when the match order is **config**.

To view the existing IPv4 basic and advanced ACL rules, use the **display acl all** command.

The **undo rule** *rule-id* command without any optional parameters deletes an entire rule. If you specify optional parameters, the **undo rule** *rule-id* command deletes the specified attributes for the rule.

The **undo rule** [*rule-id*] { **deny** | **permit** } command can only be used to delete an entire rule. You must specify all the attributes of the rule for the command.

Examples

Create an IPv4 advanced ACL rule to permit TCP packets with the destination port 80 from 129.9.0.0/16 to 202.38.160.0/24.

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule permit tcp source 129.9.0.0 0.0.255.255 destination
202.38.160.0 0.0.0.255 destination-port eq 80
```

Create IPv4 advanced ACL rules to permit all IP packets but the ICMP packets destined for 192.168.1.0/24.

```
<Sysname> system-view
[Sysname] acl advanced 3001
[Sysname-acl-ipv4-adv-3001] rule deny icmp destination 192.168.1.0 0.0.0.255
[Sysname-acl-ipv4-adv-3001] rule permit ip
```

Create IPv4 advanced ACL rules to permit inbound and outbound FTP packets.

```
<Sysname> system-view
[Sysname] acl advanced 3002
[Sysname-acl-ipv4-adv-3002] rule permit tcp source-port eq ftp
[Sysname-acl-ipv4-adv-3002] rule permit tcp source-port eq ftp-data
[Sysname-acl-ipv4-adv-3002] rule permit tcp destination-port eq ftp
[Sysname-acl-ipv4-adv-3002] rule permit tcp destination-port eq ftp-data
```

Create IPv4 advanced ACL rules to permit inbound and outbound SNMP and SNMP trap packets.

```
<Sysname> system-view
[Sysname] acl advanced 3003
[Sysname-acl-ipv4-adv-3003] rule permit udp source-port eq snmp
[Sysname-acl-ipv4-adv-3003] rule permit udp source-port eq snmptrap
[Sysname-acl-ipv4-adv-3003] rule permit udp destination-port eq snmp
[Sysname-acl-ipv4-adv-3003] rule permit udp destination-port eq snmptrap
```

Related commands

acl

acl logging interval

display acl

step

time-range

rule (IPv4 basic ACL view)

Use **rule** to create or edit an IPv4 basic ACL rule.

Use **undo rule** to delete an entire IPv4 basic ACL rule or some attributes in the rule.

Syntax

rule [*rule-id*] { **deny** | **permit** } [**counting** | **fragment** | **logging** | **source** { **object-group** *address-group-name* | *source-address source-wildcard* | **any** } | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *

undo rule *rule-id* [**counting** | **fragment** | **logging** | **source** | **time-range** | **vpn-instance**] *

undo rule [*rule-id*] { **deny** | **permit** } [**counting** | **fragment** | **logging** | **source** { **object-group** *address-group-name* | *source-address source-wildcard* | **any** } | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *

Default

No IPv4 basic ACL rules exist.

Views

IPv4 basic ACL view

Predefined user roles

network-admin

context-admin

Parameters

rule-id: Specifies a rule ID in the range of 0 to 65534. If you do not specify a rule ID when creating an ACL rule, the system automatically assigns it a rule ID. This rule ID is the nearest higher multiple

of the numbering step to the current highest rule ID, starting from the start rule ID. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the rule is numbered 30.

deny: Denies matching packets.

permit: Allows matching packets to pass.

counting: Enables rule match counting in software. If you do not specify this keyword, matches for the rule are not counted in software.

fragment: Applies the rule only to non-first fragments. If you do not specify this keyword, the rule applies to both fragments and non-fragments.

logging: Logs the number of matching packets. This feature is available only when the application module (for example, packet filtering) that uses the ACL supports the logging feature.

source { **object-group** *address-group-name* | *source-address source-wildcard* | **any** }: Matches a source address. The **object-group** *address-group-name* option specifies an object group of source IP addresses. The *source-address* and *source-wildcard* arguments specify a source IP address and a wildcard mask in dotted decimal notation. A wildcard mask of zeros represents a host address. The **any** keyword represents any source IP address.

time-range *time-range-name*: Specifies a time range for the rule. The *time-range-name* argument is a case-insensitive string of 1 to 32 characters. If the time range is not configured, the system creates the rule. However, the rule using the time range can take effect only after you configure the time range. For more information about time range, see *ACL and QoS Configuration Guide*.

vpn-instance *vpn-instance-name*: Applies the rule to an MPLS L3VPN instance. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. For an ACL used to filter packets, if you do not specify a VPN instance, the rule applies to only non-VPN packets. For an ACL used by other features, if you do not specify a VPN instance, the implementation varies by feature. For more information, see the configuration guide of the feature.

Usage guidelines

Within an ACL, the permit or deny statement of each rule must be unique. If the rule you are creating or editing has the same deny or permit statement as another rule in the ACL, the rule will not be created or changed.

The object group you specify when creating or editing a rule must already exist. Otherwise, the rule will not be created or changed.

You can edit ACL rules only when the match order is **config**.

To view the existing IPv4 basic and advanced ACL rules, use the **display acl all** command.

The **undo rule** *rule-id* command without any optional parameters deletes an entire rule. If you specify optional parameters, the **undo rule** *rule-id* command deletes the specified attributes for the rule.

The **undo rule** [*rule-id*] { **deny** | **permit** } command can only be used to delete an entire rule. You must specify all the attributes of the rule for the command.

Examples

Create a rule in IPv4 basic ACL 2000 to deny the packets from any source IP subnet but 10.0.0.0/8, 172.17.0.0/16, or 192.168.1.0/24.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule permit source 10.0.0.0 0.255.255.255
[Sysname-acl-ipv4-basic-2000] rule permit source 172.17.0.0 0.0.255.255
[Sysname-acl-ipv4-basic-2000] rule permit source 192.168.1.0 0.0.0.255
```

```
[Sysname-acl-ipv4-basic-2000] rule deny source any
```

Related commands

acl

acl logging interval

display acl

step

time-range

rule (IPv6 advanced ACL view)

Use **rule** to create or edit an IPv6 advanced ACL rule.

Use **undo rule** to delete an entire IPv6 advanced ACL rule or some attributes in the rule.

Syntax

rule [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **counting** | **destination** { **object-group** *address-group-name* | *dest-address dest-prefix* | *dest-address/dest-prefix* | **any** } | **destination-port** { **object-group** *port-group-name* | *operator port1* [*port2*] } | **dscp** *dscp* | **flow-label** *flow-label-value* | **fragment** | **icmp6-type** { *icmp6-type icmp6-code* | *icmp6-message* } | **logging** | **routing** [**type** *routing-type*] | **hop-by-hop** [**type** *hop-type*] | **source** { **object-group** *address-group-name* | *source-address source-prefix* | *source-address/source-prefix* | **any** } | **source-port** { **object-group** *port-group-name* | *operator port1* [*port2*] } | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *

undo rule *rule-id* [{ { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **established** } | **counting** | **destination** | **destination-port** | **dscp** | **flow-label** | **fragment** | **icmp6-type** | **logging** | **routing** | **hop-by-hop** | **source** | **source-port** | **time-range** | **vpn-instance**] *

undo rule [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **counting** | **destination** { **object-group** *address-group-name* | *dest-address dest-prefix* | *dest-address/dest-prefix* | **any** } | **destination-port** { **object-group** *port-group-name* | *operator port1* [*port2*] } | **dscp** *dscp* | **flow-label** *flow-label-value* | **fragment** | **icmp6-type** { *icmp6-type icmp6-code* | *icmp6-message* } | **logging** | **routing** [**type** *routing-type*] | **hop-by-hop** [**type** *hop-type*] | **source** { **object-group** *address-group-name* | *source-address source-prefix* | *source-address/source-prefix* | **any** } | **source-port** { **object-group** *port-group-name* | *operator port1* [*port2*] } | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *

Default

No IPv6 advanced ACL rules exist.

Views

IPv6 advanced ACL view

Predefined user roles

network-admin

context-admin

Parameters

rule-id: Specifies a rule ID in the range of 0 to 65534. If you do not specify a rule ID when creating an ACL rule, the system automatically assigns it a rule ID. This rule ID is the nearest higher multiple of the numbering step to the current highest rule ID, starting from the start rule ID. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the rule is numbered 30.

deny: Denies matching packets.

permit: Allows matching packets to pass.

protocol: Specifies one of the following values:

- A protocol number in the range of 0 to 255.
- A protocol name: **gre** (47), **icmpv6** (58), **ipv6**, **ipv6-ah** (51), **ipv6-esp** (50), **ospf** (89), **tcp** (6), or **udp** (17). The **ipv6** keyword specifies all protocols.

Table 10 describes the parameters that you can specify regardless of the value for the *protocol* argument.

Table 10 Match criteria and other rule information for IPv6 advanced ACL rules

Parameters	Function	Description
source { **object-group** *address-group-name* | *source-address/source-prefix* | **any** }	Specifies a source IPv6 address.	The *address-group-name* argument specifies an object group of source IPv6 addresses. The *source-address* argument specifies an IPv6 source address. The *source-prefix* argument specifies a prefix length in the range of 1 to 128. The **any** keyword represents any IPv6 source address.
destination { **object-group** *address-group-name* | *dest-address/dest-prefix* | **any** }	Specifies a destination IPv6 address.	The *address-group-name* argument specifies an object group of destination IPv6 addresses. The *dest-address* argument specifies a destination IPv6 address. The *dest-prefix* argument specifies a prefix length in the range of 1 to 128. The **any** keyword represents any IPv6 destination address.
counting	Enables rule match counting in software.	The **counting** keyword enables match counting specific to rules. If the **counting** keyword is not specified, matches for the rule are not counted in software.
dscp *dscp*	Specifies a DSCP preference.	The *dscp* argument can be a number in the range of 0 to 63, or in words, **af11** (10), **af12** (12), **af13** (14), **af21** (18), **af22** (20), **af23** (22), **af31** (26), **af32** (28), **af33** (30), **af41** (34), **af42** (36), **af43** (38), **cs1** (8), **cs2** (16), **cs3** (24), **cs4** (32), **cs5** (40), **cs6** (48), **cs7** (56), **default** (0), or **ef** (46).
flow-label	Specifies a flow label value in an IPv6 packet	The *flow-label-value* argument is in the

flow-label-value	header.	range of 0 to 1048575.
fragment	Applies the rule only to non-first fragments.	If you do not specify this keyword, the rule applies to all fragments and non-fragments.
logging	Logs the number of matching packets.	This feature requires that the module (for example, packet filtering) that uses the ACL supports logging.
routing [**type** *routing-type*]	Specifies an IPv6 routing header type.	*routing-type*: Value of the IPv6 routing header type, in the range of 0 to 255. If you specify the **type** *routing-type* option, the rule applies to the specified type of IPv6 routing header. If you do not specify the **type** *routing-type* option, the rule applies to all types of IPv6 routing headers.
hop-by-hop [**type** *hop-type*]	Specifies an IPv6 Hop-by-Hop Options header type.	*hop-type*: Value of the IPv6 Hop-by-Hop Options header type, in the range of 0 to 255. If you specify the **type** *hop-type* option, the rule applies to the specified type of IPv6 Hop-by-Hop Options header. If you do not specify the **type** *hop-type* option, the rule applies to all types of IPv6 Hop-by-Hop Options header.
time-range *time-range-name*	Specifies a time range for the rule.	The *time-range-name* argument is a case-insensitive string of 1 to 32 characters. If the time range is not configured, the system creates the rule. However, the rule using the time range can take effect only after you configure the time range. For more information about time range, see *ACL and QoS Configuration Guide*.
vpn-instance *vpn-instance-name*	Applies the rule to an MPLS L3VPN instance.	The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. For an ACL used to filter packets, if you do not specify a VPN instance, the rule applies to only non-VPN packets. For an ACL used by other features, if you do not specify a VPN instance, the implementation varies by feature. For more information, see the configuration guide of the feature.

If the *protocol* argument is **tcp** (6) or **udp** (17), set the parameters shown in Table 11.

Table 11 TCP/UDP-specific parameters for IPv6 advanced ACL rules

Parameters	Function	Description
source-port { **object-group** *port-group-name* | *operator port1* [*port2*] }	Specifies one or more UDP or TCP source ports.	The *port-group-name* argument specifies an object group of ports. The *operator* argument can be **lt** (lower than), **gt** (greater than), **eq** (equal to), **neq** (not equal to), or **range** (inclusive range). The *port1* and *port2* arguments are TCP or UDP port numbers in the range of 0 to 65535. The *port2* argument is needed only when the *operator* argument is **range**. TCP port numbers can be represented as: **chargen** (19), **bgp** (179), **cmd** (514), **daytime** (13), **discard** (9), **dns** (53), **domain** (53), **echo** (7), **exec** (512), **finger** (79), **ftp**
destination-port { **object-group** *port-group-name* | *operator port1* [*port2*] }	Specifies one or more UDP or TCP destination ports.	

		(21), **ftp-data** (20), **gopher** (70), **hostname** (101), **irc** (194), **klogin** (543), **kshell** (544), **login** (513), **lpd** (515), **nntp** (119), **pop2** (109), **pop3** (110), **smtp** (25), **sunrpc** (111), **tacacs** (49), **talk** (517), **telnet** (23), **time** (37), **uucp** (540), **whois** (43), and **www** (80). UDP port numbers can be represented as: **biff** (512), **bootpc** (68), **bootps** (67), **discard** (9), **dns** (53), **dnsix** (90), **echo** (7), **mobilip-ag** (434), **mobilip-mn** (435), **nameserver** (42), **netbios-dgm** (138), **netbios-ns** (137), **netbios-ssn** (139), **ntp** (123), **rip** (520), **snmp** (161), **snmptrap** (162), **sunrpc** (111), **syslog** (514), **tacacs-ds** (65), **talk** (517), **tftp** (69), **time** (37), **who** (513), and **xdmcp** (177).
{ **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* }*	Specifies one or more TCP flags, including ACK, FIN, PSH, RST, SYN, and URG.	Parameters specific to TCP. The value for each argument can be 0 (flag bit not set) or 1 (flag bit set). The TCP flags in a rule are ORed. For example, a rule configured with **ack** 0 **psh** 1 matches both packets that have the ACK flag bit not set and packets that have the PSH flag bit set.
established	Specifies the flags for indicating the established status of a TCP connection.	Parameter specific to TCP. The rule matches TCP connection packets with the ACK or RST flag bit set.

If the *protocol* argument is **icmpv6** (58), set the parameters shown in Table 12.

Table 12 ICMPv6-specific parameters for IPv6 advanced ACL rules

Parameters	Function	Description
icmp6-type { *icmp6-type* *icmp6-code* | *icmp6-message* }	Specifies the ICMPv6 message type and code.	The *icmp6-type* argument is in the range of 0 to 255. The *icmp6-code* argument is in the range of 0 to 255. The *icmp6-message* argument specifies a message name. Supported ICMP message names and their corresponding type and code values are listed in Table 13.

Table 13 ICMPv6 message names supported in IPv6 advanced ACL rules

ICMPv6 message name	ICMPv6 message type	ICMPv6 message code
echo-reply	129	0
echo-request	128	0
err-Header-field	4	0
frag-time-exceeded	3	1
hop-limit-exceeded	3	0
host-admin-prohib	1	1
host-unreachable	1	3
neighbor-advertisement	136	0
neighbor-solicitation	135	0
network-unreachable	1	0

packet-too-big	2	0
port-unreachable	1	4
redirect	137	0
router-advertisement	134	0
router-solicitation	133	0
unknown-ipv6-opt	4	2
unknown-next-hdr	4	1

Usage guidelines

Within an ACL, the permit or deny statement of each rule must be unique. If the rule you are creating or editing has the same deny or permit statement as another manually added rule in the ACL, the rule will not be created or changed. If the rule you are creating or editing has the same deny or permit statement as a dynamically added rule in the ACL, the rule will overwrite the dynamically added rule.

The object group you specify when creating or editing a rule must already exist. Otherwise, the rule will not be created or changed.

You can edit ACL rules only when the match order is **config**.

To view the existing IPv6 basic and advanced ACL rules, use the **display acl ipv6 all** command.

The **undo rule** *rule-id* command without any optional parameters deletes an entire rule. If you specify optional parameters, the **undo rule** *rule-id* command deletes the specified attributes for a rule.

The **undo rule** [*rule-id*] { **deny** | **permit** } command can only be used to delete an entire rule. You must specify all the attributes of the rule for the command.

Examples

Create an IPv6 advanced ACL rule to permit TCP packets with the destination port 80 from 2030:5060::/64 to FE80:5060::/96.

```
<Sysname> system-view
[Sysname] acl ipv6 advanced 3000
[Sysname-acl-ipv6-adv-3000] rule permit tcp source 2030:5060::/64 destination
fe80:5060::/96 destination-port eq 80
```

Create IPv6 advanced ACL rules to permit all IPv6 packets but the ICMPv6 packets destined for FE80:5060:1001::/48.

```
<Sysname> system-view
[Sysname] acl ipv6 advanced 3001
[Sysname-acl-ipv6-adv-3001] rule deny icmpv6 destination fe80:5060:1001:: 48
[Sysname-acl-ipv6-adv-3001] rule permit ipv6
```

Create IPv6 advanced ACL rules to permit inbound and outbound FTP packets.

```
<Sysname> system-view
[Sysname] acl ipv6 advanced 3002
[Sysname-acl-ipv6-adv-3002] rule permit tcp source-port eq ftp
[Sysname-acl-ipv6-adv-3002] rule permit tcp source-port eq ftp-data
[Sysname-acl-ipv6-adv-3002] rule permit tcp destination-port eq ftp
[Sysname-acl-ipv6-adv-3002] rule permit tcp destination-port eq ftp-data
```

Create IPv6 advanced ACL rules to permit inbound and outbound SNMP and SNMP trap packets.

```
<Sysname> system-view
```

```
[Sysname] acl ipv6 advanced 3003
[Sysname-acl-ipv6-adv-3003] rule permit udp source-port eq snmp
[Sysname-acl-ipv6-adv-3003] rule permit udp source-port eq snmptrap
[Sysname-acl-ipv6-adv-3003] rule permit udp destination-port eq snmp
[Sysname-acl-ipv6-adv-3003] rule permit udp destination-port eq snmptrap
```

Create IPv6 advanced ACL 3004, and configure two rules: one permits packets with the Hop-by-Hop Options header type as 5, and the other one denies packets with other Hop-by-Hop Options header types.

```
<Sysname> system-view
[Sysname] acl ipv6 advanced 3004
[Sysname-acl-ipv6-adv-3004] rule permit ipv6 hop-by-hop type 5
[Sysname-acl-ipv6-adv-3004] rule deny ipv6 hop-by-hop
```

Related commands

acl

acl logging interval

display acl

step

time-range

rule (IPv6 basic ACL view)

Use **rule** to create or edit an IPv6 basic ACL rule.

Use **undo rule** to delete an entire IPv6 basic ACL rule or some attributes in the rule.

Syntax

rule [*rule-id*] { **deny** | **permit** } [**counting** | **fragment** | **logging** | **routing** [**type** *routing-type*] | **source** { **object-group** *address-group-name* | *source-address source-prefix* | *source-address*/*source-prefix* | **any** } | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *

undo rule *rule-id* [**counting** | **fragment** | **logging** | **routing** | **source** | **time-range** | **vpn-instance**] *

undo rule [*rule-id*] { **deny** | **permit** } [**counting** | **fragment** | **logging** | **routing** [**type** *routing-type*] | **source** { **object-group** *address-group-name* | *source-address source-prefix* | *source-address*/*source-prefix* | **any** } | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *

Default

No IPv6 basic ACL rules exist.

Views

IPv6 basic ACL view

Predefined user roles

network-admin

context-admin

Parameters

rule-id: Specifies a rule ID in the range of 0 to 65534. If you do not specify a rule ID when creating an ACL rule, the system automatically assigns it a rule ID. This rule ID is the nearest higher multiple

of the numbering step to the current highest rule ID, starting from the start rule ID. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the rule is numbered 30.

deny: Denies matching packets.

permit: Allows matching packets to pass.

counting: Enables rule match counting in software. If you do not specify this keyword, matches for the rule are not counted in software.

fragment: Applies the rule only to non-first fragments. If you do not specify this keyword, the rule applies to both fragments and non-fragments.

logging: Logs the number of matching packets. This feature is available only when the application module (for example, packet filtering) that uses the ACL supports the logging feature.

routing [**type** *routing-type*]: Applies the rule to the specified type of IPv6 routing header or all types of IPv6 routing headers. The *routing-type* argument specifies the value of the IPv6 routing header type, in the range of 0 to 255. If you do not specify the **type** *routing-type* option, the rule applies to all types of IPv6 routing headers.

source { **object-group** *address-group-name* | *source-address source-prefix* | *source-address*/*source-prefix* | **any** }: Matches a source IPv6 address. The **object-group** *address-group-name* option specifies an object group of source IPv6 addresses. The *source-address* argument specifies a source IPv6 address. The *source-prefix* argument specifies an address prefix length in the range of 1 to 128. The **any** keyword represents any IPv6 source address.

time-range *time-range-name*: Specifies a time range for the rule. The *time-range-name* argument is a case-insensitive string of 1 to 32 characters. If the time range is not configured, the system creates the rule. However, the rule using the time range can take effect only after you configure the time range. For more information about time range, see *ACL and QoS Configuration Guide*.

vpn-instance *vpn-instance-name*: Applies the rule to an MPLS L3VPN instance. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. For an ACL used to filter packets, if you do not specify a VPN instance, the rule applies to only non-VPN packets. For an ACL used by other features, if you do not specify a VPN instance, the implementation varies by feature. For more information, see the configuration guide of the feature.

Within an ACL, the permit or deny statement of each rule must be unique. If the rule you are creating or editing has the same deny or permit statement as another rule in the ACL, the rule will not be created or changed.

The object group you specify when creating or editing a rule must already exist. Otherwise, the rule will not be created or changed.

You can edit ACL rules only when the match order is **config**.

To view the existing IPv6 basic and advanced ACL rules, use the **display acl ipv6 all** command.

The **undo rule** *rule-id* command without any optional parameters deletes an entire rule. If you specify optional parameters, the **undo rule** *rule-id* command deletes the specified attributes for a rule.

The **undo rule** [*rule-id*] { **deny** | **permit** } command can only be used to delete an entire rule. You must specify all the attributes of the rule for the command.

Examples

Create an IPv6 basic ACL rule to deny the packets from any source IP subnet but 1001::/16, 3124:1123::/32, or FE80:5060:1001::/48.

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2000
```

```
[Sysname-acl-ipv6-basic-2000] rule permit source 1001:: 16
[Sysname-acl-ipv6-basic-2000] rule permit source 3124:1123:: 32
[Sysname-acl-ipv6-basic-2000] rule permit source fe80:5060:1001:: 48
[Sysname-acl-ipv6-basic-2000] rule deny source any
```

Related commands

acl

acl logging interval

display acl

step

time-range

rule (Layer 2 ACL view)

Use **rule** to create or edit a Layer 2 ACL rule.

Use **undo rule** to delete an entire Layer 2 ACL rule or some attributes in the rule.

Syntax

rule [*rule-id*] { **deny** | **permit** } [**cos** *dot1p* | **counting** | **dest-mac** *dest-address dest-mask* | { **lsap** *lsap-type lsap-type-mask* | **type** *protocol-type protocol-type-mask* } | **source-mac** *source-address source-mask* | **time-range** *time-range-name*] *

undo rule *rule-id* [**counting** | **time-range**] *

undo rule [*rule-id*] { **deny** | **permit** } [**cos** *dot1p* | **counting** | **dest-mac** *dest-address dest-mask* | { **lsap** *lsap-type lsap-type-mask* | **type** *protocol-type protocol-type-mask* } | **source-mac** *source-address source-mask* | **time-range** *time-range-name*] *

Default

No Layer 2 ACL rules exist.

Views

Layer 2 ACL view

Predefined user roles

network-admin

context-admin

Parameters

rule-id: Specifies a rule ID in the range of 0 to 65534. If you do not specify a rule ID when creating an ACL rule, the system automatically assigns it a rule ID. This rule ID is the nearest higher multiple of the numbering step to the current highest rule ID, starting from the start rule ID. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the rule is numbered 30.

deny: Denies matching packets.

permit: Allows matching packets to pass.

cos *dot1p:* Matches an 802.1p priority. The 802.1p priority can be specified by one of the following values:

- A priority number in the range of 0 to 7.

- A priority name: **best-effort** (0), **background** (1), **spare** (2), **excellent-effort** (3), **controlled-load** (4), **video** (5), **voice** (6), or **network-management** (7).

counting: Enables rule match counting in software. If you do not specify this keyword, matches for the rule are not counted in software.

dest-mac *dest-address dest-mask:* Matches a destination MAC address range. The *dest-address* and *dest-mask* arguments represent a destination MAC address and mask in the H-H-H format.

lsap *lsap-type lsap-type-mask:* Matches the DSAP and SSAP fields in LLC encapsulation. The *lsap-type* argument is a hexadecimal number that represents the encapsulation format. The value range for the *lsap-type* argument is 0 to ffff. The *lsap-type-mask* argument is a hexadecimal number that represents the LSAP mask. The value range for the *lsap-type-mask* argument is 0 to ffff.

type *protocol-type protocol-type-mask*: Matches one or more protocols in the Layer 2. The *protocol-type* argument is a hexadecimal number that represents a protocol type in Ethernet_II and Ethernet_SNAP frames. The value range for the *protocol-type* argument is 0 to ffff. The *protocol-type-mask* argument is a hexadecimal number that represents a protocol type mask. The value range for the *protocol-type-mask* argument is 0 to ffff.

source-mac *source-address source-mask:* Matches a source MAC address range. The *source-address* argument represents a source MAC address, and the *sour-mask* argument represents a mask in the H-H-H format.

time-range *time-range-name*: Specifies a time range for the rule. The *time-range-name* argument is a case-insensitive string of 1 to 32 characters. If the time range is not configured, the system creates the rule. However, the rule using the time range can take effect only after you configure the time range. For more information about time range, see *ACL and QoS Configuration Guide*.

Usage guidelines

Within an ACL, the permit or deny statement of each rule must be unique. If the rule you are creating or editing has the same deny or permit statement as another rule in the ACL, the rule will not be created or changed.

You can edit ACL rules only when the match order is **config**.

To view the existing Layer 2 ACL rules, use the **display acl mac all** command.

The **undo rule** *rule-id* command without any optional parameters deletes an entire rule. If you specify optional parameters, the **undo rule** *rule-id* command deletes the specified attributes for the rule.

The **undo rule** [*rule-id*] { **deny** | **permit** } command can only be used to delete an entire rule. You must specify all the attributes of the rule for the command.

Examples

Create a rule in Layer 2 ACL 4000 to permit ARP packets and deny RARP packets.

```
<Sysname> system-view
[Sysname] acl mac 4000
[Sysname-acl-mac-4000] rule permit type 0806 ffff
[Sysname-acl-mac-4000] rule deny type 8035 ffff
```

Related commands

acl

display acl

step

time-range

rule comment

Use **rule comment** to configure a comment for an ACL rule.

Use **undo rule comment** to delete an ACL rule comment.

Syntax

rule *rule-id* **comment** *text*

undo rule *rule-id* **comment**

Default

A rule does not have a comment.

Views

IPv4 basic/advanced ACL view

IPv6 basic/advanced ACL view

Layer 2 ACL view

Predefined user roles

network-admin

context-admin

Parameters

rule-id: Specifies an ACL rule ID in the range of 0 to 65534. The ACL rule must already exist.

text: Specifies a comment about the ACL rule, a case-sensitive string of 1 to 127 characters.

Usage guidelines

This command adds a comment to a rule if the rule does not have a comment. It modifies the comment for a rule if the rule already has a comment.

Examples

Create a rule for IPv4 basic ACL 2000, and add a comment about the rule.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule 0 deny source 1.1.1.1 0
[Sysname-acl-ipv4-basic-2000] rule 0 comment This rule is used on gigabitethernet 1/0/1.
```

Related commands

display acl

rule insert-only enable

Use **rule insert-only enable** to enable rule ID preemption.

Use **undo rule insert-only enable** to restore the default.

Syntax

rule insert-only enable

undo rule insert-only enable

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080	Yes
NFNX3-HDB1180, NFNX3-HDB1480 , NFNX3-HDB680, NFNX3-HDB1080	No

Default

Rule ID preemption is disabled.

Views

IPv4 basic/advanced ACL view

IPv6 basic/advanced ACL view

Layer 2 ACL view

Predefined user roles

network-admin

context-admin

Usage guidelines

CAUTION:

When there are a large number of ACLs on the device, executing the **undo accelerate** command might cause the CPU usage of the device to reach the upper threshold and cause service processing exceptions.

This feature enables a new rule to preempt an existing rule ID. The existing rule is assigned the next rule ID. All continuous rule IDs after the preempted rule ID are assigned their respective next rule IDs. For example, if you create rule 1 when rules 1, 2, 3, 6, and 7 exist, rule IDs are rearranged as 1, 2, 3, 4, 6, and 7.

After this feature is enabled, you cannot modify existing rules.

Examples

Enable rule ID preemption for ACL 2000.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule insert-only enable
```

step

Use **step** to set a rule numbering step for an ACL.

Use **undo step** to restore the default.

Syntax

step *step-value*

undo step

Default

The rule numbering step is 5, and the start rule ID is 0.

Views

IPv4 basic/advanced ACL view

IPv6 basic/advanced ACL view

Layer 2 ACL view

Predefined user roles

network-admin

context-admin

Parameters

step-value: Specifies the ACL rule numbering step in the range of 1 to 20.

Usage guidelines

The rule numbering step sets the increment by which the system numbers rules automatically. If you do not specify a rule ID when creating an ACL rule, the system automatically assigns it a rule ID. This rule ID is the nearest higher multiple of the numbering step to the current highest rule ID, starting from the start rule ID. For example, if the rule numbering step is 5 and the current highest rule ID is 12, the rule is numbered 15.

The wider the numbering step, the more rules you can insert between two rules. Whenever the step changes, the rules are renumbered, starting from the start rule ID. For example, if there are five rules numbered 0, 5, 9, 10, and 15, changing the step from 5 to 2 causes the rules to be renumbered 0, 2, 4, 6, and 8.

Examples

Set the rule numbering step to 2 for IPv4 basic ACL 2000.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] step 2
```

Related commands

display acl

Contents

QoS policy commands

Traffic class commands

display traffic classifier

Use **display traffic classifier** to display traffic classes.

Syntax

display traffic classifier user-defined [*classifier-name*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

user-defined: Specifies user-defined traffic classes.

classifier-name: Specifies a traffic class by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a traffic class, this command displays all traffic classes.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the traffic classes for the master device.

Examples

Display all user-defined traffic classes.

```
<Sysname> display traffic classifier user-defined

  User-defined classifier information:

   Classifier: 1 (ID 100)
     Operator: AND
     Rule(s) :
      If-match acl 2000

   Classifier: 2 (ID 101)
     Operator: AND
     Rule(s) :
      If-match protocol ipv6

   Classifier: 3 (ID 102)
     Operator: AND
     Rule(s) :
```

```
-none-
```

Table 1 Command output

Field	Description
Classifier	Traffic class name and its match criteria.
Operator	Match operator you set for the traffic class. If the operator is AND, the traffic class matches the packets that match all its match criteria. If the operator is OR, the traffic class matches the packets that match any of its match criteria.
Rule(s)	Match criteria.

if-match

Use **if-match** to define a match criterion.

Use **undo if-match** to delete a match criterion.

Syntax

if-match [**not**] *match-criteria*

undo if-match [**not**] *match-criteria*

Default

No match criterion is configured.

Views

Traffic class view

Predefined user roles

network-admin

context-admin

Parameters

not: Matches packets that do not conform to the specified criterion.

match-criteria: Specifies a match criterion. Table 2 shows the available match criteria.

Table 2 Available match criteria

Option	Description
acl [**ipv6**] { *acl-number* | **name** *acl-name* }	Matches an ACL. The value range for the *acl-number* argument is as follows: • 2000 to 3999 for IPv4 ACLs. • 2000 to 3999 for IPv6 ACLs. The *acl-name* argument is a case-insensitive string of 1 to 63 characters, which must start with an English letter. To avoid confusion, make sure the argument is not **all**. If no VPN instance is specified in an ACL rule, the ACL rule takes effect on both non-VPN packets and VPN packets.

Option	Description
app-group *group-name*	Matches an application group. The group-name argument specifies an application group by its name. The application group must have been created. A nonexistent application group cannot match packets. For more information about creating application groups, see APR in Security Configuration Guide.
application *app-name*	Matches an application. The app-name argument specifies a user-created application by its name.
any	Matches all packets.
classifier *classifier-name*	Matches a class. The *classifier-name* argument specifies a class by its name.
control-plane protocol *protocol-name*&<1-8>	Matches a control plane protocol. The *protocol-name* argument can only be **arp**.
customer-dot1p *dot1p-value*&<1-8>	Matches 802.1p priority values in inner VLAN tags of double-tagged packets. The *dot1p-value*&<1-8> argument specifies a space-separated list of up to eight 802.1p priority values. The value range for the *dot1p-value* argument is 0 to 7.
destination-mac *mac-address*	Matches a destination MAC address. This option takes effect only on Ethernet interfaces.
dscp *dscp-value*&<1-8>	Matches DSCP values. The *dscp-value*&<1-8> argument specifies a space-separated list of up to eight DSCP values. The value range for the *dscp-value* argument is 0 to 63 or keywords shown in Table 4.
inbound-interface *interface-type interface-number*	Matches an input interface specified by its type and number. If this option is configured in a traffic class with logic AND operator, the traffic class is no longer in effect after the card or subcard where the input interface resides is removed. After the removed card or subcard is reinserted, the traffic class takes effect again. If you do not reinsert the card or subcard and add other match criteria to the traffic class, the traffic class does not take effect again.
ip-precedence *ip-precedence-value*&<1-8>	Matches IP precedence values. The *ip-precedence-value*&<1-8> argument specifies a space-separated list of up to eight IP precedence values. The value range for the *ip-precedence-value* argument is 0 to 7.
mpls-exp *exp-value*&<1-8>	Matches MPLS EXP values. The *exp-value*&<1-8> argument specifies a space-separated list of up to eight EXP values. The value range for the *exp-value* argument is 0 to 7. MPLS packets do not support IP-related match criteria.

Option	Description
packet-length { **min** *min-value* | **max** *max-value* }*	Matches the packet length. The *min-value* argument specifies the minimum packet length in bytes. The *max-value* argument specifies the maximum packet length in bytes. The maximum packet length must be greater than or equal to the minimum packet length.
protocol *protocol-name*	Matches a protocol. The *protocol-name* argument can be The *protocol-name* argument can be **ip** or **ipv6**.
qos-local-id *local-id-value*	Matches a local QoS ID in the range of 1 to 4095.
rtp payload-type { *type-value*&<0-16> | **audio** | **video** }*	Matches RTP payload types. The *type-value*&<0-16> argument specifies a space-separated list of up to 16 RTP payload type values. The value range for the *type-value* argument is 0 to 127. The **audio** keyword matches an RTP payload type value in the range of 0 to 23 or 33. The **video** keyword matches an RTP payload type value in the range of 24 to 34. Support for this option depends on the device model.
rtp start-port *start-port-number* **end-port** *end-port-number*	Matches RTP protocol ports. The value ranges for the *start-port-number* and *end-port-number* arguments are both 2000 to 65535. This criterion matches RTP packets with an even UDP destination port number in the specified RTP port number range.
source-mac *mac-address*	Matches a source MAC address. This option takes effect only on Ethernet interfaces.

Usage guidelines

In a traffic class with the logical OR operator, you can configure multiple **if match** commands for any of the available match criteria.

When you configure a match criterion that can have multiple values in one **if-match** command, follow these restrictions and guidelines:

- You can specify up to eight values for any of the following match criteria in one **if-match** command:
- If a packet matches one of the specified values, it matches the **if-match** command.
- To delete a criterion that has multiple values, the specified values in the **undo if-match** command must be the same as those specified in the **if-match** command. The order of the values can be different.

When you configure ACL-based match criteria, follow these restrictions and guidelines:

- The ACL must already exist.
- If the ACL contains deny rules, the **if-match** command is ignored and the matching process continues.

You can use both AND and OR operators to define the match relationships between the criteria for a class. For example, you can define relationships among three match criteria in traffic class **classA** as follows:

```
traffic classifier classB operator and
if-match criterion 1
```

```
if-match criterion 2
traffic classifier classA operator or
if-match criterion 3
if-match classifier classB
```

Examples

Define a match criterion for traffic class **class1** to match the packets with a destination MAC address of 0050-ba27-bed3.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match destination-mac 0050-ba27-bed3
```

Define a match criterion for traffic class **class2** to match the packets with a source MAC address of 0050-ba27-bed2.

```
<Sysname> system-view
[Sysname] traffic classifier class2
[Sysname-classifier-class2] if-match source-mac 0050-ba27-bed2
```

Define a match criterion for traffic class **class1** to match the double-tagged packets with 802.1p priority 3 in the inner VLAN tag.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match customer-dot1p 3
```

Define a match criterion for traffic class **class1** to match advanced ACL 3101.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match acl 3101
```

Define a match criterion for traffic class **class1** to match the ACL named **flow**.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match acl name flow
```

Define a match criterion for traffic class **class1** to match advanced IPv6 ACL 3101.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match acl ipv6 3101
```

Define a match criterion for traffic class **class1** to match the IPv6 ACL named **flow**.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match acl ipv6 name flow
```

Define a match criterion for traffic class **class1** to match all packets.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match any
```

Define a match criterion for traffic class **class1** to match the packets with a DSCP value of 1, 6, or 9.

```
<Sysname> system-view
[Sysname] traffic classifier class1 operator or
[Sysname-classifier-class1] if-match dscp 1 6 9
```

Define a match criterion for traffic class **class1** to match the packets with an IP precedence value of 1 or 6.

```
<Sysname> system-view
[Sysname] traffic classifier class1 operator or
[Sysname-classifier-class1] if-match ip-precedence 1 6
```

Define a match criterion for traffic class **class1** to match IP packets.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match protocol ip
```

Define a match criterion for traffic class **class1** to match the RTP packets with even UDP destination port numbers in the range of 16384 to 32767.

```
<Sysname> system-view
[Sysname] traffic classifier class1 operator or
[Sysname-classifier-class1] if-match rtp start-port 16384 end-port 32767
```

Define a match criterion for traffic class **class1** to match the packets with a local QoS ID of 3.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match qos-local-id 3
```

Define a match criterion for traffic class **class1** to match the packets of the application group **multimedia**.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match app-group multimedia
```

Define a match criterion for traffic class **class1** to match the packets of the application **3link**.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match application 3link
```

Define a match criterion for traffic class **class1** to match packets with the length in the range of 100 to 200 bytes.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match packet-length min 100 max 200
```

traffic classifier

Use **traffic classifier** to create a traffic class and enter its view, or enter the view of an existing traffic class.

Use **undo traffic classifier** to delete a traffic class.

Syntax

traffic classifier *classifier-name* [**operator** { **and** | **or** }]

undo traffic classifier *classifier-name*

Default

No traffic classes exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

classifier-name: Specifies a name for the traffic class, a case-sensitive string of 1 to 31 characters.

operator: Sets the operator to logic AND (the default) or OR for the traffic class.

and: Specifies the logic AND operator. The traffic class matches the packets that match all its criteria.

or: Specifies the logic OR operator. The traffic class matches the packets that match any of its criteria.

Examples

Create a traffic class named **class1**.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1]
```

Related commands

display traffic classifier

Traffic behavior commands

car

Use **car** to configure a CAR action in absolute value in a traffic behavior.

Use **undo car** to restore the default.

Syntax

car cir *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**green** *action* | **red** *action* | **yellow** *action*] *

car cir *committed-information-rate* [**cbs** *committed-burst-size*] **pir** *peak-information-rate* [**ebs** *excess-burst-size*] [**green** *action* | **red** *action* | **yellow** *action*] *

undo car

Default

No CAR action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

context-admin

Parameters

cir *committed-information-rate*: Specifies the committed information rate (CIR) in the range of 8 to 10000000 kbps.

cbs *committed-burst-size*: Specifies the committed burst size (CBS) in the range of 1000 to 1000000000 bytes. The default value for this argument is the product of 62.5 and the CIR.

ebs *excess-burst-size*: Specifies the excess burst size (EBS) in the range of 0 to 1000000000 bytes. The default EBS is 0.

pir *peak-information-rate*: Specifies the peak information rate (PIR) in the range of 8 to 10000000 kbps. The PIR must be specified in the same unit as the CIR.

green *action*: Specifies the action to take on packets that conform to the CIR. The default setting is **pass**.

red *action*: Specifies the action to take on packets that conform to neither CIR nor PIR. The default setting is **discard**.

yellow *action*: Specifies the action to take on packets that conform to the PIR but not to the CIR. The default setting is **pass**.

action: Sets the action to take on the packet:

- **discard**: Drops the packet.
- **pass**: Permits the packet to pass through.
- **remark-dot1p-pass** *new-cos*: Sets the 802.1p priority value of the 802.1p packet to *new-cos* and permits the packet to pass through. The *new-cos* argument is in the range of 0 to 7.
- **remark-dscp-pass** *new-dscp*: Sets the DSCP value of the packet to *new-dscp* and permits the packet to pass through. The *new-dscp* argument is in the range of 0 to 63.
- **remark-mpls-exp-pass** *new-exp*: Sets the EXP field value of the MPLS packet to *new-exp* and permits the packet to pass through. The *new-exp* argument is in the range of 0 to 7.
- **remark-prec-pass** *new-precedence*: Sets the IP precedence of the packet to *new-precedence* and permits the packet to pass through. The *new-precedence* argument is in the range of 0 to 7.

Usage guidelines

To use two rates for traffic policing, configure the **car** command with the **pir** *peak-information-rate* option. To use one rate for traffic policing, configure the **car** command without the **pir** *peak-information-rate* option.

If you execute the **car** command multiple times in the same traffic behavior, the most recent configuration takes effect.

Examples

Configure a CAR action in traffic behavior **database**:

- Set the CIR to 200 kbps, CBS to 51200 bytes, and EBS to 0.
- Transmit the conforming packets, and mark the excess packets with DSCP value 0 and transmit them.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] car cir 200 cbs 51200 ebs 0 green pass red remark-dscp-pass
0
```

car percent

Use **car percent** to configure a CAR action in percentage in a traffic behavior.

Use **undo car** to restore the default.

Syntax

car cir percent *cir-percent* [**cbs** *cbs-time* [**ebs** *ebs-time*]] [**green** *action* | **red** *action* | **yellow** *action*] *

car cir percent *cir-percent* [**cbs** *cbs-time*] **pir percent** *pir-percent* [**ebs** *ebs-time*] [**green** *action* | **red** *action* | **yellow** *action*] *

undo car

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	No
NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280	Yes

Default

No percentage-based CAR action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

context-admin

Parameters

cir percent *cir-percent*: Specifies the CIR in percentage, in the range of 1 to 100. The actual CIR value is *cir-percent* × interface bandwidth.

cbs *cbs-time*: Specifies the CBS in milliseconds. The actual CBS value is *cbs-time* × the actual CIR value. The value range for the *cbs-time* argument is 50 to 2000. The default CBS is 500.

ebs *ebs-time*: Specifies the EBS in milliseconds. The actual EBS value is *ebs-time* × the actual CIR value. The value range for the *ebs-time* argument is 0 to 2000. The default EBS is 0.

pir percent *pir-percent*: Specifies the PIR in percentage, in the range of 1 to 100. The PIR value must be greater than or equal to the CIR value.

green *action*: Specifies the action to take on packets that conform to the CIR. The default is **pass**.

red *action*: Specifies the action to take on packets that conform to neither CIR nor PIR. The default is **discard**.

yellow *action*: Specifies the action to take on packets that conform to the PIR but not to the CIR. The default is **pass**.

action: Sets the action to take on the packet:

- **discard**: Drops the packet.
- **pass**: Permits the packet to pass through.
- **remark-dot1p-pass** *new-cos*: Sets the 802.1p priority value of the packet to *new-cos* and permits the packet to pass through. The *new-cos* argument is in the range of 0 to 7.
- **remark-dscp-pass** *new-dscp*: Sets the DSCP value of the packet to *new-dscp* and permits the packet to pass through. The *new-dscp* argument is in the range of 0 to 63. Alternatively, you can specify the *new-dscp* argument with **af11**, **af12**, **af13**, **af21**, **af22**,

af23, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, **default**, or **ef**.

- **remark-mpls-exp-pass** *new-exp*: Sets the EXP field value of the MPLS packet to *new-exp* and permits the packet to pass through. The *new-exp* argument is in the range of 0 to 7.
- **remark-prec-pass** *new-precedence*: Sets the IP precedence of the packet to *new-precedence* and permits the packet to pass through. The *new-precedence* argument is in the range of 0 to 7.

Usage guidelines

To use two rates for traffic policing, configure the **car percent** command with the **pir percent** *pir-percent* option. To use one rate for traffic policing, configure the **car percent** command without the **pir percent** *pir-percent* option.

A QoS policy that uses a traffic behavior configured with percentage-based CAR can be applied in the inbound or outbound direction of an interface.

If you execute the **car percent** command multiple times in the same traffic behavior, the most recent configuration takes effect.

A QoS policy that uses a behavior configured with percentage-based CAR can be applied only to interfaces.

The actual CIR value is *cir-percent* × bandwidth. The actual PIR value is *pir-percent* × bandwidth. For a physical interface, the bandwidth is the actual interface bandwidth. For a virtual interface(for example, tunnel interface and Layer 3 aggregate interface), you must set its expected bandwidth (the default expected bandwidth is 0 kbps). For more information about the expected bandwidth, see Ethernet interface commands in *Interface Command Reference*. In the policy nesting case, the bandwidth used for the CIR and PIR calculations is determined by using the following rules:

- The top policy uses the interface bandwidth.

Examples

Configure a CAR action in percentage in traffic behavior **database**. The CAR parameters are as follows: CIR is 20% and CBS is 100 ms.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] car cir percent 20 cbs 100
```

display traffic behavior

Use **display traffic behavior** to display traffic behaviors.

Syntax

display traffic behavior user-defined [*behavior-name*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

user-defined: Specifies user-defined traffic behaviors.

behavior-name: Specifies a behavior by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a traffic behavior, this command displays all traffic behaviors.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the traffic behaviors for the master device.

Examples

Display all user-defined traffic behaviors.

```
<Sysname> display traffic behavior user-defined

  User-defined behavior information:

    Behavior: 1 (ID 100)
      Committed Access Rate:
        CIR 2222 (kbps), CBS 22222222 (Bytes), EBS 0 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
```

Table 3 Command output

Field	Description
Behavior	Name and contents of a traffic behavior.
Committed Access Rate	Information about the CAR action.
Green action	Action to take on green packets.
Yellow action	Action to take on yellow packets.
Red action	Action to take on red packets.

filter

Use **filter** to configure a traffic filtering action in a traffic behavior.

Use **undo filter** to restore the default.

Syntax

filter { **deny** | **permit** }

undo filter

Default

No traffic filtering action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

context-admin

Parameters

deny: Drops packets.

permit: Transmits packets.

Examples

Configure a traffic filtering action as **deny** in traffic behavior **database**.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] filter deny
```

gts

Use **gts** to configure a GTS action in absolute value in a traffic behavior.

Use **undo gts** to restore the default.

Syntax

gts cir *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**queue-length** *queue-length*]

undo gts

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	No

Default

No GTS action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

context-admin

Parameters

cir *committed-information-rate*: Sets the CIR in kbps, which specifies the average traffic rate. The value range for *committed-information-rate* is 8 to 10000000.

cbs *committed-burst-size*: Sets the CBS in bytes, which specifies the size of bursty traffic when the actual average rate is not greater than the CIR. The value range for *committed-burst-size* is 1000 to 1000000000. The default CBS is the product of 62.5 and the CIR.

ebs *excess-burst-size*: Sets the EBS in bytes. The value range for *excess-burst-size* is 0 to 1000000000. The default EBS is 0.

queue-length *queue-length*: Sets the maximum number of packets allowed in the queue. The default is 50. The value range for *queue-length* is 1 to 1024.

Usage guidelines

A QoS policy that uses a behavior configured with GTS can be applied only to the outbound direction of an interface.

A QoS policy that uses a behavior configured with GTS overwrites the **qos gts** command on the interface, if both are configured.

If you execute the **gts** command multiple times in the same traffic behavior, the most recent configuration takes effect.

To use two rates for traffic shaping, configure the **gts** command with the **pir** *peak-information-rate* option. To use one rate for traffic shaping, configure the **gts** command without the **pir** *peak-information-rate* option.

Examples

Configure a GTS action in absolute value in traffic behavior **database**. The GTS parameters are as follows: CIR is 200 kbps, CBS is 51200 bytes, EBS is 0, and the maximum queue length is 100.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] gts cir 200 cbs 51200 ebs 0 queue-length 100
```

Related commands

gts percent

gts percent

Use **gts percent** to configure a GTS action in percentage in a traffic behavior.

Use **undo gts** to restore the default.

Syntax

gts percent cir *cir-percent* [**cbs** *cbs-time* [**ebs** *ebs-time*]] [**queue-length** *queue-length*]

undo gts

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	No

Default

No percentage-based GTS action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

context-admin

Parameters

cir *cir-percent*: Specifies the CIR in percentage, in the range of 1 to 100. The actual CIR value is *cir-percent* × interface bandwidth.

cbs *cbs-time*: Specifies the CBS in milliseconds. The default *cbs-time* is 500 milliseconds. The actual CBS value is *cbs-time* × the actual CIR value. The value range for *cbs-time* is 50 to 2000. The default CBS is 500.

ebs *ebs-time*: Specifies the EBS in milliseconds. The default *ebs-time* is 0 milliseconds. The actual EBS value is *ebs-time* × the actual CIR value. The value range for *ebs-time* is 0 to 2000. The default EBS is 0.

queue-length *queue-length*: Specifies the maximum number of packets allowed in the queue. The default is 50. The value range for *queue-length* is 1 to 1024.

Usage guidelines

A QoS policy that uses a behavior configured with percentage-based GTS can be applied only to the outbound direction of an interface.

A QoS policy that uses a behavior configured with percentage-based GTS overwrites the **qos gts** command on the interface, if both configured.

If you execute the **gts percent** command multiple times in the same traffic behavior, the most recent configuration takes effect.

Examples

Configure a GTS action in percentage in traffic behavior **database**. The GTS parameters are as follows: CIR is 50 and CBS is 200 ms.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] gts percent cir 50 cbs 200
```

Related commands

gts

remark dot1p

Use **remark dot1p** to configure an 802.1p priority marking action or an inner-to-outer tag priority copying action in a traffic behavior.

Use **undo remark dot1p** to restore the default.

Syntax

remark dot1p *dot1p-value*

undo remark dot1p

Default

No 802.1p priority marking or inner-to-outer tag priority copying action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

context-admin

Parameters

dot1p-value: Specifies the 802.1p priority to be marked for packets, in the range of 0 to 7.

Examples

Configure traffic behavior **database** to mark matching traffic with 802.1p 2.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark dot1p 2
```

remark dscp

Use **remark dscp** to configure a DSCP marking action in a traffic behavior.

Use **undo remark dscp** to restore the default.

Syntax

remark dscp *dscp-value*

undo remark dscp

Default

No DSCP marking action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

context-admin

Parameters

dscp-value: Specifies a DSCP value, which can be a number from 0 to 63 or a keyword in Table 4.

Table 4 DSCP keywords and values

Keyword	DSCP value (binary)	DSCP value (decimal)
af11	001010	10
af12	001100	12
af13	001110	14
af21	010010	18
af22	010100	20
af23	010110	22
af31	011010	26
af32	011100	28
af33	011110	30
af41	100010	34
af42	100100	36
af43	100110	38

Keyword	DSCP value (binary)	DSCP value (decimal)
cs1	001000	8
cs2	010000	16
cs3	011000	24
cs4	100000	32
cs5	101000	40
cs6	110000	48
cs7	111000	56
default	000000	0
ef	101110	46

Usage guidelines

If you execute the **remark dscp** command multiple times in the same traffic behavior, the most recent configuration takes effect.

Examples

Configure traffic behavior **database** to mark matching traffic with DSCP 6.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark dscp 6
```

remark flow-id

Use **remark flow-id** to configure a flow ID marking action in a traffic behavior.

Use **undo remark flow-id** to restore the default.

Syntax

remark flow-id *flow-id*

undo remark flow-id *flow-id*

The following compatibility matrix shows the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	No

Default

No flow ID marking action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

context-admin

Parameters

flow-id: Specifies a flow ID in the range of 1 to 65535.

Examples

Configure traffic behavior **behavior1** to mark matching traffic with flow ID 10.

```
<Sysname> system-view
[Sysname] traffic behavior behavior1
[Sysname-behavior-behavior1] remark flow-id 10
```

remark ip-precedence

Use **remark ip-precedence** to configure an IP precedence marking action in a traffic behavior.

Use **undo remark ip-precedence** to restore the default.

Syntax

remark ip-precedence *ip-precedence-value*

undo remark ip-precedence

Default

No IP precedence marking action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

context-admin

Parameters

ip-precedence-value: Specifies the IP precedence value to be marked for packets, in the range of 0 to 7.

Usage guidelines

If you execute the **remark ip-precedence** command multiple times in the same traffic behavior, the most recent configuration takes effect.

Examples

Set the IP precedence to 6 for packets.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark ip-precedence 6
```

remark local-precedence

Use **remark local-precedence** to configure a local precedence marking action in a traffic behavior.

Use **undo remark local-precedence** to restore the default.

Syntax

remark local-precedence *local-precedence-value*

undo remark local-precedence

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	No

Default

No local precedence marking action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

context-admin

Parameters

local-precedence-value: Specifies the local precedence to be marked for packets, in the range of 0 to 7.

Examples

Configure traffic behavior **database** to mark matching traffic with local precedence 2.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark local-precedence 2
```

remark qos-local-id

Use **remark qos-local-id** to configure a local QoS ID marking action in a traffic behavior.

Use **undo remark qos-local-id** to restore the default.

Syntax

remark qos-local-id *local-id-value*

undo remark qos-local-id

Default

No local QoS ID marking action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

context-admin

Parameters

local-id-value: Specifies the local QoS ID to be marked for packets, in the range of 1 to 4095.

Usage guidelines

You can use one QoS policy to mark the local QoS ID for packets in the inbound direction. Then, you can use another QoS policy to apply other QoS features in the outbound direction based on the marked local QoS ID.

If you execute the **remark qos-local-id** command multiple times in the same traffic behavior, the most recent configuration takes effect.

Examples

Configure the action of marking packets with local QoS ID 2.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark qos-local-id 2
```

traffic behavior

Use **traffic behavior** to create a traffic behavior and enter its view, or enter the view of an existing traffic behavior.

Use **undo traffic behavior** to delete a traffic behavior.

Syntax

traffic behavior *behavior-name*

undo traffic behavior *behavior-name*

Default

No traffic behaviors exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

behavior-name: Specifies a name for the traffic behavior, a case-sensitive string of 1 to 31 characters.

Examples

Create a traffic behavior named **behavior1**.

```
<Sysname> system-view
[Sysname] traffic behavior behavior1
[Sysname-behavior-behavior1]
```

Related commands

display traffic behavior

traffic-policy

Use **traffic-policy** to nest a policy in a traffic behavior.

Use **undo traffic-policy** to remove child policies from a traffic behavior.

Syntax

traffic-policy *policy-name*

undo traffic-policy

Default

No policy is nested in a traffic behavior.

Views

Traffic behavior view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies a policy by its name, a string of 1 to 31 characters. If the policy does not exist, it is automatically created.

Usage guidelines

After you nest a child policy in a behavior of a parent policy, the system performs the following operations:

- Performs the associated behavior defined in the parent policy for a class of traffic.
- Uses the child policy to further classify the class of traffic and performs the behaviors defined in the child policy.
- Policy nesting is available for IPv4 and IPv6 packets.
- To delete the child policy after you apply the parent policy to an interface, first remove the child policy from the parent policy.

Examples

Nest child policy **child** in traffic behavior **database** of the parent policy.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] traffic-policy child
```

Related commands

traffic behavior

traffic classifier

QoS policy commands

classifier behavior

Use **classifier behavior** to associate a traffic behavior with a traffic class in a QoS policy.

Use **undo classifier** to delete a class-behavior association from a QoS policy.

Syntax

classifier *classifier-name* **behavior** *behavior-name* [**insert-before** *before-classifier-name*]

undo classifier *classifier-name*

Default

No traffic behavior is associated with a traffic class.

Views

QoS policy view

Predefined user roles

network-admin

context-admin

Parameters

classifier-name: Specifies a traffic class by its name, a case-sensitive string of 1 to 31 characters.

behavior-name: Specifies a traffic behavior by its name, a case-sensitive string of 1 to 31 characters.

insert-before *before-classifier-name*: Inserts the new traffic class before an existing traffic class in the QoS policy. The *before-classifier-name* argument specifies an existing traffic class by its name, a case-sensitive string of 1 to 31 characters. If you do not specify the **insert-before** *before-classifier-name* option, the new traffic class is placed at the end of the QoS policy.

Usage guidelines

A traffic class can be associated only with one traffic behavior in a QoS policy.

If the specified traffic class or traffic behavior does not exist, the system defines a null traffic class or traffic behavior.

The **undo classifier default-class** command performs the following operations:

- Deletes the existing class-behavior association for the system-defined class **default-class**.
- Associates the system-defined class **default-class** with the system-defined behavior **be**.

Examples

Associate traffic class **database** with traffic behavior **test** in QoS policy **user1**.

```
<Sysname> system-view
[Sysname] qos policy user1
[Sysname-qospolicy-user1] classifier database behavior test
```

Associate traffic class **database** with traffic behavior **test** in QoS policy **user1**, and insert traffic class **database** before an existing traffic class named **class-a**.

```
<Sysname> system-view
[Sysname] qos policy user1
[Sysname-qospolicy-user1] classifier database behavior test insert-before class-a
```

Related commands

qos policy

control-plane

Use **control-plane** to enter control plane view.

Syntax

control-plane slot *slot-number*

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID.

Examples

Enter the control plane view of slot 3.

```
<Sysname> system-view
[Sysname] control-plane slot 3
[Sysname-cp-slot3]
```

control-plane management

Use **control-plane management** to enter control-plane management view.

Syntax

control-plane management

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

A QoS policy applied in control-plane management view takes effect on the packets sent from the management interface to the control plane.

Examples

Enter control-plane management view.

```
<Sysname> system-view
[Sysname] control-plane management
[Sysname-cp-management]
```

display qos policy

Use **display qos policy** to display QoS policies.

Syntax

display qos policy user-defined [*policy-name* [**classifier** *classifier-name*]] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

user-defined: Specifies user-defined QoS policies.

policy-name: Specifies a QoS policy by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a QoS policy, this command displays all user-defined QoS policies.

classifier *classifier-name*: Specifies a traffic class by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a traffic class, this command displays all traffic classes.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the QoS policies for the master device.

Examples

Display all user-defined QoS policies.

```
<Sysname> display qos policy user-defined

  User-defined QoS policy information:

  Policy: 1 (ID 100)
   Classifier: 1 (ID 100)
     Behavior: 1
      Marking:
        Remark dscp 3
      Committed Access Rate:
        CIR 112 (kbps), CBS 51200 (Bytes), EBS 512 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
   Classifier: 2 (ID 101)
     Behavior: 2
      Filter enable: Permit
   Classifier: 3 (ID 102)
     Behavior: 3
      -none-
```

Table 5 Command output

Field	Description
User-defined QoS policy information	Information about a user-defined QoS policy.
System-defined QoS policy information	Information about a system-defined QoS policy.
Policy	User-defined QoS policy name.

For the description of other fields, see Table 1 and Table 3.

display qos policy advpn

Use **display qos policy advpn** to display QoS policies applied to hub-spoke tunnels on a tunnel interface.

Syntax

display qos policy advpn tunnel *number* [*ipv4-address* | *ipv6-address*] [**outbound**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

number: Specifies a tunnel interface by its number. The value range for the *number* argument is 0 to 1023.

ipv4-address: Specifies the spoke's private IPv4 address of a hub-spoke tunnel.

ipv6-address: Specifies the spoke's private IPv6 address of a hub-spoke tunnel.

outbound: Specifies the QoS policies applied to the outbound direction.

Usage guidelines

If you do not specify a spoke's private IP address of a hub-spoke tunnel, this command displays the QoS policy information for all hub-spoke tunnels on a tunnel interface. For information about hub-spoke tunnels, see ADVPN in *VPN Configuration Guide*.

For configuration commands for tunnel interfaces, see tunnel commands in *Layer 3—IP Services Command Reference*.

Examples

Display the QoS policy applied to the outgoing traffic of all hub-spoke tunnels on tunnel interface 1.

```
<Sysname> display qos policy advpn tunnel 1 outbound
Session: Tunnel1 192.168.0.3
  Direction: Outbound
  Policy: finance
   Classifier: default-class
     Matched : 0 (Packets) 0 (Bytes)
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: be
      -none-
   Classifier: finance
     Matched : 123713988 (Packets) 13608538380 (Bytes)
     Operator: AND
     Rule(s) :
      If-match any
```

```
    Behavior: finance
     Committed Access Rate:
       CIR 1500 (kbps), CBS 93750 (Bytes), EBS 0 (Bytes)
       Green action  : pass
       Yellow action : pass
       Red action    : discard
       Green packets : 14980239 (Packets) 1647826290 (Bytes)
       Yellow packets: 0 (Packets) 0 (Bytes)
       Red packets   : 108733781 (Packets) 11960715910 (Bytes)

Session: Tunnel1 192.168.0.4 (inactive)
  Direction: Outbound
  Policy: business
```

Table 6 Command output

Field	Description
Session	Hub-spoke tunnel information. A hub-spoke tunnel is uniquely identified by a tunnel interface and the spoke's private IPv4 or IPv6 address. The word **inactive** indicates that a QoS policy fails to be applied to the hub-spoke tunnel or the applied QoS policy does not exist.
Direction	Direction to which a QoS policy is applied on the hub-spoke tunnel.

For the description of other fields, see Table 1 and Table 3.

display qos policy control-plane

Use **display qos policy control-plane** to display QoS policies applied to a control plane.

Syntax

display qos policy control-plane slot *slot-number*

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID.

Examples

Display the QoS policy applied to the control plane of slot 1.

```
<Sysname> display qos policy control-plane slot 1

Control plane slot 1

  Direction: Inbound
```

```
Policy: 1
 Classifier: 1
   Operator: AND
   Rule(s) :
    If-match acl 2000
   Behavior: 1
    Marking:
      Remark dscp 3
    Committed Access Rate:
      CIR 112 (kbps), CBS 51200 (Bytes), EBS 512 (Bytes)
      Green action  : pass
      Yellow action : pass
      Red action    : discard
      Green packets : 0 (Packets) 0 (Bytes)
      Yellow packets: 0 (Packets) 0 (Bytes)
      Red packets   : 0 (Packets) 0 (Bytes)
 Classifier: 2
   Operator: AND
   Rule(s) :
    If-match protocol ipv6
   Behavior: 2
    Filter enable: Permit
    Marking:
      Remark dscp 3
 Classifier: 3
   Operator: AND
   Rule(s) :
    -none-
   Behavior: 3
    -none-
```

Table 7 Command output

Field	Description
Direction	Direction in which the QoS policy is applied.
Green packets	Statistics about green packets.
Yellow packets	Statistics about yellow packets.
Red packets	Statistics about red packets.

For the description of other fields, see Table 1 and Table 3.

display qos policy control-plane management pre-defined

Use **display qos policy control-plane management pre-defined** to display the predefined QoS policy applied in control-plane management view.

Syntax

display qos policy control-plane management pre-defined

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display the predefined QoS policy applied in control-plane management view.

```
<Sysname> display qos policy control-plane management pre-defined
Pre-defined control plane policy management
  Protocol          Priority   Bandwidth                Group
  Default           N/A        100000 (bps)            N/A
  ARP               N/A        128 (bps)               normal
  BGP               N/A        256 (bps)               critical
  BGPv6             N/A        256 (bps)               critical
  HTTP              N/A        512 (bps)               management
  HTTPS             N/A        512 (bps)               management
  ICMP              N/A        128 (bps)               monitor
  ICMPv6            N/A        128 (bps)               monitor
  OSPF Multicast    N/A        256 (bps)               critical
  OSPF Unicast      N/A        256 (bps)               critical
  OSPFv3 Multicast  N/A        256 (bps)               critical
  OSFPv3 Unicast    N/A        256 (bps)               critical
  RIP               N/A        1024 (bps)              critical
  RIPng             N/A        256 (bps)               critical
  SNMP              N/A        512 (bps)               management
  SSH               N/A        512 (bps)               management
  TELNET            N/A        512 (bps)               management
  FTP               N/A        512 (bps)               management
  TFTP              N/A        512 (bps)               management
```

Table 8 Command output

Field	Description
Pre-defined control plane policy management	Predefined QoS policy applied in control-plane management view.
Protocol	System-defined protocol packet type.
Group	Protocol group to which the protocol belongs.

display qos policy control-plane pre-defined

Use **display qos policy control-plane pre-defined** to display predefined control plane QoS policies.

Syntax

display qos policy control-plane pre-defined [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays predefined control plane QoS policies for all member devices.

Examples

Display the predefined control plane QoS policy of slot 1.

```
<Sysname> display qos policy control-plane pre-defined slot 1
Pre-defined policy information slot 1
  Protocol          Priority   Bandwidth (kbps)   Group
  Default           N/A        100000             N/A
  ARP               N/A        100000             normal
  BGP               N/A        100000             critical
  BGPv6             N/A        100000             critical
  HTTP              N/A        100000             management
  HTTPS             N/A        100000             management
  ICMP              N/A        100000             monitor
  ICMPv6            N/A        100000             monitor
  IGMP              N/A        100000             important
  IS-IS             N/A        100000             critical
  LDP               N/A        100000             critical
  LDPv6             N/A        100000             critical
  MSDP              N/A        100000             critical
  NTP               N/A        100000             important
  OSPF Multicast    N/A        100000             critical
  OSPF Unicast      N/A        100000             critical
  OSPFv3 Multicast  N/A        100000             critical
  OSPFv3 Unicast    N/A        100000             critical
  PIM Multicast     N/A        100000             critical
  PIM Unicast       N/A        100000             critical
  PIMv6 Multicast   N/A        100000             critical
  PIMv6 Unicast     N/A        100000             critical
  RADIUS            N/A        100000             management
  RIP               N/A        100000             critical
  RIPng             N/A        100000             critical
  RSVP              N/A        100000             critical
  SNMP              N/A        100000             management
  TACACS            N/A        100000             management
  VRRP              N/A        100000             important
  VRRPv6            N/A        100000             important
```

```
SSH                 N/A         100000              management
TELNET              N/A         100000              management
FTP                 N/A         100000              management
TFTP                N/A         100000              management
```

Table 9 Command output

Field	Description
Pre-defined control plane policy	Contents of the predefined control plane QoS policy.
Group	Protocol group of the protocol.

display qos policy interface

Use **display qos policy interface** to display the QoS policies applied to interfaces.

Syntax

display qos policy interface [*interface-type interface-number*] [**slot** *slot-number*] [**inbound** | **outbound**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays QoS policies applied to all interfaces except VA interfaces. For information about VA interfaces, see PPP in *Layer 2—WAN Access Configuration Guide*.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify an IRF member device, this command displays QoS policies on the master device. Only logical interfaces support this option.

inbound: Specifies the QoS policy applied to incoming traffic.

outbound: Specifies the QoS policy applied to outgoing traffic.

Usage guidelines

If you do not specify a direction, this command displays the QoS policy applied to incoming traffic and the QoS policy applied to outgoing traffic.

If you specify a VT interface, this command displays the QoS policies applied to each VA interface of the VT interface. It does not display QoS information about the VT interface.

Examples

Display the QoS policy applied to the incoming traffic of GigabitEthernet 1/0/1.

```
<Sysname> display qos policy interface gigabitethernet 1/0/1 inbound
Interface: GigabitEthernet1/0/1
  Direction: Inbound
```

```
  Policy: 1
   Classifier: 1
     Matched : 0 (Packets) 0 (Bytes)
     5-minute statistics:
      Forwarded: 0/0 (pps/bps)
      Dropped  : 0/0 (pps/bps)
     Operator: AND
     Rule(s) :
      If-match acl 2000
     Behavior: 1
      Marking:
        Remark dscp 3
      Committed Access Rate:
        CIR 112 (kbps), CBS 51200 (Bytes), EBS 512 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0 (Packets) 0 (Bytes)
        Yellow packets: 0 (Packets) 0 (Bytes)
        Red packets   : 0 (Packets) 0 (Bytes)
   Classifier: 2
     Matched : 0 (Packets) 0 (Bytes)
     5-minute statistics:
      Forwarded: 0/0 (pps/bps)
      Dropped  : 0/0 (pps/bps)
     Operator: AND
     Rule(s) :
      If-match protocol ipv6
     Behavior: 2
      Filter enable: Permit

   Classifier: 3
     Matched : 0 (Packets) 0 (Bytes)
     5-minute statistics:
      Forwarded: 0/0 (pps/bps)
      Dropped  : 0/0 (pps/bps)
     Operator: AND
     Rule(s) :
      -none-
     Behavior: 3
      -none-
```

Display the QoS policies applied to all interfaces.

```
<Sysname> display qos policy interface
Interface: GigabitEthernet1/0/1
  Direction: Inbound
  Policy: a
   Classifier: a
     Operator: AND
```

```
    Rule(s) :
     If-match any
    Behavior: a
     Committed Access Rate:
       CIR 112 (kbps), CBS 51200 (Bytes), EBS 0 (Bytes)
       Green action  : pass
       Yellow action : pass
       Red action    : discard
       Green packets : 0 (Packets)
       Red packets   : 0 (Packets)
Interface: GigabitEthernet1/0/3
  Direction: Inbound
  Policy: b
   Classifier: b
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: b
      Committed Access Rate:
        CIR 112 (kbps), CBS 51200 (Bytes), EBS 0 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0(Packets)
        Red packets   : 0 (Packets)
Interface: GigabitEthernet1/0/3
  Direction: Inbound
  Policy: a
   Classifier: a
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: a
      Committed Access Rate:
        CIR 112 (kbps), CBS 51200 (Bytes), EBS 0 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0 (Packets)
        Red packets   : 0 (Packets)
```

Table 10 Command output

Field	Description
Direction	Direction in which the QoS policy is applied.
Policy	User-defined QoS policy name or system-defined QoS policy name.
Matched	Number of matching packets.

Field	Description
Forwarded	Average rate of successfully forwarded matching packets in a statistics collection period.
Dropped	Average rate of dropped matching packets in a statistics collection period.
Green packets	Traffic statistics for green packets.
Yellow packets	Traffic statistics for yellow packets.
Red packets	Traffic statistics for red packets.

For the description of other fields, see Table 1, Table 3, and Table 5.

qos apply policy (interface view, control plane view, control-plane management view)

Use **qos apply policy** to apply a QoS policy to an interface or control plane.

Use **undo qos apply policy** to remove an applied QoS policy.

Syntax

qos apply policy *policy-name* { **inbound** | **outbound** }

undo qos apply policy *policy-name* { **inbound** | **outbound** }

Default

No QoS policy is applied.

Views

Control plane view

Control-plane management view

Interface view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies a QoS policy by its name, a case-sensitive string of 1 to 31 characters.

inbound: Applies the QoS policy to incoming traffic.

outbound: Applies the QoS policy to outgoing traffic.

Usage guidelines

When you apply a QoS policy to an interface, follow these rules:

- The bandwidth assigned to AF and EF queues in the QoS policy must be smaller than the available bandwidth of the interface. Otherwise, the QoS policy cannot be successfully applied to the interface.
- If you modify the available bandwidth of the interface to be smaller than the bandwidth for AF and EF queues, the applied QoS policy is removed.

A QoS policy configured with CBQ is not supported in control plane view or control-plane management view.

Examples

Apply QoS policy **USER1** to the incoming traffic of GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos apply policy USER1 inbound
```

qos policy

Use **qos policy** to create a QoS policy and enter its view, or enter the view of an existing QoS policy.

Use **undo qos policy** to delete a QoS policy.

Syntax

qos policy *policy-name*

undo qos policy *policy-name*

Default

No QoS policies exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies a name for the QoS policy, a case-sensitive string of 1 to 31 characters.

Usage guidelines

To delete a QoS policy that has been applied to an object, you must first remove the QoS policy from the object.

Examples

Create a QoS policy named **user1**.

```
<Sysname> system-view
[Sysname] qos policy user1
[Sysname-qospolicy-user1]
```

Related commands

classifier behavior

qos apply policy

reset qos policy advpn

Use **reset qos policy advpn** to clear the statistics for QoS policies applied to hub-spoke tunnels on a tunnel interface.

Syntax

reset qos policy advpn tunnel *number* [*ipv4-address* | *ipv6-address*] [**outbound**]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

number: Specifies a tunnel interface by its number. The value range for the *number* argument is 0 to 1023.

ipv4-address: Specifies the spoke's private IPv4 address of a hub-spoke tunnel.

ipv6-address: Specifies the spoke's private IPv6 address of a hub-spoke tunnel.

outbound: Specifies the QoS policies applied to the outbound direction.

Usage guidelines

If you do not specify a spoke's private IP address of a hub-spoke tunnel, this command clears the QoS policy statistics for all hub-spoke tunnels on a tunnel interface. For information about hub-spoke tunnels, see ADVPN in *VPN Configuration Guide*.

For configuration commands for tunnel interfaces, see tunnel commands in *VPN Command Reference*.

Examples

Clear the statistics for the QoS policy applied to the outgoing traffic of the hub-spoke tunnel with spoke's IPv4 address 192.168.0.3 on tunnel interface 1.

```
<Sysname> reset qos policy advpn tunnel 1 192.168.0.3 outbound
```

reset qos policy control-plane

Use **reset qos policy control-plane** to clear the statistics of the QoS policy applied to a control plane.

Syntax

reset qos policy control-plane slot *slot-number*

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID.

Examples

Clear the statistics of the QoS policy applied to the control plane of slot 1.

```
<Sysname> reset qos policy control-plane slot 1
```

Clear the statistics of the QoS policy applied to the control plane of slot 3 in chassis 1.

```
<Sysname> reset qos policy control-plane chassis 1 slot 3
```

QoS policy-based traffic rate statistics collection period commands

qos flow-interval

Use **qos flow-interval** to set the QoS policy-based traffic rate statistics collection period for an interface.

Use **undo qos flow-interval** to restore the default.

Syntax

qos flow-interval *interval*

undo qos flow-interval

Default

The QoS policy-based traffic rate statistics collection period is 5 minutes on an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

interval: Sets the QoS policy-based traffic rate statistics collection period in minutes. The value range for this argument is 1 to 10.

Usage guidelines

You can enable collection of per-class traffic statistics over a period of time, including the average forwarding rate and drop rate. For example, if you set the statistics collection period to 10 minutes, the system performs the following operations:

- Collects traffic statistics for the most recent 10 minutes.
- Refreshes the statistics every 10/5 minutes, 2 minutes.

The traffic rate statistics collection period of a subinterface is the same as the period configured on the main interface.

Examples

Set the QoS policy-based traffic rate statistics collection period to 10 minutes on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos flow-interval 10
```

Related commands

display qos policy interface

Traffic policing commands

Traffic policing commands

display qos car interface

Use **display qos car interface** to display the CAR configuration and statistics for interfaces.

Syntax

display qos car interface [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays the CAR configuration and statistics for all interfaces except VA interfaces. For information about VA interfaces, see PPP in *Layer 2—WAN Access Configuration Guide*.

Usage guidelines

If you specify a VT interface, this command displays the CAR configuration and statistics of each VA interface of the VT interface. It does not display QoS information about the VT interface.

Examples

Display the CAR configuration and statistics for GigabitEthernet 1/0/1.

```
<Sysname> display qos car interface gigabitethernet 1/0/1
Interface: GigabitEthernet1/0/1
 Direction: inbound
  Rule: If-match any
   CIR 128 (kbps), CBS 5120 (Bytes), PIR 128 (kbps), EBS 512 (Bytes)
   Green action  : pass
   Yellow action : pass
   Red action    : discard
   Green packets : 0 (Packets), 0 (Bytes)
   Yellow packets: 0 (Packets), 0 (Bytes)
   Red packets   : 0 (Packets), 0 (Bytes)
```

Display the CAR information on GigabitEthernet 1/0/2.

```
<Sysname> display qos car interface gigabitethernet 1/0/2
Interface: GigabitEthernet1/0/2
 Direction: inbound
  Rule: If-match any
```

```
CIR 50 (%), CBS 600 (ms), EBS 0 (ms), PIR 50 (%)
Green action  : pass
Yellow action : pass
Red action    : discard
Green packets : 0 (Packets), 0 (Bytes)
Yellow packets: 0 (Packets), 0 (Bytes)
Red packets   : 0 (Packets), 0 (Bytes)
```

Table 11 Command output

Field	Description
Interface	Interface name, including interface type and interface number.
Direction	Direction in which traffic policing is applied.
Rule	Match criteria.
CIR	CIR in kbps.
CBS	CBS in bytes.
EBS	EBS in bytes.
PIR	PIR in kbps.
Green action	Action to take on green packets.
Yellow action	Action to take on yellow packets.
Red action	Action to take on red packets.
Overhead compensation length	Packet compensation length in bytes for outbound traffic policing.
Online session count	Number of current online sessions.
Current CIR	CIR in kbps after dynamic adjustment.
Current bandwidth	The actual total traffic rate in kbps for all online sessions. This value might be greater than the current CIR multiplied by the number of current online sessions.
Bandwidth utilization threshold	Maximum bandwidth threshold in kbps. • If the **bandwidth** command is not executed on the interface, this value is the actual interface bandwidth multiplied by the maximum bandwidth percentage. • If the **bandwidth** command is executed on the interface, this value is the configured interface bandwidth multiplied by the maximum bandwidth percentage.

Related commands

bandwidth (*Interface Command Reference*)

qos car (interface view)

qos carl

display qos carl

Use **display qos carl** to display CAR lists.

Syntax

display qos carl [*carl-index*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

carl-index: Specifies a CAR list by its number in the range of 1 to 199. If you do not specify a CAR list, this command displays all CAR lists.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the CAR lists for the master device.

Examples

Display all CAR lists.

```
<Sysname> display qos carl
List  Rules
1     destination-ip-address range 1.1.1.1 to 1.1.1.2 per-address shared-bandwidth
2     destination-ip-address subnet 1.1.1.1 22 per-address shared-bandwidth
4     dscp 1 2 3 4 5 6 7 cs1
5     mac 0000-0000-0000
6     mpls-exp 0 1 2
9     precedence 0 1 2 3 4 5 6 7
10    source-ip-address range 1.1.1.1 to 1.1.1.2
11    source-ip-address subnet 1.1.1.1 31
```

qos car

Use **qos car** to configure a CAR policy on an interface.

Use **undo qos car** to delete a CAR policy from an interface.

Syntax

qos car { **inbound** | **outbound** } { **any** | **acl** [**ipv6**] *acl-number* | **carl** *carl-index* } **cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**green** *action* | **red** *action* | **yellow** *action*] *

qos car { **inbound** | **outbound** } { **any** | **acl** [**ipv6**] *acl-numbe*r | **carl** *carl-index* } **cir** *committed-information-rate* [**cbs** *committed-burst-size*] **pir** *peak-information-rate* [**ebs** *excess-burst-size*] [**green** *action* | **red** *action* | **yellow** *action*] *

undo qos car { **inbound** | **outbound** } { **any** | **acl** [**ipv6**] *acl-number* | **carl** *carl-index* }

Default

No CAR policy is configured.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

inbound: Performs CAR for incoming packets on the interface.

outbound: Performs CAR for outgoing packets on the interface.

any: Performs CAR for all IP packets in the specified direction.

acl [**ipv6**] *acl-number*: Performs CAR for packets matching an ACL specified by its number. The value range for the *acl-number* argument is 2000 to 2999 for basic ACLs and 3000 to 3999 for advanced ACLs. If you do not specify **ipv6**, this option specifies an IPv4 ACL. If you specify **ipv6**, this option specifies an IPv6 ACL.

carl *carl-index*: Performs CAR for packets matching a CAR list specified by its number in the range of 1 to 199.

cir *committed-information-rate*: Specifies the CIR in kbps. The value range for *committed-information-rate* is 8 to 10000000.

cbs *committed-burst-size*: Specifies the CBS in bytes, which is the size of bursty traffic when the actual average rate is not greater than the CIR. The value range for *committed-burst-size* is 1875 to 19375000. The default CBS is the product of 62.5 and the CIR.

ebs *excess-burst-size*: Specifies the EBS in bytes. The value range for *excess-burst-size* is 0 to 19375000. The default EBS is 0.

pir *peak-information-rate*: Specifies the PIR in kbps. The value range for *peak-information-rate* is 8 to 10000000.

green: Specifies the action to take on packets when the traffic rate conforms to the CIR. The default is **pass**.

red: Specifies the action to take on packets when the traffic rate conforms to neither CIR nor PIR. The default is **discard**.

yellow: Specifies the action to take on packets when the traffic rate exceeds the CIR but conforms to the PIR. The default is **pass**.

action: Specifies the action to take on packets:

- **continue**: Continues to process the packet by using the next CAR policy.
- **discard**: Drops the packet.
- **pass**: Permits the packet to pass through.
- **remark-dot1p-continue** *new-cos*: Sets the 802.1p priority value of the 802.1p packet to *new-cos* and continues to process the packet by using the next CAR policy. The *new-cos* argument is in the range of 0 to 7.
- **remark-dot1p-pass** *new-cos*: Sets the 802.1p priority value of the 802.1p packet to *new-cos* and permits the packet to pass through. The *new-cos* argument is in the range of 0 to 7.
- **remark-dscp-continue** *new-dscp*: Remarks the packet with a new DSCP value and continues to process the packet by using the next CAR policy. The *new-dscp* argument is in the range of 0 to 63. Alternatively, you can specify the *new-dscp* argument with **af11**, **af12**,

af13, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, **default**, or **ef**.

- **remark-dscp-pass** *new-dscp*: Remarks the packet with a new DSCP value and permits the packet to pass through. The *new-dscp* argument is in the range of 0 to 63. Alternatively, you can specify the *new-dscp* argument with **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, **default**, or **ef**.
- **remark-mpls-exp-continue** *new-exp*: Sets the EXP field value of the MPLS packet to *new-exp* and continues to process the packet by using the next CAR policy. The *new-exp* argument is in the range of 0 to 7.
- **remark-mpls-exp-pass** *new-exp*: Sets the EXP field value of the MPLS packet to *new-exp* and permits the packet to pass through. The *new-exp* argument is in the range of 0 to 7.
- **remark-prec-continue** *new-precedence*: Re-marks the packet with a new IP precedence and continues to process the packet by using the next CAR policy. The *new-precedence* argument is in the range of 0 to 7.
- **remark-prec-pass** *new-precedence*: Re-marks the packet with a new IP precedence and permits the packet to pass through. The *new-precedence* argument is in the range of 0 to 7.

Usage guidelines

To use two rates for traffic policing, configure the **qos car** command with the **pir** *peak-information-rate* option. To use one rate for traffic policing, configure the **qos car** command without the **pir** *peak-information-rate* option.

You can configure multiple **qos car** commands on an interface to define multiple CAR policies. These CAR policies are executed in their configuration order.

When you reference an ACL, follow these restrictions and guidelines:

- If the ACL does not exist or contains no rules, the ACL is not used to match packets.
- If the **vpn-instance** *vpn-instance* option is specified in a rule, the rule takes effect only on VPN packets. If the **vpn-instance** *vpn-instance* option is not specified in a rule, the rule takes effect on both VPN packets and non-VPN packets.

Dynamic traffic policing allows you to dynamically adjust the bandwidth allowed per IP address on an interface to improve bandwidth usage.

When the following conditions exist, the dynamic traffic policing feature is activated on an interface:

- A CAR list is used and he **per-address** parameter is specified in the CAR list.
- Only one CAR list-based CAR policy is applied to the same direction of an interface, and the **max-cir** parameter is specified.

Examples

Perform CAR for all packets in the outbound direction of GigabitEthernet 1/0/1. The CAR parameters are as follows:

- CIR is 200 kbps.
- CBS is 5120 bytes.
- EBS is 0.
- Conforming packets are transmitted.
- Excess packets are set with an IP precedence of 0 and transmitted.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] qos car outbound any cir 200 cbs 5000 ebs 0 green pass red
remark-prec-pass 0
```

Related commands

display qos car interface

qos carl

qos carl

Use **qos carl** to create or modify a CAR list.

Use **undo qos carl** to delete a CAR list.

Syntax

qos carl *carl-index* { **dscp** *dscp-list* | **mac** *mac-address* | **mpls-exp** *mpls-exp-value* | **precedence** *precedence-value* | { **destination-ip-address** | **source-ip-address** } { **range** *start-ip-address* **to** *end-ip-address* | **subnet** *ip-address mask-length* } [**per-address** [**shared-bandwidth**]] }

undo qos carl *carl-index*

Default

No CAR list is configured.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

carl-index: Specifies a CAR list by its number in the range of 1 to 199.

dscp *dscp-list*: Specifies a list of DSCP values. A DSCP value can be a number from 0 to 63 or any of the following keywords **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, **default**, or **ef**. You can configure up to eight DSCP values in one command line. If the same DSCP value is specified multiple times, the system considers the values to be one value. If a packet matches one of the defined DSCP values, it matches the **if-match** clause.

mac *mac-address*: Specifies a MAC address in hexadecimal format.

mpls-exp *mpls-exp-value*: Specifies an MPLS EXP value in the range of 0 to 7. You can configure up to eight MPLS EXP values in one command line. If the same MPLS EXP value is specified multiple times, the system considers the values to be one value. If a packet matches one of the defined MPLS EXP values, it matches the **if-match** clause.

precedence *precedence*: Specifies a precedence value in the range of 0 to 7. You can configure up to eight IP precedence values in one command line. If the same IP precedence value is specified multiple times, the system considers the values to be one value. If a packet matches one of the defined IP precedence values, it matches the **if-match** clause.

destination-ip-address: Configures a destination IP address-based CAR list.

source-ip-address: Configures a source IP address-based CAR list.

range *start-ip-address* **to** *end-ip-address*: Specifies an IP address range by the start address and end address. The value for *end-ip-address* must be greater than the value for *start-ip-address*.

subnet *ip-address mask-length*: Specifies a subnet by the IP subnet address and IP subnet address mask length. The value range for *mask-length* is 22 to 31.

per-address: Performs per-IP address rate limiting within the network segment. When this keyword is specified, the CIR is dedicated bandwidth for each IP address and is not shared by any other IP address. If you do not specify this keyword, the following events occur:

- Rate limiting is performed for the entire network segment.
- All of the CIR is allocated among all IP addresses in proportion to the traffic load of each IP address.

shared-bandwidth: Specifies that traffic of all IP addresses within the network segment shares the remaining bandwidth (the CIR). If you specify this keyword, all of the CIR is allocated evenly among all IP addresses with traffic load.

Usage guidelines

You can create a CAR list based on IP precedence, MAC address, MPLS EXP, DSCP, or IP network segment.

If you execute this command multiple times for the same CAR list, the most recent configuration takes effect. If you execute this command multiple times for different CAR lists, multiple CAR lists are created.

To perform rate limiting for a single IP address, use the **qos car acl** command in interface view.

Examples

Apply CAR list 1 to the outbound direction of GigabitEthernet 1/0/1 to meet the following requirements:

- The rate of each host on the subnet 1.1.1.0/24 is limited to 512 kbps.
- Traffic of IP addresses in the subnet does not share the remaining bandwidth.

```
<Sysname> system-view
[Sysname] qos carl 1 source-ip-address subnet 1.1.1.0 24 per-address
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos car outbound carl 1 cir 512 cbs 5120 ebs 0 green pass red discard
```

Apply CAR list 2 to the outbound direction of GigabitEthernet 1/0/1 to meet the following requirements:

- The rate of each host in the IP address range of 1.1.2.100 to 1.1.2.199 is limited to 5 Mbps.
- Traffic of IP addresses in the subnet shares the remaining bandwidth.

```
<Sysname> system-view
[Sysname] qos carl 2 source-ip-address range 1.1.2.100 to 1.1.2.199 per-address shared-bandwidth
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos car outbound carl 2 cir 5120 cbs 51200 ebs 51200 green pass red discard
```

Related commands

display qos carl

qos car

GTS commands

The following compatibility matrixes show the support of hardware platforms for GTS:

Models	GTS compatibility
NFNX5-HD6480, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	No

display qos gts interface

Use **display qos gts interface** to display the GTS configuration and statistics for interfaces.

Syntax

display qos gts interface [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays the GTS configuration and statistics for all interfaces except VA interfaces. For information about VA interfaces, see PPP in *Layer 2—WAN Access Configuration Guide*.

Usage guidelines

If you specify a VT interface, this command displays the GTS configuration and statistics of each VA interface of the VT interface. It does not display QoS information about the VT interface.

Examples

Display the GTS configuration and statistics for all interfaces.

```
<Sysname> display qos gts interface
Interface: GigabitEthernet1/0/1
 Rule: If-match acl 2001
  CIR 512 (kbps), CBS 51200 (Bytes), PIR 5120 (kbps), EBS 0 (Bytes)
  Queue Length: 100 (Packets)
  Queue Size: 70 (Packets)
  Passed   : 0 (Packets) 0 (Bytes)
  Discarded: 0 (Packets) 0 (Bytes)
  Delayed  : 0 (Packets) 0 (Bytes)

Interface: GigabitEthernet1/0/2
 Rule: If-match acl 2001
```

```
CIR 64 (kbps), CBS 51200 (Bytes), EBS 0 (Bytes)
Queue Length: 100 (Packets)
Queue Size: 70 (Packets)
Passed   : 0 (Packets) 0 (Bytes)
Discarded: 0 (Packets) 0 (Bytes)
Delayed  : 0 (Packets) 0 (Bytes)
```

Table 12 Command output

Field	Description
Interface	Interface name, including the interface type and interface number.
Rule	Match criteria.
CIR	CIR in kbps (if the CIR is specified in absolute value) or in percentage (if the CIR is specified in percentage).
CBS	CBS in bytes (if the CBS is specified in absolute value) or in ms (if the CBS is specified in milliseconds). When the CBS is specified in milliseconds, the actual CBS value is *cbs-time* × the actual CIR value.
EBS	EBS in bytes (if the EBS is specified in absolute value) or in ms (if the EBS is specified in milliseconds). When the EBS is specified in milliseconds, the actual EBS value is *ebs-time* × the actual CIR value.
PIR	PIR in kbps (if the PIR is specified in absolute value) or in percentage (if the PIR is specified in percentage).
Queue Length	Number of packets that the buffer can hold.
Queue Size	Number of packets in the buffer.
Passed	Number and bytes of packets that have been forwarded.
Discarded	Number and bytes of dropped packets.
Delayed	Number and bytes of delayed packets.

qos gts

Use **qos gts** to set GTS parameters on an interface.

Use **undo qos gts** to delete the GTS configuration on an interface.

Syntax

qos gts { **any** | **acl** [**ipv6**] *acl-number* } **cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**queue-length** *queue-length*]

undo qos gts { **any** | **acl** [**ipv6**] *acl-number* }

Default

No GTS parameters are configured.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

any: Shapes all packets.

acl [**ipv6**] *acl-number*: Performs GTS for packets matching an ACL specified by its number. The value range for the *acl-number* argument is 2000 to 3999 for basic ACLs and 3000 to 3999 for advanced ACLs. If you do not specify **ipv6**, this option specifies an IPv4 ACL. If you specify **ipv6**, this option specifies an IPv6 ACL.

cir *committed-information-rate*: Specifies the CIR in kbps. The value range for *committed-information-rate* is 8 to 32000000.

cbs *committed-burst-size*: Specifies the CBS in bytes. The value range for *committed-burst-size* is 512 to 1000000000. The default CBS is the product of 62.5 and the CIR.

ebs *excess-burst-size*: Specifies the EBS in bytes, which is the traffic exceeding CBS when two token buckets are used. The value range for *excess-burst-size* is 0 to 1000000000. The default EBS is 0.

queue-length *queue-length*: Specifies the maximum number of packets allowed in the queue. The value range for *queue-length* is 1 to 1024. The default is 50.

Usage guidelines

To use two rates for traffic shaping, configure the **qos gts** command with the **pir** *peak-information-rate* option. To use one rate for traffic shaping, configure the **qos gts** command without the **pir** *peak-information-rate* option.

When you reference an ACL, follow these restrictions and guidelines:

- If the ACL does not exist or contains no rules, the ACL is not used to match packets.
- If the **vpn-instance** *vpn-instance* option is specified in a rule, the rule takes effect only on VPN packets. If the **vpn-instance** *vpn-instance* option is not specified in a rule, the rule takes effect on both VPN packets and non-VPN packets.

Examples

Shape the packets matching ACL 2001 on GigabitEthernet 1/0/1. The GTS parameters are as follows:

- The CIR is 200 kbps.
- The CBS is 51200 bytes.
- The EBS is 0.
- The maximum buffer queue length is 100.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos gts acl 2001 cir 200 cbs 51200 ebs 0 queue-length 100
```

Rate limit commands

The following compatibility matrixes show the support of hardware platforms for rate limit:

Models	Rate limit compatibility
NFNX5-HD6480, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	No

display qos lr

Use **`display qos lr`** to display the rate limit configuration and statistics for interfaces.

Syntax

`display qos lr interface` [*`interface-type interface-number`*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

`interface-type interface-number`: Specifies an interface by its type and number. If you do not specify an interface, this command displays the rate limit configuration and statistics for all interfaces except VA interfaces. For information about VA interfaces, see PPP in *Layer 2—WAN Access Configuration Guide*.

Usage guidelines

If you specify a VT interface, this command displays the rate limit configuration and statistics of each VA interface of the VT interface. It does not display QoS information about the VT interface.

Examples

Display the rate limit configuration and statistics for all interfaces.

```
<Sysname> display qos lr interface
Interface: GigabitEthernet1/0/1
 Direction: Outbound
  CIR 2000 (kbps), CBS 20480 (Bytes), EBS 0 (Bytes)
  Passed   : 1000 (Packets) 1000 (Bytes)
  Discarded: 1000 (Packets) 1000 (Bytes)
  Delayed  : 1000 (Packets) 1000 (Bytes)
  Active shaping: No
Interface: GigabitEthernet1/0/2
 Direction: Outbound
  CIR 64 (kbps), CBS 512 (Bytes), EBS 0 (Bytes)
  Passed   : 1000 (Packets) 1000 (Bytes)
  Discarded: 1000 (Packets) 1000 (Bytes)
  Delayed  : 1000 (Packets) 1000 (Bytes)
  Active shaping: No
```

Table 13 Command output

Field	Description
Interface	Interface name, including the interface type and interface number.
Direction	Direction in which the rate limit configuration is applied.
CIR	CIR in kbps (if the CIR is specified in absolute value) or in percentage (if the CIR is specified in percentage).

Field	Description
CBS	CBS in bytes (if the CBS is specified in absolute value) or in ms (if the CBS is specified in milliseconds). When the CBS is specified in milliseconds, the actual CBS value is *cbs-time* × the actual CIR value.
EBS	EBS in bytes (if the EBS is specified in absolute value) or in ms (if the EBS is specified in milliseconds). When the EBS is specified in milliseconds, the actual EBS value is *ebs-time* × the actual CIR value.
Passed	Number and bytes of packets that have passed.
Discarded	Number and bytes of dropped packets.
Delayed	Number and bytes of delayed packets.
Active shaping	Indicates whether the rate limit configuration is activated: • **Yes**—Activated. • **No**—Not activated.

qos lr

Use **qos lr** to configure rate limiting on an interface.

Use **undo qos lr** to delete the rate limit configuration on an interface.

Syntax

qos lr outbound cir *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]]

undo qos lr outbound

Default

No rate limit is configured.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

outbound: Limits the rate of outgoing packets.

cir *committed-information-rate*: Specifies the CIR in kbps. The value range for *committed-information-rate* is 5 to 1000000.

cbs *committed-burst-size*: Specifies the CBS in the range of 100 to 100000 bytes. The default CBS is the product of 62.5 and the CIR.

ebs *excess-burst-size*: Specifies the EBS in bytes, which is the traffic exceeding CBS when two token buckets are used. The value range for *excess-burst-size* is 0 to 100000. The default is 0.

Examples

Limit the rate of outgoing packets on GigabitEthernet 1/0/1, with CIR 256 kbps and CBS 51200 bytes.

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos lr outbound cir 256 cbs 51200
```

qos overhead layer

Use **qos overhead layer physical** to include the physical layer header in calculating the packet length for rate limiting.

Use **undo qos overhead layer physical** to restore the default.

Syntax

qos overhead layer physical

undo qos overhead layer physical

Default

The device calculates the packet length for rate limiting based on the data link layer frame.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command allows the device to include a 24-byte physical layer header in calculating the packet length for rate limiting. As a best practice, configure this command in scenarios where packets are small and precise rate limiting is required. To save computing resources, do not configure this command if the device processes large packets.

This command takes effect only on Layer 3 Ethernet interfaces and Layer 3 aggregate interfaces.

Examples

Include the physical layer header in calculating the packet length for rate limiting.

```
<Sysname> system-view
[Sysname] qos overhead layer physical
```

Related commands

display qos lr

qos lr

qos lr percent

Contents

Time range commands

display time-range

Use **display time-range** to display time range configuration and status.

Syntax

display time-range { *time-range-name* | **all** }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

time-range-name: Specifies a time range name, a case-insensitive string of 1 to 32 characters.

all: Displays the configuration and status of all existing time ranges.

Examples

Display the configuration and status of time range **t4**.

```
<Sysname> display time-range t4
Current time is 17:12:34 11/23/2010 Tuesday

Time-range : t4 (Inactive)
 10:00 to 12:00 Mon
 14:00 to 16:00 Wed
 from 00:00:00 1/1/2011 to 00:00:00 1/1/2012
 from 00:00:00 6/1/2011 to 00:00:00 7/1/2011
```

Table 1 Command output

Field	Description
Current time	Current system time.
Time-range	Configuration and status of the time range, including its name, status (active or inactive), and start time and end time.

time-range

Use **time-range** to create or edit a time range.

Use **undo time-range** to delete a time range or a statement in the time range.

Syntax

time-range *time-range-name* { *start-time* **to** *end-time days* [**from** *time1 date1*] [**to** *time2 date2*] | **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2* }

undo time-range *time-range-name* [*start-time* **to** *end-time days* [**from** *time1 date1*] [**to** *time2 date2*] | **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2*]

Default

No time ranges exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

time-range-name: Specifies a time range name. The name is a case-insensitive string of 1 to 32 characters. To avoid confusion, it cannot be **all**.

start-time **to** *end-time*: Specifies a periodic statement. Both *start-time* and *end-time* are in hh:mm format (24-hour clock). The value is in the range of 00:00 to 23:59 for the start time, and 00:00 to 24:00 for the end time. The end time must be greater than the start time.

days: Specifies the day or days of the week (in words or digits) on which the periodic statement is valid. If you specify multiple values, separate each value with a space, and make sure they do not overlap. These values can take one of the following forms:

- A digit in the range of 0 to 6, for Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday.
- A day of a week in abbreviated words: **Sun**, **Mon**, **Tue**, **Wed**, **Thu**, **Fri**, and **Sat**.
- **working-day** for Monday through Friday.
- **off-day** for Saturday and Sunday.
- **daily** for the whole week.

from *time1 date1*: Specifies the start time and date of an absolute statement. The *time1* argument specifies the time of the day in hh:mm or hh:mm:ss format (24-hour clock). Its value is in the range of 00:00:00 to 23:59:59. The *date1* argument specifies a date in MM/DD/YYYY or YYYY/MM/DD format, where MM is the month of the year in the range of 1 to 12, DD is the day of the month with the range varying by MM, and YYYY is the year in the calendar in the range of 1970 to 2100. If you do not specify this option, the start time is 01/01/1970 00:00:00 AM, the earliest time available in the system.

to *time2 date2*: Specifies the end time and date of the absolute time statement. The *time2* argument has the same format as the *time1* argument, but its value is in the range of 00:00:00 to 24:00:00. The *date2* argument has the same format and value range as the *date1* argument. The end time must be greater than the start time. If you do not specify this option, the end time is 12/31/2100 24:00:00 PM, the maximum time available in the system.

Usage guidelines

If an existing time range name is provided, this command adds a statement to the time range.

You can create multiple statements in a time range. Each time statement can take one of the following forms:

- Periodic statement in the *start-time* **to** *end-time days* format. A periodic statement recurs periodically on a day or days of the week.
- Absolute statement in the **from** *time1 date1* **to** *time2 date2* format. An absolute statement does not recur.

- Compound statement in the *start-time* **to** *end-time days* **from** *time1 date1* **to** *time2 date2* format. A compound statement recurs on a day or days of the week only within the specified period. For example, to create a time range that is active from 08:00 to 12:00 on Monday between January 1, 2015, 00:00 and December 31, 2015, 23:59, use the **time-range test 08:00 to 12:00 Mon from 00:00 01/01/2015 to 23:59 12/31/2015** command.

You can create a maximum of 1024 time ranges, each with a maximum of 32 periodic statements and 12 absolute statements. The active period of a time range is calculated as follows:

1. Combining all periodic statements.
2. Combining all absolute statements.
3. Taking the intersection of the two statement sets as the active period of the time range.

Examples

Create a periodic time range **t1**, setting it to be active between 8:00 to 18:00 during working days.

```
<Sysname> system-view
[Sysname] time-range t1 08:00 to 18:00 working-day
```

Create an absolute time range **t2**, setting it to be active in the whole year of 2011.

```
<Sysname> system-view
[Sysname] time-range t2 from 00:00 1/1/2011 to 24:00 12/31/2011
```

Create a compound time range **t3**, setting it to be active from 08:00 to 12:00 on Saturdays and Sundays of the year 2011.

```
<Sysname> system-view
[Sysname] time-range t3 08:00 to 12:00 off-day from 00:00 1/1/2011 to 24:00 12/31/2011
```

Create a compound time range **t4**, setting it to be active from 10:00 to 12:00 on Mondays and from 14:00 to 16:00 on Wednesdays in January and June of the year 2011.

```
<Sysname> system-view
[Sysname] time-range t4 10:00 to 12:00 1 from 00:00 1/1/2011 to 24:00 1/31/2011
[Sysname] time-range t4 14:00 to 16:00 3 from 00:00 6/1/2011 to 24:00 6/30/2011
```

Create an absolute time range **t5**, setting it to be active between 8:00 to 18:00 on January 1st, 2018.

```
<Sysname> system-view
[Sysname] time-range t5 from 08:00:00 1/1/2018 to 18:00:00 1/1/2018
```

Related commands

display time-range

NSFOCUS Firewall Series

NF IP Multicast Command Reference

NSFOCUS Technologies, Inc.

Document version: 6W600-20230221

Preface

This command reference describes the commands for configuring IP multicast features, including multicast routing and forwarding, PIM, IGMP, IPv6 multicast routing and forwarding, and MLD.

This preface includes the following topics about the documentation:

- Audience.
- Conventions.

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators.

Conventions

The following information describes the conventions used in the documentation.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select a minimum of one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
CAUTION:	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Contents

Multicast routing and forwarding commands

delete ip rpf-route-static

Use **delete ip rpf-route-static** to delete all static multicast routes.

Syntax

delete ip rpf-route-static [**vpn-instance** *vpn-instance-name*]

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command deletes all static multicast routes on the public network.

Usage guidelines

This command deletes all static multicast routes. To delete a specified static multicast route, use the **undo ip rpf-route-static** command.

Examples

Delete all static multicast routes on the public network.

```
<Sysname> system-view
[Sysname] delete ip rpf-route-static
This will erase all multicast static routes and their configurations, you must reconfigure all static routes.
Are you sure?[Y/N]:y
```

Related commands

ip rpf-route-static

display mrib interface

Use **display mrib interface** to display information about interfaces maintained by the MRIB.

Syntax

display mrib [**vpn-instance** *vpn-instance-name*] **interface** [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays information about interfaces maintained by the MRIB on the public network.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays information about all interfaces maintained by the MRIB.

Examples

Display information about interfaces maintained by the MRIB on the public network.

```
<Sysname> display mrib interface
 Interface: GigabitEthernet1/0/1
     Index: 0x00004444
     Current state: up
     MTU: 1500
     Type: BROADCAST
     Protocol: PIM-DM
     PIM protocol state: Enabled
     Address list:
          1. Local address : 8.12.0.2/16
             Remote address: 0.0.0.0
             Reference     : 1
             State         : NORMAL
```

Table 1 Command output

Field	Description
Interface	Interface name.
Index	Index number of the interface.
Current state	Current status of the interface: up or down.
MTU	MTU value.
Type	Interface type: • **BROADCAST**—Broadcast link interface. • **P2P**—P2P interface. • **LOOP**—Loopback interface. • **REGISTER**—Register interface. • **NBMA**—NBMA interface. • **MTUNNEL**—Multicast tunnel interface. This field is empty if the interface is Null 0.
Protocol	Protocol running on the interface: PIM-DM, PIM-SM, IGMP, PROXY, or MD.
PIM protocol state	Whether PIM is enabled: Enabled or Disabled.
Address list	Interface address list.
Local address	Local IP address.
Remote address	Remote end IP address. This field is displayed only when the interface is

Field	Description
	vlink type.
Reference	Number of times that the address has been referenced.
State	Status of the interface address: NORMAL or DEL.

display multicast boundary

Use **display multicast boundary** to display multicast boundary information.

Syntax

display multicast [**vpn-instance** *vpn-instance-name*] **boundary** [*group-address* [*mask-length* | *mask*]] [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays multicast boundary information on the public network.

group-address: Specifies a multicast group by its IP address in the range of 224.0.0.0 to 239.255.255.255. If you do not specify a multicast group, this command displays multicast boundary information for all multicast groups.

mask-length: Specifies an address mask length in the range of 4 to 32. The default is 32.

mask: Specifies an address mask. The default is 255.255.255.255.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays multicast boundary information for all interfaces.

Examples

Display information about all multicast boundaries on the public network.

```
<Sysname> display multicast boundary
 Boundary            Interface
 224.1.1.0/24        GE1/0/1
 239.2.2.0/24        GE1/0/2
```

Table 2 Command output

Field	Description
Boundary	Multicast group associated with the multicast boundary.
Interface	Boundary interface associated with the multicast boundary.

Related commands

multicast boundary

display multicast fast-forwarding cache

Use **display multicast fast-forwarding cache** to display multicast fast forwarding entries.

Syntax

display multicast [**vpn-instance** *vpn-instance-name*] **fast-forwarding cache** [*source-address* | *group-address*] * [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays multicast fast forwarding entries on the public network.

source-address: Specifies a multicast source address.

group-address: Specifies a multicast group address in the range of 224.0.1.0 to 239.255.255.255.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays multicast fast forwarding entries for the master device.

Examples

Display multicast fast forwarding entries on the public network.

```
<Sysname> display multicast fast-forwarding cache
Total 1 entries, 1 matched

 (60.1.1.200, 225.0.0.2)
    Status     : Enabled
    Source port: 2001                  Destination port: 2002
    Protocol   : 2                     Flag            : 0x2
    Incoming interface: GigabitEthernet1/0/3
    List of 1 outgoing interfaces:
        GigabitEthernet1/0/2
          Status: Enabled              Flag: 0x14
```

Table 3 Command output

Field	Description
Total 1 entries, 1 matched	Total number of (S, G) entries in the multicast fast forwarding table, and the total number of matching (S, G) entries.

Field	Description
(60.1.1.200, 225.0.0.2)	(S, G) entry.
Protocol	Protocol number.
Flag	Flag of the (S, G) entry or the outgoing interface in the entry. This field displays one flag or the sum of multiple flags. In this example, the value 0x2 means that the entry has only one flag 0x2. The value 0x14 means that the interface has flags 0x4 and 0x10. The following flags are available for an entry: • **0x1**—The entry is created because of packets passed through between cards. • **0x2**—The entry is added by multicast forwarding. The following flags are available for an outgoing interface: • **0x1**—The interface is added to the entry because of packets passed through between cards. • **0x2**—The interface is added to an existing entry. • **0x4**—The MAC address of the interface is needed for fast forwarding. • **0x8**—The interface is an outgoing interface associated with the incoming VLAN interface. • **0x10**—The interface is associated with the entry. • **0x20**—The interface is to be deleted.
Status	Status of the (S, G) entry or the outgoing interface: • **Enabled**—Available. • **Disabled**—Unavailable.
Incoming interface	Incoming interface of the (S, G) entry.
List of 1 outgoing interfaces	Outgoing interface list of the (S, G) entry.

Related commands

`reset multicast fast-forwarding cache all`

display multicast forwarding df-info

Use **`display multicast forwarding df-info`** to display DF information.

Syntax

`display multicast` [**`vpn-instance`** *`vpn-instance-name`*] **`forwarding df-info`** [*`rp-address`*] [**`verbose`**] [**`slot`** *`slot-number`*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays DF information on the public network.

rp-address: Specifies a BIDIR-PIM RP by its IP address.

verbose: Specifies detailed information. If you do not specify this keyword, the command displays brief information about DFs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays DF information for the master device.

Usage guidelines

In a BIDIR-PIM domain, only the DF on each subnet can forward multicast data destined for a multicast group toward the RP of the group. For more information about the DF, see *IP Multicast Configuration Guide*.

Examples

Display brief information about DFs on an ADVPN network.

```
<Sysname> display multicast forwarding df-info
Total 1 RPs, 1 matched

00001. RP address: 1.1.1.1
     Flags: 0x0
     Uptime: 00:00:53
     RPF interface: Tunnel2, 192.168.0.1
     List of 2 DF interfaces:
       1: LoopBack0
       2: Tunnel2, 192.168.0.3
```

Display brief information about DFs on the public network.

```
<Sysname> display multicast forwarding df-info
Total 1 RPs, 1 matched

00001. RP address: 7.11.0.2
     Flags: 0x0
     Uptime: 04:14:40
     RPF interface: GigabitEthernet1/0/1
     List of 1 DF interfaces:
       1: GigabitEthernet1/0/2
```

Display detailed information about DFs on the public network.

```
<Sysname> display multicast forwarding df-info verbose
Total 1 RPs, 1 matched

00001. RP address: 7.11.0.2
     MID: 2, Flags: 0x0
     Uptime: 03:37:22
       Product information: 0x7a2f762f, 0x718fee9f, 0x4b82f137, 0x71c32184
     RPF interface: GigabitEthernet1/0/1
       Product information: 0xa567d6fc, 0xadeb03e3
       Tunnel  information: 0xdfb107d4, 0x7aa5d510
     List of 1 DF interfaces:
```

```
1: GigabitEthernet1/0/2
   Product information: 0xa986152b, 0xb74a9a2f
   Tunnel  information: 0x297ca208, 0x76985b89
```

Table 4 Command output

Field	Description
Total 1 RPs, 1 matched	Total number of RPs, and the total number of matching RPs.
00001	Sequence number of the entry to which the RP is designated.
RP address	IP address of the RP.
MID	ID of the entry to which the RP is designated. Each entry to which the RP is designated has a unique MID.
Flags	Entry flag. This field displays one flag or the sum of multiple flags. In this example, the value 0x0 means that the entry has only one flag 0x0. The following flags are available for an entry: • **0x0**—The entry is in correct state. • **0x4**—The entry fails to update. • **0x8**—DF interface information fails to update for the entry. • **0x40**—The entry is to be deleted. • **0x100**—The entry is being deleted. • **0x200**—The entry is in GR state.
Uptime	Length of time for which the entry has been up.
RPF interface	RPF interface to the RP.
List of 1 DF interfaces	DF interface list.
Tunnel2, 192.168.0.3	ADVPN tunnel interface, and the IP address of the remote end.

display multicast forwarding event

Use **display multicast forwarding event** to display statistics of multicast forwarding events.

Syntax

display multicast [**vpn-instance** *vpn-instance-name*] **forwarding event** [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays statistics of the multicast forwarding events on the public network.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays statistics of multicast forwarding events for the master device.

Examples

Display statistics of multicast forwarding events on the public network.

```
<Sysname> display multicast forwarding event
Total active events sent: 0
Total inactive events sent: 0
Total NoCache events sent: 2
Total NoCache events dropped: 0
Total WrongIF events sent: 0
Total WrongIF events dropped: 0
Total SPT switch events sent: 0
NoCache rate limit: 1024 packets/s
WrongIF rate limit: 1 packets/10s
Total timer of register suppress timeout: 0
```

Table 5 Command output

Field	Description
Total active events sent	Number of times that entry-active events have been sent.
Total inactive events sent	Number of times that entry-inactive events have been sent.
Total NoCache events sent	Number of times that NoCache events have been sent.
Total NoCache events dropped	Number of times that NoCache events have been dropped.
Total WrongIF events sent	Number of times that WrongIF events have been sent.
Total WrongIF events dropped	Number of times that WrongIF events have been dropped.
Total SPT switch events sent	Number of times that SPT-switch events have been sent.
NoCache rate limit	Rate limit for sending NoCache events, in pps.
WrongIF rate limit	Rate limit for sending WrongIF events, in packets per 10 seconds.
Total timer of register suppress timeout	Number of times that the registration suppression has timed out in total.

Related commands

reset multicast forwarding event

display multicast forwarding-table

Use **display multicast forwarding-table** to display multicast forwarding entries.

Syntax

display multicast [**vpn-instance** *vpn-instance-name*] **forwarding-table** [*source-address* [**mask** { *mask-length* | *mask* }] | *group-address* [**mask** { *mask-length* | *mask* }] | **incoming-interface** *interface-type interface-number* | **outgoing-interface** { **exclude** | **include** | **match** } *interface-type interface-number* | **slot** *slot-number* | **statistics**] *

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays multicast forwarding entries on the public network.

source-address: Specifies a multicast source address.

group-address: Specifies a multicast group address in the range of 224.0.0.0 to 239.255.255.255.

mask-length: Specifies an address mask length. The default value is 32. For a multicast group address, the value range for this argument is 4 to 32. For a multicast source address, the value range for this argument is 0 to 32.

mask: Specifies an address mask. The default value is 255.255.255.255.

incoming-interface: Specifies the multicast forwarding entries that contain the specified incoming interface.

interface-type interface-number: Specifies an incoming interface by its type and number.

outgoing-interface: Specifies the multicast forwarding entries that contain the specified outgoing interface.

exclude: Specifies the multicast forwarding entries that do not contain the specified interface in the outgoing interface list.

include: Specifies the multicast forwarding entries that contain the specified interface in the outgoing interface list.

match: Specifies the forwarding entries that contain only the specified interface in the outgoing interface list.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays multicast forwarding entries for the master device.

statistics: Displays statistics for the multicast forwarding table.

Examples

Display multicast forwarding entries on an ADVPN network.

```
<Sysname> display multicast forwarding-table
Total 1 entries, 1 matched

00001. (172.168.0.2, 227.0.0.1)
     Flags: 0x0
     Uptime: 00:08:32, Timeout in: 00:03:26
     Incoming interface: Tunnel1, 12.1.1.3
     List of 2 outgoing interface:
            1:  Tunnel1, 12.1.1.1
            2:  Tunnel1, 12.1.1.2
     Matched 19648 packets(20512512 bytes), Wrong If 0 packet
     Forwarded 19648 packets(20512512 bytes)
```

Display multicast forwarding entries on the public network.

```
<Sysname> display multicast forwarding-table
Total 1 entries, 1 matched

00001. (172.168.0.2, 227.0.0.1)
     Flags: 0x0
     Uptime: 00:08:32, Timeout in: 00:03:26
     Incoming interface: Vlan-interface10
          Incoming sub-VLAN: VLAN 11
          Outgoing sub-VLAN: VLAN 12
                             VLAN 13
     List of 1 outgoing interfaces:
       1: Vlan-interface20
          Sub-VLAN: VLAN 21
                    VLAN 22
     Matched 19648 packets(20512512 bytes), Wrong If 0 packet
     Forwarded 19648 packets(20512512 bytes)
```

Table 6 Command output

Field	Description
Total 1 entries, 1 matched	Total number of (S, G) entries, and the total number of matching (S, G) entries.
00001	Sequence number of the (S, G) entry.
(172.168.0.2,227.0.0.1)	(S, G) entry.
Flags	Entry flag. This field displays one flag or the sum of multiple flags. In this example, the value 0x0 means that the entry has only one flag 0x0. The following entries are available for an entry: • **0x0**—The entry is in correct state. • **0x1**—The entry is in inactive state. • **0x2**—The entry is null. • **0x4**—The entry fails to update. • **0x8**—Outgoing interface information fails to update for the entry. • **0x10**—Data-group information fails to update for the entry. • **0x20**—A register outgoing interface is available. • **0x40**—The entry is to be deleted. • **0x80**—The entry is in registration suppression state. • **0x100**—The entry is being deleted. • **0x200**—The entry is in GR state. • **0x800**—The entry has the associated ARP entry for the multicast source address. • **0x400000**—The entry is created by the IGMP proxy. • **0x2000000**—The entry is a BIDIR-PIM forwarding entry.
Uptime	Length of time for which the (S, G) entry has been up.
Timeout in	Length of time in which the (S, G) entry will expire.
Incoming interface	Incoming interface of the (S, G) entry.
List of 1 outgoing interfaces	Outgoing interface list of the (S, G) entry.
Tunnel1, 12.1.1.1	ADVPN tunnel interface, and the IP address of the remote end.

Field	Description
Matched 19648 packets(20512512 bytes), Wrong If 0 packet	Number of packets (bytes) that match the (S, G) entry, and number of packets with incoming interface errors. The numbers are displayed as 0 if an outgoing interface of the (S, G) entry is on the specified slot.
Forwarded 19648 packets(20512512 bytes)	Number of packets (bytes) that have been forwarded. The numbers are displayed as 0 if an outgoing interface of the (S, G) entry is on the specified slot.

Related commands

reset multicast forwarding-table

display multicast forwarding-table df-list

Use **display multicast forwarding-table df-list** to display information about the DF list in multicast forwarding entries.

Syntax

display multicast [**vpn-instance** *vpn-instance-name*] **forwarding-table df-list** [*group-address*] [**verbose**] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays information about the DF list in multicast forwarding entries on the public network.

group-address: Specifies a multicast group address in the range of 224.0.0.0 to 239.255.255.255.

verbose: Specifies detailed information about the DF list in multicast forwarding entries. If you do not specify this keyword, the command displays brief information about the DF list in multicast forwarding entries.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about the DF list in multicast forwarding entries for the master device.

Examples

Display brief information about the DF list in multicast forwarding entries on the public network.

```
<Sysname> display multicast forwarding-table df-list
Total 1 entries, 1 matched

00001. (0.0.0.0, 225.0.0.1)
     List of 1 DF interfaces:
```

```
       1: GigabitEthernet1/0/1
```

Display detailed information about the DF list in multicast forwarding entries on the public network.

```
<Sysname> display multicast forwarding-table df-list verbose
Total 1 entries, 1 matched

00001. (0.0.0.0, 225.0.0.1)
       List of 1 DF interfaces:
         1: GigabitEthernet1/0/1
            Product information: 0x347849f6, 0x14bd6837
            Tunnel  information: 0xc4857986, 0x128a9c8f
```

Table 7 Command output

Field	Description
Total 1 entries, 1 matched	Total number of forwarding entries, and the total number of matching entries.
00001	Sequence number of the entry.
(0.0.0.0, 225.0.0.1)	(*, G) entry.
List of 1 DF interfaces	DF interface list.

display multicast routing-table

Use **display multicast routing-table** to display multicast routing entries.

Syntax

display multicast [**vpn-instance** *vpn-instance-name*] **routing-table** [*source-address* [**mask** { *mask-length* | *mask* }] | *group-address* [**mask** { *mask-length* | *mask* }] | **incoming-interface** *interface-type interface-number* | **outgoing-interface** { **exclude** | **include** | **match** } *interface-type interface-number*] *

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays multicast routing entries on the public network.

source-address: Specifies a multicast source address.

group-address: Specifies a multicast group address in the range of 224.0.0.0 to 239.255.255.255.

mask-length: Specifies an address mask length. The default value is 32. For a multicast group address, the value range for this argument is 4 to 32. For a multicast source address, the value range for this argument is 0 to 32.

mask: Specifies an address mask. The default is 255.255.255.255.

incoming-interface: Specifies the multicast routing entries that contain the specified incoming interface.

interface-type interface-number: Specifies an interface by its type and number.

outgoing-interface: Specifies the multicast routing entries that contain the specified outgoing interface.

exclude: Specifies the multicast routing entries that do not contain the specified interface in the outgoing interface list.

include: Specifies the multicast routing entries that contain the specified interface in the outgoing interface list.

match: Specifies the multicast routing entries that contain only the specified interface in the outgoing interface list.

Usage guidelines

Multicast routing entries are the basis of multicast forwarding. You can use this command to view the establishment state of (S, G) entries.

Examples

Display multicast routing entries on an ADVPN network.

```
<Sysname> display multicast routing-table
 Total 1 entries

 00001. (172.168.0.2, 227.0.0.1)
       Uptime: 00:00:28
       Upstream Interface: Tunnel1, 12.1.1.3
       List of 2 downstream interfaces
           1:  Tunnel1, 12.1.1.1
           2:  Tunnel1, 12.1.1.2
```

Display multicast routing entries on the public network.

```
<Sysname> display multicast routing-table
 Total 1 entries

 00001. (172.168.0.2, 227.0.0.1)
       Uptime: 00:00:28
       Upstream Interface: GigabitEthernet1/0/1
       List of 2 downstream interfaces
           1:  GigabitEthernet1/0/2
           2:  GigabitEthernet1/0/3
```

Table 8 Command output

Field	Description
Total 1 entries	Total number of (S, G) entries.
00001	Sequence number of the (S, G) entry.
(172.168.0.2, 227.0.0.1)	(S, G) entry.
Uptime	Length of time for which the (S, G) entry has been up.
Upstream Interface	Upstream interface at which (S, G) packets should arrive.

Field	Description
List of 2 downstream interfaces	List of downstream interfaces that need to forward (S, G) packets.
Tunnel1, 12.1.1.1	ADVPN tunnel interface, and the IP address of the remote end.

Related commands

reset multicast routing-table

display multicast routing-table static

Use **display multicast routing-table static** to display static multicast routing entries.

Syntax

display multicast [**vpn-instance** *vpn-instance-name*] **routing-table static** [*source-address* { *mask-length* | *mask* }]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays static multicast routing entries on the public network.

source-address: Specifies a multicast source address.

mask-length: Specifies an address mask length in the range of 0 to 32.

mask: Specifies an address mask.

Usage guidelines

This command displays only valid static multicast routing entries.

Examples

Display static multicast routing entries on the public network.

```
<Sysname> display multicast routing-table static
Destinations: 3        Routes: 4

Destination/Mask   Pre  RPF neighbor    Interface
1.1.0.0/16         10   7.12.0.1        GE1/0/1
                        7.11.0.1        GE1/0/2
2.2.2.0/24         20   7.11.0.1        GE1/0/3
3.3.3.3/32         50   7.12.0.1        GE1/0/4
```

Table 9 Command output

Field	Description
Destinations	Number of the multicast destination addresses.
Routes	Number of routes.
Destination/Mask	Destination address and its mask length.
Pre	Route preference.
RPF neighbor	IP address of the RPF neighbor to the reachable destination.
Interface	Outgoing interface to the reachable destination.

display multicast rpf-info

Use **display multicast rpf-info** to display RPF information for a multicast source.

Syntax

display multicast [**vpn-instance** *vpn-instance-name*] **rpf-info** *source-address* [*group-address*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays RPF information for a multicast source on the public network.

source-address: Specifies a multicast source address.

group-address: Specifies a multicast group address in the range of 224.0.1.0 to 239.255.255.255.

Examples

Display RPF information for multicast source 192.168.1.55 on the public network.

```
<Sysname> display multicast rpf-info 192.168.1.55
 RPF information about source 192.168.1.55:
     RPF interface: GigabitEthernet1/0/1, RPF neighbor: 10.1.1.1
     Referenced route/mask: 192.168.1.0/24
     Referenced route type: igp
     Route selection rule: preference-preferred
     Load splitting rule: disable
     Source AS: 0
     C-multicast route target: 0x0000000000000000
```

Table 10 Command output

Field	Description
RPF neighbor	IP address of the RPF neighbor.
Referenced route/mask	Referenced route and its mask length.
Referenced route type	Type of the referenced route: • **igp**—IGP unicast route. • **egp**—EGP unicast route. • **unicast (direct)**—Directly connected unicast route. • **unicast**—Other unicast routes, such as static unicast route. • **multicast static**—Static multicast route. • **mbgp**—MBGP route.
Route selection rule	Rule for RPF route selection: • Route preference. • Longest prefix match.
Load splitting rule	Status of the load splitting rule: enable or disable.
Source AS	AS number of the source-side PE.
C-multicast route target	Route target attribute value of the C-multicast route.

Related commands

display multicast forwarding-table

display multicast routing-table

ip rpf-route-static

Use **ip rpf-route-static** to configure a static multicast route.

Use **undo ip rpf-route-static** to delete a static multicast route.

Syntax

ip rpf-route-static [**vpn-instance** *vpn-instance-name*] *source-address* { *mask-length* | *mask* } { *rpf-nbr-address* | *interface-type interface-number* } [**preference** *preference*]

undo ip rpf-route-static [**vpn-instance** *vpn-instance-name*] *source-address* { *mask-length* | *mask* } { *rpf-nbr-address* | *interface-type interface-number* }

Default

No static multicast routes exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command configures a static multicast route on the public network.

source-address: Specifies a multicast source address.

mask-length: Specifies an address mask length in the range of 0 to 32.

mask: Specifies an address mask.

rpf-nbr-address: Specifies an RPF neighbor by its IP address.

interface-type interface-number: Specifies an interface by its type and number. The interface connects the RPF neighbor.

preference: Sets a route preference in the range of 1 to 255. The default value is 1.

Usage guidelines

If the interface connected to an RPF neighbor is a point-to-point interface, you must specify the interface by its type and number.

If the interface connected to an RPF neighbor is not a point-to-point interface, you must specify the interface by its IP address. This type of interfaces includes Layer 3 Ethernet, Layer 3 aggregate, Loopback, and VLAN interfaces.

The configured static multicast route might not take effect when one of the following conditions exists:

- The outgoing interface iteration fails.
- The specified interface is not in the public network or the same VPN instance as the current interface.
- The specified interface is not a point-to-point interface.
- The specified interface is down.

If multiple static multicast routes within the same multicast source address range are available, only the one with the highest route preference can become active. You can use the **display multicast routing-table static** command to verify that the configured static multicast route has taken effect.

The **undo ip rpf-route-static** command deletes the specified static multicast route, but the **delete ip rpf-route-static** command deletes all static multicast routes.

Examples

Configure a static multicast route to multicast source 10.1.1.0/24 and specify the interface with IP address 192.168.1.23 as the RPF neighbor on the public network.

```
<Sysname> system-view
[Sysname] ip rpf-route-static 10.1.1.0 24 192.168.1.23
```

Related commands

delete ip rpf-route-static

display multicast routing-table static

load-splitting (MRIB view)

Use **load-splitting** to enable multicast load splitting.

Use **undo load-splitting** to restore the default.

Syntax

load-splitting { **source** | **source-group** }

undo load-splitting

Default

Multicast load splitting is disabled.

Views

MRIB view

Predefined user roles

network-admin

context-admin

Parameters

source: Enables multicast load splitting based on multicast source.

source-group: Enables multicast load splitting based on multicast source and group.

Usage guidelines

This command does not take effect on BIDIR-PIM.

Examples

Enable multicast load splitting based on multicast source on the public network.

```
<Sysname> system-view
[Sysname] multicast routing
[Sysname-mrib] load-splitting source
```

longest-match (MRIB view)

Use **longest-match** to specify the longest prefix match principle for RPF route. The device will use the matching route with the longest prefix as the RPF route.

Use **undo longest-match** to restore the default.

Syntax

longest-match

undo longest-match

Default

Route preference is used for RPF route selection. The route with the highest preference is used as the RPF route.

Views

MRIB view

Predefined user roles

network-admin

context-admin

Examples

Specify the longest prefix match principle for RPF route selection on the public network.

```
<Sysname> system-view
[Sysname] multicast routing
```

```
[Sysname-mrib] multicast longest-match
```

multicast boundary

Use **multicast boundary** to configure a multicast forwarding boundary.

Use **undo multicast boundary** to delete a multicast forwarding boundary.

Syntax

multicast boundary *group-address* { *mask-length* | *mask* }

undo multicast boundary { *group-address* { *mask-length* | *mask* } | **all** }

Default

No multicast forwarding boundaries are configured on an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

group-address: Specifies a multicast group address in the range of 224.0.0.0 to 239.255.255.255.

mask-length: Specifies an address mask length in the range of 4 to 32.

mask: Specifies an address mask.

all: Specifies all forwarding boundaries configured on the interface.

Usage guidelines

A multicast forwarding boundary sets the boundary condition for the multicast groups in the specified address range. If the destination address of a multicast packet matches the set boundary condition, the packet is not forwarded.

You can configure an interface as a multicast forwarding boundary for different multicast group ranges by executing this command multiple times on the interface.

You do not need to enable IP multicast routing before you execute this command.

Assume that Set A and Set B are multicast forwarding boundary sets with different address ranges, and B is a subset of A. A takes effect on the interface no matter whether A is configured earlier or later than B.

Examples

Configure GigabitEthernet 1/0/1 as the forwarding boundary of multicast groups in the range of 239.2.0.0/16.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] multicast boundary 239.2.0.0 16
```

Related commands

display multicast boundary

multicast forwarding-table cache-unknown per-entry

Use **multicast forwarding-table cache-unknown per-entry** to set the maximum number of unknown multicast packets that can be cached for an (S, G) entry.

Use **undo multicast forwarding-table cache-unknown per-entry** to restore the default.

Syntax

multicast forwarding-table cache-unknown per-entry *per-entry-limit*

undo multicast forwarding-table cache-unknown per-entry

Default

The device can cache only one unknown multicast packet for an (S, G) entry.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

per-entry-limit: Specifies the maximum number of unknown multicast packets that can be cached for an (S, G) entry. The value range for this argument is 0 to 256. If you set the value to 0, the device cannot cache unknown multicast packets.

Examples

Set the maximum number to 20 for unknown multicast packets that can be cached for an (S, G) entry.

```
<Sysname> system-view
[Sysname] multicast forwarding-table cache-unknown per-entry 20
```

Related commands

multicast forwarding-table cache-unknown total

multicast forwarding-table cache-unknown total

Use **multicast forwarding-table cache-unknown total** to set the maximum number of all unknown multicast packets that can be cached.

Use **undo multicast forwarding-table cache-unknown total** to restore the default.

Syntax

multicast forwarding-table cache-unknown total *total-limit*

undo multicast forwarding-table cache-unknown total

Default

The device can cache 1024 unknown multicast packets in total.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

total-limit: Specifies the maximum number of all unknown multicast packets that can be cached. The value range for this argument is 0 to 65535. If you set the value to 0, the device cannot cache unknown multicast packets.

Usage guidelines

As a best practice, set the value in this command to be far greater than the value set in the **multicast forwarding-table cache-unknown per-entry** command.

Examples

Set the maximum number to 10000 for all unknown multicast packets that can be cached.

```
<Sysname> system-view
[Sysname] multicast forwarding-table cache-unknown total 10000
```

Related commands

multicast forwarding-table cache-unknown per-entry

multicast routing

Use **multicast routing** to enable IP multicast routing and enter MRIB view.

Use **undo multicast routing** to disable IP multicast routing.

Syntax

multicast routing [**vpn-instance** *vpn-instance-name*]

undo multicast routing [**vpn-instance** *vpn-instance-name*]

Default

IP multicast routing is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command enables IP multicast routing on the public network.

Usage guidelines

Other Layer 3 multicast commands take effect only when IP multicast routing is enabled on the public network or for a VPN instance.

The device does not forward multicast packets before IP multicast routing is enabled.

Examples

Enable IP multicast routing on the public network, and enter MRIB view.

```
<Sysname> system-view
[Sysname] multicast routing
[Sysname-mrib]
```

Enable IP multicast routing for the VPN instance **mvpn**, and enter MRIB view.

```
<Sysname> system-view
[Sysname] multicast routing vpn-instance mvpn
[Sysname-mrib-mvpn]
```

reset multicast fast-forwarding cache

Use **reset multicast fast-forwarding cache** to clear multicast fast forwarding entries.

Syntax

reset multicast [**vpn-instance** *vpn-instance-name*] **fast-forwarding cache** { { *source-address* | *group-address* } * | **all** } [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears multicast fast forwarding entries on the public network.

source-address: Specifies a multicast source address.

group-address: Specifies a multicast group address in the range of 224.0.0.0 to 239.255.255.255.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears multicast fast forwarding entries for the master device.

all: Specifies all multicast fast forwarding entries.

Examples

Clear all multicast fast forwarding entries on the public network.

```
<Sysname> reset multicast fast-forwarding cache all
```

Clear the multicast fast forwarding entry for multicast source and group (20.0.0.2, 225.0.0.2) on the public network.

```
<Sysname> reset multicast fast-forwarding cache 20.0.0.2 225.0.0.2
```

Related commands

display multicast fast-forwarding cache

reset multicast forwarding event

Use **reset multicast forwarding event** to clear statistics for multicast forwarding events.

Syntax

reset multicast [**vpn-instance** *vpn-instance-name*] **forwarding event**

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears statistics for the multicast forwarding events on the public network.

Examples

Clear statistics for multicast forwarding events on the public network.

```
<Sysname> reset multicast forwarding event
```

Related commands

display multicast forwarding event

reset multicast forwarding-table

Use **reset multicast forwarding-table** to clear multicast forwarding entries.

Syntax

reset multicast [**vpn-instance** *vpn-instance-name*] **forwarding-table** { { *source-address* [**mask** { *mask-length* | *mask* }] | *group-address* [**mask** { *mask-length* | *mask* }] | **incoming-interface** { *interface-type interface-number* } } * | **all** }

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears multicast forwarding entries on the public network.

source-address: Specifies a multicast source address.

group-address: Specifies a multicast group address in the range of 224.0.0.0 to 239.255.255.255.

mask-length: Specifies an address mask length. The default value is 32. For a multicast group address, the value range for this argument is 4 to 32. For a multicast source address, the value range for this argument is 0 to 32.

mask: Specifies an address mask. The default is 255.255.255.255.

incoming-interface: Specifies the multicast forwarding entries that contain the specified incoming interface.

interface-type interface-number: Specifies an incoming interface by its type and number.

all: Specifies all multicast forwarding entries.

Usage guidelines

When you clear a multicast forwarding entry, the associated multicast routing entry is also cleared.

Examples

Clear multicast forwarding entries for multicast group 225.5.4.3 on the public network.

```
<Sysname> reset multicast forwarding-table 225.5.4.3
```

Related commands

display multicast forwarding-table

reset multicast routing-table

Use **reset multicast routing-table** to clear multicast routing entries.

Syntax

reset multicast [**vpn-instance** *vpn-instance-name*] **routing-table** { { *source-address* [**mask** { *mask-length* | *mask* }] | *group-address* [**mask** { *mask* | *mask-length* }] | **incoming-interface** *interface-type interface-number* } * | **all** }

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears multicast routing entries on the public network.

source-address: Specifies a multicast source address.

group-address: Specifies a multicast group address in the range of 224.0.0.0 to 239.255.255.255.

mask-length: Specifies an address mask length. The default value is 32. For a multicast group address, the value range for this argument is 4 to 32. For a multicast source address, the value range for this argument is 0 to 32.

mask: Specifies an address mask. The default is 255.255.255.255.

incoming-interface: Specifies the routing entries that contain the specified incoming interface.

interface-type interface-number: Specifies an incoming interface by its type and number.

all: Specifies all multicast routing entries.

Usage guidelines

When you clear a multicast routing entry, the associated multicast forwarding entry is also cleared.

Examples

Clear multicast routing entries for multicast group 225.5.4.3 on the public network.

```
<Sysname> reset multicast routing-table 225.5.4.3
```

Related commands

display multicast routing-table

Contents

IGMP commands

display igmp group

Use **display igmp group** to display information about IGMP multicast groups (multicast groups that hosts have joined through IGMP).

Syntax

display igmp [**vpn-instance** *vpn-instance-name*] **group** [*group-address* | **interface** *interface-type interface-number*] [**static** | **verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays information about IGMP multicast groups on the public network.

group-address: Specifies a multicast group by its IP address in the range of 224.0.1.0 to 239.255.255.255. If you do not specify a multicast group, this command displays information about all IGMP multicast groups.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays information about IGMP multicast groups for all interfaces.

static: Specifies IGMP multicast groups that hosts have joined statically. If you do not specify this keyword, the command displays information about IGMP multicast groups that hosts have joined dynamically.

verbose: Displays detailed information.

Examples

Display information about IGMP multicast groups that hosts have dynamically joined on the public network.

```
<Sysname> display igmp group
IGMP groups in total: 3
 GigabitEthernet1/0/1(10.10.1.20):
  IGMP groups reported in total: 3
   Group address   Last reporter   Uptime      Expires
   225.1.1.1       10.10.1.10      00:02:04    00:01:15
   225.1.1.2       10.10.1.10      00:02:04    00:01:15
   225.1.1.3       10.10.1.10      00:02:04    00:01:15
```

Table 1 Command output

Field	Description
IGMP groups in total	Total number of IGMP multicast groups.
IGMP groups reported in total	Total number of IGMP multicast groups that hosts attached to the interface have joined dynamically.
Group address	Multicast group address.
Last reporter	Address of the last host that reported its membership to the multicast group.
Uptime	Length of time since the multicast group was reported.
Expire	Remaining lifetime for the multicast group. This field displays **Off** if the timer is disabled.

Display detailed information about IGMP multicast group 232.1.1.1 that hosts have dynamically joined on the public network. In this example, the router is configured with IGMP SSM mappings.

```
<Sysname> display igmp group 232.1.1.1 verbose
GigabitEthernet1/0/1(10.10.1.20):
  IGMP groups reported in total: 3
   Group: 232.1.1.1
     Uptime: 00:00:34
     Exclude expires: 00:04:16
     Mapping expires: 00:02:16
     Last reporter: 10.10.1.10
     Last-member-query-counter: 0
     Last-member-query-timer-expiry: Off
     Mapping last-member-query-counter: 0
     Mapping last-member-query-timer-expiry: Off
     Group mode: Exclude
     Version1-host-present-timer-expiry: Off
     Version2-host-present-timer-expiry: 00:02:11
     Mapping version1-host-present-timer-expiry: Off
     Source list (sources in total: 1):
       Source: 10.1.1.1
          Uptime: 00:00:03
          V3 expires: 00:04:16
          Mapping expires: 00:02:16
          Last-member-query-counter: 0
          Last-member-query-timer-expiry: Off
```

Table 2 Command output

Field	Description
IGMP groups reported in total	Total number of IGMP multicast groups that hosts attached to the interface have joined dynamically.
Group	Multicast group address.
Uptime	Length of time since the multicast group was reported.
Exclude expires	Remaining lifetime for the multicast group in Exclude mode. This field displays **Off** if the timer is disabled.

Field	Description
Mapping expires	Remaining time for the multicast group specified in IGMP SSM mappings. This field is displayed only when the device is configured with IGMP SSM mappings.
Last reporter	Address of the last host that reported its membership to this multicast group.
Last-member-query-counter	Number of IGMP group-specific queries or IGMP source-and-group-specific queries sent for the multicast group.
Last-member-query-timer-expiry	Remaining time for the last member query timer for the multicast group. This field displays **Off** if the timer is disabled.
Mapping last-member-query-counter	Number of IGMP group-specific queries or IGMP source-and-group-specific queries sent for the multicast group specified in IGMP SSM mappings. This field is displayed only when the device is configured with IGMP SSM mappings.
Mapping last-member-query-timer-expiry	Remaining time for the last member query timer of the multicast group specified in IGMP SSM mappings. This field displays **Off** if the timer is disabled. This field is displayed only when the device is configured with IGMP SSM mappings.
Group mode	Multicast source filtering mode: • **Include**—Include mode. • **Exclude**—Exclude mode. For a device that runs IGMPv1 or IGMPv2: • If IGMP SSM mappings are not configured, this field displays **Exclude**. • If IGMP SSM mappings are configured, this field displays **Include** or **Exclude** depending on the SSM mappings and the multicast groups that the host joins.
Version1-host-present-timer-expiry	Remaining time for the IGMPv1 host present timer. This field displays **Off** if the timer is disabled. This field is displayed only when the device runs IGMPv2 or IGMPv3.
Version2-host-present-timer-expiry	Remaining time for the IGMPv2 host present timer. This field displays **Off** if the timer is disabled. This field is displayed only when the device runs IGMPv3.
Mapping version1-host-present-timer-expiry	Remaining time for the IGMPv1 host present timer when the device is configured with IGMP SSM mappings. This field displays **Off** if the timer is disabled. This field is displayed only when the device is configured with IGMP SSM mappings.
Source list (sources in total)	List of multicast sources and total number of multicast sources. This field is displayed only when the device runs IGMPv3 or when the device is configured with IGMP SSM mappings.
Source	Multicast source address. This field is displayed only when the device runs IGMPv3 or when the device is configured with IGMP SSM mappings.
Uptime	Length of time since the multicast source was reported.

Field	Description
	This field is displayed only when the device runs IGMPv3 or when the device is configured with IGMP SSM mappings.
V3 expires	Remaining time for the multicast source when the device runs IGMPv3. This field displays **Off** if the timer is disabled and displays three hyphens (---) if the multicast source is specified in IGMP SSM mappings. This field is displayed only when the device runs IGMPv3 or when the device is configured with IGMP SSM mappings.
Mapping expires	Remaining time for the multicast source specified in IGMP SSM mappings. This field is displayed only when the device is configured with IGMP SSM mappings.
Last-member-query-counter	Number of IGMP group-specific queries or IGMP group-and-source-specific queries sent for the multicast source and group. This field is displayed only when the device runs IGMPv3 or is configured with IGMP SSM mappings.
Last-member-query-timer-expiry	Remaining time for the last member query timer for the multicast source and group. This field displays **Off** if the timer is disabled. This field is displayed only when the device runs IGMPv3 or is configured with IGMP SSM mappings.

Display information about IGMP multicast groups that hosts have statically joined on the public network.

```
<Sysname> display igmp group static
 Entries in total: 2
   Group address   Source address  Interface           Expires
   225.1.1.1       0.0.0.0         GE1/0/1             Never
   225.2.2.2       1.1.1.1         GE1/0/1             Never
```

Table 3 Command output

Field	Description
Entries in total	Total number of the multicast groups that hosts have joined statically.
Group address	Multicast group address.
Source address	Multicast source address.
Interface	Interface name.
Expires	Remaining lifetime for the multicast group. This field always displays **Never** because the multicast group never expires.

Related commands

`reset igmp group`

display igmp interface

Use **`display igmp interface`** to display IGMP information for interfaces.

Syntax

display igmp [**vpn-instance** *vpn-instance-name*] **interface** [*interface-type interface-number*] [**proxy**] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays IGMP information for interfaces on the public network.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays IGMP information for all IGMP-enabled interfaces.

proxy: Displays the IGMP proxy interface information. If you do not specify this keyword, the command displays IGMP information about all interfaces.

verbose: Displays detailed IGMP information.

Examples

Display detailed IGMP information for GigabitEthernet 1/0/1 (non-proxy interface) on the public network.

```
<Sysname> display igmp interface gigabitethernet 1/0/1 verbose
 GigabitEthernet1/0/1(10.10.1.20):
   IGMP is enabled.
   IGMP version: 2
   Query interval for IGMP: 125s
   Other querier present time for IGMP: 255s
   Maximum query response time for IGMP: 10s
   Last member query interval: 1s
   Last member query count: 2
   Startup query interval: 31s
   Startup query count: 2
   General query timer expiry (hh:mm:ss): 00:00:54
   Querier for IGMP: 10.10.1.20 (This router)
   IGMP activity: 1 join(s), 0 leave(s)
   Multicast routing on this interface: Enabled
   Robustness: 2
   Require-router-alert: Disabled
   Fast-leave: Disabled
   Startup-query: Off
   Other-querier-present-timer-expiry (hh:mm:ss): Off
  IGMP groups reported in total: 1
```

Display detailed IGMP information for all IGMP proxy interfaces on the public network.

```
<Sysname> display igmp interface proxy verbose
```

```
GigabitEthernet1/0/2(20.10.1.20):
  IGMP proxy is enabled.
  IGMP version: 2
  Multicast routing on this interface: Enabled
  Require-router-alert: Disabled
  Version1-querier-present-timer-expiry (hh:mm:ss): Off
```

Table 4 Command output

Field	Description
GigabitEthernet1/0/1(10.10.1.20)	Interface and its IP address.
IGMP is enabled	IGMP is enabled on the interface.
IGMP version	Version of IGMP that the interface runs.
Query interval for IGMP	IGMP general query interval, in seconds.
Other querier present time for IGMP	IGMP other querier present interval, in seconds.
Maximum query response time for IGMP	Maximum response time for IGMP general queries, in seconds.
Last member query interval	Interval for sending IGMP group-specific queries or IGMP group-and-source-specific queries, in seconds.
Last member query count	Number of IGMP group-specific queries or IGMP group-and-source-specific queries sent for the multicast group.
Startup query interval	Interval for sending IGMP general queries on startup, in seconds.
Startup query count	Number of IGMP general queries that the device sends on startup.
General query timer expiry	Remaining time for the IGMP general query timer. This field displays **Off** if the timer is disabled.
Querier for IGMP	IP address of the IGMP querier. This field is not displayed when the device runs IGMPv1 and the device is not the IGMP querier. NOTE: In IGMPv1, the PIM DR acts as the IGMP querier. You can use the **display pim interface** command to display PIM information.
No querier elected	No IGMP querier election is performed. This field is displayed when the device runs IGMPv1 and is not the IGMP querier. NOTE: In IGMPv1, the PIM DR acts as the IGMP querier. You can use the **display pim interface** command to display PIM information.
IGMP activity: 1 join(s), 0 leave(s)	Statistics of IGMP activities: • **join(s)**—Total number of multicast groups that this interface has joined. • **leave(s)**—Total number of multicast groups that this interface has left.
Multicast routing on this interface	Whether IP multicast routing is enabled: Enabled or Disabled.
Robustness	Robustness variable of the IGMP querier.
Require-router-alert	Whether the feature of dropping IGMP messages without

Field	Description
	Router-Alert is enabled: Enabled or Disabled,
Fast-leave	Whether the fast-leave processing feature is enabled: Enabled or Disabled.
Startup-query	Whether the IGMP querier sends IGMP general queries at the startup query interval on startup: • **On**—The IGMP querier performs the above action. • **Off**—The IGMP querier does not perform the above action.
Other-querier-present-timer-expiry	Remaining time for the other querier present timer. This field displays **Off** if the timer is disabled.
IGMP groups reported in total	Total number of multicast groups that the interface has joined dynamically. This field is not displayed if the interface does not join multicast groups.
IGMP proxy is enabled	IGMP proxying is enabled on the interface.
Version1-querier-present-timer-expiry	Remaining time for the IGMPv1 querier present timer. This field displays **Off** if the timer is disabled.

display igmp proxy group

Use **display igmp proxy group** to display information about multicast groups maintained by the IGMP proxy.

Syntax

display igmp [**vpn-instance** *vpn-instance-name*] **proxy group** [*group-address* | **interface** *interface-type interface-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays information about multicast groups maintained by the IGMP proxy on the public network.

group-address: Specifies a multicast group by its IP address in the range of 224.0.1.0 to 239.255.255.255. If you do not specify a multicast group, this command displays information about all multicast groups maintained by the IGMP proxy.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays information about multicast groups maintained by the IGMP proxy for all interfaces.

verbose: Displays detailed information.

Examples

Display information about multicast groups maintained by the IGMP proxy on the public network.

```
<Sysname> display igmp proxy group
IGMP proxy group records in total: 2
 GigabitEthernet1/0/1(1.1.1.20):
  IGMP proxy group records in total: 2
   Group address      Member state      Expires
   225.1.1.1          Delay             00:00:02
   225.1.1.2          Idle              Off
```

Display detailed information about multicast group 225.1.1.1 maintained by the IGMP proxy on the public network.

```
<Sysname> display igmp proxy group 225.1.1.1 verbose
 GigabitEthernet1/0/1(1.1.1.20):
  IGMP proxy group records in total: 2
   Group: 225.1.1.1
     Group mode: Include
     Member state: Delay
     Expires: 00:00:02
     Source list (sources in total: 1):
       1.1.1.1
```

Table 5 Command output

Field	Description
IGMP groups records in total	Total number of multicast groups maintained by the IGMP proxy.
GigabitEthernet1/0/1(1.1.1.20)	IGMP proxy interface and its IP address.
Pending proxy group	Pending multicast groups maintained by the IGMP proxy.
Group address/Group	Multicast group address.
Member state	Member host states: • **Delay**—The member host has joined a group and started a delay timer. • **Idle**—The member host has joined a group, but didn't start a delay timer.
Expires	Remaining delay time for the member host to send a responding report. This field displays **Off** if the timer is disabled.
Group mode	Multicast source filtering mode: Include or Exclude.
Source list	Multicast source list for the multicast group maintained by the IGMP proxy.
sources in total	Total number of multicast sources.

display igmp proxy routing-table

Use **display igmp proxy routing-table** to display multicast routing entries maintained by the IGMP proxy.

Syntax

display igmp [**vpn-instance** *vpn-instance-name*] **proxy routing-table** [*source-address* [**mask** { *mask-length* | *mask* }] | *group-address* [**mask** { *mask-length* | *mask* }]] * [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays multicast routing entries maintained by the IGMP proxy on the public network.

source-address: Specifies a multicast source by its IP address. If you do not specify a multicast source, this command displays multicast routing entries for all multicast sources maintained by the IGMP proxy.

group-address: Specifies a multicast group address by its IP address in the range of 224.0.1.0 to 239.255.255.255. If you do not specify a multicast group, this command displays multicast routing entries for all multicast groups maintained by the IGMP proxy.

mask-length: Specifies a mask length of the multicast group address or multicast source address. For a multicast source address, the value range for this argument is 0 to 32. For a multicast group address, the value range for this argument is 4 to 32. The default value is 32 in both cases.

mask: Specifies a mask of the multicast group address or multicast source address. The default value is 255.255.255.255.

verbose: Displays detailed information about multicast routing entries maintained by the IGMP proxy.

Examples

Display multicast routing entries maintained by the IGMP proxy on the public network.

```
<Sysname> display igmp proxy routing-table
 Total 1 (*, G) entries, 2 (S, G) entries.

 (172.168.0.12, 227.0.0.1)
     Upstream interface: GigabitEthernet1/0/1
     Downstream interfaces (1 in total):
         1: GigabitEthernet1/0/2
             Protocol: IGMP

(*, 225.1.1.1)
     Upstream interface: GigabitEthernet1/0/1
     Downstream interfaces (1 in total):
         1: GigabitEthernet1/0/2
             Protocol: STATIC

  (2.2.2.2, 225.1.1.1)
```

```
     Upstream interface: GigabitEthernet1/0/1
     Downstream interfaces (2 in total):
         1: LoopBack1
             Protocol: STATIC
         2: GigabitEthernet1/0/2
             Protocol: PROXY
```

Display detailed information about multicast routing entries maintained by the IGMP proxy on the public network.

```
<Sysname> display igmp proxy routing-table verbose
 Total 1 (*, G) entries, 2 (S, G) entries.

 (172.168.0.12, 227.0.0.1)
     Upstream interface: GigabitEthernet1/0/1
     Downstream interfaces (1 in total):
         1: GigabitEthernet1/0/2
             Protocol: IGMP
             Querier state: Querier
             Join/Prune state:Join

     Non-downstream interfaces: None

 (*, 225.1.1.1)
     Upstream interface: GigabitEthernet1/0/1
     Downstream interfaces (1 in total):
         1: GigabitEthernet1/0/2
             Protocol: STATIC
             Querier state: Querier
             Join/Prune state:Join

     Non-downstream interfaces (1 in total):
         1: GigabitEthernet1/0/2
             Protocol: IGMP
             Querier state: Non-querier
             Join/Prune state:Join

(2.2.2.2, 225.1.1.1)
     Upstream interface: GigabitEthernet1/0/1
     Downstream interfaces (2 in total):
         1: LoopBack1
             Protocol: STATIC
             Querier state: Querier
             Join/Prune state: Join
         2: GigabitEthernet1/0/2
             Protocol: PROXY
             Querier state: Querier
             Join/Prune state: Join

     Non-downstream interfaces: None
```

Table 6 Command output

Field	Description
Total 1 (*, G) entries, 2 (S, G) entries	Total number of (*, G) entries, and the total number of (S, G) entries.
(172.168.0.12, 227.0.0.1)	(S, G) entry.
Upstream interface	Incoming interface of the (S, G) entry.
Downstream interfaces (1 in total)	Outgoing interfaces of the (S, G) entry, and the total number of outgoing interfaces.
Non-downstream interfaces (1 in total)	Non-outgoing interfaces of the (S, G) entry, and the total number of non-outgoing interfaces.
1: GigabitEthernet1/0/2	Index of an interface, and the interface.
Protocol	Protocol type: • **IGMP**—Dynamic IGMP. • **PROXY**—IGMP proxy. • **STATIC**—Static IGMP.
Querier state	Querier state: • Querier. • Non-querier.
Join/Prune state	Joined or pruned state of the interface: • **NI**—Default state. • **Join**—Joined state. • **Prune**—Pruned state.

display igmp ssm-mapping

Use **display igmp ssm-mapping** to display IGMP SSM mappings.

Syntax

display igmp [**vpn-instance** *vpn-instance-name*] **ssm-mapping** *group-address*

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays information about the IGMP SSM mappings on the public network.

group-address: Specifies a multicast group by its IP address in the range of 224.0.1.0 to 239.255.255.255.

Examples

Display IGMP SSM mappings for multicast group 232.1.1.1 on the public network.

```
<Sysname> display igmp ssm-mapping 232.1.1.1
 Group: 232.1.1.1
 Source list:
        1.2.3.4
        5.5.5.5
        10.1.1.1
        100.1.1.10
```

Table 7 Command output

Field	Description
Group	Multicast group address.
Source list	List of multicast source addresses.

igmp

Use **igmp** to enter IGMP view.

Use **undo igmp** to delete the configurations in IGMP view.

Syntax

igmp [**vpn-instance** *vpn-instance-name*]

undo igmp [**vpn-instance** *vpn-instance-name*]

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command applies to the public network.

Examples

Enter IGMP view for the public network.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp]
```

Enter IGMP view for the VPN instance **mvpn**.

```
<Sysname> system-view
[Sysname] igmp vpn-instance mvpn
[Sysname-igmp-mvpn]
```

igmp enable

Use **igmp enable** to enable IGMP on an interface.

Use **undo igmp enable** to disable IGMP on an interface.

Syntax

igmp enable

undo igmp enable

Default

IGMP is disabled on an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command takes effect only when IP multicast routing is enabled on the public network or for the VPN instance to which the interface belongs.

Other IGMP configurations on the interface take effects only when IGMP is enabled on the interface.

Examples

Enable IP multicast routing on the public network, and enable IGMP on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] multicast routing
[Sysname-mrib] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp enable
```

Related commands

multicast routing

igmp fast-leave

Use **igmp fast-leave** to enable fast-leave processing on an interface.

Use **undo igmp fast-leave** to disable fast-leave processing on an interface.

Syntax

igmp fast-leave [**group-policy** *ipv4-acl-number*]

undo igmp fast-leave

Default

Fast-leave processing is disabled. The IGMP querier sends IGMP group-specific or group-and-source-specific queries after receiving a leave message.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-acl-number: Specifies an IPv4 basic ACL by its number in the range of 2000 to 2999. If you specify an ACL, the fast-leave processing feature takes effect only on the multicast groups that the ACL permits. The feature takes effect on all multicast groups when one of the following conditions exists:

- You do not specify an ACL.
- The specified ACL does not exist.
- The specified ACL does not have valid rules.

Usage guidelines

The fast-leave processing feature enables an IGMP querier to suppress IGMP group-specific or group-and-source-specific queries upon receiving IGMP leave messages permitted by the ACL.

When you configure a rule in the IPv4 basic ACL, follow these restrictions and guidelines:

- If the **vpn-instance** *vpn-instance* option is specified, the rule does not take effect.
- The **source** *source-address source-wildcard* option specifies a multicast group address.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

Examples

Enable fast-leave processing on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp fast-leave
```

igmp group-policy

Use **igmp group-policy** to configure a multicast group policy on an interface to control the multicast groups that hosts attached to the interface can join.

Use **undo igmp group-policy** to delete the multicast group policy on an interface.

Syntax

igmp group-policy *ipv4-acl-number* [*version-number*]

undo igmp group-policy

Default

No multicast group policy exists on an interface. Hosts attached to the interface can join any multicast groups.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-acl-number: Specifies an IPv4 basic or advanced ACL by its number in the range of 2000 to 3999. Hosts can join only the multicast groups that the ACL permits. If the ACL does not exist or does not have valid rules, hosts cannot join any multicast groups.

version-number: Specifies an IGMP version in the range of 1 to 3. By default, this command takes effect on IGMP reports of all versions.

Usage guidelines

A multicast group policy filters IGMP reports to control the multicast groups that the hosts can join.

This command does not take effect on static member interfaces because static member interfaces do not send IGMP reports.

When you configure a rule in the IPv4 ACL, follow these restrictions and guidelines:

- If the **vpn-instance** *vpn-instance* option is specified, the rule does not take effect.
- In a basic ACL, the **source** *source-address source-wildcard* option specifies a multicast group address.
- In an advanced ACL, the **source** *source-address source-wildcard* option specifies a multicast source address. The **destination** *dest-address dest-wildcard* option specifies a multicast group address.

  To match the following IGMP reports, set the **source** *source-address source-wildcard* option to 0.0.0.0:

  - IGMPv1 and IGMPv2 reports.
  - IGMPv3 IS_EX and IGMPv3 TO_EX reports that do not carry multicast source addresses.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure a multicast group policy on GigabitEthernet 1/0/1 so that hosts attached to the interface can join only multicast group 225.1.1.1.

```
<Sysname> system-view
[Sysname] acl basic 2005
[Sysname-acl-ipv4-basic-2005] rule permit source 225.1.1.1 0
[Sysname-acl-ipv4-basic-2005] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp group-policy 2005
```

igmp last-member-query-count

Use **igmp last-member-query-count** to set the IGMP last member query count on an interface.

Use **undo igmp last-member-query-count** to restore the default.

Syntax

igmp last-member-query-count *count*

undo igmp last-member-query-count

Default

The IGMP last member query count equals the IGMP querier's robustness variable.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

count: Specifies an IGMP last member query count in the range of 1 to 255.

Usage guidelines

You can set the IGMP last member query count for an interface in interface view or globally for all interfaces in IGMP view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the IGMP last member query count to 6 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp last-member-query-count 6
```

Related commands

last-member-query-count (IGMP view)

igmp last-member-query-interval

Use **igmp last-member-query-interval** to set the IGMP last member query interval on an interface.

Use **undo igmp last-member-query-interval** to restore the default.

Syntax

igmp last-member-query-interval *interval*

undo igmp last-member-query-interval

Default

The IGMP last member query interval is 1 second.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies an IGMP last member query interval in the range of 1 to 25 seconds.

Usage guidelines

You can set the IGMP last member query interval for an interface in interface view or globally for all interfaces in IGMP view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the IGMP last member query interval to 6 seconds on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp last-member-query-interval 6
```

Related commands

last-member-query-interval (IGMP view)

igmp max-response-time

Use **igmp max-response-time** to set the maximum response time for IGMP general queries on an interface.

Use **undo igmp max-response-time** to restore the default.

Syntax

igmp max-response-time *time*

undo igmp max-response-time

Default

The maximum response time for IGMP general queries is 10 seconds.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

time: Specifies the maximum response time for IGMP general queries, in the range of 1 to 3174 seconds.

Usage guidelines

You can set the maximum response time for an interface in interface view or globally for all interfaces in IGMP view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the maximum response time for IGMP general queries to 25 seconds on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp max-response-time 25
```

Related commands

max-response-time (IGMP view)

igmp non-stop-routing

Use **igmp non-stop-routing** to enable IGMP NSR.

Use **undo igmp non-stop-routing** to disable IGMP NSR.

Syntax

igmp non-stop-routing

undo igmp non-stop-routing

Default

IGMP NSR is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Examples

Enable IGMP NSR.

```
<Sysname> system-view
[Sysname] igmp non-stop-routing
```

igmp other-querier-present-interval

Use **igmp other-querier-present-interval** to set the IGMP other querier present timer on an interface.

Use **undo igmp other-querier-present-interval** to restore the default.

Syntax

igmp other-querier-present-interval *interval*

undo igmp other-querier-present-interval

Default

The IGMP other querier present timer is calculated by using the following formula:

[IGMP general query interval] × [IGMP querier's robustness variable] + [maximum response time for IGMP general queries] / 2.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies an IGMP other querier present timer in the range of 1 to 31744 seconds.

Usage guidelines

You can set the IGMP other querier present timer for an interface in interface view or globally for all interfaces in IGMP view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the IGMP other querier present timer to 125 seconds on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp other-querier-present-interval 125
```

Related commands

other-querier-present-interval (IGMP view)

igmp proxy enable

Use **igmp proxy enable** to enable IGMP proxying on an interface.

Use to **undo igmp proxy enable** to disable IGMP proxying on an interface.

Syntax

igmp proxy enable

undo igmp proxy enable

Default

IGMP proxying is disabled on an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command takes effect only when IP multicast routing is enabled on the public network or for the VPN instance to which the interface belongs.

Examples

Enable IP multicast routing on the public network, and enable IGMP proxying on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] multicast routing-enable
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp proxy enable
```

Related commands

multicast routing

igmp proxy forwarding

Use **igmp proxy forwarding** to enable multicast forwarding on a non-querier interface.

Use **undo igmp proxy forwarding** to disable multicast forwarding on a non-querier interface.

Syntax

igmp proxy forwarding

undo igmp proxy forwarding

Default

Multicast forwarding is disabled for a non-querier interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

Typically, only IGMP queriers can forward multicast traffic but non-queriers cannot. This mechanism prevents multicast data from being repeatedly forwarded. If a router interface on the IGMP proxy failed the querier election, enable multicast forwarding on the interface to forward multicast data to attached receivers.

Examples

Enable multicast forwarding on GigabitEthernet 1/0/1. (GigabitEthernet 1/0/1 is a non-querier interface on the IGMP proxy device.)

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp proxy forwarding
```

igmp query-interval

Use **igmp query-interval** to set the IGMP general query interval on an interface.

Use **undo igmp query-interval** to restore the default.

Syntax

igmp query-interval *interval*

undo igmp query-interval

Default

The IGMP general query interval is 125 seconds.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies an IGMP general query interval in the range of 1 to 31744 seconds.

Usage guidelines

You can set the IGMP general query interval for an interface in interface view or globally for all interfaces in IGMP view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the IGMP general query interval to 60 seconds on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp query-interval 60
```

Related commands

query-interval (IGMP view)

igmp robust-count

Use **igmp robust-count** to set the IGMP querier's robustness variable on an interface.

Use **undo igmp robust-count** to restore the default.

Syntax

igmp robust-count *count*

undo igmp robust-count

Default

The IGMP querier's robustness variable is 2.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

count: Specifies an IGMP querier's robustness variable in the range of 1 to 255.

Usage guidelines

The IGMP querier's robustness variable defines the number of times to retransmit queries if packet loss occurs. A higher robustness variable makes the IGMP querier more robust, but it increases timeout time for multicast groups.

You can set the IGMP querier's robustness variable for an interface in interface view or globally for all interfaces in IGMP view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the IGMP querier's robustness variable to 5 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp robust-count 5
```

Related commands

robust-count (IGMP view)

igmp startup-query-count

Use **igmp startup-query-count** to set the IGMP startup query count on an interface.

Use **undo igmp startup-query-count** to restore the default.

Syntax

igmp startup-query-count *count*

undo igmp startup-query-count

Default

The IGMP startup query count equals the IGMP querier's robustness variable.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

count: Specifies an IGMP startup query count in the range of 1 to 255.

Usage guidelines

You can set the IGMP startup query count for an interface in interface view or globally for all interfaces in IGMP view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the IGMP startup query count to 5 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp startup-query-count 5
```

Related commands

startup-query-count (IGMP view)

igmp startup-query-interval

Use **igmp startup-query-interval** to set the IGMP startup query interval on an interface.

Use **undo igmp startup-query-interval** to restore the default.

Syntax

igmp startup-query-interval *interval*

undo igmp startup-query-interval

Default

The IGMP startup query interval equals one quarter of the IGMP general query interval.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies an IGMP startup query interval in the range of 1 to 31744 seconds.

Usage guidelines

You can set the IGMP startup query interval for an interface in interface view or globally for all interfaces in IGMP view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the IGMP startup query interval to 100 seconds on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp startup-query-interval 100
```

Related commands

startup-query-interval (IGMP view)

igmp static-group

Use **igmp static-group** to configure an interface as a static group member of a multicast group.

Use **undo igmp static-group** to restore the default.

Syntax

igmp static-group *group-address* [**source** *source-address*]

undo igmp static-group { **all** | *group-address* [**source** *source-address*]

Default

An interface is not a static group member of multicast groups.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

group-address: Specifies a multicast group by its IP address in the range of 224.0.1.0 to 239.255.255.255.

source *source-address*: Specifies a multicast source by its IP address. If you do not specify a multicast source, this command configures an interface as a static member of the multicast groups with all multicast source addresses.

all: Specifies all multicast groups that the interface has statically joined.

Usage guidelines

For multicast routing entries to be created, you must specify a multicast source if the specified multicast group is in the SSM group range.

Examples

Configure GigabitEthernet 1/0/1 as a static group member of multicast group 224.1.1.1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp static-group 224.1.1.1
```

Configure GigabitEthernet 1/0/1 as a static group member of multicast source and group (192.168.1.1, 232.1.1.1).

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp static-group 232.1.1.1 source 192.168.1.1
```

igmp version

Use **igmp version** to specify an IGMP version on an interface.

Use **undo igmp version** to restore the default.

Syntax

igmp version *version-number*

undo igmp version

Default

The IGMP version on an interface is 2.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

version-number: Specifies an IGMP version in the range of 1 to 3.

Usage guidelines

CAUTION:
For IGMP to operate correctly, specify the same IGMP version for all devices on the same subnet.

Examples

Specify IGMP version 1 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp version 1
```

last-member-query-count (IGMP view)

Use **last-member-query-count** to set the IGMP last member query count globally.

Use **undo last-member-query-count** to restore the default.

Syntax

last-member-query-count *count*

undo last-member-query-count

Default

The IGMP last member query count equals the IGMP querier's robustness variable.

Views

IGMP view

Predefined user roles

network-admin

context-admin

Parameters

count: Specifies an IGMP last member query count in the range of 1 to 255.

Usage guidelines

You can set the IGMP last member query count globally for all interfaces in IGMP view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the global IGMP last member query count to 6 on the public network.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] last-member-query-count 6
```

Related commands

igmp last-member-query-count

last-member-query-interval (IGMP view)

Use **last-member-query-interval** to set the IGMP last member query interval globally.

Use **undo last-member-query-interval** to restore the default.

Syntax

last-member-query-interval *interval*

undo last-member-query-interval

Default

The IGMP last member query interval is 1 second.

Views

IGMP view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies an IGMP last member query interval in the range of 1 to 25 seconds.

Usage guidelines

You can set the IGMP last member query interval globally for all interfaces in IGMP view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the global IGMP last member query interval to 6 seconds on the public network.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] last-member-query-interval 6
```

Related commands

igmp last-member-query-interval

max-response-time (IGMP view)

Use **max-response-time** to set the maximum response time for IGMP general queries globally.

Use **undo max-response-time** to restore the default.

Syntax

max-response-time *time*

undo max-response-time

Default

The maximum response time for IGMP general queries is 10 seconds.

Views

IGMP view

Predefined user roles

network-admin

context-admin

Parameters

time: Specifies the maximum response time for IGMP general queries in the range of 1 to 3174 seconds.

Usage guidelines

You can set the maximum response time globally for all interfaces in IGMP view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

#Set the global maximum response time for IGMP general queries to 25 seconds on the public network.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] max-response-time 25
```

Related commands

igmp max-response-time

other-querier-present-interval (IGMP view)

Use **other-querier-present-interval** to set the IGMP other querier present timer globally.

Use **undo other-querier-present-interval** to restore the default.

Syntax

other-querier-present-interval *interval*

undo other-querier-present-interval

Default

The IGMP other querier present timer is calculated by using the following formula:

[IGMP general query interval] × [IGMP querier's robustness variable] + [maximum response time for IGMP general queries] / 2.

Views

IGMP view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies an IGMP other querier present timer in the range of 1 to 31744 seconds.

Usage guidelines

You can set the IGMP other querier present timer globally for all interfaces in IGMP view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the global IGMP other querier present timer to 125 seconds on the public network.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] other-querier-present-interval 125
```

Related commands

igmp other-querier-present-interval

proxy multipath (IGMP view)

Use **proxy multipath** to enable load splitting on an IGMP proxy device.

Use **undo proxy multipath** to disable load splitting on an IGMP proxy device.

Syntax

proxy multipath

undo proxy multipath

Default

The load splitting feature is disabled on the IGMP proxy device.

Views

IGMP view

Predefined user roles

network-admin

context-admin

Usage guidelines

Use this feature when the IGMP proxy device has multiple proxy interfaces. All proxy interfaces on the IGMP proxy device share multicast traffic on a per-group basis. If you do not enable this feature, only the proxy interface with the highest IP address forwards multicast data.

Examples

Enable load splitting on the IGMP proxy device on the public network.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] proxy multipath
```

query-interval (IGMP view)

Use **query-interval** to set the IGMP general query interval globally.

Use **undo query-interval** to restore the default.

Syntax

query-interval *interval*

undo query-interval

Default

The IGMP general query interval is 125 seconds.

Views

IGMP view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies an IGMP general query interval in the range of 1 to 31744 seconds.

Usage guidelines

You can set the IGMP general query interval globally for all interfaces in IGMP view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the global IGMP general query interval to 60 seconds on the public network.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] query-interval 60
```

Related commands

igmp query-interval

reset igmp group

Use **reset igmp group** to clear dynamic IGMP multicast group entries.

Syntax

reset igmp [**vpn-instance** *vpn-instance-name*] **group** { **all** | **interface** *interface-type interface-number* { **all** | *group-address* [**mask** { *mask* | *mask-length* }] [*source-address* [**mask** { *mask* | *mask-length* }]] } }

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears dynamic IGMP multicast group entries on the public network.

all: Specifies all interfaces (the first **all**), or all IGMP multicast groups (the second **all**).

interface-type interface-number: Specifies an interface by its type and number.

group-address: Specifies a multicast group by its IP address in the range of 224.0.0.0 to 239.255.255.255.

source-address: Specifies a multicast source address. If you do not specify a multicast source, this command clears dynamic IGMP multicast group entries for all multicast source addresses.

mask: Specifies an address mask. The default is 255.255.255.255.

mask-length: Specifies an address mask length. The default is 32. For a multicast group address, the value range for this argument is 4 to 32. For a multicast source address, the value range for this argument is 0 to 32.

Usage guidelines

CAUTION:
This command might interrupt the multicast information transmission.

Examples

Clear dynamic IGMP multicast group entries for all interfaces on the public network.

```
<Sysname> reset igmp group all
```

Clear all dynamic IGMP multicast group entries for GigabitEthernet 1/0/1 on the public network.

```
<Sysname> reset igmp group interface gigabitethernet 1/0/1 all
```

Clear the dynamic IGMP multicast group entry of group 225.0.0.1 for GigabitEthernet 1/0/1 on the public network.

```
<Sysname> reset igmp group interface gigabitethernet 1/0/1 225.0.0.1
```

Related commands

display igmp group

robust-count (IGMP view)

Use **robust-count** to set the IGMP querier's robustness variable globally.

Use **undo robust-count** to restore the default.

Syntax

robust-count *count*

undo robust-count

Default

The IGMP querier's robustness variable is 2.

Views

IGMP view

Predefined user roles

network-admin

context-admin

Parameters

count: Specifies an IGMP querier's robustness variable in the range of 1 to 255.

Usage guidelines

The IGMP querier's robustness variable defines the number of times to retransmit queries if packet loss occurs. A higher robustness variable makes the IGMP querier more robust, but it increases the timeout time for multicast groups.

You can set the IGMP querier's robustness variable globally for all interfaces in IGMP view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the global IGMP querier's robustness variable to 5 on the public network.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] robust-count 5
```

Related commands

igmp robust-count

ssm-mapping (IGMP view)

Use **ssm-mapping** to configure an IGMP SSM mapping.

Use **undo ssm-mapping** to delete IGMP SSM mappings.

Syntax

ssm-mapping *source-address ipv4-acl-number*

undo ssm-mapping { *source-address* | **all** }

Default

No IGMP SSM mappings exist.

Views

IGMP view

Predefined user roles

network-admin

context-admin

Parameters

source-address: Specifies a multicast source by its IP address.

ipv4-acl-number: Specifies a basic ACL number in the range of 2000 to 2999. Multicast groups in IGMP reports permitted by the ACL are associated with the multicast source. If the ACL does not exist or does not have valid rules, no multicast groups are associated with the multicast source.

all: Specifies all IGMP SSM mappings.

Usage guidelines

When you configure a rule in the IPv4 basic ACL, follow these restrictions and guidelines:

- If the **vpn-instance** *vpn-instance* option is specified, the rule does not take effect.

- The **source** *source-address source-wildcard* option specifies a multicast group address.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

Examples

Configure an IGMP SSM mapping with multicast source 125.1.1.1 and multicast group range 232.1.1.0/24 on the public network.

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 232.1.1.1 0.0.0.255
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] igmp
[Sysname-igmp] ssm-mapping 125.1.1.1 2001
```

Related commands

display igmp ssm-mapping

startup-query-count (IGMP view)

Use **startup-query-count** to set the IGMP startup query count globally.

Use **undo startup-query-count** to restore the default.

Syntax

startup-query-count *count*

undo startup-query-count

Default

The IGMP startup query count equals the IGMP querier's robustness variable.

Views

IGMP view

Predefined user roles

network-admin

context-admin

Parameters

count: Specifies an IGMP startup query count in the range of 1 to 255.

Usage guidelines

You can set the IGMP startup query count globally for all interfaces in IGMP view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the global IGMP startup query count to 5 on the public network.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] startup-query-count 5
```

Related commands

igmp startup-query-count

startup-query-interval (IGMP view)

Use **startup-query-interval** to set the IGMP startup query interval globally.

Use **undo startup-query-interval** to restore the default.

Syntax

startup-query-interval *interval*

undo startup-query-interval

Default

The IGMP startup query interval equals one quarter of the IGMP general query interval.

Views

IGMP view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies an IGMP startup query interval in the range of 1 to 31744 seconds.

Usage guidelines

You can set the IGMP startup query interval globally for all interfaces in IGMP view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the global IGMP startup query interval to 100 seconds on the public network.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] startup-query-interval 100
```

Related commands

igmp startup-query-interval

Contents

PIM commands

anycast-rp (PIM view)

Use **anycast-rp** to add an anycast RP member to an Anycast RP set.

Use **undo anycast-rp** to remove an anycast RP member from an Anycast RP set.

Syntax

anycast-rp *anycast-rp-address member-address*

undo anycast-rp *anycast-rp-address member-address*

Default

No Anycast RP sets exist.

Views

PIM view

Predefined user roles

network-admin

context-admin

Parameters

anycast-rp-address: Specifies an Anycast RP address. It must be a legal unicast IP address that is not in the range of 127.0.0.0/8.

member-address: Specifies an Anycast RP member address. It must be a legal unicast IP address that is not in the range of 127.0.0.0/8 and must be different from the Anycast RP address.

Usage guidelines

To add multiple RP member addresses to an Anycast RP set, execute this command multiple times with the same Anycast RP address but different RP member addresses.

To configure multiple Anycast RP sets, execute this command multiple times with different Anycast RP addresses.

Examples

Add Anycast RP members 1.1.0.1 and 1.2.0.1 to Anycast RP set 1.1.0.0 on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] anycast-rp 1.1.0.0 1.1.0.1
[Sysname-pim] anycast-rp 1.1.0.0 1.2.0.1
```

Related commands

display pim rp-info

auto-rp enable (PIM view)

Use **auto-rp enable** to enable Auto-RP listening.

Use **undo auto-rp enable** to disable Auto-RP listening.

Syntax

auto-rp enable

undo auto-rp enable

Default

Auto-RP listening is disabled.

Views

PIM view

Predefined user roles

network-admin

context-admin

Usage guidelines

After Auto-RP listening is enabled, the device can receive and forward Auto-RP announcement and discovery messages, but it cannot send these messages unsolicitedly.

Examples

Enable Auto-RP listening on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] auto-rp enable
```

bidir-pim enable (PIM view)

Use **bidir-pim enable** to enable BIDIR-PIM.

Use **undo bidir-pim enable** to disable BIDIR-PIM.

Syntax

bidir-pim enable

undo bidir-pim enable

Default

BIDIR-PIM is disabled.

Views

PIM view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command takes effect only when IP multicast routing is enabled on the public network or for a VPN instance to which the device belongs.

Examples

Enable IP multicast routing on the public network, and enable BIDIR-PIM.

```
<Sysname> system-view
[Sysname] multicast routing
[Sysname-mrib] quit
```

```
[Sysname] pim
[Sysname-pim] bidir-pim enable
```

Related commands

multicast routing

bidir-rp-limit (PIM view)

Use **bidir-rp-limit** to set the maximum number of BIDIR-PIM RPs.

Use **undo bidir-rp-limit** to restore the default.

Syntax

bidir-rp-limit *limit*

undo bidir-rp-limit

Default

The maximum number of BIDIR-PIM RPs is 128.

Views

PIM view

Predefined user roles

network-admin

context-admin

Parameters

limit: Specifies the maximum number of BIDIR-PIM RPs, in the range of 1 to 128.

Usage guidelines

In a BIDIR-PIM domain, one DF election per RP is implemented on all PIM interfaces. To avoid unnecessary DF elections, do not configure multiple BIDIR-PIM RPs.

This command sets a limit on the number of BIDIR-PIM RPs. If the number of RPs exceeds the limit, excess RPs can be used only for DF election rather than multicast data forwarding.

Examples

Set the maximum number of BIDIR-PIM RPs to 3 on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] bidir-rp-limit 3
```

bsm-fragment enable (PIM view)

Use **bsm-fragment enable** to enable bootstrap message (BSM) semantic fragmentation.

Use **undo bsm-fragment enable** to disable BSM semantic fragmentation.

Syntax

bsm-fragment enable

undo bsm-fragment enable

Default

BSM semantic fragmentation is enabled.

Views

PIM view

Predefined user roles

network-admin

context-admin

Usage guidelines

Disable BSM semantic fragmentation if the PIM-SM or BIDIR-PIM domain contains a device that does not support BSM semantic fragmentation.

Examples

Disable BSM semantic fragmentation on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] undo bsm-fragment enable
```

bsm-reflection enable (PIM view)

Use **bsm-reflection enable** to enable the device to forward BSMs out of their incoming interfaces.

Use **undo bsm-reflection enable** to disable the device from forwarding BSMs out of their incoming interfaces.

Syntax

bsm-reflection enable

undo bsm-reflection enable

Default

The device forwards BSMs out of their incoming interfaces.

Views

PIM view

Predefined user roles

network-admin

context-admin

Usage guidelines

Disable this feature if all the devices in the PIM-SM or BIDIR-PIM domain have consistent routing information.

Examples

Disable the device from forwarding BSMs out of their incoming interfaces on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] undo bsm-reflection enable
```

bsr-policy (PIM view)

Use **bsr-policy** to configure a BSR policy.

Use **undo bsr-policy** to restore the default.

Syntax

bsr-policy *ipv4-acl-number*

undo bsr-policy

Default

No BSR policy exists, and all bootstrap messages are regarded as legal.

Views

PIM view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-acl-number: Specifies an IPv4 basic ACL by its number in the range of 2000 to 2999.

Usage guidelines

A BSR policy filters bootstrap messages to guard against BSR spoofing.

When you configure a rule in the IPv4 basic ACL, follow these restrictions and guidelines:

- If the **vpn-instance** *vpn-instance* option is specified, the rule does not take effect.
- The **source** *source-address source-wildcard* option specifies a BSR address.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure a BSR policy on the public network so that only the devices on subnet 10.1.1.0/24 can act as the BSR.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule permit source 10.1.1.0 0.0.0.255
[Sysname-acl-ipv4-basic-2000] quit
[Sysname] pim
[Sysname-pim] bsr-policy 2000
```

Related commands

c-bsr (PIM view)

c-bsr (PIM view)

Use **c-bsr** to configure a candidate-BSR (C-BSR).

Use **undo c-bsr** to remove the configuration of a C-BSR.

Syntax

c-bsr *ip-address* [**scope** *group-address* { *mask-length* | *mask* }] [**hash-length** *hash-length* | **priority** *priority*] *

undo c-bsr *ip-address* [**scope** *group-address* { *mask-length* | *mask* }]

Default

No C-BSRs exist.

Views

PIM view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the IP address of a C-BSR. You must specify the IP address of a local PIM interface.

scope *group-address*: Specifies a multicast group by its IP address in the range of 239.0.0.0 to 239.255.255.255. If you do not specify a multicast group, this command designates the C-BSR to the global-scoped zone.

mask-length: Specifies an address mask length in the range of 8 to 32.

mask: Specifies an address mask.

hash-length *hash-length*: Specifies a hash mask length in the range of 0 to 32. The default setting is 30.

priority *priority*: Specifies a C-BSR priority in the range of 0 to 255. The default setting is 64. The greater the value, the higher the priority.

Usage guidelines

If you execute this command for a zone multiple times, the most recent configuration takes effect.

You can configure the same C-BSR for different zones.

Examples

Configure the interface with IP address 1.1.1.1 as a C-BSR for the global-scoped zone on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr 1.1.1.1
```

c-rp (PIM view)

Use **c-rp** to configure a candidate-RP (C-RP).

Use **undo c-rp** to remove the configuration of a C-RP.

Syntax

c-rp *ip-address* [**advertisement-interval** *adv-interval* | **group-policy** *ipv4-acl-number* | **holdtime** *hold-time* | **priority** *priority*] * [**bidir**]

undo c-rp *ip-address*

Default

No C-RPs exist.

Views

PIM view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the IP address of a C-RP. You must specify the IP address of a local PIM interface.

advertisement-interval *adv-interval*: Specifies a C-RP advertisement interval in the range of 1 to 65535 seconds. The default value is 60 seconds.

group-policy *ipv4-acl-number*: Specifies an IPv4 basic ACL by its number in the range of 2000 to 2999. If you specify an ACL, this command designates the C-RP to IPv4 multicast groups in C-RP advertisement messages that the ACL permits. The C-RP is designated to all IPv4 multicast groups when one of the following conditions exists:

- You do not specify an ACL.
- The specified ACL does not exist.
- The specified ACL does not have valid rules.

holdtime *hold-time*: Specifies a C-RP lifetime in the range of 1 to 65535 seconds. The default value is 150 seconds.

priority *priority*: Specifies a C-RP priority in the range of 0 to 255. The default setting is 192. The greater the value, the lower the priority.

bidir: Specifies BIDIR-PIM to which the C-RP is designated. If you do not specify this keyword, the C-RP provides services for PIM-SM.

Usage guidelines

To designate a C-RP to multiple multicast group ranges, create multiple rules that specify different multicast group ranges in the ACL.

When you configure a rule in the IPv4 basic ACL, follow these restrictions and guidelines:

- If the **vpn-instance** *vpn-instance* option is specified, the rule does not take effect.
- The **source** *source-address source-wildcard* option specifies a multicast group range.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

If you execute this command by using the same C-RP address multiple times, the most recent configuration takes effect.

Examples

Configure the interface with IP address 1.1.1.1 as a C-RP for multicast group ranges 225.1.0.0/16 and 226.2.0.0/16 and set its priority to 10 on the public network.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule permit source 225.1.0.0 0.0.255.255
[Sysname-acl-ipv4-basic-2000] rule permit source 226.2.0.0 0.0.255.255
[Sysname-acl-ipv4-basic-2000] quit
[Sysname] pim
[Sysname-pim] c-rp 1.1.1.1 group-policy 2000 priority 10
```

crp-policy (PIM view)

Use **crp-policy** to configure a C-RP policy.

Use **undo crp-policy** to restore the default.

Syntax

crp-policy *ipv4-acl-number*

undo crp-policy

Default

No C-RP policy exists, and all C-RP messages are regarded as legal.

Views

PIM view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-acl-number: Specifies an IPv4 advanced ACL number in the range of 3000 to 3999.

Usage guidelines

A C-RP policy filters C-RP advertisement messages to guard against C-RP spoofing.

The device uses only the prefixes of the multicast group ranges in advertisement messages to match the destination field in ACL rules. For example, the multicast group range in an advertisement message is 224.1.0.0/16. If the prefix 224.1.0.0 is in the range specified by the destination field of an ACL rule, the specified C-RPs are designated to this multicast group range.

When you configure a rule in the IPv4 advanced ACL, follow these restrictions and guidelines:

- If the **vpn-instance** *vpn-instance* option is specified, the rule does not take effect.
- The **source** *source-address source-wildcard* option specifies an RP address.
- The **destination** *dest-address dest-wildcard* option specifies a multicast group address.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure a C-RP policy on the public network so that only devices in the range of 1.1.1.1/24 can be C-RPs for the groups in the range of 225.1.1.0/24.

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule permit ip source 1.1.1.1 0.0.0.255 destination 225.1.1.0
0.0.0.255
[Sysname-acl-ipv4-adv-3000] quit
[Sysname] pim
[Sysname-pim] crp-policy 3000
```

Related commands

c-rp (PIM view)

display interface register-tunnel

Use **display interface register-tunnel** to display register-tunnel interface information.

Syntax

display interface [**register-tunnel** [*interface-number*]] [**brief** [**description** | **down**]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

register-tunnel [*interface-number*]: Specifies a register-tunnel interface by its number. The device has only one register-tunnel interface, Register-Tunnel 0. If you specify the **register-tunnel** keyword, this command displays information about Register-Tunnel 0 regardless of whether you specify an interface number. If you do not specify the **register-tunnel** keyword, this command displays information about all interfaces.

brief: Displays brief information. If you do not specify this keyword, the command displays detailed information.

description: Displays the full interface description. If you do not specify this keyword, the command displays only the first 27 characters of the interface description.

down: Displays information about the interfaces in down state and the reasons why the interfaces are down. If you do not specify this keyword, the command displays information about interfaces in all states.

Usage guidelines

The register-tunnel interface is a virtual interface that is automatically created by the system. You cannot configure it or delete it, but you can display the interface information by using this command.

In the initial stage of multicast source registration, the register-tunnel interface is used to establish a channel between the source-side DR and the RP to transmit multicast register messages. The process of initial source registration is as follows:

1. After receiving the first multicast data from the source, the source-side DR encapsulates the multicast data into a register message. Then, it forwards the message to the RP through the register-tunnel interface.
2. The register message reaches RP on the register-tunnel interface on the RP. The RP decapsulates the register message and forwards the multicast data to the receiver hosts. At the same time, the RP learns the IP address of the multicast source.
3. The RP sends a join message toward the multicast source to build an SPT.
4. After the SPT is built, the multicast data travels to the RP along the SPT rather than through the register-tunnel interface.

Examples

Display detailed information about Register-Tunnel 0.

```
<Sysname> display interface register-tunnel 0
Register-Tunnel0
```

```
Current state: UP
Line protocol state: DOWN
Description: Register-Tunnel0 Interface
Maximum transmission unit: 1536
Internet protocol processing: Disabled
Physical: Unknown
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

Display brief information about Register-Tunnel 0.

```
<Sysname> display interface register-tunnel 0 brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP         Description
REG0                 UP   --       --
```

Table 1 Command output

Field	Description
Current state	Physical link state of the interface. This field always displays **UP**.
Line protocol state	Data link layer state of interface. This field always displays **DOWN**.
Description	Description of the interface. It is not configurable.
Maximum transmission unit	MTU of the register-tunnel interface. It is not configurable.
Internet protocol processing: Disabled	The interface is not assigned an IP address and cannot process IP packets.
Physical	Physical type of the interface. This field always displays **Unknown**, because the physical type of the interface is unknown.
Last 300 seconds input rate	Average incoming rate in the last 300 seconds. This field always displays **0**.
Last 300 seconds output rate	Average outgoing rate in the last 300 seconds. This field always displays **0**.
Input	Number of incoming packets, incoming bytes, and discarded packets. This field always displays **0**.
Output	Number of outgoing packets, outgoing bytes, and discarded packets. This field always displays **0**.
Brief information on interfaces in route mode	Brief information about Layer 3 interfaces.
Link	Physical link state of the interface. This field always displays **UP**.
Protocol	Data link layer protocol state of the interface. This field always displays two hyphens (--) because the interface does not support a data link layer protocol.
Primary IP	Primary IP address of the interface. This field always displays two hyphens (**--**) because the interface does not have a primary IP address.
Cause	Cause for the physical link state of an interface to be **DOWN**. This field always displays **Not connected** because no physical connection exists.
Description	Description of the interface. This field is empty because the interface

Field	Description
	cannot be configured with a description.

Related command

reset counters interface register-tunnel

display pim bsr-info

Use **display pim bsr-info** to display BSR information.

Syntax

display pim [**vpn-instance** *vpn-instance-name*] **bsr-info**

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays BSR information on the public network.

Examples

Display BSR information on the public network.

```
<Sysname> display pim bsr-info
 Scope: non-scoped
     State: Accept Preferred
     Bootstrap timer: 00:01:44
     Elected BSR address: 12.12.12.1
       Priority: 64
       Hash mask length: 30
       Uptime: 00:21:56

 Scope: 239.4.0.0/16
     State: Accept Any
     Scope-zone expiry timer: 00:21:12

 Scope: 239.1.0.0/16
     State: Elected
     Bootstrap timer: 00:00:26
     Elected BSR address: 17.1.11.1
       Priority: 64
       Hash mask length: 30
       Uptime: 02:53:37
```

```
    Candidate BSR address: 17.1.11.1
      Priority: 64
      Hash mask length: 30

Scope: 239.2.2.0/24
    State: Candidate
    Bootstrap timer: 00:01:56
    Elected BSR address: 61.2.37.1
      Priority: 64
      Hash mask length: 30
      Uptime: 02:53:32
    Candidate BSR address: 17.1.12.1
      Priority: 64
      Hash mask length: 30

Scope: 239.3.3.0/24
    State: Pending
    Bootstrap timer: 00:00:07
    Candidate BSR address: 17.1.13.1
      Priority: 64
      Hash mask length: 30
```

Table 2 Command output

Field	Description
Bootstrap timer	Aging timer for the BSR.
Scope-zone expiry timer	Aging timer for the scoped zone.
Elected BSR address	Address of the elected BSR.
Candidate BSR address	Address of the C-BSR.
Priority	BSR priority.
Uptime	Length of time the BSR has been up.

display pim claimed-route

Use **display pim claimed-route** to display information about all routes that PIM uses.

Syntax

display pim [**vpn-instance** *vpn-instance-name*] **claimed-route** [*source-address*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays information about all routes that PIM uses on the public network.

source-address: Specifies a multicast source by its IP address. If you do not specify a multicast source, this command displays information about all routes that PIM uses.

Examples

Display information about all routes that PIM uses on the public network.

```
<Sysname> display pim claimed-route
 RPF-route selecting rule: longest-match

 Route/mask: 7.11.0.0/16 (unicast (direct))
     RPF interface: GigabitEthernet1/0/1, RPF neighbor: 8.0.0.2
     Total number of (S,G) or (*,G) dependent on this route entry: 4
     (7.11.0.10, 225.1.1.1)
     (7.11.0.10, 226.1.1.1)
     (7.11.0.10, 227.1.1.1)
     (*, 228.1.1.1)
 Route/mask: 7.12.0.0/16 (multicast static)
     RPF interface: GigabitEthernet1/0/2, RPF neighbor: 8.0.0.3,
     Config NextHop: 8.0.0.5
     Total number of (S,G) or (*,G) dependent on this route entry: 2
     (7.12.0.10, 226.1.1.1)
     (7.12.0.10, 225.1.1.1)
```

Table 3 Command output

Field	Description
Route/mask	Route entry. Route types in parentheses include: • **igp**—IGP unicast route. • **egp**—EGP unicast route. • **unicast (direct)**—Direct unicast route. • **unicast**—Other unicast route, such as static unicast route. • **mbgp**—MBGP route. • **multicast static**—Static multicast route.
RPF interface	Name of the RPF interface.
RPF neighbor	IP address of the RPF neighbor.
Config NextHop	Address of the configured next hop. This field is displayed only when the static multicast route is configured with a next hop.
Total number of (S,G) or (*,G) dependent on this route entry	Total number of (S, G) or (*, G) entries associated with the RPF route and the entry list.

display pim c-rp

Use **display pim c-rp** to display C-RP information.

Syntax

display pim [**vpn-instance** *vpn-instance-name*] **c-rp** [**local**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays information about learned C-RPs on the public network.

local: Specifies local C-RPs. If you do not specify this keyword, the command displays information about all C-RPs.

Usage guidelines

You can view information about learned C-RPs only on the BSR. On other devices, you can view information about the locally configured C-RPs.

Examples

Display information about learned C-RPs on the public network.

```
<Sysname> display pim c-rp
 Scope: non-scoped
     Group/MaskLen: 224.0.0.0/4
       C-RP address             Priority  HoldTime  Uptime    Expires
       1.1.1.1 (local)          192       150       03:01:36  00:02:29
       2.2.2.2                  192       150       1d:13h    00:02:02
     Group/MaskLen: 226.1.1.0/24 [B] Expires: 00:00:33
     Group/MaskLen: 225.1.0.0/16 [B]
       C-RP Address             Priority  HoldTime  Uptime    Expires
       3.3.3.3                  192       150       12w:5d    00:02:05
```

Display information about the locally configured C-RPs.

```
<Sysname> display pim c-rp local
 Candidate RP: 12.12.12.9(Loop1)
     Priority: 192
     HoldTime: 150
     Advertisement interval: 60
     Next advertisement scheduled at: 00:00:48
```

Table 4 Command output

Field	Description
Group/MaskLen	Multicast group to which the C-RP is designated.
[B]	BIDIR-PIM C-RP. This field is not displayed if the C-RP is a PIM-SM C-RP.
C-RP address	IP address of the C-RP. If the C-RP resides on the device where the

Field	Description
	command is executed, this field displays **(local)** after the address.
Priority	Priority of the C-RP.
HoldTime	Lifetime of the C-RP.
Uptime	Length of time the C-RP has been up: • **w**—Weeks. • **d**—Days. • **h**—Hours.
Expires	Remaining lifetime for the C-RP and the multicast group.
Candidate RP	IP address of the locally configured C-RP.
Advertisement interval	Interval between two advertisement messages sent by the locally configured C-RP.
Next advertisement scheduled at	Remaining time for the locally configured C-RP to send the next advertisement message.

display pim df-info

Use **display pim df-info** to display BIDIR-PIM DF information.

Syntax

display pim [**vpn-instance** *vpn-instance-name*] **df-info** [*rp-address*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays BIDIR-PIM DF information on the public network.

rp-address: Specifies a BIDIR-PIM RP by its IP address.

Examples

Display BIDIR-PIM DF information on the public network.

```
<Sysname> display pim df-info
RP address: 12.12.12.12
  Interface: GigabitEthernet1/0/4
    State     : Win        DF preference: 10
    DF metric : 1562       DF uptime    : 00:06:59
    DF address: 30.1.1.11 (local)
  Interface: Tunnel2, 100.1.1.12
    State     : Lose       DF preference: 0
```

```
DF metric : 0          DF uptime    : 00:06:59
DF address: 100.1.1.12
```

Table 5 Command output

Field	Description
RP address	IP address of the BIDIR-PIM RP.
Interface	DF interface. If the interface is an NBMA mode-enabled ADVPN tunnel interface, this field also displays the IP address of the remote end.
State	DF election state: • **Win**—The interface wins the DF election. • **Lose**—The interface loses the DF election. • **Offer**—The interface is in the initial state of the DF election. • **Backoff**—The interface is acting as the DF, but there are more appropriate devices running for the DF. This field displays a hyphen (-) if the interface does not participate in the DF election.
DF preference	Advertised route preference for DF election.
DF metric	Advertised route metric for DF election.
DF uptime	Length of time the DF has been up.
DF address	IP address of DF. If the DF resides on the device where the command is executed, this field displays **(local)** after the IP address.

display pim interface

Use **display pim interface** to display PIM information for interfaces.

Syntax

display pim [**vpn-instance** *vpn-instance-name*] **interface** [*interface-type interface-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays PIM information for interfaces on the public network.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays PIM information for all interfaces.

verbose: Displays detailed PIM information. If you do not specify this keyword, the command displays brief PIM information.

Examples

Display brief PIM information for all interfaces on the public network.

```
<Sysname> display pim interface
 Interface         NbrCnt  HelloInt  DR-Pri     DR-Address
 GE1/0/1           1       30        1          10.1.1.2
 GE1/0/2           0       30        1          172.168.0.2    (local)
 GE1/0/3           1       30        1          20.1.1.2
```

Table 6 Command output

Field	Description
NbrCnt	Number of PIM neighbors.
HelloInt	Interval for sending hello messages.
DR-Pri	Priority for DR election.
DR-Address	IP address of the DR. If the DR resides on the device where the command is executed, this field displays **(local)** after the address.

Display detailed PIM information for GigabitEthernet 1/0/1 on the public network.

```
<Sysname> display pim interface gigabitethernet 1/0/1 verbose
 Interface: GigabitEthernet1/0/1, 10.1.1.1
     PIM version: 2
     PIM mode: Sparse
     PIM DR: 10.1.1.2
     PIM DR Priority (configured): 1
     PIM neighbors count: 1
     PIM hello interval: 30 s
     PIM LAN delay (negotiated): 500 ms
     PIM LAN delay (configured): 500 ms
     PIM override interval (negotiated): 2500 ms
     PIM override interval (configured): 2500 ms
     PIM neighbor tracking (negotiated): disabled
     PIM neighbor tracking (configured): disabled
     PIM generation ID: 0xF5712241
     PIM require generation ID: disabled
     PIM hello hold interval: 105 s
     PIM assert hold interval: 180 s
     PIM triggered hello delay: 5 s
     PIM J/P interval: 60 s
     PIM J/P hold interval: 210 s
     PIM state-refresh capable (negotiated): enabled
     PIM state-refresh capable (configured): enabled
     PIM state-refresh interval: 60 s
     PIM state-refresh rate limit: 30 s
     PIM state-refresh TTL: 255
     PIM graft retry interval: 3 s
     PIM BSR domain border: disabled
```

```
PIM BFD: disabled
PIM passive: disabled
PIM prune-pending: disabled
Number of routers on network not using DR priority: 0
Number of routers on network not using LAN delay: 0
Number of routers on network not using neighbor tracking: 2
```

Table 7 Command output

Field	Description
PIM version	Version of the PIM protocol.
PIM mode	PIM mode: dense or sparse.
PIM DR	IP address of the DR.
PIM DR Priority (configured)	Configured priority for DR election.
PIM neighbors count	Total number of PIM neighbors.
PIM hello interval	Interval between two hello messages.
PIM LAN delay (negotiated)	Negotiated PIM message propagation delay.
PIM LAN delay (configured)	Configured PIM message propagation delay.
PIM override interval (negotiated)	Negotiated interval for overriding prune messages.
PIM override interval (configured)	Configured interval for overriding prune messages.
PIM neighbor tracking (negotiated)	Negotiated neighbor tracking status: enabled or disabled.
PIM neighbor tracking (configured)	Configured neighbor tracking status: enabled or disabled.
PIM require generation ID	Whether the feature of discarding hello messages without Generation_ID is enabled.
PIM hello hold interval	PIM neighbor lifetime.
PIM assert hold interval	Assert holdtime timer.
PIM triggered hello delay	Maximum delay for sending hello messages.
PIM J/P interval	Interval between two join or prune messages.
PIM J/P hold interval	Joined/pruned state holdtime timer.
PIM state-refresh capable (negotiated)	Negotiated state refresh status.
PIM state-refresh capable (configured)	Configured state refresh status.
PIM state-refresh rate limit	Waiting time for accepting a new state refresh message.
PIM state-refresh TTL	TTL value in state refresh messages.
PIM BSR domain border	Whether a PIM domain border is configured.
PIM BFD	Whether PIM is enabled to work with BFD.
PIM passive	Whether PIM passive mode is enabled on the interface.
PIM prune-pending	Whether PIM prune delay is enabled on the interface.
Number of routers on network not using DR priority	Number of routers that do not use the DR priority field on the subnet where the interface resides.
Number of routers on network not using LAN delay	Number of routers that do not use the LAN delay field on the subnet where the interface resides.
Number of routers on network not using	Number of routers that are not enabled with neighbor tracking

Field	Description
neighbor tracking	on the subnet where the interface resides.

display pim nbma-link

Use **display pim nbma-link** to display remote end information maintained by PIM for ADVPN tunnel interfaces.

Syntax

display pim [**vpn-instance** *vpn-instance-name*] **nbma-link** [**interface** { *interface-type interface-number* }]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays remote end information maintained by PIM for ADVPN tunnel interfaces on the public network.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays remote end information maintained by PIM for all ADVPN tunnel interfaces.

Examples

Display remote end information maintained by PIM for ADVPN tunnel interfaces on the public network.

```
<Sysname> display pim nbma-link
Interface: Tunnel1
Number of links: 1
    Remote address: 10.0.0.1
      Private index    : 0XCC000000
      Private interface: Multicast-NBMA0
Interface: Tunnel2
Number of links: 1
    Remote address: 20.0.0.2
      Private index    : 0XCC000001
      Private interface: Multicast-NBMA1
```

Display remote end information maintained by PIM for ADVPN interface **tunnel1** on the public network.

```
<Sysname> display pim nbma-link interface tunnel 1
Interface: Tunnel1
Number of links: 1
    Remote address: 10.0.0.1
```

```
Private index    : 0XCC000000
Private interface: Multicast-NBMA0
```

Table 8 Command output

Field	Description
Interface	Local ADVPN tunnel interface.
Number of links	Number of remote ends.
Remote address	IP address of the remote end.
Private index	Index of the remote end.
Private interface	Interface name of the remote end.

display pim neighbor

Use **display pim neighbor** to display PIM neighbor information.

Syntax

display pim [**vpn-instance** *vpn-instance-name*] **neighbor** [*neighbor-address* | **interface** *interface-type interface-number* | **verbose**] *

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays PIM neighbor information on the public network.

neighbor-address: Specifies a PIM neighbor by its IP address. If you do not specify a PIM neighbor, this command displays information about all PIM neighbors.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays PIM neighbor information on all interfaces.

verbose: Displays detailed PIM neighbor information. If you do not specify this keyword, the command displays brief PIM neighbor information.

Examples

Display brief information about all PIM neighbors on the public network.

```
<Sysname> display pim neighbor
 Total Number of Neighbors = 2

 Neighbor        Interface           Uptime   Expires  DR-Priority Mode
 10.1.1.2        GE1/0/1             02:50:49 00:01:31 1           B
 20.1.1.2        GE1/0/2             02:49:39 00:01:42 1           P
```

Display detailed information about the PIM neighbor with IP address 11.110.0.20 on the public network.

```
<Sysname> display pim neighbor 11.110.0.20 verbose
 Neighbor: 11.110.0.20
     Interface: GigabitEthernet1/0/3
     Uptime: 00:00:10
     Expiry time: 00:00:30
     DR Priority: 1
     Generation ID: 0x2ACEFE15
     Holdtime: 105 s
     LAN delay: 500 ms
     Override interval: 2500 ms
     State refresh interval: 60 s
     Neighbor tracking: Disabled
     Bidirectional PIM: Disabled
```

Table 9 Command output

Field	Description
Total Number of Neighbors	Total number of PIM neighbors.
Neighbor	IP address of the PIM neighbor.
Interface	Interface that connects to the PIM neighbor.
Uptime	Length of time the PIM neighbor has been up.
Expires/Expiry time	Remaining lifetime for the PIM neighbor. If the PIM neighbor is always up and reachable, this field displays **never**.
DR-Priority/DR Priority	Priority of the PIM neighbor.
Mode	PIM mode: • **B**—The PIM mode is BIDIR-PIM. • **P**—The RPF proxy vector is enabled. This field is empty if the PIM mode is not BIDIR-PIM and the RPF vector is disabled.
Generation ID	Generation ID of the PIM neighbor. (A random value represents a status change of the PIM neighbor.)
Holdtime	Lifetime of the PIM neighbor. If the PIM neighbor is always up and reachable, this field displays **forever**.
LAN delay	PIM message propagation delay on a shared-media LAN.
Override interval	Interval for overriding prune messages.
State refresh interval	Interval for refreshing state. This field is displayed only when the PIM neighbor operates in the PIM-DM mode and the state refresh capability is enabled.
Neighbor tracking	Neighbor tracking status: enabled or disabled.
Bidirectional PIM	Whether BIDIR-PIM is enabled.

display pim routing-table

Use **display pim routing-table** to display PIM routing entries.

Syntax

display pim [**vpn-instance** *vpn-instance-name*] **routing-table** [*group-address* [**mask** { *mask-length* | *mask* }] | *source-address* [**mask** { *mask-length* | *mask* }] | **flags** *flag-value* | **fsm** | **incoming-interface** *interface-type interface-number* | **mode** *mode-type* | **outgoing-interface** { **exclude** | **include** | **match** } *interface-type interface-number* | **extranet** { **source-vpn-instance** *source-vpn-instance-name* | **source-public-instance** | **receive-vpn-instance** *receive-vpn-instance-name* | **receive-public-instance** }] *

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays PIM routing entries on the public network.

group-address: Specifies a multicast group by its IP address in the range of 224.0.0.0 to 239.255.255.255. If you do not specify a multicast group, this command displays PIM routing entries for all multicast groups.

source-address: Specifies a multicast source by its IP address.

mask-length: Specifies an address mask length in the range of 0 to 32. The default value is 32.

mask: Specifies an address mask. The default value is 255.255.255.255.

flags *flag-value*: Specifies a flag. If you do not specify a flag, this command displays PIM routing entries that contain all flags. The following lists the values for the *flag-value* argument and their meanings:

- **act**: Specifies PIM routing entries that have been used for routing data.
- **del**: Specifies PIM routing entries to be deleted.
- **exprune**: Specifies PIM routing entries containing outgoing interfaces pruned by other multicast routing protocols.
- **ext**: Specifies PIM routing entries containing outgoing interfaces provided by other multicast routing protocols.
- **loc**: Specifies PIM routing entries on the devices that reside on the same subnet as the multicast source.
- **niif**: Specifies PIM routing entries containing unknown incoming interfaces.
- **nonbr**: Specifies PIM routing entries with PIM neighbor lookup failure.
- **rpt**: Specifies PIM routing entries on the RPT branches where (S, G) prunes have been sent to the RP.
- **rq**: Specifies PIM routing entries of the receiving side of the data-MDT switchover.
- **spt**: Specifies PIM routing entries on the SPT.
- **sq**: Specifies PIM routing entries of the originator side of data-MDT switchover.

- **swt**: Specifies PIM routing entries in the process of RPT-to-SPT switchover.
- **wc**: Specifies PIM routing entries with wildcards.

fsm: Displays detailed information about the finite state machine.

incoming-interface *interface-type interface-number*: Specifies an incoming interface. If you do not specify an incoming interface, this command displays PIM routing entries that contain all incoming interfaces.

mode *mode-type*: Specifies a PIM mode. If you do not specify a PIM mode, this command displays PIM routing entries in all PIM modes. The available PIM modes include:

- **bidir**: Specifies BIDIR-PIM.
- **dm**: Specifies PIM-DM.
- **sm**: Specifies PIM-SM.
- **ssm**: Specifies PIM-SSM.

outgoing-interface { **exclude** | **include** | **match** } *interface-type interface-number*: Specifies an outgoing interface. If you do not specify an outgoing interface, this command displays PIM routing entries that contain all outgoing interfaces. Whether an outgoing interface is contained in the PIM routing table depends on the following conditions:

- If you specify an excluded interface, this command displays PIM routing entries that do not contain the specified outgoing interface.
- If you specify an included interface, this command displays PIM routing entries that contain the specified outgoing interface.
- If you specify a matching interface, this command displays PIM routing entries that contain only the specified outgoing interface.

extranet: Displays information about the PIM routing entries for MVPN extranet.

- **source-vpn-instance** *source-vpn-instance-name*: Specifies the MPLS L3VPN instance to which the multicast source belongs. The *source-vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters.
- **source-public-instance**: Specifies the public network where the multicast source resides.
- **receive-vpn-instance** *receive-vpn-instance-name*: Specifies the MPLS L3VPN instance to which the multicast receiver belongs. The *receive-vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters.
- **receive-public-instance**: Specifies the public network where the multicast receiver resides.

Examples

Display PIM routing entries on an ADVPN network.

```
<Sysname> display pim routing-table
 Total 0 (*, G) entries; 1 (S, G) entries

 (172.168.0.12, 227.0.0.1)
     RP: 2.2.2.2
     Protocol: pim-sm, Flag: SPT LOC ACT
     UpTime: 02:54:43
     Upstream interface: Tunnel2, 13.1.1.1
         Upstream neighbor: 12.1.1.1
         RPF prime neighbor: 12.1.1.1
     Downstream interface information:
```

```
     Total number of downstream interfaces: 1
         1: Tunnel2, 13.1.1.2
             Protocol: pim-sm, UpTime: 02:54:43, Expires: 00:02:47
```

Display PIM routing entries on the public network.

```
<Sysname> display pim routing-table
 Total 0 (*, G) entries; 1 (S, G) entries

 (172.168.0.12, 227.0.0.1)
     RP: 2.2.2.2
     Protocol: pim-sm, Flag: SPT LOC ACT
     UpTime: 02:54:43
     Upstream interface: GigabitEthernet1/0/1
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface information:
     Total number of downstream interfaces: 1
         1: GigabitEthernet1/0/2
             Protocol: pim-sm, UpTime: 02:54:43, Expires: 00:02:47
```

Display PIM routing entries for MVPN extranet.

```
<Sysname> display pim vpn-instance vpn1 routing-table extranet receive-vpn-instance vpn2
 Total 1 (*, G) entries; 1 (S, G) entries
 (*, 225.0.0.2)
     RP: 1.2.2.2
     Protocol: pim-sm, Flag: WC
     UpTime: 07:06:11
     Upstream interface: Register-Tunnel0
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface information:
     Total number of downstream interfaces: 2
         1: GigabitEthernet1/0/1
             Protocol: pim-sm, UpTime: 07:06:11, Expires: -
         2: Extranet (VPN: vpn2)
             Protocol: MD, UpTime: 01:12:52, Expires: -

(11.1.1.53, 225.0.0.2)
     RP: 1.2.2.2
     Protocol: pim-sm, Flag: SPT LOC ACT
     UpTime: 07:06:10
     Upstream interface: MTunnel0
         Upstream neighbor: 1.1.1.1
         RPF prime neighbor: 1.1.1.1
     Downstream interface information:
     Total number of downstream interfaces: 2
         1: GigabitEthernet1/0/1
             Protocol: pim-sm, UpTime: 07:06:11, Expires: -
         2: Extranet (VPN: vpn2)
             Protocol: MD, UpTime: 01:29:07, Expires: -
```

Table 10 Command output

Field	Description
Total 0 (*, G) entries; 1 (S, G) entries	Total number of (*, G) entries, and the total number of (S, G) entries.
(172.168.0.12, 227.0.0.1)	(S, G) entry.
Protocol	PIM mode.
Flag	Flag of the (S, G) entry or (*, G) entry: • **ACT**—The entry has been used for routing data. • **DEL**—The entry is to be removed. • **EXPRUNE**—Some outgoing interfaces are pruned by other multicast routing protocols. • **EXT**—The entry contains outgoing interfaces provided by other multicast routing protocols. • **LOC**—The entry is on a router directly connected to the same subnet with the multicast source. • **NIIF**—The entry contains unknown incoming interfaces. • **NONBR**—The entry has a PIM neighbor lookup failure. • **RPT**—The entry is on an RPT branch where (S, G) prunes have been sent to the RP. • **SPT**—The entry is on the SPT. • **SQ**—The entry triggers the default-MDT to data-MDT switchover. • **SWT**—The entry is in the process of RPT-to-SPT switchover. • **WC**—The entry contains a wildcard.
Uptime	Length of time for which the (S, G) entry or (*, G) entry has been up.
Upstream interface	Upstream (incoming) interface of the (S, G) entry or (*, G) entry. If the upstream interface is an NBMA mode-enabled ADVPN tunnel interface, this field also displays the IP address of the remote end.
Upstream neighbor	Upstream neighbor of the (S, G) entry or (*, G) entry.
RPF prime neighbor	RPF neighbor of the (S, G) or (*, G) entry: • For a (*, G) entry, if the RPF neighbor is the RP, the field displays **NULL**. • For an (S, G) entry, if the RPF neighbor is a router that directly connects to the multicast source, this field displays **NULL**.
Downstream interface information	Information about the downstream interfaces: • Total number of downstream interfaces. • Names of the downstream interfaces. • Protocol type on the downstream interfaces. • Uptime of the downstream interfaces. • Expiration time of the downstream interfaces. • IP addresses of the remote ends associated with the downstream ADVPN tunnel interfaces.
Extranet	PIM routing entry for MVPN extranet. • In the upstream interface list, the source VPN is displayed after **Extranet**. • In the downstream interface list, the receiver VPN is displayed after **Extranet**.

display pim rp-info

Use **display pim rp-info** to display PIM RP information.

Syntax

display pim [**vpn-instance** *vpn-instance-name*] **rp-info** [*group-address*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays RP information on the public network.

group-address: Specifies a multicast group by its IP address in the range of 224.0.1.0 to 239.255.255.255. If you do not specify a multicast group, this command displays RP information for all multicast groups.

Examples

Display RP information for multicast group 224.0.1.1 on the public network.

```
<Sysname> display pim rp-info 224.0.1.1
 BSR RP address is: 2.2.2.2
     Priority: 192
     HoldTime: 180
     Uptime: 03:01:10
     Expires: 00:02:30

 Static RP address is: 3.3.3.5
     Preferred: Yes
     Configured ACL: 2003

 RP mapping for this group is: 3.3.3.5

 Anycast-RP 3.3.3.5 members:
     Member address           State
     1.1.0.1                  Active
     1.2.0.2                  Local
     1.2.0.1                  Remote
```

Display RP information for all multicast groups on the public network.

```
<Sysname> display pim rp-info
 BSR RP information:
   Scope: non-scoped
     Group/MaskLen: 224.0.0.0/4
       RP address               Priority  HoldTime  Uptime    Expires
```

```
    1.1.1.1 (local)          192       180       03:01:36  00:02:29
    2.2.2.2                  192       180       1d:13h    00:02:02
  Group/MaskLen: 225.1.0.0/16 [B]
    RP address               Priority  HoldTime  Uptime    Expires
    3.3.3.3                  192       180       12w:5d    00:02:05

Static RP information:
    RP address               ACL   Mode    Preferred
    3.3.3.1                  2000  pim-sm  No
    3.3.3.2                  2001  pim-sm  Yes
    3.3.3.3                  2002  pim-sm  No
    3.3.3.4                        pim-sm  No
    3.3.3.5                  2002  pim-sm  Yes

Anycast-RP information:
    RP address               Member address          State
    3.3.3.5                  1.1.0.1                 Active
    3.3.3.5                  1.1.0.2                 Local
    3.3.3.5                  1.2.0.1                 Remote
```

Table 11 Command output

Field	Description
BSR RP address is	IP address of the RP.
BSR RP information	Information about the RP.
Group/MaskLen	Multicast group to which the RP is designated.
[B]	The RP is a BIDIR-PIM RP. This field is not displayed if the RP is a PIM-SM RP.
RP address	IP address of the RP. If the RP resides on the device where the command is executed, this field displays **(local)** after the address.
Priority	Priority of the RP.
HoldTime	RP lifetime.
Uptime	Length of time the RP has been up.
Expires	Remaining lifetime for the RP.
Preferred	Whether the static RP is preferred.
Configured ACL/ACL	ACL defining the multicast groups to which the static RP is designated.
Mode	RP service mode: PIM-SM or BIDIR-PIM.
RP mapping for this group	IP address of the RP that provides services for the multicast group.
Anycast-RP 3.3.3.5 members	Members of Anycast RP 3.3.3.5.
Member address	IP address of the Anycast RP member.
State	State of the interface from which the member address originates: • **Active**—Activated local interface. • **Local**—Inactivated local interface. • **Remote**—Remote interface.

display pim statistics

Use **display pim statistics** to display statistics for PIM packets.

Syntax

display pim statistics

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display statistics for PIM packets.

```
<Sysname> display pim statistics
 Received PIM packets: 3295
 Sent PIM packets    : 5975
                Valid       Invalid        Succeeded   Failed
    Hello     : 3128        0              4333        0
    Reg       : 14          0              0           0
    Reg-stop  : 0           0              0           0
    JP        : 151         0              561         0
    BSM       : 0           0              1081        0
    Assert    : 0           0              0           0
    Graft     : 0           0              0           0
    Graft-ACK: 0            0              0           0
    C-RP      : 0           0              0           0
    SRM       : 0           0              0           0
    DF        : 0           0              0           0
    AutoRP    : 0           0              0           0
```

Table 12 Command output

Field	Description
Received PIM packets	Total number of received PIM protocol packets.
Sent PIM packets	Total number of sent PIM protocol packets.
Valid	Number of received legal PIM protocol packets.
Invalid	Number of received illegal PIM protocol packets.
Succeeded	Number of PIM protocol packets that were sent successfully.
Failed	Number of PIM protocol packets that failed to be sent.
Hello	Hello message statistics.
Reg	Register message statistics.
Reg-stop	Register-stop message statistics.

Field	Description
JP	Join or prune message statistics.
BSM	Bootstrap message statistics.
Assert	Assert message statistics.
Graft	Graft message statistics.
Graft-ACK	Graft-ACK message statistics.
C-RP	C-RP message statistics.
SRM	State refresh message statistics.
DF	Designated forwarder statistics.
AutoRP	Auto-RP message statistics.

hello-option dr-priority (PIM view)

Use **hello-option dr-priority** to set the DR priority globally.

Use **undo hello-option dr-priority** to restore the default.

Syntax

hello-option dr-priority *priority*

undo hello-option dr-priority

Default

The DR priority is 1.

Views

PIM view

Predefined user roles

network-admin

context-admin

Parameters

priority: Specifies a DR priority in the range of 0 to 4294967295. The greater the value, the higher the priority.

Usage guidelines

You can set the DR priority globally for all interfaces in PIM view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the global DR priority to 3 on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] hello-option dr-priority 3
```

Related commands

pim hello-option dr-priority

hello-option holdtime (PIM view)

Use **hello-option holdtime** to set the PIM neighbor lifetime globally.

Use **undo hello-option holdtime** to restore the default.

Syntax

hello-option holdtime *time*

undo hello-option holdtime

Default

The PIM neighbor lifetime is 105 seconds.

Views

PIM view

Predefined user roles

network-admin

context-admin

Parameters

time: Specifies a PIM neighbor lifetime in the range of 1 to 65535 seconds. If you set the value to 65535 seconds, PIM neighbors are always reachable.

Usage guidelines

You can set the PIM neighbor lifetime globally for all interfaces in PIM view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the global PIM neighbor lifetime to 120 seconds on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] hello-option holdtime 120
```

Related commands

pim hello-option holdtime

hello-option lan-delay (PIM view)

Use **hello-option lan-delay** to set the PIM message propagation delay on a shared-media LAN globally.

Use **undo hello-option lan-delay** to restore the default.

Syntax

hello-option lan-delay *delay*

undo hello-option lan-delay

Default

The PIM message propagation delay on a shared-media LAN is 500 milliseconds.

Views

PIM view

Predefined user roles

network-admin

context-admin

Parameters

delay: Specifies a PIM message propagation delay on a shared-media LAN, in the range of 1 to 32767 milliseconds.

Usage guidelines

You can set the PIM message propagation delay globally for all interfaces in PIM view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the global PIM message propagation delay on a shared-media LAN to 200 milliseconds on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] hello-option lan-delay 200
```

Related commands

hello-option override-interval (PIM view)

pim hello-option lan-delay

pim hello-option override-interval

hello-option neighbor-tracking (PIM view)

Use **hello-option neighbor-tracking** to enable neighbor tracking globally.

Use **undo hello-option neighbor-tracking** to disable neighbor tracking globally.

Syntax

hello-option neighbor-tracking

undo hello-option neighbor-tracking

Default

Neighbor tracking is disabled.

Views

PIM view

Predefined user roles

network-admin

context-admin

Usage guidelines

You can enable neighbor tracking globally for all interfaces in PIM view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Enable neighbor tracking globally on the public network.

```
<Sysname> system-view
[Sysname] pim
```

```
[Sysname-pim] hello-option neighbor-tracking
```

Related commands

pim hello-option neighbor-tracking

hello-option override-interval (PIM view)

Use **hello-option override-interval** to set the override interval globally.

Use **undo hello-option override-interval** to restore the default.

Syntax

hello-option override-interval *interval*

undo hello-option override-interval

Default

The override interval is 2500 milliseconds.

Views

PIM view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies an override interval in the range of 1 to 65535 milliseconds.

Usage guidelines

You can set the override interval globally for all interfaces in PIM view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the global override interval to 2000 milliseconds on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] hello-option override-interval 2000
```

Related commands

hello-option lan-delay (PIM view)

pim hello-option lan-delay

pim hello-option override-interval

holdtime join-prune (PIM view)

Use **holdtime join-prune** to set the joined or pruned state holdtime globally.

Use **undo holdtime join-prune** to restore the default.

Syntax

holdtime join-prune *time*

undo holdtime join-prune

Default

The joined or pruned state holdtime is 210 seconds.

Views

PIM view

Predefined user roles

network-admin

context-admin

Parameters

time: Specifies a joined or pruned state holdtime in the range of 1 to 65535 seconds.

Usage guidelines

You can set the joined or pruned state holdtime globally for all interfaces in PIM view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

To prevent the upstream neighbors from aging out, you must set the join or prune interval to be less than the joined or pruned state holdtime.

Examples

Set the global joined or pruned state holdtime to 280 seconds on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] holdtime join-prune 280
```

Related commands

pim holdtime join-prune

timer join-prune (PIM view)

jp-pkt-size (PIM view)

Use **jp-pkt-size** to set the maximum size of a join or prune message.

Use **undo jp-pkt-size** to restore the default.

Syntax

jp-pkt-size *size*

undo jp-pkt-size

Default

The maximum size of a join or prune message is 1200 bytes.

Views

PIM view

Predefined user roles

network-admin

context-admin

Parameters

size: Specifies the maximum size of a join or prune message, in the range of 100 to 8100 bytes.

Examples

Set the maximum size of a join or prune message to 1500 bytes on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] jp-pkt-size 1500
```

pim

Use **pim** to enter PIM view.

Use **undo pim** to remove all configurations in PIM view.

Syntax

pim [**vpn-instance** *vpn-instance-name*]

undo pim [**vpn-instance** *vpn-instance-name*]

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, you enter public network PIM view.

Examples

Enable IP multicast routing on the public network and enter PIM view of the public network.

```
<Sysname> system-view
[Sysname] multicast routing
[Sysname-mrib] quit
[Sysname] pim
[Sysname-pim]
```

Enable IP multicast routing for VPN instance **mvpn** and enter PIM view of VPN instance **mvpn**.

```
<Sysname> system-view
[Sysname] multicast routing vpn-instance mvpn
[Sysname-mrib-mvpn] quit
[Sysname] pim vpn-instance mvpn
[Sysname-pim-mvpn]
```

Related commands

multicast routing-enable

pim bfd enable

Use **pim bfd enable** to enable BFD for PIM.

Use **undo pim bfd enable** to disable BFD for PIM.

Syntax

pim bfd enable

undo pim bfd enable

Default

BFD is disabled for PIM.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command takes effect only when PIM-DM or PIM-SM is enabled on the interface.

Examples

Enable IP multicast routing on the public network. Then, enable PIM-DM on Tunnel 10, and enable BFD for PIM on the interface.

```
<Sysname> system-view
[Sysname] multicast routing
[Sysname-mrib] quit
[Sysname] interface Tunnel 10
[Sysname-Tunnel10] pim dm
[Sysname-Tunnel10] pim bfd enable
```

Related commands

pim dm

pim sm

pim bsr-boundary

Use **pim bsr-boundary** to configure a PIM-SM domain border (a bootstrap message boundary).

Use **undo pim bsr-boundary** to restore the default.

Syntax

pim bsr-boundary

undo pim bsr-boundary

Default

An interface is not a PIM-SM domain border.

Views

Interface view

Predefined user roles

network-admin

context-admin

Examples

Configure Tunnel 10 as a PIM-SM domain border.

```
<Sysname> system-view
[Sysname] interface Tunnel 10
[Sysname-Tunnel10] pim bsr-boundary
```

Related commands

c-bsr (PIM view)

multicast boundary

pim dm

Use **pim dm** to enable PIM-DM.

Use **undo pim dm** to disable PIM-DM.

Syntax

pim dm

undo pim dm

Default

PIM-DM is disabled.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command takes effect only when IP multicast routing is enabled on the public network or for the VPN instance to which the interface belongs.

Examples

Enable IP multicast routing on the public network, and enable PIM-DM on Tunnel 10.

```
<Sysname> system-view
[Sysname] multicast routing
[Sysname-mrib] quit
[Sysname] interface Tunnel 10
[Sysname-Tunnel10] pim dm
```

Related commands

multicast routing

pim hello-option dr-priority

Use **pim hello-option dr-priority** to set the DR priority on an interface.

Use **undo pim hello-option dr-priority** to restore the default.

Syntax

pim hello-option dr-priority *priority*

undo pim hello-option dr-priority

Default

The DR priority is 1.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

priority: Specifies a DR priority in the range of 0 to 4294967295. The greater the value, the higher the priority.

Usage guidelines

You can set the DR priority for an interface in interface view or globally for all interfaces in PIM view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the DR priority to 3 on Tunnel 10.

```
<Sysname> system-view
[Sysname] interface Tunnel 10
[Sysname-Tunnel10] pim hello-option dr-priority 3
```

Related commands

hello-option dr-priority (PIM view)

pim hello-option holdtime

Use **pim hello-option holdtime** to set the PIM neighbor lifetime on an interface.

Use **undo pim hello-option holdtime** to restore the default.

Syntax

pim hello-option holdtime *time*

undo pim hello-option holdtime

Default

The PIM neighbor lifetime is 105 seconds.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

time: Specifies a PIM neighbor lifetime in the range of 1 to 65535 seconds. If you set the value to 65535 seconds, the PIM neighbor is always reachable.

Usage guidelines

You can set the PIM neighbor lifetime for an interface in interface view or globally for all interfaces in PIM view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the PIM neighbor lifetime to 120 seconds on Tunnel 10.

```
<Sysname> system-view
[Sysname] interface Tunnel 10
[Sysname-Tunnel10] pim hello-option holdtime 120
```

Related commands

hello-option holdtime (PIM view)

pim hello-option lan-delay

Use **pim hello-option lan-delay** to set the PIM message propagation delay on a shared-media LAN for an interface.

Use **undo pim hello-option lan-delay** to restore the default.

Syntax

pim hello-option lan-delay *delay*

undo pim hello-option lan-delay

Default

The PIM message propagation delay on a shared-media LAN is 500 milliseconds.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

delay: Specifies a PIM message propagation delay on a shared-media LAN in the range of 1 to 32767 milliseconds.

Usage guidelines

You can set the PIM message propagation delay for an interface in interface view or globally for all interfaces in PIM view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the PIM message propagation delay on a shared-media LAN to 200 milliseconds on Tunnel 10.

```
<Sysname> system-view
[Sysname] interface Tunnel 10
[Sysname-Tunnel10] pim hello-option lan-delay 200
```

Related commands

hello-option lan-delay (PIM view)

hello-option override-interval (PIM view)

pim hello-option override-interval

pim hello-option neighbor-tracking

Use **pim hello-option neighbor-tracking** to enable neighbor tracking on an interface.

Use **pim hello-option neighbor-tracking disable** to disable neighbor tracking on an interface when neighbor tracking is enabled globally.

Use **undo pim hello-option neighbor-tracking** to restore neighbor tracking setting on an interface to be consistent with the global setting.

Syntax

pim hello-option neighbor-tracking

pim hello-option neighbor-tracking disable

undo pim hello-option neighbor-tracking

Default

Neighbor tracking is disabled on an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

You can enable neighbor tracking for an interface in interface view or globally for all interfaces in PIM view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Enable neighbor tracking on Tunnel 10.

```
<Sysname> system-view
[Sysname] interface Tunnel 10
[Sysname-Tunnel10] pim hello-option neighbor-tracking
```

Disable neighbor tracking on Tunnel 10 when neighbor tracking is enabled globally on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] hello-option neighbor-tracking
[Sysname-pim] quit
[Sysname] interface Tunnel 10
[Sysname-Tunnel10] pim hello-option neighbor-tracking disable
```

Related commands

hello-option neighbor-tracking (PIM view)

pim hello-option override-interval

Use **pim hello-option override-interval** to set the override interval on an interface.

Use **undo pim hello-option override-interval** to restore the default.

Syntax

pim hello-option override-interval *interval*

undo pim hello-option override-interval

Default

The override interval is 2500 milliseconds.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies an override interval in the range of 1 to 65535 milliseconds.

Usage guidelines

You can set the override interval for an interface in interface view or globally for all interfaces in PIM view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the override interval to 2000 milliseconds on Tunnel 10.

```
<Sysname> system-view
[Sysname] interface Tunnel 10
[Sysname-Tunnel10] pim hello-option override-interval 2000
```

Related commands

hello-option lan-delay (PIM view)

hello-option override-interval (PIM view)

pim hello-option lan-delay

pim holdtime join-prune

Use **pim holdtime join-prune** to set the joined or pruned state holdtime on an interface.

Use **undo pim holdtime join-prune** to restore the default.

Syntax

pim holdtime join-prune *time*

undo pim holdtime join-prune

Default

The joined or pruned state holdtime is 210 seconds.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

time: Specifies a joined or pruned state holdtime in the range of 1 to 65535 seconds.

Usage guidelines

You can set the joined or pruned state holdtime for an interface in interface view or globally for all interfaces in PIM view. For an interface, the interface-specific configuration takes priority over the global configuration.

To prevent the upstream neighbors from aging out, you must configure the join or prune interval to be less than the joined or pruned state holdtime.

Examples

Set the joined or pruned state holdtime to 280 seconds on Tunnel 10.

```
<Sysname> system-view
[Sysname] interface Tunnel 10
[Sysname-Tunnel10] pim holdtime join-prune 280
```

Related commands

holdtime join-prune (PIM view)

pim timer join-prune

pim nbma-mode

Use **pim nbma-mode** to enable NBMA mode for an ADVPN tunnel interface.

Use **undo pim nbma-mode** to disable NBMA mode on an ADVPN tunnel interface.

Syntax

pim nbma-mode

undo pim nbma-mode

Default

NBMA mode is disabled for an ADVPN tunnel interface.

Views

Tunnel interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command is not available for PIM-DM.

This command takes effect only when PIM-SM is enabled on the interface on the public network or for the VPN instance to which the device belongs.

Examples

Enable IP multicast routing on the public network, and enable NBMA mode on ADVPN tunnel interface **tunnel2**.

```
<Sysname> system-view
[Sysname] multicast routing
[Sysname-mrib] quit
[Sysname] interface tunnel 2 mode advpn gre
```

```
[Sysname-Tunnel2] pim sm
[Sysname-Tunnel2] pim nbma-mode
```

pim neighbor-policy

Use **pim neighbor-policy** to configure a PIM hello policy.

Use **undo pim neighbor-policy** to restore the default.

Syntax

pim neighbor-policy *ipv4-acl-number*

undo pim neighbor-policy

Default

No PIM hello policy exists on an interface, and all PIM hello messages are regarded as legal.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-acl-number: Specifies an IPv4 basic ACL number in the range of 2000 to 2999.

Usage guidelines

A PIM hello policy filters PIM hello messages to guard against hello message spoofing.

When you configure a rule in the IPv4 basic ACL, follow these restrictions and guidelines:

- If the **vpn-instance** *vpn-instance* option is specified, the rule does not take effect.
- The **source** *source-address source-wildcard* option specifies a source IP address.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure a PIM hello policy on Tunnel 10 so that only the devices on subnet 10.1.1.0/24 can become PIM neighbors of this router.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule permit source 10.1.1.0 0.0.0.255
[Sysname-acl-ipv4-basic-2000] quit
[Sysname] interface Tunnel 10
[Sysname-Tunnel10] pim neighbor-policy 2000
```

pim non-stop-routing

Use **pim non-stop-routing** to enable PIM NSR.

Use **undo pim non-stop-routing** to disable PIM NSR.

Syntax

pim non-stop-routing

undo pim non-stop-routing

Default

PIM NSR is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Examples

Enable PIM NSR.

```
<Sysname> system-view
[Sysname] pim non-stop-routing
```

pim passive

Use **pim passive** to enable PIM passive mode on an interface.

Use **undo pim passive** to disable PIM passive mode on an interface.

Syntax

pim passive

undo pim passive

Default

PIM passive mode is disabled on an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command takes effect only when PIM-DM or PIM-SM is enabled on the interface.

Examples

Enable IP multicast routing on the public network. Then, enable PIM-DM and enable PIM passive mode on Tunnel 10.

```
<Sysname> system-view
[Sysname] multicast routing
[Sysname-mrib] quit
[Sysname] interface Tunnel 10
[Sysname-Tunnel10] pim dm
[Sysname-Tunnel10] pim passive
```

pim prune-pending

Use **pim prune-pending** to enable PIM prune delay on an interface.

Use **undo pim prune-pending** to disable PIM prune delay on an interface.

Syntax

pim prune-pending

undo pim prune-pending

Default

PIM prune delay is disabled on an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command takes effect only when PIM-DM or PIM-SM is enabled on the interface.

By default, an interface determines whether to starts the prune delay timer when it receives a prune message based on the number of PIM neighbors it. An interface starts the prune delay timer only when it has more than one PIM neighbor. When the prune delay timer expires, the device remove the receiving interface from the output interface list of the (S, G) entry.

In a DRNI-capable Layer 3 multicast network, the IP addresses of the two DR interfaces on DR devices are the same, the upstream device will consider the DR devices as one PIM neighbor and will not start the prune delay timer. When one DR device sends a prune message to the upstream device, the upstream device immediately remote the DR interface from the output interface list of the (S, G) entry. If the other DR device has receivers connected and the network is complex, the upstream device need to wait a long time to receive prune messages from the DR device. This situation causes multicast traffic interruption for a long time.

This feature allows the device to enable PIM prune delay and start the prune delay timer regardless of the number of PIM neighbors on an interface. The value of the timer is the sum of the override interval (configured by using the **pim hello-option override-interval** command) and the PIM message propagation delay (configured by using the **pim hello-option lan-delay** command).

Examples

Enable PIM prune delay on the public network. Then, enable PIM-DM and enable PIM passive mode on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] multicast routing
[Sysname-mrib] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] pim dm
[Sysname-GigabitEthernet1/0/1] pim prune-pending
```

Related commands

pim hello-option lan-delay

pim hello-option override-interval

pim require-genid

Use **pim require-genid** to enable dropping hello messages without the generation ID options.

Use **undo pim require-genid** to restore the default.

Syntax

pim require-genid

undo pim require-genid

Default

Hello messages without the generation ID options are accepted.

Views

Interface view

Predefined user roles

network-admin

context-admin

Examples

Enable Tunnel 10 to drop hello messages without the generation ID options.

```
<Sysname> system-view
[Sysname] interface Tunnel 10
[Sysname-Tunnel10] pim require-genid
```

pim sm

Use **pim sm** to enable PIM-SM.

Use **undo pim sm** to disable PIM-SM.

Syntax

pim sm

undo pim sm

Default

PIM-SM is disabled.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command takes effect only when IP multicast routing is enabled on the public network or for the VPN instance to which the interface belongs.

Examples

Enable IP multicast routing on the public network, and enable PIM-SM on Tunnel 10.

```
<Sysname> system-view
[Sysname] multicast routing
```

```
[Sysname-mrib] quit
[Sysname] interface Tunnel 10
[Sysname-Tunnel10] pim sm
```

Related commands

multicast routing

pim state-refresh-capable

Use **pim state-refresh-capable** to enable the state refresh feature on an interface.

Use **undo pim state-refresh-capable** to disable the state refresh feature.

Syntax

pim state-refresh-capable

undo pim state-refresh-capable

Default

The state refresh feature is enabled.

Views

Interface view

Predefined user roles

network-admin

context-admin

Examples

Disable the state refresh feature on Tunnel 10.

```
<Sysname> system-view
[Sysname] interface Tunnel 10
[Sysname-Tunnel10] undo pim state-refresh-capable
```

Related commands

state-refresh-interval (PIM view)

state-refresh-rate-limit (PIM view)

state-refresh-ttl (PIM view)

pim timer graft-retry

Use **pim timer graft-retry** to set a graft retry timer.

Use **undo pim timer graft-retry** to restore the default.

Syntax

pim timer graft-retry *interval*

undo pim timer graft-retry

Default

The graft retry timer is 3 seconds.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies a graft retry timer in the range of 1 to 65535 seconds.

Examples

Set the graft retry timer to 80 seconds on Tunnel 10

```
<Sysname> system-view
[Sysname] interface Tunnel 10
[Sysname-Tunnel10] pim timer graft-retry 80
```

pim timer hello

Use **pim timer hello** to set the hello interval on an interface.

Use **undo pim timer hello** to restore the default.

Syntax

pim timer hello *interval*

undo pim timer hello

Default

The hello interval is 30 seconds.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies a hello interval in the range of 0 to 18000 seconds. If you set the value to 0 seconds, the interface does not send hello messages.

Usage guidelines

You can set the hello interval for an interface in interface view or globally for all interfaces in PIM view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the hello interval to 40 seconds on Tunnel 10.

```
<Sysname> system-view
[Sysname] interface Tunnel 10
[Sysname-Tunnel10] pim timer hello 40
```

Related commands

timer hello (PIM view)

pim timer join-prune

Use **pim timer join-prune** to set the join or prune interval on an interface.

Use **undo pim timer join-prune** to restore the default.

Syntax

pim timer join-prune *interval*

undo pim timer join-prune

Default

The join or prune interval is 60 seconds.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies a join or prune interval in the range of 0 to 18000 seconds. If you set the value to 0 seconds, the interface does not send join or prune messages.

Usage guidelines

You can set the join or prune interval for an interface in interface view or globally for all interfaces in PIM view. For an interface, the interface-specific configuration takes priority over the global configuration.

The configuration takes effect after the current interval ends.

To prevent the upstream neighbors from aging out, you must set the join or prune interval to be less than the joined or pruned state holdtime.

Examples

Set the join or prune interval to 80 seconds on Tunnel 10.

```
<Sysname> system-view
[Sysname] interface Tunnel 10
[Sysname-Tunnel10] pim timer join-prune 80
```

Related commands

pim holdtime join-prune

timer join-prune (PIM view)

pim triggered-hello-delay

Use **pim triggered-hello-delay** to set the triggered hello delay (maximum delay for sending a hello message).

Use **undo pim triggered-hello-delay** to restore the default.

Syntax

pim triggered-hello-delay *delay*

undo pim triggered-hello-delay

Default

The triggered hello delay is 5 seconds.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

delay: Specifies a triggered hello delay in the range of 1 to 60 seconds.

Examples

Set the triggered hello delay to 3 seconds on Tunnel 10.

```
<Sysname> system-view
[Sysname] interface Tunnel 10
[Sysname-Tunnel10] pim triggered-hello-delay 3
```

register-policy (PIM view)

Use **register-policy** to configure a PIM register policy.

Use **undo register-policy** to restore the default.

Syntax

register-policy *ipv4-acl-number*

undo register-policy

Default

No PIM register policy exists, and all PIM register messages are regarded as legal.

Views

PIM view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-acl-number: Specifies an IPv4 advanced ACL number in the range of 3000 to 3999.

Usage guidelines

A PIM register policy enables an RP to filter PIM register messages so that the RP is designated only to multicast groups permitted by the ACL.

When you configure a rule in the IPv4 advanced ACL, follow these restrictions and guidelines:

- If the **vpn-instance** *vpn-instance* option is specified, the rule does not take effect.
- The **source** *source-address source-wildcard* option specifies a multicast source address.
- The **destination** *dest-address dest-wildcard* option specifies a multicast group range.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure a PIM register policy on the public network. Then, the device accepts only register messages from the sources on the subnet 10.10.0.0/16 to the groups on the subnet 225.1.0.0/16.

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule permit ip source 10.10.0.0 0.0.255.255 destination
225.1.0.0 0.0.255.255
[Sysname-acl-ipv4-adv-3000] quit
[Sysname] pim
[Sysname-pim] register-policy 3000
```

register-suppression-timeout (PIM view)

Use **register-suppression-timeout** to set the register suppression time.

Use **undo register-suppression-timeout** to restore the default.

Syntax

register-suppression-timeout *interval*

undo register-suppression-timeout

Default

The register suppression time is 60 seconds.

Views

PIM view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies a register suppression time in the range of 1 to 65535 seconds.

Examples

Set the register suppression time to 70 seconds on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] register-suppression-timeout 70
```

register-whole-checksum (PIM view)

Use **register-whole-checksum** to configure the device to calculate the checksum based on an entire register message.

Use **undo register-whole-checksum** to restore the default.

Syntax

register-whole-checksum

undo register-whole-checksum

Default

The device calculates the checksum based on the register message header.

Views

PIM view

Predefined user roles

network-admin

context-admin

Examples

Configure the device to calculate the checksum based on an entire register message on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] register-whole-checksum
```

snmp-agent trap enable pim

Use **snmp-agent trap enable pim** to enable SNMP notifications for PIM.

Use **undo snmp-agent trap enable pim** to disable SNMP notifications for PIM.

Syntax

snmp-agent trap enable pim [**candidate-bsr-win-election** | **elected-bsr-lost-election** | **neighbor-loss**] *

undo snmp-agent trap enable pim [**candidate-bsr-win-election** | **elected-bsr-lost-election** | **neighbor-loss**] *

Default

SNMP notifications for PIM are enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

candidate-bsr-win-election: Specifies notifications about winning the BSR election.

elected-bsr-lost-election: Specifies notifications about losing the BSR election.

neighbor-loss: Specifies notifications about losing neighbors.

Usage guidelines

If you do not specify an optional keyword, this command enables or disables PIM to generate SNMP notifications.

To report critical PIM events to an NMS, enable SNMP notifications for PIM. For PIM event notifications to be sent correctly, you must also configure SNMP as described in *Network Management and Monitoring Configuration Guide*.

Examples

Disable SNMP notifications for PIM.

```
<Sysname> system-view
[Sysname] undo snmp-agent trap enable pim
```

source-lifetime (PIM view)

Use **source-lifetime** to set the multicast source lifetime.

Use **undo source-lifetime** to restore the default.

Syntax

source-lifetime *time*

undo source-lifetime

Default

The multicast source lifetime is 210 seconds.

Views

PIM view

Predefined user roles

network-admin

context-admin

Parameters

time: Specifies a multicast source lifetime in the range of 0 to 31536000 seconds. If you set the value to 0 seconds, multicast sources never age out.

Examples

Set the multicast source lifetime to 200 seconds on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] source-lifetime 200
```

source-policy (PIM view)

Use **source-policy** to configure a multicast source policy.

Use **undo source-policy** to restore the default.

Syntax

source-policy *ipv4-acl-number*

undo source-policy

Default

No multicast source policy exists. The device does not filter multicast data packets.

Views

PIM view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-acl-number: Specifies an IPv4 basic or advanced ACL number in the range of 2000 to 3999.

Usage guidelines

A multicast source policy filters multicast data packets to control information available to downstream receivers.

When you configure a rule in the IPv4 ACL, follow these restrictions and guidelines:

- If the **vpn-instance** *vpn-instance* option is specified, the rule does not take effect.
- In a basic ACL, the **source** *source-address source-wildcard* option specifies a source IP address.
- In an advanced ACL, the **source** *source-address source-wildcard* option specifies a source IP address. The **destination** *dest-address dest-wildcard* option specifies a multicast group address.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure a multicast source policy on the public network to accept multicast data from source 10.10.1.2 and to deny multicast data from source 10.10.1.1.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule permit source 10.10.1.2 0
[Sysname-acl-ipv4-basic-2000] rule deny source 10.10.1.1 0
[Sysname-acl-ipv4-basic-2000] quit
[Sysname] pim
[Sysname-pim] source-policy 2000
```

spt-switch-threshold (PIM view)

Use **spt-switch-threshold** to configure a criterion for an RPT-to-SPT switchover.

Use **undo spt-switch-threshold** to remove criteria for RPT-to-SPT switchovers.

Syntax

spt-switch-threshold { *traffic-rate* | **immediacy** | **infinity** } [**group-policy** *ipv4-acl-number*]

undo spt-switch-threshold [*traffic-rate* | **immediacy** | **infinity**] [**group-policy** *ipv4-acl-number*]

Default

The first multicast packet triggers an RPT-to-STP switchover.

Views

PIM view

Predefined user roles

network-admin

context-admin

Parameters

traffic-rate: Specifies a traffic rate threshold for triggering an RPT-to-STP switchover, in the range of 1 to 4194304 kbps.

immediacy: Triggers an RPT-to-STP switchover immediately.

infinity: Disables RPT-to-STP switchover.

group-policy *ipv4-acl-number*: Specifies an IPv4 basic ACL number in the range of 2000 to 2999. If you specify an ACL, the configuration applies to the multicast groups that the ACL permits. The configuration applies to all multicast groups when one of the following conditions exists:

- You do not specify an ACL.
- The specified ACL does not exist.
- The specified ACL does not have valid rules.

Usage guidelines

When you configure a rule in the IPv4 basic ACL, follow these restrictions and guidelines:

- If the **vpn-instance** *vpn-instance* option is specified, the rule does not take effect.
- The **source** *source-address source-wildcard* option specifies a multicast group address.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

You can configure multiple traffic rate thresholds by executing this command multiple times. However, if you specify the same ACL in the command, the most recent configuration takes effect. If the configured traffic rate thresholds are applied to the same multicast group, the first configuration takes effect.

The source-side DR cannot encapsulate multicast packets in register packets sent to the RP. To avoid multicast traffic forwarding failure, do not disable RPT-to-STP switchover on the devices that might become an RP.

Examples

Set the traffic rate threshold to 4 kbps for triggering an RPT-to-STP switchover on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] spt-switch-threshold 4
```

Disable RPT-to-STP switchover on a receiver-side DR on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] spt-switch-threshold infinity
```

ssm-policy (PIM view)

Use **ssm-policy** to configure the SSM group range.

Use **undo ssm-policy** to restore the default.

Syntax

ssm-policy *ipv4-acl-number*

undo ssm-policy

Default

The SSM group range is 232.0.0.0/8.

Views

PIM view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-acl-number: Specifies an IPv4 basic ACL number in the range of 2000 to 2999.

Usage guidelines

This command defines a multicast group range that is used by PIM-SSM. For multicast packets that are permitted by the ACL, the PIM-SSM mode is used. For multicast packets that are not permitted by the ACL, the PIM-SM mode is used.

When you configure a rule in the IPv4 basic ACL, follow these restrictions and guidelines:

- If the **vpn-instance** *vpn-instance* option is specified, the rule does not take effect.
- The **source** *source-address source-wildcard* option specifies a multicast group range.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure the SSM group range as 232.1.0.0/16.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule permit source 232.1.0.0 0.0.255.255
[Sysname-acl-ipv4-basic-2000] quit
[Sysname] pim
[Sysname-pim] ssm-policy 2000
```

state-refresh-interval (PIM view)

Use **state-refresh-interval** to set the state refresh interval.

Use **undo state-refresh-interval** to restore the default.

Syntax

state-refresh-interval *interval*

undo state-refresh-interval

Default

The state refresh interval is 60 seconds.

Views

PIM view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies a state refresh interval in the range of 1 to 255 seconds.

Examples

Set the state refresh interval to 70 seconds on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] state-refresh-interval 70
```

Related commands

pim state-refresh-capable

state-refresh-rate-limit (PIM view)

state-refresh-ttl (PIM view)

state-refresh-rate-limit (PIM view)

Use **state-refresh-rate-limit** to set the waiting time to accept a new state refresh message.

Use **undo state-refresh-rate-limit** to restore the default.

Syntax

state-refresh-rate-limit *time*

undo state-refresh-rate-limit

Default

The device waits 30 seconds before it accepts a new state refresh message.

Views

PIM view

Predefined user roles

network-admin

context-admin

Parameters

time: Specifies the waiting time to accept a new refresh message, in the range of 1 to 65535 seconds.

Examples

Set the waiting time to 45 seconds to accept a new state refresh message on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] state-refresh-rate-limit 45
```

Related commands

pim state-refresh-capable

state-refresh-interval (PIM view)

state-refresh-ttl (PIM view)

state-refresh-ttl (PIM view)

Use **state-refresh-ttl** to set the TTL value for state refresh messages.

Use **undo state-refresh-ttl** to restore the default.

Syntax

state-refresh-ttl *ttl-value*

undo state-refresh-ttl

Default

The TTL value for state refresh messages is 255.

Views

PIM view

Predefined user roles

network-admin

context-admin

Parameters

ttl-value: Specifies the TTL value for state refresh messages, in the range of 1 to 255.

Examples

Set the TTL value to 45 for state refresh messages on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] state-refresh-ttl 45
```

Related commands

pim state-refresh-capable (PIM view)

state-refresh-interval (PIM view)

state-refresh-rate-limit (PIM view)

static-rp (PIM view)

Use **static-rp** to configure a static RP.

Use **undo static-rp** to delete a static RP.

Syntax

static-rp *rp-address* [*ipv4-acl-number* | **bidir** | **preferred**] *

undo static-rp *rp-address*

Default

No static RPs exist.

Views

PIM view

Predefined user roles

network-admin

context-admin

Parameters

rp-address: Specifies the IP address of the static RP. The IP address must be valid and cannot be on the subnet 127.0.0.0/8. For a static PIM-SM RP, you must specify a used IP address. For a static BIDIR-PIM RP, you can specify an unused IP address.

ipv4-acl-number: Specifies an IPv4 basic ACL number in the range of 2000 to 2999. If you specify an ACL, the static RP is designated only to multicast groups that the ACL permits. The static RP is designated to all multicast groups when one of the following conditions exists:

- You do not specify an ACL.
- The specified ACL does not exist.
- The specified ACL does not have valid rules.

bidir: Configures the static RP as a BIDIR-PIM RP. If you do not specify this keyword, this command configures the static RP as a PIM-SM RP.

preferred: Gives priority to the static RP if a dynamic RP also exists on the network. The dynamic RP takes effect only when the static RP fails. If you do not specify this keyword, the dynamic RP has priority, and the static RP takes effect only when the dynamic RP fails.

Usage guidelines

You do not need to enable PIM on an interface that acts as a static RP.

When you configure a rule in the IPv4 basic ACL, follow these restrictions and guidelines:

- If the **vpn-instance** *vpn-instance* option is specified, the rule does not take effect.
- The **source** *source-address source-wildcard* option specifies a multicast group address.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

When rules in the ACL used by a static RP change, new RPs are dynamically elected for all multicast groups.

You can configure multiple static RPs by using this command multiple times. However, if you specify the same static RP address or use the same ACL in the command, the most recent configuration takes effect. If you configure multiple static RPs for the same multicast group, the static RP with the highest IP address is used.

Examples

Configure the interface with IP address 11.110.0.6 as a static RP for multicast group range 225.1.1.0/24 and give priority to this static RP on the public network.

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 225.1.1.0 0.0.0.255
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] pim
[Sysname-pim] static-rp 11.110.0.6 2001 preferred
```

Related commands

display pim rp-info

timer hello (PIM view)

Use **timer hello** to set the hello interval globally.

Use **undo timer hello** to restore the default.

Syntax

timer hello *interval*

undo timer hello

Default

The hello interval is 30 seconds.

Views

PIM view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies a hello interval in the range of 0 to 18000 seconds. If you set the value to 0 seconds, the device does not send hello messages.

Usage guidelines

You can set the hello interval globally for all interfaces in PIM view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the global hello interval to 40 seconds on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] timer hello 40
```

Related commands

pim timer hello

timer join-prune (PIM view)

Use **timer join-prune** to set the join or prune interval globally.

Use **undo timer join-prune** to restore the default.

Syntax

timer join-prune *interval*

undo timer join-prune

Default

The join or prune interval is 60 seconds.

Views

PIM view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies a join or prune interval in the range of 0 to 18000 seconds. If you set the value to 0 seconds, the device does not send join or prune messages.

Usage guidelines

You can set the join or prune interval globally for all interfaces in PIM view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

The configuration takes effect after the current interval ends.

To prevent the upstream neighbors from expiring, you must set the join or prune interval to be less than the joined or pruned state holdtime.

Examples

Set the global join or prune interval to 80 seconds on the public network.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] timer join-prune 80
```

Related commands

holdtime join-prune (PIM view)

pim timer join-prune

Contents

IPv6 multicast routing and forwarding commands

display ipv6 mrib interface

Use **display ipv6 mrib interface** to display information about interfaces maintained by the IPv6 MRIB.

Syntax

display ipv6 mrib [**vpn-instance** *vpn-instance-name*] **interface** [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays information about interfaces maintained by the IPv6 MRIB on the public network.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays information about all interfaces maintained by the IPv6 MRIB.

Examples

Display information about interfaces maintained by the IPv6 MRIB on the public network.

```
<Sysname> display ipv6 mrib interface
 Interface: GigabitEthernet1/0/1
     Index: 0x00004444
     Current state: up
     MTU: 1500
     Type: BROADCAST
     Protocol: MLD/PROXY
     PIM protocol state: Disabled
     Address list:
          1. Local address : FE80:7:11::1/10
             Remote address: ::
             Reference     : 1
             State         : NORMAL
```

Table 1 Command output

Field	Description
Interface	Interface name.
Index	Index number of the interface.
Current state	Current status of the interface: up or down.
MTU	MTU value.
Type	Interface type: • **BROADCAST**—Broadcast link interface. • **P2P**—P2P interface. • **LOOP**—Loopback interface. • **REGISTER**—Register interface. • **NBMA**—NBMA interface. • **MTUNNEL**—Multicast tunnel interface. This field is empty if the interface is Null 0.
Protocol	Protocol running on the interface: MLD or PROXY.
PIM protocol state	Whether IPv6 PIM is enabled: Enabled or Disabled.
Address list	Interface address list.
Local address	Local IP address.
Remote address	Remote end IP address. This field is displayed only when the interface is vlink type.
Reference	Number of times that the address has been used.
State	Status of the interface address: **NORMAL** or **DEL**.

display ipv6 multicast boundary

Use **display ipv6 multicast boundary** to display IPv6 multicast boundary information.

Syntax

display ipv6 multicast [**vpn-instance** *vpn-instance-name*] **boundary** { **group** [*ipv6-group-address* [*prefix-length*]] | **scope** [*scope-id*] } [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays IPv6 multicast boundary information on the public network.

group: Displays the IPv6 multicast boundary information for the specified groups.

ipv6-group-address: Specifies an IPv6 multicast group address in the range of FFxy::/16, where "x" and "y" represent any hexadecimal numbers in the range of 0 to F. If you do not specify an IPv6 multicast group, this command displays IPv6 multicast boundary information for all IPv6 multicast groups.

prefix-length: Specifies an address prefix length in the range of 8 to 128. The default is 128.

scope: Displays the IPv6 multicast group boundary information in the admin-scoped zone.

scope-id: Specifies an admin-scope zone by its ID in the range of 3 to 15, which is identified by the scope field in the IPv6 multicast group address. If you do not specify an admin-scoped zone, this command displays IPv6 multicast boundary information for all IPv6 admin-scoped zones.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays IPv6 multicast boundary information for all interfaces.

Examples

Display IPv6 multicast boundary information of all IPv6 multicast groups for all interfaces on the public network.

```
<Sysname> display ipv6 multicast boundary group
 Boundary                                                  Interface
 FF1E::/64                                                 GE1/0/1
```

Display IPv6 multicast boundary information in all IPv6 admin-scope zones for all interfaces on the public network.

```
<Sysname> display ipv6 multicast boundary scope
 Boundary            Interface
        3            GigabitEthernet1/0/1
```

Table 2 Command output

Field	Description
Boundary	IPv6 multicast group or IPv6 admin-scoped zone associated with the IPv6 multicast boundary.
Interface	Boundary interface associated with the IPv6 multicast boundary.

Related commands

ipv6 multicast boundary

display ipv6 multicast fast-forwarding cache

Use **display ipv6 multicast fast-forwarding cache** to display IPv6 multicast fast forwarding entries.

Syntax

display ipv6 multicast [**vpn-instance** *vpn-instance-name*] **fast-forwarding cache** [*ipv6-source-address* | *ipv6-group-address*] * [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays IPv6 multicast fast forwarding entries on the public network.

ipv6-source-address: Specifies an IPv6 multicast source address.

ipv6-group-address: Specifies an IPv6 multicast group address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv6 multicast fast forwarding entries for the master device.

Examples

Display IPv6 multicast fast forwarding entries on the public network.

```
<Sysname> display ipv6 multicast fast-forwarding cache
Total 1 entries, 1 matched

(FE1F:60::200, FF0E::1)
     Status     : Enabled
     Source port: 2001                   Destination port: 2002
     Protocol   : 2                      Flag            : 0x2
     Incoming interface: GigabitEthernet1/0/3
     List of 1 outgoing interfaces:
     GigabitEthernet1/0/2
          Status: Enabled              Flag: 0x14
```

Table 3 Command output

Field	Description
Total 1 entries, 1 matched	Total number of (S, G) entries, and the total number of matching (S, G) entries.
(FE1F:60::200, FF0E::1)	(S, G) entry.
Protocol	Protocol number.
Flag	Flag for the (S, G) entry or the outgoing interface of the entry. This field displays one flag or the sum of multiple flags. In this example, the value 0x2 means that the entry has only one flag 0x2. The value 0x14 means that the outgoing interface has flags 0x10 and 0x4. The following flags are available for an entry: • **0x1**—The entry is created because of packets passed through between cards. • **0x2**—The entry is added by IPv6 multicast forwarding. The following flags are available for an outgoing interface: • **0x1**—The interface is added to the entry because of packets passed through between cards. • **0x2**—The interface is added to an existing entry. • **0x4**—The MAC address of the interface is needed for fast forwarding. • **0x8**—The interface is an outgoing interface associated with the incoming VLAN interface. • **0x10**—The interface is associated with the entry.

Field	Description
	• **0x20**—The interface is to be deleted.
Status	Status of the (S, G) entry or the outgoing interface: • **Enabled**—Available. • **Disabled**—Unavailable.
Incoming interface	Incoming interface of the (S, G) entry.
List of 1 outgoing interfaces	Outgoing interface list of the (S, G) entry.

Related commands

reset ipv6 multicast fast-forwarding cache all

display ipv6 multicast forwarding df-info

Use **display ipv6 multicast forwarding df-info** to display DF information.

Syntax

display ipv6 multicast [**vpn-instance** *vpn-instance-name*] **forwarding df-info** [*ipv6-rp-address*] [**verbose**] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays information about DFs on the public network.

ipv6-rp-address: Specifies an IPv6 BIDIR-PIM RP by its IPv6 address.

verbose: Displays detailed information. If you do not specify this keyword, the command displays brief information about DFs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays DF information for the master device.

Usage guidelines

In an IPv6 BIDIR-PIM domain, only the DF on each subnet can forward IPv6 multicast data destined for an IPv6 multicast group toward the RP of the group. For more information about DFs, see *IP Multicast Configuration Guide*.

Examples

Display brief DF information on an ADVPN network.

```
<Sysname> display ipv6 multicast forwarding df-info
Total 1 RPs, 1 matched

00001. RP address: 2::2
```

```
     Flags: 0x0
     Uptime: 00:00:14
     RPF interface: LoopBack0
     List of 2 DF interfaces:
       1: Tunnel2, FE80::1
       2: Tunnel2, FE80::3
```

Display brief information about DFs on the public network.

```
<Sysname> display ipv6 multicast forwarding df-info
Total 1 RPs, 1 matched

00001. RP address: 7:11::1
     Flags: 0x0
     Uptime: 01:46:40
     RPF interface: GigabitEthernet1/0/1
     List of 1 DF interface:
       1: GigabitEthernet1/0/2
```

Display detailed information about DFs on the public network.

```
<Sysname> display ipv6 multicast forwarding df-info verbose
Total 1 RPs, 1 matched

00001. RP address: 7:11::1
     MID: 2, Flags: 0x0
     Uptime: 00:03:53
       Product information: 0x7a2f762f, 0x718fee9f, 0x4b82f137, 0x71c32184
     RPF interface: GigabitEthernet1/0/1
       Product information: 0xa567d6fc, 0xadeb03e3
       Tunnel  information: 0xdfb107d4, 0x7aa5d510
     List of 1 DF interface:
       1: GigabitEthernet1/0/2
          Product information: 0xa986152b, 0xb74a9a2f
          Tunnel  information: 0x297ca208, 0x76985b89
```

Table 4 Command output

Field	Description
Total 1 RPs, 1 matched	Total number of RPs, and the total number of matching RPs.
00001	Sequence number of the entry to which the RP is designated.
RP address	IPv6 address of the RP.
MID	ID of the entry to which the RP is designated. Each entry to which the RP is designated has a unique MID.
Flags	Entry flag. This field displays one flag or the sum of multiple flags. In this example, the value 0x0 means that the entry has only one flag 0x0. The following flags are available for an entry: • **0x0**—The entry is in correct state. • **0x4**—The entry fails to update. • **0x8**—DF interface information fails to update for the entry. • **0x40**—The entry is to be deleted.

Field	Description
	• **0x100**—The entry is being deleted. • **0x200**—The entry is in GR state.
Uptime	Length of time for which the entry has been up.
RPF interface	RPF interface to the RP.
List of 1 DF interfaces	DF interface list.
Tunnel2, FE80::1	ADVPN tunnel interface, and the IPv6 link-local address of the remote end.

display ipv6 multicast forwarding event

Use **display ipv6 multicast forwarding event** to display statistics of IPv6 multicast forwarding events.

Syntax

display ipv6 multicast [**vpn-instance** *vpn-instance-name*] **forwarding event** [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays statistics of IPv6 multicast forwarding events on the public network.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays statistics of IPv6 multicast forwarding events for the master device.

Examples

Display statistics of IPv6 multicast forwarding events on the public network.

```
<Sysname> display ipv6 multicast forwarding event
Total active events sent: 0
Total inactive events sent: 0
Total NoCache events sent: 2
Total NoCache events dropped: 0
Total WrongIF events sent: 0
Total WrongIF events dropped: 0
Total SPT switch events sent: 0
NoCache rate limit: 1024 packets/s
WrongIF rate limit: 1 packets/10s
Total timer of register suppress timeout: 0
```

Table 5 Command output

Field	Description
Total active events sent	Number of times that entry-active events have been sent.
Total inactive events sent	Number of times that entry-inactive events have been sent.
Total NoCache events sent	Number of times that NoCache events have been sent.
Total NoCache events dropped	Number of times that NoCache events have been dropped.
Total WrongIF events sent	Number of times that WrongIF events have been sent.
Total WrongIF events dropped	Number of times that WrongIF events have been dropped.
Total SPT switch events sent	Number of times that SPT-switch events have been sent.
NoCache rate limit	Rate limit for sending NoCache events, in pps.
WrongIF rate limit	Rate limit for sending WrongIF events, in packets per 10 seconds.
Total timer of register suppress timeout	Number of times that the registration suppression has timed out in total.

Related commands

reset ipv6 multicast forwarding event

display ipv6 multicast forwarding-table

Use **display ipv6 multicast forwarding-table** to display IPv6 multicast forwarding entries.

Syntax

display ipv6 multicast [**vpn-instance** *vpn-instance-name*] **forwarding-table** [*ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*] | **incoming-interface** *interface-type interface-number* | **outgoing-interface** { **exclude** | **include** | **match** } *interface-type interface-number* | **slot** *slot-number* | **statistics**] *

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays IPv6 multicast forwarding entries on the public network.

ipv6-source-address: Specifies an IPv6 multicast source address.

ipv6-group-address: Specifies an IPv6 multicast group address in the range of FFxy::/16, where "x" and "y" represent any hexadecimal numbers in the range of 0 to F.

prefix-length: Specifies an address prefix length. The default value is 128. For an IPv6 multicast group address, the value range for this argument is 8 to 128. For an IPv6 multicast source address, the value range for this argument is 0 to 128.

incoming-interface: Specifies the IPv6 forwarding entries that contain the specified incoming interface.

interface-type interface-number: Specifies an interface by its type and number.

outgoing-interface: Specifies the IPv6 forwarding entries that contain the specified outgoing interface.

exclude: Specifies the IPv6 forwarding entries that do not contain the specified interface in the outgoing interface list.

include: Specifies the IPv6 forwarding entries that contain the specified interface in the outgoing interface list.

match: Specifies the IPv6 forwarding entries that contain only the specified interface in the outgoing interface list.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv6 multicast forwarding entries for the master device.

statistics: Displays statistics for the IPv6 multicast forwarding table.

Examples

Display IPv6 multicast forwarding entries on an ADVPN network.

```
<Sysname> display ipv6 multicast forwarding-table
Total 1 entries, 1 matched

00001. (1::1, ff0e::1)
     Flags: 0x0
     Uptime: 00:08:32, Timeout in: 00:03:26
     Incoming interface: Tunnel1, FE80::20:11
     List of 1 outgoing interfaces:
             1:  Tunnel1, FE80::20:12
             2:  Tunnel1, FE80::20:13
     Matched 19648 packets(20512512 bytes), Wrong If 0 packet
     Forwarded 19648 packets(20512512 bytes)
```

Display IPv6 multicast forwarding entries on the public network.

```
<Sysname> display ipv6 multicast forwarding-table
Total 1 entries, 1 matched

00001. (1::1, ff0e::1)
     Flags: 0x0
     Uptime: 00:08:32, Timeout in: 00:03:26
     Incoming interface: Vlan-interface10
          Incoming sub-VLAN: VLAN 11
          Outgoing sub-VLAN: VLAN 12
                             VLAN 13
     List of 1 outgoing interface:
       1: Vlan-interface20
          Sub-VLAN: VLAN 21
                    VLAN 22
```

```
Matched 19648 packets(20512512 bytes), Wrong If 0 packet
Forwarded 19648 packets(20512512 bytes)
```

Table 6 Command output

Field	Description
Total 1 entries, 1 matched	Total number of (S, G) entries, and the total number of matching (S, G) entries.
00001	Sequence number of the (S, G) entry.
(1::1, ff0e::1)	(S, G) entry.
Flags	Entry flag. This field displays one flag or the sum of multiple flags. In this example, the value 0x0 means that the entry has only one flag 0x0. The following flags are available for an entry: • **0x0**—The entry is in correct state. • **0x1**—The entry is in inactive state. • **0x2**—The entry is null. • **0x4**—The entry fails to update. • **0x8**—The outgoing interface information fails to update for the entry. • **0x20**—A register outgoing interface is available. • **0x40**—The entry is to be deleted. • **0x80**—The entry is in registration suppression state. • **0x100**—The entry is being deleted. • **0x200**—The entry is in GR state. • **0x800**—The entry has the associated ND entry for the IPv6 multicast source address. • **0x4000000**—The entry is created by the MLD proxy.
Uptime	Length of time for which the (S, G) entry has been up.
Timeout in	Length of time in which the (S, G) entry will time out.
Incoming interface	Incoming interface of the (S, G) entry.
List of 1 outgoing interfaces	Outgoing interface list of the (S, G) entry.
Tunnel1, FE80::20:12	ADVPN tunnel interface, and the IPv6 link-local address of the remote end.
Matched 19648 packets (20512512 bytes), Wrong If 0 packet	Number of packets (bytes) that match the (S, G) entry, and number of packets with incoming interface errors. The numbers are displayed as 0 if an outgoing interface of the (S, G) entry is on the specified slot.
Forwarded 19648 packets (20512512 bytes)	Number of packets (bytes) that have been forwarded. The numbers are displayed as 0 if an outgoing interface of the (S, G) entry is on the specified slot.

Related commands

reset ipv6 multicast forwarding-table

display ipv6 multicast forwarding-table df-list

Use **display ipv6 multicast forwarding-table df-list** to display information about the DF list in IPv6 multicast forwarding entries.

Syntax

display ipv6 multicast [**vpn-instance** *vpn-instance-name*] **forwarding-table df-list** [*ipv6-group-address*] [**verbose**] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays information about the DF list in IPv6 multicast forwarding entries on the public network.

ipv6-group-address: Specifies an IPv6 multicast address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F.

verbose: Displays detailed information. If you do not specify this keyword, the command displays brief information.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about the DF list in IPv6 multicast forwarding entries for the master device.

Examples

Display brief information about the DF list in IPv6 multicast forwarding entries on the public network.

```
<Sysname> display ipv6 multicast forwarding-table df-list
Total 1 entries, 1 matched

00001. (::, FF1E::1)
     List of 1 DF interfaces:
       1: GigabitEthernet1/0/1
```

Display detailed information about the DF list in IPv6 multicast forwarding entries on the public network.

```
<Sysname> display ipv6 multicast forwarding-table df-list verbose
Total 1 entries, 1 matched

00001. (::, FF1E::1)
       List of 1 DF interfaces:
         1: GigabitEthernet1/0/1
            Product information: 0x347849f6, 0x14bd6837
```

```
Tunnel  information: 0xc4857986, 0x128a9c8f
```

Table 7 Command output

Field	Description
Total 1 entries, 1 matched	Total number of entries, and the total number of matching entries.
00001	Sequence number of the entry.
(::, FF1E::1)	(*, G) entry.
List of 1 DF interfaces	DF interface list.

display ipv6 multicast routing-table

Use **display ipv6 multicast routing-table** to display IPv6 multicast routing entries.

Syntax

display ipv6 multicast [**vpn-instance** *vpn-instance-name*] **routing-table** [*ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*] | **incoming-interface** *interface-type interface-number* | **outgoing-interface** { **exclude** | **include** | **match** } *interface-type interface-number*] *

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays IPv6 multicast routing entries on the public network.

ipv6-source-address: Specifies an IPv6 multicast source address.

ipv6-group-address: Specifies an IPv6 multicast group address in the range of FFxy::/16, where "x" and "y" represent any hexadecimal numbers in the range of 0 to F.

prefix-length: Specifies an address prefix length. The default is 128. For an IPv6 multicast group address, the value range for this argument is 8 to 128. For an IPv6 multicast source address, the value range for this argument is 0 to 128.

incoming-interface: Displays the IPv6 routing entries that contain the specified incoming interface.

interface-type interface-number: Specifies an interface by its type and number.

outgoing-interface: Displays the IPv6 routing entries that contain the specified outgoing interface.

exclude: Displays the IPv6 routing entries that do not contain the specified interface in the outgoing interface list.

include: Displays the IPv6 routing entries that contain the specified interface in the outgoing interface list.

match: Displays the IPv6 routing entries that contain only the specified interface in the outgoing interface list.

Usage guidelines

IPv6 multicast routing entries are the basis of IPv6 multicast forwarding. You can use this command to view the establishment state of (S, G) entries.

Examples

Display IPv6 multicast routing entries on an ADVPN network.

```
<Sysname> display ipv6 multicast routing-table
 Total 1 entries

00001. (2001::2, FFE3::101)
       Uptime: 00:00:14
       Upstream Interface: Tunnel1, FE80::20:11
       List of 2 downstream interfaces
           1:  Tunnel1, FE80::20:12
           2:  Tunnel1, FE80::20:13
```

Display IPv6 multicast routing entries on the public network.

```
<Sysname> display ipv6 multicast routing-table
 Total 1 entries

 00001. (2001::2, FFE3::101)
       Uptime: 00:00:14
       Upstream Interface: GigabitEthernet1/0/1
       List of 2 downstream interfaces
           1:  GigabitEthernet1/0/2
           2:  GigabitEthernet1/0/3
```

Table 8 Command output

Field	Description
Total 1 entries	Total number of (S, G) entries.
00001	Sequence number of the (S, G) entry.
(2001::2, FFE3::101)	(S, G) entry.
Uptime	Length of time for which the (S, G) entry has been up.
Upstream Interface	Upstream interface at which the (S, G) packets should arrive.
List of 2 downstream interfaces	List of downstream interfaces that forward (S, G) packets.
Tunnel11, FE80::20:12	ADVPN tunnel interface, and the IPv6 link-local address of the remote end.

Related commands

reset ipv6 multicast routing-table

display ipv6 multicast rpf-info

Use **display ipv6 multicast rpf-info** to display RPF information for an IPv6 multicast source.

Syntax

display ipv6 multicast [**vpn-instance** *vpn-instance-name*] **rpf-info** *ipv6-source-address* [*ipv6-group-address*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays RPF information for an IPv6 multicast source on the public network.

ipv6-source-address: Specifies an IPv6 multicast source address.

ipv6-group-address: Specifies an IPv6 multicast group address in the range of FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F.

Examples

Display RPF information for IPv6 multicast source 2001::101 on the public network.

```
<Sysname> display ipv6 multicast rpf-info 2001::101
 RPF information about source 2001::101:
     RPF interface: GigabitEthernet1/0/1, RPF neighbor: FE80::A01:101:1
     Referenced prefix/prefix length: 2001::/64
     Referenced route type: igp
     Route selection rule: preference-preferred
     Load splitting rule: disable
     Source AS: 0
     C-multicast route target: 0x0000000000000000
```

Table 9 Command output

Field	Description
RPF information about source 2001::101	RPF information of the IPv6 multicast source 2001::101.
RPF interface	Type and number of the RPF interface.
RPF neighbor	IPv6 address (link-local address) of the RPF neighbor.
Referenced prefix/prefix length	Referenced route and its prefix length.
Referenced route type	Type of the referenced route: • **igp**—IPv6 IGP unicast route. • **egp**—IPv6 EGP unicast route. • **unicast (direct)** —IPv6 directly connected unicast

Field	Description
	route. • **unicast**—Other IPv6 unicast route, such as IPv6 unicast static route. • **mbgp**—IPv6 MBGP route.
Route selection rule	RPF route selection rule: • Route preference. • Longest prefix match.
Load splitting rule	Whether load splitting is enabled.
Source AS	AS number of the source-side PE.
C-multicast route target	Route target attribute value of the C-multicast route.

Related commands

display ipv6 multicast forwarding-table

display ipv6 multicast routing-table

ipv6 multicast boundary

Use **ipv6 multicast boundary** to configure an IPv6 multicast forwarding boundary.

Use **undo ipv6 multicast boundary** to delete an IPv6 multicast forwarding boundary.

Syntax

ipv6 multicast boundary { *ipv6-group-address prefix-length* | **scope** { *scope-id* | **admin-local** | **global** | **organization-local** | **site-local** } }

undo ipv6 multicast boundary { *ipv6-group-address prefix-length*| **all** | **scope** { *scope-id* | **admin-local** | **global** | **organization-local** | **site-local** } }

Default

An interface is not an IPv6 multicast forwarding boundary.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-group-address: Specifies an IPv6 multicast group address in the range of FFxy::/16, where "x" and "y" represent any hexadecimal numbers in the range of 0 to F.

prefix-length: Specifies the address prefix length in the range of 8 to 128.

all: Specifies all IPv6 multicast boundaries configured on the interface.

scope-id: Specifies the ID of an admin-scoped zone, in the range of 3 to 15, which is identified by the scope field in the IPv6 multicast group address.

admin-local: Specifies the scoped zone as admin-local, which has a scope ID of 4.

global: Specifies the scoped zone as global, which has a scope ID of 14.

organization-local: Specifies the scoped zone as organization-local, which has a scope ID of 8.

site-local: Specifies the scoped zone as site-local, which has a scope ID of 5.

Usage guidelines

A multicast forwarding boundary sets the boundary condition for the IPv6 multicast groups in the specified address range. If the destination address of an IPv6 multicast packet matches the set boundary condition, the packet is not forwarded.

An interface can act as a forwarding boundary for multiple IPv6 multicast groups in different address ranges. You can implement this by using this command on the interface for each multicast address range. These multicast groups must be in the same scope. The latest configuration of a scope overwrites the previous one.

You do not need to enable IPv6 multicast routing before you execute this command.

Assume that Set A and Set B are both IPv6 multicast forwarding boundary sets with different address ranges, and that B is a subset of A. A takes effect on the interface no matter whether A is configured earlier or later than B.

Examples

Configure GigabitEthernet 1/0/1 as the forwarding boundary of IPv6 multicast groups in the range of FF03::/16.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 multicast boundary ff03:: 16
```

Configure GigabitEthernet 1/0/1 as the forwarding boundary of IPv6 multicast groups in the admin-local scope.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 multicast boundary scope 4
```

Related commands

display ipv6 multicast boundary

ipv6 multicast forwarding-table cache-unknown per-entry

Use **ipv6 multicast forwarding-table cache-unknown per-entry** to set the maximum number of unknown IPv6 multicast packets that can be cached for an (S, G) entry.

Use **undo ipv6 multicast forwarding-table cache-unknown per-entry** to restore the default.

Syntax

ipv6 multicast forwarding-table cache-unknown per-entry *per-entry-limit*

undo ipv6 multicast forwarding-table cache-unknown per-entry

Default

The device can cache only one unknown IPv6 multicast packet for an (S, G) entry.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

per-entry-limit: Specifies the maximum number of unknown IPv6 multicast packets that can be cached for an (S, G) entry. The value range for this argument is 0 to 256. If you set the value to 0, the device cannot cache unknown IPv6 multicast packets.

Examples

Set the maximum number to 20 for unknown IPv6 multicast packets that can be cached for an (S, G) entry.

```
<Sysname> system-view
[Sysname] ipv6 multicast forwarding-table cache-unknown per-entry 20
```

Related commands

ipv6 multicast forwarding-table cache-unknown total

ipv6 multicast forwarding-table cache-unknown total

Use **ipv6 multicast forwarding-table cache-unknown total** to set the maximum number of all unknown IPv6 multicast packets that can be cached.

Use **undo multicast forwarding-table cache-unknown total** to restore the default.

Syntax

ipv6 multicast forwarding-table cache-unknown total *total-limit*

undo ipv6 multicast forwarding-table cache-unknown total

Default

The device can cache 1024 unknown IPv6 multicast packets in total.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

total-limit: Specifies the maximum number of all unknown IPv6 multicast packets that can be cached. The value range for this argument is 0 to 65535. If you set the value to 0, the device cannot cache unknown IPv6 multicast packets.

Usage guidelines

As a best practice, set the value in this command to be far greater than the value set in the **ipv6 multicast forwarding-table cache-unknown per-entry** command.

Examples

Set the maximum number to 10000 for all unknown IPv6 multicast packets that can be cached.

```
<Sysname> system-view
[Sysname] ipv6 multicast forwarding-table cache-unknown total 10000
```

Related commands

ipv6 multicast forwarding-table cache-unknown per-entry

ipv6 multicast routing

Use **ipv6 multicast routing** to enable IPv6 multicast routing and enter IPv6 MRIB view.

Use **undo ipv6 multicast routing** to disable IPv6 multicast routing.

Syntax

ipv6 multicast routing [**vpn-instance** *vpn-instance-name*]

undo ipv6 multicast routing [**vpn-instance** *vpn-instance-name*]

Default

IPv6 multicast routing is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command enables IPv6 multicast routing on the public network.

Usage guidelines

Other Layer 3 IPv6 multicast commands take effect only when IPv6 multicast routing is enabled on the public network or for the VPN instance to which the device belongs.

The device does not forward any IPv6 multicast packets before IPv6 multicast routing is enabled.

Examples

Enable IPv6 multicast routing on the public network, and enter IPv6 MRIB view.

```
<Sysname> system-view
[Sysname] ipv6 multicast routing
[Sysname-mrib6]
```

Enable IPv6 multicast routing for VPN instance **mvpn**, and enter IPv6 MRIB view.

```
<Sysname> system-view
[Sysname] ipv6 multicast routing vpn-instance mvpn
[Sysname-mrib6-mvpn]
```

load-splitting (IPv6 MRIB view)

Use **load-splitting** to enable IPv6 multicast load splitting.

Use **multicast load-splitting** to restore the default.

Syntax

load-splitting { **source** | **source-group** }

undo load-splitting

Default

IPv6 multicast load splitting is disabled.

Views

IPv6 MRIB view

Predefined user roles

network-admin

context-admin

Parameters

source: Enables IPv6 multicast load splitting based on IPv6 multicast source.

source-group: Enables IPv6 multicast load splitting based on IPv6 multicast source and group.

Examples

Enable IPv6 multicast load splitting based on IPv6 multicast source on the public network.

```
<Sysname> system-view
[Sysname] ipv6 multicast routing
[Sysname-mrib6] load-splitting source
```

longest-match (IPv6 MRIB view)

Use **longest-match** to specify the longest prefix match principle for RPF route selection.

Use **undo longest-match** to restore the default.

Syntax

longest-match

undo longest-match

Default

Route preference is used for RPF route selection. The route with the highest route preference is used as the RPF route.

Views

IPv6 MRIB view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command enables the device to use the matching route with the longest prefix as the RPF route.

Examples

Specify the longest prefix match principle for RPF route selection on the public network.

```
<Sysname> system-view
[Sysname] ipv6 multicast routing
[Sysname-mrib6] longest-match
```

reset ipv6 multicast fast-forwarding cache

Use **reset ipv6 multicast fast-forwarding cache** to clear IPv6 multicast fast forwarding entries.

Syntax

reset ipv6 multicast [**vpn-instance** *vpn-instance-name*] **fast-forwarding cache** { { *ipv6-source-address* | *ipv6-group-address* } * | **all** } [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears IPv6 multicast fast forwarding entries on the public network.

ipv6-source-address: Specifies an IPv6 multicast source address.

ipv6-group-address: Specifies an IPv6 multicast group address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears IPv6 multicast fast forwarding entries for the master device.

all: Specifies all IPv6 multicast fast forwarding entries.

Examples

Clear all IPv6 multicast fast forwarding entries on the public network.

```
<Sysname> reset ipv6 multicast fast-forwarding cache all
```

Clear the IPv6 multicast fast forwarding entry for IPv6 multicast source and group (FE1F:20::2, FF0E::1) on the public network.

```
<Sysname> reset ipv6 multicast fast-forwarding cache fe1f:20::2 ff0e::1
```

Related commands

display ipv6 multicast fast-forwarding cache

reset ipv6 multicast forwarding event

Use **reset ipv6 multicast forwarding event** to clear statistics for IPv6 multicast forwarding events.

Syntax

reset ipv6 multicast [**vpn-instance** *vpn-instance-name*] **forwarding event**

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears statistics for the IPv6 multicast forwarding events on the public network.

Examples

Clear statistics for the IPv6 multicast forwarding events on the public network.

```
<Sysname> reset ipv6 multicast forwarding event
```

Related commands

display ipv6 multicast forwarding event

reset ipv6 multicast forwarding-table

Use **reset ipv6 multicast forwarding-table** to clear IPv6 multicast forwarding entries.

Syntax

reset ipv6 multicast [**vpn-instance** *vpn-instance-name*] **forwarding-table** { { *ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*] | **incoming-interface** { *interface-type interface-number* } } * | **all** }

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears IPv6 multicast forwarding entries on the public network.

ipv6-source-address: Specifies an IPv6 multicast source address.

ipv6-group-address: Specifies an IPv6 multicast group address in the range of FFxy::/16, where "x" and "y" represent any hexadecimal numbers in the range of 0 to F.

prefix-length: Specifies the address prefix length. The default value is 128. For an IPv6 multicast group address, the value range for this argument is 8 to 128. For an IPv6 multicast source address, the value range for this argument is 0 to 128.

incoming-interface: Specifies the IPv6 multicast forwarding entries that contain the specified incoming interface.

interface-type interface-number: Specifies an interface by its type and number.

all: Specifies all IPv6 multicast forwarding entries.

Usage guidelines

When you clear an IPv6 multicast forwarding entry, the associated IPv6 multicast routing entry is also cleared.

Examples

Clear IPv6 multicast forwarding entries for IPv6 multicast group FF0E::1 on the public network.

```
<Sysname> reset ipv6 multicast forwarding-table ff0e::1
```

Related commands

display ipv6 multicast forwarding-table

reset ipv6 multicast routing-table

Use **reset ipv6 multicast routing-table** to clear IPv6 multicast routing entries.

Syntax

reset ipv6 multicast [**vpn-instance** *vpn-instance-name*] **routing-table** { { *ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*] | **incoming-interface** *interface-type interface-number* } * | **all** }

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears IPv6 multicast routing entries on the public network.

ipv6-source-address: Specifies an IPv6 multicast source address.

ipv6-group-address: Specifies an IPv6 multicast group address in the range of FFxy::/16, where "x" and "y" represent any hexadecimal numbers in the range of 0 to F.

prefix-length: Specifies an address prefix length. The default is 128. For an IPv6 multicast group address, the value range for this argument is 8 to 128. For an IPv6 multicast source address, the value range for this argument is 0 to 128.

incoming-interface: Specifies the IPv6 multicast routing entries that contain the specified incoming interface.

interface-type interface-number: Specifies an interface by its type and number.

all: Specifies all IPv6 multicast routing entries.

Usage guidelines

When you clear an IPv6 multicast routing entry, the associated IPv6 multicast forwarding entry is also cleared.

Examples

Clear IPv6 multicast routing entries for IPv6 multicast group FF03::101 on the public network.

```
<Sysname> reset ipv6 multicast routing-table ff03::101
```

Related commands

display ipv6 multicast routing-table

Contents

MLD commands

display mld group

Use **display mld group** to display information about MLD multicast groups (IPv6 multicast groups that hosts have joined through MLD).

Syntax

display mld [**vpn-instance** *vpn-instance-name*] **group** [*ipv6-group-address* | **interface** *interface-type interface-number*] [**static** | **verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays information about MLD multicast groups on the public network.

ipv6-group-address: Specifies an IPv6 multicast group address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F. If you do not specify an IPv6 multicast group, this command displays information about all MLD multicast groups.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays information about MLD multicast groups for all interfaces.

static: Specifies MLD multicast groups that hosts have joined statically. If you do not specify this keyword, the command displays information about MLD multicast groups that hosts have joined dynamically.

verbose: Displays detailed information about MLD multicast groups.

Examples

Display information about MLD multicast groups that hosts have dynamically joined on the public network.

```
<Sysname> display mld group
MLD groups in total: 1
 GigabitEthernet1/0/1(FE80::101):
  MLD groups reported in total: 1
   Group address: FF03::101
    Last reporter: FE80::10
    Uptime: 00:02:04
    Expires: 00:01:15
```

Table 1 Command output

Field	Description
MLD groups in total	Total number of MLD multicast groups.
MLD groups reported in total	Total number of MLD multicast groups that the hosts attached to the interface have joined dynamically.
Group address	IPv6 multicast group address.
Last reporter	IPv6 address of the receiver host that last reported membership for the group.
Uptime	Length of time since the IPv6 multicast group was joined.
Expires	Remaining lifetime for the IPv6 multicast group. This field displays **Off** if the timer is disabled.

Display detailed information about MLD multicast group FF3E::101 that hosts have statically joined on the public network. In this example, the router is configured with MLD SSM mappings.

```
<Sysname> display mld group ff3e::101 verbose
 GigabitEthernet1/0/1(FE80::101):
  MLD groups reported in total: 1
   Group: FF3E::101
     Uptime: 00:01:46
     Exclude expires: 00:04:16
     Mapping expires: 00:02:16
     Last reporter: FE80::10
     Last-listener-query-counter: 0
     Last-listener-query-timer-expiry: Off
     Mapping last-listener-query-counter: 0
     Mapping last-listener-query-timer-expiry: Off
     Group mode: Exclude
     Version1-host-present-timer-expiry: Off
     Source list (sources in total: 1):
       Source: 10::10
          Uptime: 00:00:09
          V2 expires: 00:04:11
          Mapping expires: 00:02:16
          Last-listener-query-counter: 0
          Last-listener-query-timer-expiry: Off
```

Table 2 Command output

Field	Description
MLD groups reported in total	Total number of MLD multicast groups that the hosts attached to the interface have joined dynamically.
Group	IPv6 multicast group address.
Uptime	Length of time since the IPv6 multicast group was reported.
Exclude expires	Remaining time for the IPv6 multicast group in Exclude mode. This field displays **Off** if the timer is disabled.
Mapping expires	Remaining time for the IPv6 multicast group specified in MLD SSM mappings.

Field	Description
	This field is displayed only when the device is configured with MLD SSM mappings.
Last reporter	IPv6 address of the receiver host that last reported membership for this group.
Last-listener-query-counter	Number of MLD multicast-address-specific queries or MLD multicast-address-and-source-specific queries sent for the group.
Last-listener-query-timer-expiry	Remaining time for the MLD last listener query timer for the multicast group. This field displays **Off** if the timer is disabled.
Mapping last-listener-query-counter	Number of MLD multicast-address-specific queries or MLD multicast-address-and-source-specific queries sent for the IPv6 multicast group specified in MLD SSM mappings. This field is displayed only when the device is configured with MLD SSM mappings.
Mapping last-listener-query-timer-expiry	Remaining time for the last listener query timer of the IPv6 multicast group specified in MLD SSM mappings. This field displays **Off** if the timer is disabled. This field is displayed only when the device is configured with MLD SSM mappings.
Group mode	IPv6 multicast source filtering mode: • **Include**—Include mode. • **Exclude**—Exclude mode. For a device that runs MLDv1: • If MLD SSM mappings are not configured, this field displays **Exclude**. • If MLD SSM mappings are configured, this field displays **Include** or **Exclude** depending on the SSM mappings and the IPv6 multicast groups that the host joins.
Version1-host-present-timer-expiry	Remaining time for the MLDv1 host present timer. This field displays **Off** if the timer is disabled. This field is displayed only when the device runs MLDv2.
Source list (sources in total 1)	List of IPv6 multicast sources and total number of IPv6 multicast sources. This field is displayed only when the device runs MLDv2 or is configured with MLD SSM mappings.
Source	IPv6 multicast source address. This field is displayed only when the device runs MLDv2 or the device is configured with MLD SSM mappings.
Uptime	Length of time since the IPv6 multicast source was reported. This field is displayed only when the device runs MLDv2 or is configured with MLD SSM mappings.
V2 expires	Remaining time for the IPv6 multicast source when the device runs MLDv2. This field displays **Off** if the timer is disabled. This field displays three hyphens (---) if the IPv6 multicast source is specified in MLD SSM mappings. This field is displayed only when the device runs MLDv2 or is configured with MLD SSM mappings.
Mapping expires	Remaining time for the IPv6 multicast sources specified in MLD

Field	Description
	SSM mappings.
Last-listener-query-counter	Number of MLD multicast-address-specific queries or MLD multicast-address-and-source-specific queries sent for the IPv6 multicast source and group. This field is displayed only when the device runs MLDv2 or is configured with MLD SSM mappings.
Last-listener-query-timer-expiry	Remaining time for the last listener query timer for the IPv6 multicast source and group. This field displays **Off** if the timer is disabled. This field is displayed only when the device runs MLDv2 or is configured with MLD SSM mappings.

Display information about the MLD multicast groups that hosts have statically joined on the public network.

```
<Sysname> display mld group static
 Entries in total: 2
  (*, FF03::101)
   Interface: GE1/0/1
   Expires: Never

  (2001::101, FF3E::202)
   Interface: GE1/0/1
   Expires: Never
```

Table 3 Command output

Field	Description
Entries in total	Total number of the IPv6 multicast groups that hosts have joined statically.
(*, FF03::101)	(*, G) entry.
(2001::101, FF3E::202)	(S, G) entry.
Expires	Remaining lifetime for the IPv6 multicast group. This field always displays **Never**, which means that the IPv6 multicast group never expires.

Related commands

reset mld group

display mld interface

Use **display mld interface** to display MLD information for interfaces.

Syntax

display mld [**vpn-instance** *vpn-instance-name*] **interface** [*interface-type interface-number*] [**proxy**] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays MLD information for interfaces on the public network.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays MLD information for all interfaces.

proxy: Displays the MLD proxy interface information. If you do not specify this keyword, the command displays MLD information for all interfaces.

verbose: Displays detailed MLD information.

Examples

Display detailed MLD information for GigabitEthernet 1/0/1 (non-proxy interface) on the public network.

```
<Sysname> display mld interface gigabitethernet 1/0/1 verbose
 GigabitEthernet1/0/1(FE80::200:AFF:FE01:101):
   MLD is enabled.
   MLD version: 1
   Query interval for MLD: 125s
   Other querier present time for MLD: 255s
   Maximum query response time for MLD: 10s
   Last listener query interval: 1s
   Last listener query count: 2
   Startup query interval: 31s
   Startup query count: 2
   General query timer expiry (hh:mm:ss): 00:00:23
   Querier for MLD: FE80::200:AFF:FE01:101 (This router)
   MLD activity: 1 join(s), 0 done(s)
   IPv6 multicast routing on this interface: Enabled
   Robustness: 2
   Require-router-alert: Disabled
   Fast-leave: Disabled
   Startup-query: Off
   Other-querier-present-timer-expiry (hh:mm:ss): Off
  MLD groups reported in total: 1
```

Display detailed MLD information for all MLD proxy interfaces on the public network.

```
<Sysname> display mld interface proxy verbose
 GigabitEthernet1/0/2(FE80::100:CEF:FE01:101):
   MLD proxy is enabled.
   MLD version: 1
   IPv6 multicast routing on this interface: Enabled
   Require-router-alert: Disabled
   Version1-querier-present-timer-expiry (hh:mm:ss): Off
```

Table 4 Command output

Field	Description
GigabitEthernet1/0/1(FE80::200:AFF:FE01:101)	Interface and its IPv6 link-local address.
MLD is enabled	MLD is enabled on the interface.
MLD version	Version of MLD that the interface runs.
Query interval for MLD	MLD query interval, in seconds.
Other querier present time for MLD	MLD other querier present interval, in seconds.
Maximum query response time for MLD	Maximum response time for MLD general query messages, in seconds.
Last listener query interval	Interval for sending MLD multicast-address-specific queries or MLD multicast-address-and-source-specific queries, in seconds.
Last listener query count	Number of MLD multicast-address-specific queries or MLD multicast-address-and-source-specific queries sent for the group.
Startup query interval	MLD startup query interval, in seconds.
Startup query count	Number of MLD general queries sent on startup.
General query timer expiry	Remaining time for the MLD general query timer. This field displays **Off** if the timer is disabled.
Querier for MLD	IPv6 link-local address of the MLD querier.
MLD activity: 1 join(s), 0 done(s)	MLD activity statistics: • **join(s)**—Total number of IPv6 multicast groups that the interface has joined. • **done(s)**—Total number of IPv6 multicast groups that the interface has left.
IPv6 multicast routing on this interface	Whether IPv6 multicast routing is enabled: Enabled or Disabled.
Robustness	Robustness variable of the MLD querier.
Require-router-alert	Whether the feature of dropping MLD messages without Router-Alert is enabled: Enabled or Disabled.
Fast-leave	Whether fast-leave processing is enabled: Enabled or Disabled.
Startup-query	Whether the MLD querier sends MLD general queries at the startup query interval on startup: • **On**—The MLD querier performs the above action. • **Off**—The MLD querier does not perform the above action.
Other-querier-present-timer-expiry	Remaining time for MLD other querier present timer. This field displays **Off** if the timer is disabled.
MLD groups reported in total	Total number of IPv6 multicast groups that the interface has joined dynamically. This field is not displayed if the interface does not join IPv6 multicast groups.
MLD proxy is enabled	MLD proxying is enabled.

Field	Description
Version1-querier-present-timer-expiry	Remaining time for the MLDv1 querier present timer. This field displays **Off** if the timer is disabled.

display mld proxy group

Use **display mld proxy group** to display information about IPv6 multicast groups maintained by the MLD proxy.

Syntax

display mld [**vpn-instance** *vpn-instance-name*] **proxy group** [*ipv6-group-address* | **interface** *interface-type interface-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays information about IPv6 multicast groups maintained by the MLD proxy on the public network.

ipv6-group-address: Specifies an IPv6 multicast group by its IPv6 address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F. If you do not specify an IPv6 multicast group, this command displays IPv6 multicast group membership entries for all IPv6 multicast groups.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays information about IPv6 multicast groups maintained by the MLD proxy for all interfaces.

verbose: Displays detailed information.

Examples

Display information about IPv6 multicast groups maintained by the MLD proxy on the public network.

```
<Sysname> display mld proxy group
MLD proxy group records in total: 2
 GigabitEthernet1/0/1(FE80::16:1):
  MLD proxy group records in total: 2
   Group address: FF1E::1
    Member state: Idle
    Expires: Off

   Group address: FF1E::2
    Member state: Idle
```

```
    Expires: Off
```

Display detailed information about IPv6 multicast group FF1E::1 maintained by the MLD proxy on the public network.

```
<Sysname> display mld proxy group ff1e::1 verbose
 GigabitEthernet1/0/1(FE80::16:1):
  MLD proxy group records in total: 2
   Group: FF1E::1
     Group mode: Include
     Member state: Idle
     Expires: Off
     Source list (sources in total: 1):
       100::1
```

Table 5 Command output

Field	Description
MLD proxy group records in total	Total number of IPv6 multicast group membership entries maintained by the MLD proxy.
GigabitEthernet1/0/1(FE80::16:1)	Interface and its IPv6 address.
Pending proxy group	Pending IPv6 multicast group membership entries maintained by the MLD proxy.
Group address/Group	IPv6 multicast group address.
Member state	Member host states: • **Delay**—The member host has joined a group and started a delay timer. • **Idle**—The member host has joined a group, but didn't start a delay timer.
Expires	Remaining delay time for a member host to send a responding report. This field displays **Off** if the timer is disabled.
Group mode	IPv6 multicast source filtering mode: • Include. • Exclude.
Source list (sources in total: 1)	List of IPv6 multicast sources in the group membership database maintained by the MLD proxy, and the total number of the IPv6 multicast sources.

display mld proxy routing-table

Use **display mld proxy routing-table** to display IPv6 multicast routing entries maintained by the MLD proxy.

Syntax

display mld [**vpn-instance** *vpn-instance-name*] **proxy routing-table** [*ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*]] * [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays IPv6 multicast routing entries maintained by the MLD proxy on the public network.

ipv6-source-address: Specifies an IPv6 multicast source by its IPv6 address. If you do not specify an IPv6 multicast source, this command displays IPv6 multicast routing entries maintained by the MLD proxy for all IPv6 multicast sources.

ipv6-group-address: Specifies an IPv6 multicast group by its IPv6 address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F. If you do not specify an IPv6 multicast group, this command displays IPv6 multicast routing entries for all IPv6 multicast groups maintained by the MLD proxy.

prefix-length: Specifies an address prefix length. For an IPv6 multicast source address, the value range for this argument is 0 to 128. For an IPv6 multicast group address, the value range for this argument is 8 to 128. The default value is 128.

verbose: Displays detailed information about IPv6 multicast routing entries maintained by the MLD proxy.

Examples

Display IPv6 multicast routing entries maintained by the MLD proxy on the public network.

```
<Sysname> display mld proxy routing-table
 Total 1 (*, G) entries, 2 (S, G) entries.

 (100::1, FF1E::1)
     Upstream interface: GigabitEthernet1/0/1
     Downstream interfaces (1 in total):
         1: GigabitEthernet1/0/2
             Protocol: MLD

 (*, FF1E::2)
     Upstream interface: GigabitEthernet1/0/1
     Downstream interfaces (1 in total):
         1: GigabitEthernet1/0/2
             Protocol: STATIC

 (2::2, FF1E::2)
     Upstream interface: GigabitEthernet1/0/1
     Downstream interfaces (2 in total):
         1: LoopBack1
             Protocol: STATIC
         2: GigabitEthernet1/0/2
             Protocol: PROXY
```

Display detailed information about IPv6 multicast routing entries maintained by the MLD proxy on the public network.

```
<Sysname> display mld proxy routing-table verbose
 Total 1 (*, G) entries, 2 (S, G) entries.

 (100::1, FF1E::1)
     Upstream interface: GigabitEthernet1/0/1
     Downstream interfaces (1 in total):
         1: GigabitEthernet1/0/2
             Protocol: MLD
             Querier state: Querier
             Join/Prune state: Join

     Non-downstream interfaces: None

 (*, FF1E::2)
     Upstream interface: GigabitEthernet1/0/1
     Downstream interfaces (1 in total):
         1: GigabitEthernet1/0/2
             Protocol: STATIC
             Querier state: Querier
             Join/Prune state: Join

     Non-downstream interfaces (1 in total):
         1: GigabitEthernet1/0/3
             Protocol: MLD
             Querier state: Non-querier
             Join/Prune state: Join

 (2::2, FF1E::2)
     Upstream interface: GigabitEthernet1/0/1
     Downstream interfaces (2 in total):
         1: LoopBack1
             Protocol: STATIC
             Querier state: Querier
             Join/Prune state: Join
         2: GigabitEthernet1/0/2
             Protocol: PROXY
             Querier state: Querier
             Join/Prune state: Join

     Non-downstream interfaces: None
```

Table 6 Command output

Field	Description
Total 1 (*, G) entries, 2 (S, G) entries	Total number of (*, G), and the total number of (S, G) entries.
(100::1, FF1E::1)	(S, G) entry.

Field	Description
Upstream interface	Incoming interface of a forwarding entry.
Downstream interfaces (1 in total)	Outgoing interfaces, and the total number of outgoing interfaces.
Non-downstream interfaces (1 in total)	Non-outgoing interfaces, and the total number of non-outgoing interfaces.
1: GigabitEthernet1/0/2	Index of an outgoing interface and the outgoing interface.
Protocol	Protocol type: • **MLD**—Dynamic MLD. • **PROXY**—MLD proxy. • **STATIC**—Static MLD.
Querier state	Querier state: • Querier. • Non-querier.
Join/Prune state	Joined or pruned state of the interface: • **NI**—Default state. • **Join**—Joined state. • **Prune**—Pruned state.

display mld ssm-mapping

Use **display mld ssm-mapping** to display MLD SSM mappings.

Syntax

display mld [**vpn-instance** *vpn-instance-name*] **ssm-mapping** *ipv6-group-address*

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays MLD SSM mappings on the public network.

ipv6-group-address: Specifies an IPv6 multicast group by its IPv6 address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F.

Examples

Display MLD SSM mappings for IPv6 multicast group FF3E::101 on the public network.

```
<Sysname> display mld ssm-mapping ff3e::101
 Group: FF3E::101
 Source list:
```

```
1::1
1::2
10::1
100::10
```

Table 7 Command output

Field	Description
Group	IPv6 multicast group address.
Source list	List of IPv6 multicast source addresses.

last-listener-query-count (MLD view)

Use **last-listener-query-count** to set the MLD last listener query count globally.

Use **undo last-listener-query-count** to restore the default.

Syntax

mld last-member-query-count *count*

undo mld last-member-query-count

Default

The MLD last listener query count equals the MLD querier's robustness variable.

Views

MLD view

Predefined user roles

network-admin

context-admin

Parameters

count: Specifies an MLD last listener query count in the range of 1 to 255.

Usage guidelines

You can set the MLD last listener query count globally for all interfaces in MLD view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the global MLD last listener query count to 6 on the public network.

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] last-listener-query-count 6
```

Related commands

mld last-listener-query-count

last-listener-query-interval (MLD view)

Use **last-listener-query-interval** to set the MLD last listener query interval globally.

Use **undo last-listener-query-interval** to restore the default.

Syntax

last-listener-query-interval *interval*

undo last-listener-query-interval

Default

The MLD last listener query interval is 1 second.

Views

MLD view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies an MLD last listener query interval in the range of 1 to 25 seconds.

Usage guidelines

You can set the MLD last listener query interval globally for all interfaces in MLD view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the global MLD last listener query interval to 6 seconds on the public network.

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] last-listener-query-interval 6
```

Related commands

mld last-listener-query-interval

max-response-time (MLD view)

Use **max-response-time** to set the maximum response time for MLD general queries globally.

Use **undo max-response-time** to restore the default.

Syntax

max-response-time *time*

undo max-response-time

Default

The maximum response time for MLD general queries is 10 seconds.

Views

MLD view

Predefined user roles

network-admin

context-admin

Parameters

time: Specifies the maximum response time for MLD general queries in the range of 1 to 3174 seconds.

Usage guidelines

You can set the maximum response time globally for all interfaces in MLD view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the global maximum response time for MLD general queries to 25 seconds on the public network.

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] max-response-time 25
```

Related commands

mld max-response-time

mld

Use **mld** to enter MLD view.

Use **undo mld** to delete the configurations in MLD view.

Syntax

mld [**vpn-instance** *vpn-instance-name*]

undo mld [**vpn-instance** *vpn-instance-name*]

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command takes effect on the public network.

Examples

Enter MLD view of the public network.

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld]
```

Enter MLD view of VPN instance **mvpn**.

```
<Sysname> system-view
[Sysname] mld vpn-instance mvpn
[Sysname-mld-mvpn]
```

mld enable

Use **mld enable** to enable MLD on an interface.

Use **undo mld enable** to disable MLD on an interface.

Syntax

mld enable

undo mld enable

Default

MLD is disabled on an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command takes effect only when IPv6 multicast routing is enabled on the public network or for the VPN instance to which the interface belongs.

Other MLD configurations on the interface take effect only when MLD is enabled on the interface.

Examples

Enable IPv6 multicast routing on the public network, and enable MLD for GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] ipv6 multicast routing
[Sysname-mrib6] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld enable
```

Related commands

ipv6 multicast routing

mld fast-leave

Use **mld fast-leave** to enable fast-leave processing on an interface.

Use **undo mld fast-leave** to disable fast-leave processing on an interface.

Syntax

mld fast-leave [**group-policy** *ipv6-acl-number*]

undo mld fast-leave

Default

Fast-leave processing is disabled. The MLD querier sends MLD multicast-address-specific or multicast-address-and-source-specific queries after receiving a done message.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-acl-number: Specifies an IPv6 basic ACL by its number in the range of 2000 to 2999. If you specify an ACL, the fast-leave processing feature takes effect only on the IPv6 multicast groups that the ACL permits. The feature takes effect on all IPv6 multicast groups when one of the following conditions exists:

- You do not specify an ACL.
- The specified ACL does not exist.
- The specified ACL does not have valid rules.

Usage guidelines

The fast-leave processing feature enables an MLD querier to suppress MLD multicast-address-specific or multicast-address-and-source-specific queries upon receiving MLD done messages permitted by the ACL.

When you configure a rule in the IPv6 basic ACL, follow these restrictions and guidelines:

- If the **vpn-instance** *vpn-instance* option is specified, the rule does not take effect.
- The **source** *source-address source-prefix* option specifies an IPv6 multicast group address.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

Examples

Enable fast-leave processing on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld fast-leave
```

mld group-policy

Use **mld group-policy** to configure an IPv6 multicast group policy on an interface to control the IPv6 multicast groups that hosts attached to the interface can join.

Use **undo mld group-policy** to delete the IPv6 multicast group policy on an interface.

Syntax

mld group-policy *ipv6-acl-number* [*version-number*]

undo mld group-policy

Default

No IPv6 multicast group policy exists. Hosts attached to the interface can join any IPv6 multicast groups.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-acl-number: Specifies an IPv6 basic or advanced ACL by its number in the range of 2000 to 3999. Receiver hosts can join only the IPv6 multicast groups that the ACL permits. If the ACL does not exist or have valid rules, receiver hosts cannot join IPv6 multicast groups.

version-number: Specifies an MLD version number, 1 or 2. By default, this command takes effect on both MLDv1 reports and MLDv2 reports.

Usage guidelines

An IPv6 multicast group policy filters MLD reports to control the IPv6 multicast groups that hosts can join.

This command does not take effect on static member interfaces because static member interfaces do not send MLD reports.

When you configure a rule in the IPv6 ACL, follow these restrictions and guidelines:

- If the **vpn-instance** *vpn-instance* option is specified, the rule does not take effect.
- In a basic ACL, the **source** *source-address source-prefix* option specifies an IPv6 multicast group address.
- In an advanced ACL, the **source** *source-address source-prefix* option specifies an IPv6 multicast source address. The **destination** *dest-address dest-prefix* option specifies an IPv6 multicast group address.

  To match the following MLD reports, set the **source** *source-address source-prefix* option to 0::0:

  - MLDv1 reports.
  - MLDv2 IS_EX and MLDv2 TO_EX reports that do not carry multicast source addresses.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure an IPv6 multicast group policy on GigabitEthernet 1/0/1 so that hosts attached to the interface can join only IPv6 multicast group FF03::101.

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2005
[Sysname-acl-ipv6-basic-2005] rule permit source ff03::101 128
[Sysname-acl-ipv6-basic-2005] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld group-policy 2005
```

mld last-listener-query-count

Use **mld last-listener-query-count** to set the MLD last member query count on an interface.

Use **undo mld last-listener-query-count** to restore the default.

Syntax

mld last-listener-query-count *count*

undo mld last-listener-query-count

Default

The MLD last listener query count equals the MLD querier's robustness variable.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

count: Specifies an MLD last listener query count in the range of 1 to 255.

Usage guidelines

You can set the MLD last listener query count for an interface in interface view or globally for all interfaces in MLD view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the MLD last listener query count to 6 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld last-listener-query-count 6
```

Related commands

last-listener-query-count (MLD view)

mld last-listener-query-interval

Use **mld last-listener-query-interval** to set the MLD last listener query interval on an interface.

Use **undo mld last-listener-query-interval** to restore the default.

Syntax

mld last-listener-query-interval *interval*

undo mld last-listener-query-interval

Default

The MLD last listener query interval is 1 second.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies an MLD last listener query interval in the range of 1 to 25 seconds.

Usage guidelines

You can set the MLD last listener query interval for an interface in interface view or globally for all interfaces in MLD view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the MLD last listener query interval to 6 seconds on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] mld last-listener-query-interval 6
```

Related commands

last-listener-query-interval (MLD view)

mld max-response-time

Use **mld max-response-time** to set the maximum response time for MLD general queries on an interface.

Use **undo mld max-response-time** to restore the default.

Syntax

mld max-response-time *time*

undo mld max-response-time

Default

The maximum response time for MLD general queries is 10 seconds.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

time: Specifies the maximum response time for MLD general queries, in the range of 1 to 3174 seconds.

Usage guidelines

You can set the maximum response time for an interface in interface view or globally for all interfaces in MLD view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the maximum response time for MLD general queries to 25 seconds on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld max-response-time 25
```

Related commands

max-response-time (MLD view)

mld non-stop-routing

Use **mld non-stop-routing** to enable MLD NSR.

Use **undo mld non-stop-routing** to disable MLD NSR.

Syntax

mld non-stop-routing

undo mld non-stop-routing

Default

MLD NSR is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Examples

Enable MLD NSR.

```
<Sysname> system-view
[Sysname] mld non-stop-routing
```

mld other-querier-present-timeout

Use **mld other-querier-present-timeout** to set the MLD other querier present timer on an interface.

Use **undo mld other-querier-present-timeout** to restore the default.

Syntax

mld other-querier-present-timeout *time*

undo mld other-querier-present-timeout

Default

The MLD other querier present timer is calculated by using the following formula:

[MLD general query interval] × [MLD querier's robustness variable] + [maximum response time for MLD general queries] / 2.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

time: Specifies an MLD other querier present timer in the range of 1 to 31744 seconds.

Usage guidelines

You can set the MLD other querier present timer for an interface in interface view or globally for all interfaces in MLD view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the MLD other querier present timer to 125 seconds on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld other-querier-present-timeout 125
```

Related commands

other-querier-present-timeout (MLD view)

mld proxy enable

Use **mld proxy enable** to enable MLD proxying on an interface.

Use **undo mld proxy enable** to disable MLD proxying on an interface.

Syntax

mld proxy enable

undo mld proxy enable

Default

MLD proxying is disabled on an interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command takes effect only when IPv6 multicast routing is enabled on the public network or for the VPN instance to which the interface belongs.

Examples

Enable IPv6 multicast routing on the public network, and enable MLD proxying on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] ipv6 multicast routing
[Sysname-mrib6] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld proxy enable
```

Related commands

ipv6 multicast routing

mld proxy forwarding

Use **mld proxy forwarding** to enable IPv6 multicast forwarding on a non-querier interface.

Use **undo mld proxy forwarding** to disable IPv6 multicast forwarding on a non-querier interface.

Syntax

mld proxy forwarding

undo mld proxy forwarding

Default

IPv6 multicast forwarding is disabled for a non-querier interface.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

Typically, only MLD queriers can forward IPv6 multicast traffic and non-queriers cannot. This prevents IPv6 multicast data from being repeatedly forwarded. If a router interface on the MLD proxy device failed the querier election, enable multicast forwarding capability on this interface to forward multicast data to attached receivers.

Examples

Enable IPv6 multicast forwarding on GigabitEthernet 1/0/1 (non-querier interface).

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld proxy forwarding
```

mld query-interval

Use **mld query-interval** to set the MLD general query interval on an interface.

Use **undo mld query-interval** to restore the default.

Syntax

mld query-interval *interval*

undo mld query-interval

Default

The MLD general query interval is 125 seconds.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies an MLD general interval in the range of 1 to 31744 seconds.

Usage guidelines

You can set the MLD general interval for an interface in interface view or globally for all interfaces in MLD view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the MLD general query interval to 60 seconds on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld query-interval 60
```

Related commands

query-interval (MLD view)

mld robust-count

Use **mld robust-count** to set the MLD querier's robustness variable on an interface.

Use **undo mld robust-count** to restore the default.

Syntax

mld robust-count *count*

undo mld robust-count

Default

The MLD querier's robustness variable is 2.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

count: Specifies an MLD querier's robustness variable in the range of 1 to 255.

Usage guidelines

The MLD querier's robustness variable defines the number of times to retransmit MLD queries if packet loss occurs. A higher robustness variable makes the MLD querier more robust, but it increases the timeout time for IPv6 multicast groups.

You can set the MLD querier's robustness variable for an interface in interface view or globally for all interfaces in MLD view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the MLD querier's robustness variable to 5 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld robust-count 5
```

Related commands

robust-count (MLD view)

mld startup-query-count

Use **mld startup-query-count** to set the MLD startup query count on an interface.

Use **undo mld startup-query-count** to restore the default.

Syntax

mld startup-query-count *count*

undo mld startup-query-count

Default

The MLD startup query count equals the MLD querier's robustness variable.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

count: Specifies an MLD startup query count in the range of 1 to 255.

Usage guidelines

You can set the MLD startup query count for an interface in interface view or globally for all interfaces in MLD view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the MLD startup query count to 5 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld startup-query-count 5
```

Related commands

startup-query-count (MLD view)

mld startup-query-interval

Use **mld startup-query-interval** to set the MLD startup query interval on an interface.

Use **undo mld startup-query-interval** to restore the default.

Syntax

mld startup-query-interval *interval*

undo mld startup-query-interval

Default

The MLD startup query interval equals one quarter of the MLD general query interval.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies an MLD startup query interval in the range of 1 to 31744 seconds.

Usage guidelines

You can set the MLD startup query interval for an interface in interface view or globally for all interfaces in MLD view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the MLD startup query interval to 100 seconds on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld startup-query-interval 100
```

Related commands

startup-query-interval (MLD view)

mld static-group

Use **mld static-group** to configure an interface as a static group member of an IPv6 multicast group.

Use **undo mld static-group** to restore the default.

Syntax

mld static-group *ipv6-group-address* [**source** *ipv6-source-address*]

undo mld static-group { **all** | *ipv6-group-address* [**source** *ipv6-source-address*] }

Default

An interface is not a static member of IPv6 multicast groups.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-group-address: Specifies an IPv6 multicast group by its IPv6 address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F.

ipv6-source-address: Specifies an IPv6 multicast source by its IPv6 address. If you do not specify an IPv6 multicast source, this command configures an interface as a static group member of the multicast groups with all IPv6 multicast source addresses.

all: Specifies all IPv6 multicast groups that the interface has statically joined.

Usage guidelines

For IPv6 multicast routing entries to be created, specify an IPv6 multicast source address if the specified IPv6 multicast group address is in the SSM group range.

Examples

Configure GigabitEthernet 1/0/1 as a static group member of IPv6 multicast group FF03::101.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld static-group ff03::101
```

Configure GigabitEthernet 1/0/1 as a static group member of IPv6 multicast source and group (2001::101, FF3E::202).

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld static-group ff3e::202 source 2001::101
```

mld version

Use **mld version** to specify an MLD version for an interface.

Use **undo mld version** to restore the default.

Syntax

mld version *version-number*

undo mld version

Default

The MLD version is 1.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

version-number: Specifies an MLD version, 1 or 2.

Usage guidelines

CAUTION:
For MLD to operate correctly, specify the same MLD version for all devices on the same subnet.

Examples

Specify MLD version 2 for GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld version 2
```

other-querier-present-timeout (MLD view)

Use **other-querier-present-timeout** to set the MLD other querier present timer globally.

Use **undo other-querier-present-timeout** to restore the default.

Syntax

other-querier-present-timeout *time*

undo other-querier-present-timeout

Default

The MLD other querier present timer is calculated by using the following formula:

[MLD general query interval] × [MLD querier's robustness variable] + [maximum response time for MLD general queries] / 2.

Views

MLD view

Predefined user roles

network-admin

context-admin

Parameters

time: Specifies an MLD other querier present timer in the range of 1 to 31744 seconds.

Usage guidelines

You can set the MLD other querier present timer globally for all interfaces in MLD view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the global MLD other querier present timer to 125 seconds on the public network.

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] other-querier-present-timeout 125
```

Related commands

mld other-querier-present-timeout

proxy multipath (MLD view)

Use **proxy multipath** to enable load splitting on the MLD proxy.

Use **undo proxy multipath** to disable load splitting on the MLD proxy.

Syntax

proxy multipath

undo proxy multipath

Default

The load splitting feature is disabled on the MLD proxy.

Views

MLD view

Predefined user roles

network-admin

context-admin

Usage guidelines

Use this feature when the MLD proxy has multiple proxy interfaces. All proxy interfaces on the MLD proxy share IPv6 multicast traffic on a per-group basis. If you do not enable this feature, only the proxy interface with the highest IPv6 address forwards IPv6 multicast traffic.

Examples

Enable load splitting on the MLD proxy device on the public network.

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] proxy multipath
```

query-interval (MLD view)

Use **query-interval** to set the MLD general query interval globally.

Use **undo query-interval** to restore the default.

Syntax

query-interval *interval*

undo query-interval

Default

The MLD general query interval is 125 seconds.

Views

MLD view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies an MLD general query interval in the range of 1 to 31744 seconds.

Usage guidelines

You can set the MLD general query interval globally for all interfaces in MLD view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the global MLD general query interval to 60 seconds on the public network.

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] query-interval 60
```

Related commands

mld query-interval

reset mld group

Use **reset mld group** to clear dynamic MLD multicast group entries.

Syntax

reset mld [**vpn-instance** *vpn-instance-name*] **group** { **all** | **interface** *interface-type interface-number* { **all** | *ipv6-group-address* [*prefix-length*] [*ipv6-source-address* [*prefix-length*]] } }

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears dynamic MLD multicast group entries on the public network.

all: The first **all** specifies all interfaces, and the second **all** specifies all MLD multicast groups.

interface-type interface-number: Specifies an interface by its type and number.

ipv6-group-address: Specifies an IPv6 multicast group by its IPv6 address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F.

ipv6-source-address: Specifies an IPv6 multicast source by its IPv6 address. If you do not specify an IPv6 multicast source, this command clears dynamic MLD multicast group entries for all IPv6 multicast sources.

prefix-length: Specifies an address prefix length. The default is 128. For a multicast source address, the value range for this argument is 0 to 128. For a multicast group address, the value range for this argument is 8 to 128.

Usage guidelines

CAUTION:

This command might interrupt the IPv6 multicast information transmission.

Examples

Clear dynamic MLD multicast groups for all interfaces on the public network.

```
<Sysname> reset mld group all
```

Clear all dynamic MLD multicast group entries for GigabitEthernet 1/0/1 on the public network.

```
<Sysname> reset mld group interface gigabitethernet 1/0/1 all
```

Clear the dynamic entry of the MLD multicast group FF03::101:10 for GigabitEthernet 1/0/1 on the public network.

```
<Sysname> reset mld group interface gigabitethernet 1/0/1 ff03::101:10
```

Related commands

display mld group

robust-count (MLD view)

Use **robust-count** to set the MLD querier's robustness variable globally.

Use **undo robust-count** to restore the default.

Syntax

robust-count *count*

undo robust-count

Default

The MLD querier's robustness variable is 2.

Views

MLD view

Predefined user roles

network-admin

context-admin

Parameters

count: Specifies an MLD querier's robustness variable in the range of 1 to 255.

Usage guidelines

The MLD querier's robustness variable defines the number of times to retransmit MLD queries if packet loss occurs. A higher robustness variable makes the MLD querier more robust, but it increases the timeout time for IPv6 multicast groups.

You can set the MLD querier's robustness variable globally for all interfaces in MLD view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the global MLD querier's robustness variable to 5 on the public network.

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] robust-count 5
```

Related commands

mld robust-count

ssm-mapping (MLD view)

Use **ssm-mapping** to configure an MLD SSM mapping.

Use **undo ssm-mapping** to delete MLD SSM mappings.

Syntax

ssm-mapping *ipv6-source-address ipv6-acl-number*

undo ssm-mapping { *ipv6-source-address* | **all** }

Default

No MLD SSM mappings exist.

Views

MLD view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-source-address: Specifies an IPv6 multicast source by its IPv6 address.

ipv6-acl-number: Specifies an IPv6 basic ACL number in the range of 2000 to 2999. IPv6 multicast groups in MLD reports permitted by the ACL are associated with the IPv6 multicast source. If the ACL does not exist or does not have valid rules, no IPv6 multicast groups are associated with the IPv6 multicast source.

all: Specifies all MLD SSM mappings.

Usage guidelines

When you configure a rule in the IPv6 basic ACL, follow these restrictions and guidelines:

- If the **vpn-instance** *vpn-instance* option is specified, the rule does not take effect.

- The **source** *source-address source-prefix* **option specifies an** IPv6 multicast group address.
- Among the other optional parameters, only the **fragment keyword and the time-range** *time-range-name* option take effect.

Examples

Configure an MLD SSM mapping with IPv6 multicast source 1::1 and IPv6 multicast group range FF3E::/64 on the public network.

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2001
[Sysname-acl-ipv6-basic-2001] rule permit source ff3e:: 64
[Sysname-acl-ipv6-basic-2001] quit
[Sysname] mld
[Sysname-mld] ssm-mapping 1::1 2001
```

Related commands

display mld ssm-mapping

startup-query-count (MLD view)

Use **startup-query-count** to set the MLD startup query count globally.

Use **undo startup-query-count** to restore the default.

Syntax

startup-query-count *count*

undo startup-query-count

Default

The MLD startup query count equals the MLD querier's robustness variable.

Views

MLD view

Predefined user roles

network-admin

context-admin

Parameters

count: Specifies an MLD startup query count in the range of 1 to 255.

Usage guidelines

You can set the MLD startup query count globally for all interfaces in MLD view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the global MLD startup query count to 5 on the public network.

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] startup-query-count 5
```

Related commands

mld startup-query-count

startup-query-interval (MLD view)

Use **startup-query-interval** to set the MLD startup query interval globally.

Use **undo startup-query-interval** to restore the default.

Syntax

startup-query-interval *interval*

undo startup-query-interval

Default

The MLD startup query interval equals one quarter of the MLD general query interval.

Views

MLD view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies an MLD startup query interval in the range of 1 to 31744 seconds.

Usage guidelines

You can set the MLD startup query interval globally for all interfaces in MLD view or for an interface in interface view. For an interface, the interface-specific configuration takes priority over the global configuration.

Examples

Set the global MLD startup query interval to 100 seconds on the public network.

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] startup-query-interval 100
```

Related commands

mld startup-query-interval

NSFOCUS Firewall Series

NF Network Management and Monitoring Command Reference

NSFOCUS Technologies, Inc.

Document version: 6W600-20230221

Preface

This command reference describes the commands for configuring network management and monitoring features, including system maintenance and debugging (ping, tracert, and system debugging), NQA, NTP, EAA, process monitoring and maintenance, NETCONF, information center, SNMP, NetStream, RMON, flow log, event MIB, fast log output, mirroring, and CWMP.

This preface includes the following topics about the documentation:

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators.

Conventions

The following information describes the conventions used in the documentation.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select a minimum of one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
CAUTION:	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Contents

Information center commands

diagnostic-logfile save

Use **diagnostic-logfile save** to manually save diagnostic logs from the diagnostic log file buffer to the diagnostic log file.

Syntax

diagnostic-logfile save

Views

Any view

Predefined user roles

network-admin

context-admin

Usage guidelines

You can specify the directory to save the diagnostic log file by using the **info-center diagnostic-logfile directory** command.

The system clears the diagnostic log file buffer after saving the buffered diagnostic logs to the diagnostic log file.

If the diagnostic log file buffer is empty, this command displays a success message event though no logs are saved to the diagnostic log file.

Examples

Manually save diagnostic logs from the diagnostic log file buffer to the diagnostic log file.

```
<Sysname> diagnostic-logfile save
The contents in the diagnostic log file buffer have been saved to the file
flash:/diagfile/diagfile.log.
```

Related commands

info-center diagnostic-logfile enable

info-center diagnostic-logfile directory

display character-set

Use **display character-set** to display the character set encoding used on the device or the login terminal.

Syntax

display character-set [**terminal**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

terminal: Displays the character set encoding used on the login terminal. If you do not specify this keyword, this command displays the character set encoding used on the device. By default, the device uses the GB18030 encoding and the encoding cannot be changed.

Usage guidelines

For the user' login terminal to correctly display Chinese characters in log messages received from the device, the device and the terminal must use the same character set encoding.

Use the **display character-set terminal** command to identify the character set encoding used on the login terminal. The device will send test characters in both UTF-8 and GB18030 encodings to the terminal. The test characters will be displayed as 中文 for the character set encoding used on the terminal.

Examples

Display the character set encoding used on the device.

```
<Sysname> system-view
[Sysname] display character-set
Current character set encoding: GB18030
```

Display the character set encoding used on the login terminal.

```
<Sysname> system-view
[Sysname] display character-set terminal
Character set           Test characters
UTF-8                   涓  枸
GB18030                 中文
```

Table 1 Command output

Field	Description
Current character set encoding	Character set encoding used on the device.
Character set	Character set encoding used by the device to send test strings to the terminal. Options are UTF-8 and GB18030.
Test characters	Parsing result of the test characters. The test characters will be displayed as 中文 for the character set encoding used on the login terminal.

Related commands

info-center syslog utf-8 enable

display diagnostic-logfile summary

Use **display diagnostic-logfile summary** to display the diagnostic log file configuration.

Syntax

display diagnostic-logfile summary

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display the diagnostic log file configuration.

```
<Sysname> display diagnostic-logfile summary
  Diagnostic log file: Enabled.
  Diagnostic log file size quota: 10 MB
  Diagnostic log file directory: flash:/diagfile
  Writing frequency: 24 hour 0 min 0 sec
```

Table 2 Command output

Field	Description
Diagnostic log file	Status of the diagnostic log file: • **Enabled**—Diagnostic logs can be output to the diagnostic log file. • **Disabled**—Diagnostic logs cannot be output to the diagnostic log file.
Diagnostic log file size quota	Maximum size for the diagnostic log file, in MB.
Log file directory	Directory where the diagnostic log file is saved.
Writing frequency	Interval at which the system saves diagnostic logs from the buffer to the diagnostic log file.

display info-center

Use **`display info-center`** to display information center configuration.

Syntax

`display info-center`

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display information center configuration.

```
<Sysname> display info-center
Information Center: Enabled
Console: Enabled
Monitor: Enabled
Log host: Enabled
    192.168.0.1, log output filter: loghost1
```

```
    port number: 5000, host facility: local7
Log buffer: Enabled
    Max buffer size 1024, current buffer size 512,
    Current messages 0, dropped messages 0, overwritten messages 0
Log file: Enabled
Security log file: Enabled
Information timestamp format:
    Log host: Date
    Other output destination: Date
```

display info-center filter

Use **display info-center filter** to display information about log output filters.

Syntax

display info-center filter [*filtername*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

filter-name: Specifies an existing log output filter by its name. If you do not specify a log output filter, this command display information about all log output filters.

Examples

Display information about log output filter **loghost1**.

```
<Sysname> display info-center filter loghost1
 Log output filter: loghost1
 Module                       Rule
 ARP                          Debugging
 CFGLOG                       Deny
 Default                      Informational
```

Table 3 Command output

Field	Description
Log output filter:	Name of the log output filter.
Module	Module to which the log output filter applies.
Rule	Rules in the log output filter.

Related commands

info-center filter

display info-center source

Use **display info-center source** to display the log output rules by source modules.

Syntax

display info-center source [**module** *module-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

module *module-name*: Specifies a module. The *module-name* argument is a case insensitive string that represents the complete module name. To view the names of supported modules, execute the **display info-center source module ?** command. If you do not specify a module, this command displays the log output rules for all modules.

Usage guidelines

By default, the information center outputs logs of different modules according to the default log output rules (see Table 10). You can use the **info-center source** command to change the log output rules. The **display info-center source** command displays the current log output rules of log source modules.

Examples

Display the current log output rules for all modules.

```
<Sysname> display info-center source
 Module   Console       Monitor       Loghost       Logbuffer     Logfile
 ACL      DEBUG         DEBUG         INFO          INFO          INFO
 ADJ4     DEBUG         DEBUG         INFO          INFO          INFO
 ADJ6     DEBUG         DEBUG         INFO          INFO          INFO
```

…

Display the current log output rules for the EDEV module.

```
<Sysname> display info-center source module EDEV
 Module   Console       Monitor       Loghost       Logbuffer     Logfile
 EDEV     DEBUG         DEBUG         INFO          INFO          INFO
```

Table 4 Command output

Field	Description
Module	Module name.
Console	Lowest level of logs that can be output to the console. This field displays **deny** if no logs of the module can be output to the console.
Monitor	Lowest level of logs that can be output to the monitor terminal. This field displays **deny** if no logs of the module can be output to the monitor terminal.
Loghost	Lowest level of logs that can be output to the log host.

	This field displays **deny** if no logs of the module can be output to the log host.
Logbuffer	Lowest level of logs that can be output to the log buffer. This field displays **deny** if no logs of the module can be output to the log buffer.
Logfile	Lowest level of logs that can be output to the log file. This field displays **deny** if no logs of the module can be output to the log file.

Related commands

info-center source

display logbuffer

Use **display logbuffer** to display log buffer information and buffered logs.

Syntax

display logbuffer [**module** *module-name* [**submodule** *submodule-name*]] [**reverse**] [**level** *severity* | **size** *buffersize* | **slot** *slot-number*] * [**last-mins** *mins*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

module *module-name*: Displays information for the log buffer of a module. The *module-name* argument is a case-insensitive string that represents the complete module name. To view the names of supported modules, execute the **display logbuffer module ?** command. If you do not specify a module, this command displays the information for the general log buffer.

submodule *submodule-name*: Displays log buffer information for a submodule of the specified module. The *submodule--name* argument is a case-insensitive string that represents the complete submodule name. To view the names of supported submodules, execute the **display logbuffer module module-name submodule ?** command. If you do not specify a submodule, this command displays log buffer information for all submodules of the specified module.

reverse: Displays log entries chronologically, with the most recent entry at the top. If you do not specify this keyword, the command displays log entries chronologically, with the oldest entry at the top.

level *severity*: Specifies a severity level in the range of 0 to 7. If you do not specify a severity level, this command displays log information for all levels.

Table 5 Log levels

Severity value	Level	Description
0	Emergency	The system is unusable. For example, the system authorization has expired.
1	Alert	Action must be taken immediately. For example, traffic on an interface exceeds the upper limit.

Severity value	Level	Description
2	Critical	Critical condition. For example, the device temperature exceeds the upper limit, the power module fails, or the fan tray fails.
3	Error	Error condition. For example, the link state changes.
4	Warning	Warning condition. For example, an interface is disconnected, or the memory resources are used up.
5	Notification	Normal but significant condition. For example, a terminal logs in to the device, or the device reboots.
6	Informational	Informational message. For example, a command or a **ping** operation is executed.
7	Debugging	Debugging message.

size *buffersize*: Specifies the number of latest logs to be displayed. The value range is 1 to 1024. If you do not specify this option, the command displays all logs in the log buffer.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all member devices.

last-mins *mins*: Displays logs buffered over the last specified period of time. The *mins* argument specifies a time period in the range of 1 to 43200 minutes. If you do not specify a time period, the command displays all logs in the log buffer.

Examples

Display log buffer information and buffered logs.

```
<Sysname> display logbuffer
Log buffer: Enabled
Max buffer size: 1024
Actual buffer size: 512
Dropped messages: 0
Overwritten messages: 718
Current messages: 512
Some messages might not be displayed due to permission issues.
%Jun 17 15:57:09:578 2017 Sysname SYSLOG/7/SYS_RESTART:System restarted --
…
```

Display log buffer information and logs buffered over the last 5 minutes.

```
<Sysname> display logbuffer last-mins 5
Log buffer: Enabled
Max buffer size: 1024
Actual buffer size: 512
Dropped messages: 0
Overwritten messages: 0
Current messages: 191
%Jan  1 01:00:06:784 2018 Sysname SHELL/6/SHELL_CMD:
-Line=vty0-IPAddr=192.168.1.242-User=**; Command is display current-configuration
%Jan  1 01:03:19:691 2018 Sysname SHELL/5/SHELL_LOGIN: VTY logged in from 192.168.1.33.
%Jan  1 01:03:21:269 2018 Sysname SHELL/6/SHELL_CMD:
-Line=vty1-IPAddr=192.168.1.33-User=**; Command is display logbuffer last-mins 5
```

Table 6 Command output

Field	Description
Log buffer	Status of the log buffer: • **Enabled**—Logs can be output to the log buffer. • **Disabled**—Logs cannot be output to the buffer.
Max buffer size	Maximum buffer size supported by the device.
Actual buffer size	Maximum buffer size configured by using the **info-center logbuffer size** command.
Dropped messages	Number of dropped messages.
Overwritten messages	Number of overwritten messages.
Current messages	Number of current messages.
Some messages might not be displayed due to permission issues.	The log information displayed by the **display logbuffer** command varies by user role. For information about user roles, see RBAC configuration in *Fundamentals Configuration Guide*.

Related commands

info-center logbuffer

reset logbuffer

display logbuffer summary

Use **display logbuffer summary** to display the log buffer summary.

Syntax

display logbuffer summary [**level** *severity* | **slot** *slot-number*] *

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

level *severity*: Specifies a severity level in the range of 0 to 7. If you do not specify a severity level, this command displays log information of all levels in the log buffer. For more information about log levels, see Table 5.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all member devices.

Usage guidelines

This command displays only the summary of the general log buffer.

Examples

Display the summary of the log buffer.

```
<Sysname> display logbuffer summary
```

```
Slot EMERG ALERT  CRIT ERROR  WARN NOTIF  INFO DEBUG
   1     0     0     0     7     0    34    38     0
```

Table 7 Command output

Field	Description
EMERG	Represents emergency. For more information, see Table 5.
ALERT	Represents alert. For more information, see Table 5.
CRIT	Represents critical. For more information, see Table 5.
ERROR	Represents error. For more information, see Table 5.
WARN	Represents warning. For more information, see Table 5.
NOTIF	Represents notification. For more information, see Table 5.
INFO	Represents informational. For more information, see Table 5.
DEBUG	Represents debug. For more information, see Table 5.

display logfile summary

Use **`display logfile summary`** to display the log file configuration.

Syntax

`display logfile summary`

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Usage guidelines

This command displays only the general log file configuration.

Examples

Display the log file configuration.

```
<Sysname> display logfile summary
  Log file: Enabled.
  Log file size quota: 10 MB
  Log file directory: flash:/logfile
  Writing frequency: 24 hour 0 min 10 sec
```

Table 8 Command output

Field	Description
Log file	Log file status: • **Enabled**—Logs can be output to the log file. • **Disabled**—Logs cannot be output to the log file.

Field	Description
Log file size quota	Maximum log file size, in MB.
Log file directory	Log file directory.
Writing frequency	Log file writing frequency.

display security-logfile summary

Use **display security-logfile summary** to display the summary of the security log file.

Syntax

display security-logfile summary

Views

Any view

Predefined user roles

security-audit

Usage guidelines

To use this command, a local user must have the security-audit user role. For information about configuring the security-audit user role, see AAA commands in *Security Command Reference*.

Examples

Display the summary of the security log file.

```
<Sysname> display security-logfile summary
  Security log file: Enabled
  Security log file size quota: 10 MB
  Security log file directory: flash:/seclog
  Alarm threshold: 80%
  Current usage: 30%
  Writing frequency: 24 hour 0 min 0 sec
```

Table 9 Command output

Field	Description
Security log file	Status of the security log file: • **Enabled**—Security logs can be output to the security log file. • **Disabled**—Security logs cannot be output to the security log file.
Security log file size quota	Maximum storage space reserved for the security log file.
Security log file directory	Security log file directory.
Alarm threshold	Alarm threshold of the security log file usage.
Current usage	Current usage of the security log file.
Writing frequency	Security log file writing frequency.

Related commands

authorization-attribute (*Security Command Reference*)

enable log updown

Use **enable log updown** to enable an interface to generate link up or link down logs when the interface state changes.

Use **undo enable log updown** to disable an interface from generating link up or link down logs when the interface state changes.

Syntax

enable log updown

undo enable log updown

Default

All interfaces are allowed to generate link up and link down logs.

Views

Interface view

Predefined user roles

network-admin

context-admin

Examples

Disable GigabitEthernet 1/0/1 from generating link up or link down logs.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo enable log updown
```

info-center diagnostic-logfile directory

Use **info-center diagnostic-logfile directory** to configure the directory to save the diagnostic log file.

Syntax

info-center diagnostic-logfile directory *dir-name*

Default

The diagnostic log file is saved in the **diagfile** folder under the root directory of the default file system.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

dir-name: Specifies a directory by its name, a string of 1 to 64 characters.

Usage guidelines

The specified directory must have been created.

This command cannot survive an IRF reboot or a master/subordinate switchover.

Examples

Set the diagnostic log file directory to **flash:/test**.

```
<Sysname> mkdir test
Creating directory flash:/test... Done.
<Sysname> system-view
[Sysname] info-center diagnostic-logfile directory flash:/test
```

info-center diagnostic-logfile enable

Use **info-center diagnostic-logfile enable** to enable saving of diagnostic logs to the diagnostic log file.

Use **undo info-center diagnostic-logfile enable** to disable saving of diagnostic logs to the diagnostic log file.

Syntax

info-center diagnostic-logfile enable

undo info-center diagnostic-logfile enable

Default

Saving of diagnostic logs to the diagnostic log file is enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command enables saving diagnostic logs to the diagnostic log file for centralized management. You can view the diagnostic logs to monitor device activities and to troubleshoot problems.

Examples

Enable saving diagnostic logs to the diagnostic log file.

```
<Sysname> system-view
[Sysname] info-center diagnostic-logfile enable
```

info-center diagnostic-logfile frequency

Use **info-center diagnostic-logfile frequency** to configure the interval at which the system saves diagnostic logs from the diagnostic log file buffer to the diagnostic log file.

Use **undo info-center diagnostic-logfile frequency** to restore the default.

Syntax

info-center diagnostic-logfile frequency *freq-sec*

undo info-center diagnostic-logfile frequency

Default

The diagnostic log file saving interval is 86400 seconds.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

freq-sec: Specifies the diagnostic log file saving interval in seconds. The value range is 10 to 86400.

Usage guidelines

The system outputs diagnostic logs to the diagnostic log file buffer, and then saves the buffered logs to the diagnostic log file at the specified interval.

Examples

Set the diagnostic log file saving interval to 600 seconds.

```
<Sysname> system-view
[Sysname] info-center diagnostic-logfile frequency 600
```

Related commands

info-center diagnostic-logfile enable

info-center diagnostic-logfile quota

Use **info-center diagnostic-logfile quota** to set the maximum size for the diagnostic log file.

Use **undo info-center diagnostic-logfile quota** to restore the default.

Syntax

info-center diagnostic-logfile quota *size*

undo info-center diagnostic-logfile quota

Default

The maximum size for the diagnostic log file is 10 MB.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

size: Specifies the maximum size for the diagnostic log file, in MB. The value range is 1 to 10.

Examples

Set the maximum size to 6 MB for the diagnostic log file.

```
<Sysname> system-view
[Sysname] info-center diagnostic-logfile quota 6
```

info-center enable

Use **info-center enable** to enable the information center.

Use **undo info-center enable** to disable the information center.

Syntax

info-center enable

undo info-center enable

Default

The information center is enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Examples

Enable the information center.

```
<Sysname> system-view
[Sysname] info-center enable
Information center is enabled.
```

info-center filter

Use **info-center filter** to create a log output filter.

Use **undo info-center filter** to delete a log output filter.

Syntax

info-center filter *filter-name* { *module-name* | **default** } { **deny** | **level** *severity* }

undo info-center filter *filter-name* [*module-name* | **default**]

Default

No log output filters exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

filter-name: Specifies a name for the log output filter, a case-insensitive string of 1 to 8 characters.

module-name: Specifies a module by its name. To view the names of supported modules, execute the **info-center filter** *filter-name* **?** command.

default: Specifies all supported modules.

deny: Disables log output.

level *severity*: Specifies a log severity level by its name. Supported severity levels are **alert**, **critical**, **debugging**, **emergency**, **error**, **informational**, **notification**, and **warning**. See Table 5 for more information about the log severity levels. The log output filter applies to logs of the specified severity level and all higher levels.

Usage guidelines

A log output filter contains a set of log output filter rules for modules. You can create multiple log output filters. When specifying a log host, you can apply a log output filter to control log output to the log host.

You can also use the **info-center source** command to configure log output rules for the log host output destination. The system chooses the settings to control log output to a log host in the following order:

1. Log output filter specified for the log host by using the **info-center loghost** command.
2. Log output rules configured for the log host output destination by using the **info-center source** command.
3. Default log output rules (see Table 10).

Follow these restrictions and guidelines when you configure a log output filter:

- To set a log output filter rule for a module, use the *module-name* argument to specify the module name.

  If you set log output filter rules for the same module multiple times, the most recent configuration takes effect.
- To set a general log output filter rule for all modules, use the **default** keyword. The general log output filter rule applies to all modules that do not have module-specific filter rules.

  If you set a general log output filter rule multiple times, the most recent configuration takes effect.
- If no general log output filter rule is set, the system outputs logs with severity levels **informational** through **alert** for modules that do not have module-specific filter rules.
- To remove a module-specific log output filter rule, you must use the *module-name* argument. You cannot use the **default** keyword to remove module-specific log output filter rules. If you do not specify any parameters, the entire log output filter is deleted.

Examples

Create log output filter **loghost1**. In the log output filter, enable the ARP module to output logs with severity levels **notification** through **alert**, enable the SNMP module to output logs with severity levels **warning** through **alert**, and disable log output of all other modules.

```
<Sysname> system-view
[Sysname] info-center filter loghost1 arp level notification
[Sysname] info-center filter loghost1 snmp level warning
[Sysname] info-center filter loghost1 default deny
```

Related commands

display info-center filter

info-center loghost

info-center source

info-center format

Use **info-center format** to set the format for logs sent to log hosts.

Use **undo info-center format** to restore the default.

Syntax

info-center format { **cmcc** | **sgcc** | **unicom** }

undo info-center format

Default

Logs are sent to log hosts in non-customized format.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

cmcc: Specifies the China Mobile Communications Corporation (CMCC) format.

sgcc: Specifies the State Grid Corporation of China (SGCC) format.

unicom: Specifies the China Unicom format.

Usage guidelines

Logs can be sent to log hosts in non-customized, China Unicom, SGCC, or CMCC format. For more information about log formats, see information center configuration in *Network Management and Monitoring Configuration Guide*.

Examples

Set the log format to China Unicom for logs sent to log hosts.

```
<Sysname> system-view
[Sysname] info-center format unicom
```

info-center logbuffer

Use **info-center logbuffer** to enable log output to the log buffer.

Use **undo info-center logbuffer** to disable log output to the log buffer.

Syntax

info-center logbuffer

undo info-center logbuffer

Default

Log output to the log buffer is enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command enables log output to log buffers based on the log source modules.

- Logs generated by modules or submodules that have separate log buffers are saved to their respective log buffers.

  For example, session logs are saved to the session log buffer.
- Logs generated by other modules are saved to the general log buffer.

To view log buffer information and buffered logs, use the **display logbuffer** command.

To set the log buffer size, use the **info-center logbuffer size** command.

Examples

Enable log output to the log buffer.

```
<Sysname> system-view
[Sysname] info-center logbuffer
```

Related commands

display logbuffer

info-center enable

info-center logbuffer size

Use **info-center logbuffer size** to set the maximum number of logs that can be buffered.

Use **undo info-center logbuffer size** to restore the default.

Syntax

info-center logbuffer [**module** *module-name*] **size** *buffersize*

undo info-center logbuffer [**module** *module-name*] **size**

Default

A maximum of 512 logs can be buffered.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

module *module-name*: Sets the size for the log buffer of a module. The *module-name* argument is a case-insensitive string that represents the complete module name. To view the names of supported modules, execute the **info-center logbuffer module ?** command. If you do not specify a module, this command sets the size for the general log buffer.

buffersize: Specifies the maximum log buffer size. The value range is 0 to 1024.

Examples

Set the maximum log buffer size to 50.

```
<Sysname> system-view
[Sysname] info-center logbuffer size 50
```

Restore the default maximum log buffer size.

```
<Sysname> system-view
[Sysname] undo info-center logbuffer size
```

Related commands

display logbuffer

info-center enable

info-center logfile directory

Use **info-center logfile directory** to specify the directory to save the log file.

Syntax

info-center logfile directory *dir-name*

Default

The log file is saved in the **logfile** folder under the root directory of the default file system.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

dir-name: Specifies a directory by its name, a string of 1 to 64 characters.

Usage guidelines

The specified log file directory must have been created.

The log file uses the .log extension.

This command cannot survive an IRF reboot or a master/subordinate switchover.

Examples

Set the log file directory to **flash:/test**.

```
<Sysname> mkdir test
Creating directory flash:/test... Done.
<Sysname> system-view
[Sysname] info-center logfile directory flash:/test
```

Related commands

info-center logfile enable

info-center logfile enable

Use **info-center logfile enable** to enable the log file feature.

Use **undo info-center logfile enable** to disable the log file feature.

Syntax

info-center logfile enable

undo info-center logfile enable

Default

The log file feature is enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

After you configure this command, the system outputs logs to log files according to the log source modules.

- Logs generated by modules or submodules that have separate log files are output to their respective log files.

  For example, session logs are output to the log file named **session.log**.

  The modules and submodules that have separate log files are predefined and they cannot be changed.
- Logs generated by other modules are output to the general log file.

Examples

Enable log output to the log file.

```
<Sysname> system-view
[Sysname] info-center logfile enable
```

info-center logfile frequency

Use **info-center logfile frequency** to configure the interval at which the system saves logs from the log file buffer to the log file.

Use **undo info-center logfile frequency** to restore the default.

Syntax

info-center logfile frequency *freq-sec*

undo info-center logfile frequency

Default

The log file saving interval is 86400 seconds.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

freq-sec: Specifies the log file saving interval in seconds. The value range is 1 to 86400.

Usage guidelines

This command enables the system to automatically save logs in the log file buffer to the log file at the specified interval.

Examples

Set the log file saving interval to 60000 seconds.

```
<Sysname> system-view
```

```
[Sysname] info-center logfile frequency 60000
```

Related commands

info-center logfile enable

info-center logfile module alarm-threshold

Use **info-center logfile module alarm-threshold** to set the log file usage alarm threshold for a module.

Use **undo info-center logfile module alarm-threshold** to restore the default.

Syntax

info-center logfile module *module-name* **alarm-threshold** *usage*

undo info-center logfile module *module-name* **alarm-threshold**

Default

The log file usage alarm threshold is 80% of the log file size. When the log file usage ratio of a module reaches 80%, the system outputs a message to inform the user.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

module *module-name*: Specifies a module. The *module-name* argument is a case insensitive string that represents the complete module name. To view the names of supported modules, execute the **info-center logfile module ?** command.

usage: Specifies an alarm threshold in percentage in the range of 0 to 100. Set the value to 0 to disable the log file usage alarm feature.

Usage guidelines

After you set the alarm threshold for the log file usage of a module, the system outputs a message to inform the user when the threshold is reached. The user can then back up the log file to avoid loss of log data.

Examples

Set the log file usage alarm threshold to 90% of the log file size for the session module.

```
<Sysname> system-view
[Sysname] info-center logfile module SESSION alarm-threshold 90
```

info-center logfile size-quota

Use **info-center logfile size-quota** to set the maximum log file size.

Use **undo info-center logfile size-quota** to restore the default.

Syntax

info-center logfile [**module** *module-name*] **size-quota** *size*

undo info-center logfile [**module** *module-name*] **size-quota**

Default

The maximum log file size for the general log file and module-specific log file is 10 MB and 1 MB, respectively.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

module *module-name*: Sets the maximum log file size for a module. The *module-name* argument is a case-insensitive string that represents the complete module name. To view the names of supported modules, execute the **info-center logfile module ?** command. If you do not specify a module, this command sets the size for the general log file.

size: Specifies the maximum log file size in MB. The value range is 1 to 10.

Examples

Set the maximum log file size to 2 MB.

```
<Sysname> system-view
[Sysname] info-center logfile size-quota 2
```

Related commands

info-center logfile enable

info-center logging suppress duplicates

Use **info-center logging suppress duplicates** to enable duplicate log suppression.

Use **undo info-center logging suppress duplicates** to disable duplicate log suppression.

Syntax

info-center logging suppress duplicates

undo info-center logging suppress duplicates

Default

Duplicate log suppression is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

Outputting consecutive duplicate logs wastes system and network resources and increases device maintenance costs. You can enable this feature to suppress output of consecutive duplicate logs.

Examples

Enable duplicate log suppression on device A.

```
<Sysname> system-view
```

```
[Sysname] info-center logging suppress duplicates
```

info-center logging suppress module

Use **info-center logging suppress module** to configure a log suppression rule for a module.

Use **undo info-center logging suppress module** to delete a log suppression rule.

Syntax

info-center logging suppress module *module-name* **mnemonic** { **all** | *mnemonic-value* }

undo info-center logging suppress module *module-name* **mnemonic** { **all** | *mnemonic-value* }

Default

The device does not suppress output of any logs from any modules.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

module-name: Specifies a log source module by its name, a case-insensitive string of 1 to 8 characters. To view the list of available log source modules, use the **info-center logging suppress module ?** command.

mnemonic { **all** | *mnemonic-value* }: Configures a mnemonic filter for log suppression.

- **all**: Suppresses output of all logs of the module.
- *mnemonic-value*: Suppresses output of logs with the specified mnemonic value. The *mnemonic-value* argument is a case-insensitive string of 1 to 32 characters, which must be the complete value contained in the mnemonic field of the log message. Log suppression will fail if a partial mnemonic value is specified.

Usage guidelines

You can configure log suppression rules to filter out the logs that you are not concerned with. A log suppression rule suppresses output of all logs or only logs with a specific mnemonic value for a module.

Examples

Configure a log suppression rule to suppress output of logs with the **shell_login** mnemonic value for the shell module.

```
<Sysname> system-view
[Sysname] info-center logging suppress module shell mnemonic shell_login
```

Related commands

info-center source

info-center loghost

Use **info-center loghost** to specify a log host and to configure output parameters.

Use **undo info-center loghost** to remove a log host.

Syntax

info-center loghost [**vpn-instance** *vpn-instance-name*] { *hostname* | *ipv4-address* | **ipv6** *ipv6-address* } [**facility** *local-number* | **filter** *filter-name* | **format** { **cmcc** | **default** | **sgcc** | **unicom** } | **port** *port-number* | **source-ip** *source-ip-address*] *

undo info-center loghost [**vpn-instance** *vpn-instance-name*] { *hostname* | *ipv4-address* | **ipv6** *ipv6-address* }

Default

No log hosts are specified.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If the log host is on the public network, do not specify this option.

hostname: Specifies a log host by its name, a case-insensitive string of 1 to 253 characters. The host name can contain letters, digits, and special characters including hyphen (-), underscore (_), and dot (.).

ipv4-address: Specifies a log host by its IPv4 address.

ipv6 *ipv6-address*: Specifies a log host by its IPv6 address.

facility *local-number*: Specifies a logging facility from local0 to local7 for the log host. The default value is local7. Logging facilities are used to mark different logging sources, and query and filer logs.

filter *filter-name*: Specifies a log output filter to control log output to the log host. The *filter-name* argument represents the filter name, a case-insensitive string of 1 to 8 characters. If you do not specify a log output filter, the log output rules configured by using the **info-center source** command for the log host destination are used.

format { **cmcc** | **default** | **unicom** | **sgcc** }: Specifies a format for logs sent to log hosts. If you do not specify this keyword, the format specified by the **info-center format** command is used.

- **cmcc**: Specifies the China Mobile Communications Corporation (CMCC) format.
- **default**: Specifies the non-customized format.
- **sgcc**: Specifies the State Grid Corporation of China (SGCC) format.
- **unicom**: Specifies the China Unicom format.

port *port-number*: Specifies the port number of the log host, in the range of 1 to 65535. The default is 514. It must be the same as the value configured on the log host. Otherwise, logs cannot be sent to the log host.

source-ip *source-ip-address*: Specifies the source IP address for logs sent to the specified log hosts. If you do not specify this option, the source IP address specified by the **info-center loghost source** command is used.

Usage guidelines

The **info-center loghost** command takes effect only after the information center is enabled by using **info-center enable** command.

Examples

Output logs to the log host at 1.1.1.1.

```
<Sysname> system-view
[Sysname] info-center loghost 1.1.1.1
```

Related commands

info-center filter

info-center format

info-center source

info-center loghost locate-info with-sn

Use **info-center loghost locate-info with-sn** to add the device serial number to the location field of logs sent to log hosts.

Use **undo info-center loghost locate-info with-sn** to restore the default.

Syntax

info-center loghost locate-info with-sn

undo info-center loghost locate-info with-sn

Default

The device does not add the device serial number to the location field of logs sent to log hosts.

Views

System view

Predefined user roles

network-admin

context-admin

Examples

Add the device serial number to the location field of logs sent to log hosts.

```
<Sysname> system-view
[Sysname] info-center loghost locate-info with-sn
```

info-center loghost source

Use **info-center loghost source** to specify a source IP address for logs sent to log hosts.

Use **undo info-center loghost source** to restore the default.

Syntax

info-center loghost source *interface-type interface-number*

undo info-center loghost source

Default

The source IP address of logs sent to log hosts is the primary IP address of the outgoing interface.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

The system uses the primary IP address of the specified interface as the source IP address of the logs sent to log hosts.

The **info-center loghost source** command takes effect only after the information center is enabled by using **info-center enable** command.

The source IP address specified by the **info-center loghost source** command applies to all log hosts and that specified by the **info-center loghost** command applies to the specified log hosts. For a log host, the source IP address specified by the **info-center loghost** command takes precedence over that specified by the **info-center loghost source** command.

Examples

Use the IP address of interface Loopback 0 as the source IP address of the logs sent to log hosts.

```
<Sysname> system-view
[Sysname] interface loopback 0
[Sysname-LoopBack0] ip address 2.2.2.2 32
[Sysname-LoopBack0] quit
[Sysname] info-center loghost source loopback 0
```

Related commands

info-center loghost

info-center security-logfile alarm-threshold

Use **info-center security-logfile alarm-threshold** to set the alarm threshold for security log file usage.

Use **undo info-center security-logfile alarm-threshold** to restore the default.

Syntax

info-center security-logfile alarm-threshold *usage*

undo info-center security-logfile alarm-threshold

Default

The alarm threshold for security log file usage is 80. When the usage of the security log file reaches 80%, the system outputs a message to inform the administrator.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

usage: Specifies an alarm threshold. The value must be an integer in the range of 1 to 100.

Usage guidelines

When the security log file is full, the system deletes the oldest logs and then writes new logs to the security log file. This feature helps avoid security log loss by setting an alarm threshold for the security log file usage. When the threshold is reached, the system outputs log information to inform the administrator. The administrator can log in to the device with the security-audit user role and back up the security log file.

Examples

Set the alarm threshold for security log file usage to 90.

```
<Sysname> system-view
[Sysname] info-center security-logfile alarm-threshold 90
```

Related commands

info-center security-logfile size-quota

info-center security-logfile directory

Use **info-center security-logfile directory** to specify the security log file directory.

Syntax

info-center security-logfile directory *dir-name*

Default

The security log file is saved in the **seclog** folder under the root directory of the default file system.

Views

System view

Predefined user roles

security-audit

Parameters

dir-name: Specifies a directory by its name, a string of 1 to 64 characters.

Usage guidelines

The specified directory must have been created.

To use this command, a local user must have the security-audit user role.

This command cannot survive an IRF reboot or a master/subordinate switchover.

Examples

Set the security log file directory to **flash:/test**.

```
<Sysname> mkdir test
Creating directory flash:/test... Done.
<Sysname> system-view
[Sysname] info-center security-logfile directory flash:/test
```

info-center security-logfile enable

Use **info-center security-logfile enable** to enable saving of security logs to the security log file.

Use **undo info-center security-logfile enable** to restore the default.

Syntax

info-center security-logfile enable

undo info-center security-logfile enable

Default

Saving of security logs to the security log file is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This feature enables the system to output security logs to the security log file buffer, and then saves the buffered logs to the security log file regularly.

Examples

Enable saving security logs to the security log file.

```
<Sysname> system-view
[Sysname] info-center security-logfile enable
```

info-center security-logfile frequency

Use **info-center security-logfile frequency** to configure the interval for saving security logs to the security log file.

Use **undo info-center security-logfile frequency** to restore the default.

Syntax

info-center security-logfile frequency *freq-sec*

undo info-center security-logfile frequency

Default

The security log file saving interval is 86400 seconds.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

freq-sec: Specifies the security log file saving interval in seconds. The value range is 10 to 86400 seconds.

Usage guidelines

The system outputs security logs to the security log file buffer, and then saves the buffered logs to the security log file at the specified interval.

Examples

Set the security log file saving interval to 600 seconds.

```
<Sysname> system-view
[Sysname] info-center security-logfile frequency 600
```

Related commands

info-center security-logfile enable

info-center security-logfile size-quota

Use **info-center security-logfile size-quota** to set the maximum size for the security log file.

Use **undo info-center security-logfile size-quota** to restore the default.

Syntax

info-center security-logfile size-quota *size*

undo info-center security-logfile size-quota

Default

The maximum size for the security log file is 10 MB.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

size: Sets the maximum size for the security log file, in MB. The value range is 1 to 10.

Examples

Set the maximum size to 6 MB for the security log file.

```
<Sysname> system-view
[Sysname] info-center security-logfile size-quota 6
```

Related commands

info-center security-logfile alarm-threshold

info-center source

Use **info-center source** to configure a log output rule for a module.

Use **undo info-center source** to restore the default.

Syntax

info-center source { *module-name* | **default** } { **console** | **logbuffer** | **logfile** | **loghost** | **monitor** } { **deny** | **level** *severity* }

undo info-center source { *module-name* | **default** } { **console** | **logbuffer** | **logfile** | **loghost** | **monitor** }

Default

Table 10 lists the default log output rules.

Table 10 Default output rules

Destination	Log source modules	Output switch	Severity
Console	All supported modules	Enabled	Debugging
Monitor terminal	All supported modules	Disabled	Debugging
Log host	All supported modules	Enabled	Informational
Log buffer	All supported modules	Enabled	Informational
Log file	All supported modules	Enabled	Informational

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

module-name: Specifies a module by its name. You can use the **info-center source ?** command to view the modules supported by the device.

default: Specifies all supported modules.

console: Outputs logs to the console.

logbuffer: Outputs logs to the log buffer.

logfile: Outputs logs to the log file.

loghost: Outputs logs to the log host.

monitor: Outputs logs to the monitor terminal.

deny: Disables log output.

level *severity*: Specifies a severity level in the range of 0 to 7. The smaller the severity value, the higher the severity level. See Table 5 for more information. Logs at the specified severity level and higher levels are allowed to be output.

Usage guidelines

If you do not set an output rule for a module, the module uses the output rule set by using the **default** keyword. If no rule is set by using the **default** keyword, the module uses the default output rule.

To modify or remove an output rule set for a module, you must use the *module-name* argument. A new output rule configured by using the **default** keyword does not take effect on the module.

If you execute this command for a module multiple times, the most recent configuration takes effect.

If you execute this command for the **default** modules multiple times, the most recent configuration takes effect.

Examples

Output only VLAN module's information with the emergency level to the console.

```
<Sysname> system-view
[Sysname] info-center source default console deny
```

```
[Sysname] info-center source vlan console level emergency
```

Based on the previous configuration, disable output of VLAN module's information to the console so no system information is output to the console.

```
<Sysname> system-view
[Sysname] undo info-center source vlan console
```

info-center synchronous

Use **info-center synchronous** to enable synchronous information output.

Use **undo info-center synchronous** to disable synchronous information output.

Syntax

info-center synchronous

undo info-center synchronous

Default

Synchronous information output is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

System log output interrupts ongoing configuration operations, including obscuring previously entered commands. Synchronous information output shows the obscured commands. It also provides a command prompt in command editing mode, or a [Y/N] string in interaction mode so you can continue your operation from where you were stopped.

Examples

Enable synchronous information output, and then execute the **display current-configuration** command to view the current configuration of the device.

```
<Sysname> system-view
[Sysname] info-center synchronous
Info-center synchronous output is on
[Sysname] display current-
```

At this time, the system receives log information. It displays the log information first, and then displays your previous input, which is **display current-** in this example.

```
%May 21 14:33:19:425 2007 Sysname SHELL/5/SHELL_LOGIN: VTY logged in from 192.168.1.44
[Sysname] display current-
```

Enter **configuration** to complete the **display current-configuration** command, and press the **Enter** key to execute the command.

Enable synchronous information output, and then save the current configuration (enter interactive information).

```
<Sysname> system-view
[Sysname] info-center synchronous
Info-center synchronous output is on
[Sysname] save
```

```
The current configuration will be written to the device. Are you sure? [Y/N]:
```

At this time, the system receives the log information. It displays the log information first and then displays [Y/N].

```
%May 21 14:33:19:425 2007 Sysname SHELL/5/SHELL_LOGIN: VTY logged in from 192.168.1.44
[Y/N]:
```

Enter **Y** or **N** to complete your input.

info-center syslog min-age

Use **info-center syslog min-age** to set the minimum storage period for logs in the log buffer and log file.

Use **undo info-center syslog min-age** to restore the default.

Syntax

info-center syslog [**module** *module-name*] **min-age** *min-age*

undo info-center syslog [**module** *module-name*] **min-age**

Default

The minimum storage period is not set.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

module *module-name*: Sets the minimum storage period for logs in the log buffer and log file of a module. The *module-name* argument is a case-insensitive string that represents the complete module name. To view the names of supported modules, execute the **info-center syslog module ?** command. If you do not specify a module, this command sets the minimum storage period for logs in the general log buffer and general log file.

min-age: Sets the minimum storage period in hours. The value range is 1 to 8760.

Examples

Set the minimum storage period to 168 hours.

```
<Sysname> system-view
[Sysname] info-center syslog min-age 168
```

info-center syslog trap buffersize

Use **info-center syslog trap buffersize** to set the maximum number of log traps that can be stored in the log trap buffer.

Use **undo info-center syslog trap buffersize** to restore the default.

Syntax

info-center syslog trap buffersize *buffersize*

undo info-center syslog trap buffersize

Default

The log trap buffer can store a maximum of 1024 traps.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

buffersize: Specifies the maximum number of log traps that can be stored in the log trap buffer. The value range is 0 to 65535. Value 0 indicates that the device does not buffer log traps.

Usage guidelines

Log traps are SNMP notifications stored in the log trap buffer. After the **snmp-agent trap enable syslog** command is configured, the device sends log messages in SNMP notifications to the log trap buffer. You can view the log traps by accessing the MIB corresponding to the trap buffer.

The default buffer size is usually used. You can adjust the buffer size according to your network condition. New traps overwrite the oldest traps when the log trap buffer is full.

Examples

Set the log trap buffer size to 2048.

```
<Sysname> system-view
[Sysname] info-center syslog trap buffersize 2048
```

Related commands

snmp-agent trap enable syslog

info-center syslog utf-8 enable

Use **info-center syslog utf-8 enable** to enable the information center to use the UTF-8 encoding.

Use **undo info-center syslog utf-8 enable** to restore the default.

Syntax

info-center syslog utf-8 enable

undo info-center syslog utf-8 enable

Default

The information center uses the GB18030 encoding.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

For the user' login terminal to correctly display Chinese characters in log messages received from the information center, the information center and the terminal must use the same character set encoding.

The information center supports both GB18030 and UTF-8 encodings. By default, the GB18030 encoding is used.

If the login terminal uses the UTF-8 encoding, you can use this command to enable the information center to use the UTF-8 encoding.

Examples

Enable the information center to use the UTF-8 encoding.

```
<Sysname> system-view
[Sysname] info-center syslog utf-8 enable
```

Related commands

display character-set

info-center timestamp

Use **info-center timestamp** to set the timestamp format for logs sent to the console, monitor terminal, log buffer, and log file.

Use **undo info-center timestamp** to restore the default.

Syntax

info-center timestamp { **boot** | **date** | **none** }

undo info-center timestamp

Default

The timestamp format for logs sent to the console, monitor terminal, log buffer, and log file is **date**.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

boot: Sets the timestamp format to xxx.yyy, where xxx is the most significant 32 bits (in milliseconds) and yyy is the least significant 32 bits. For example, 0.21990989 equals Jun 25 14:09:26:881 2007. The **boot** time shows the time since system startup.

date: Sets the timestamp format to MMM DD hh:mm:ss:ms YYYY, such as Dec 8 10:12:21:708 2007. The **date** time shows the current system time.

- MMM: Abbreviations of the months in English, which could be Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, or Dec.
- DD: Date, starting with a space if it is less than 10, for example " 7".
- hh:mm:ss:ms: Local time, with hh in the range of 00 to 23, mm and ss in the range of 00 to 59, and ms in the range of 0 to 999.
- YYYY: Year.

none: Indicates no time information is provided.

Examples

Set the timestamp format to **boot** for logs sent to the console, monitor terminal, log buffer, and log file.

```
<Sysname> system-view
```

```
[Sysname] info-center timestamp boot
```

Related commands

info-center timestamp loghost

info-center timestamp loghost

Use **info-center timestamp loghost** to set the timestamp format for logs sent to log hosts.

Use **undo info-center timestamp loghost** to restore the default.

Syntax

info-center timestamp loghost { **date** [**with-milliseconds**] | **iso** [**with-milliseconds**] | **no-year-date** | **none** }

undo info-center timestamp loghost

Default

The timestamp format for logs sent to log hosts is **date**.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

date: Sets the timestamp format to mmm dd hh:mm:ss yyyy, such as Dec 8 10:12:21 2007. The **date** time shows the current system time.

iso: Sets the ISO 8601 timestamp format, for example, 2009-09-21T15:32:55.

with-milliseconds: Sets the timestamp to be accurate to milliseconds for logs output to log hosts in date or ISO 8601 format. The millisecond value is appended to the time information in the timestamp with a dot as the separator. If you do not specify this keyword, the timestamp in date or ISO 8601 format is accurate to seconds.

- Example of a timestamp in date format with millisecond accuracy: Dec 8 10:12:21.708 2018.
- Example of a timestamp in ISO 8601 format with millisecond accuracy: 2018-09-21T15:32:55.708.

no-year-date: Sets the timestamp format to the current system date and time without year.

none: Indicates that no timestamp information is provided.

Examples

Set the timestamp format to **no-year-date** for logs sent to log hosts.

```
<Sysname> system-view
[Sysname] info-center timestamp loghost no-year-date
```

Related commands

info-center timestamp

info-center trace-logfile quota

Use **info-center trace-logfile quota** to set the maximum size for the trace log file.

Use **undo info-center trace-logfile quota** to restore the default.

Syntax

info-center trace-logfile quota *size*

undo info-center trace-logfile quota

Default

The maximum trace log file size is 1 MB.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

size: Sets the maximum size for the trace log file, in MB.The value range is 1 to 10.

Examples

Set the maximum size to 6 MB for the trace log file.

```
<Sysname> system-view
[Sysname] info-center trace-logfile quota 6
```

logfile save

Use **logfile save** to manually save logs in the log file buffer to the log file.

Syntax

logfile save

Views

Any view

Predefined user roles

network-admin

context-admin

Usage guidelines

You can specify the directory to save the log file by using the **info-center logfile directory** command.

The system clears the log file buffer after saving the buffered logs to the log file automatically or manually.

If the log file buffer is empty, this command displays a success message event though no logs are saved to the log file.

Examples

Manually save logs from the log file buffer to the log file.

```
<Sysname> logfile save
The contents in the log file buffer have been saved to the file flash:/logfile/logfile.log.
```

Related commands

info-center logfile enable

info-center logfile directory

reset logbuffer

Use **reset logbuffer** to clear the log buffer.

Syntax

reset logbuffer [**module** *module-name* [**submodule** *submodule-name*]]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

module *module-name*: Clears the log buffer of a module. The *module-name* argument is a case-insensitive string that represents the complete module name. To view the names of supported modules, execute the **reset logbuffer module ?** command. If you do not specify a module, this command clears the general log buffer.

submodule *submodule-name*: Clears the log buffer of a submodule of the specified module. The *submodule--name* argument is a case-insensitive string that represents the complete submodule name. To view the names of supported submodules, execute the **display logbuffer module module-name submodule ?** command. If you do not specify a submodule, this command clears the log buffers of all submodules of the specified module.

Examples

Clear the log buffer.

```
<Sysname> reset logbuffer
```

Related commands

display logbuffer

security syslog rate-limit

Use **security syslog rate-limit** to set the maximum number of security logs that can be sent per second.

Use **undo security syslog rate-limit** to restore the default.

Syntax

security syslog rate-limit *max-value*

undo security syslog rate-limit

Default

The device can send a maximum of 1000 security logs per second to the information center.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

max-value: Sets the maximum number of security logs that can be sent per second. The value range for this argument is 0 to 10000. Value 0 indicates that the device does not send security logs to the information center.

Usage guidelines

When the device processes the following security services, a large number of security logs will be generated and sent to the information center, which will cause overload of the information center:

- AFT.
- ASPF.
- Data filtering.
- File filtering.
- URL filtering.
- NAT.
- Session management.
- Anti-virus.
- Application audit and management.
- IPS.
- NetShare Control.
- Server connection detection.
- Attack detection and prevention.

This feature allows you to set the maximum number of security logs that can be sent per second to the information center. With this feature configured, the device will discard the subsequent security logs when the maximum number of security logs that can be sent per second is reached. Please configure the maximum number of security logs that can be sent per second as required.

Examples

Set 1000 as the maximum number of security logs that can be sent per second.

```
<Sysname> system-view
[Sysname] security syslog rate-limit 1000
```

security-logfile save

Use **security-logfile save** to manually save security logs from the security log file buffer to the security log file.

Syntax

security-logfile save

Views

Any view

Predefined user roles

security-audit

Usage guidelines

The system clears the security log file buffer after saving the buffered security logs to the security log file automatically or manually.

If the security log file buffer is empty, this command displays a success message event though no security logs are saved to the security log file.

To use this command, a local user must have the security-audit user role.

Examples

Manually save the security logs in the security log file buffer to the security log file.

```
<Sysname> security-logfile save
The contents in the security log file buffer have been saved to the file
flash:/seclog/seclog.log.
```

Related commands

info-center security-logfile directory

authorization-attribute (*Security Command Reference*)

snmp-agent trap enable syslog

Use **snmp-agent trap enable syslog** to enable SNMP notifications for log messages.

Use **undo snmp-agent trap enable syslog** to disable SNMP notifications for log messages.

Syntax

snmp-agent trap enable syslog

undo snmp-agent trap enable syslog

Default

The device does not send SNMP notifications for log messages.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command enables the device to send an SNMP notification for each log message it outputs. The device encapsulates logs in SNMP notifications and then sends them to the SNMP module and the log trap buffer.

For the SNMP module to send the received SNMP notifications correctly, you must also configure SNMP on the device. For more information about SNMP configuration, see the network management and monitoring configuration guide for the device.

To view the traps in the log trap buffer, access the MIB corresponding to the log trap buffer. The log trap buffer size can be set by using the **info-center syslog trap buffersize** command.

Examples

Enable the device to send SNMP notifications for log messages.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable syslog
```

Related commands

info-center syslog trap buffersize

terminal debugging

Use **terminal debugging** to enable output of debugging messages to the current terminal.

Use **undo terminal debugging** to disable output of debugging messages to the current terminal.

Syntax

terminal debugging

undo terminal debugging

Default

Output of debugging messages to the current terminal is disabled.

Views

User view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command enables output of debugging-level log messages to the current terminal.

To enable output of debugging messages to the console, perform the following tasks:

1. Execute the **terminal debugging** command.
2. Enable the information center. The information center is enabled by default.
3. Use a debugging command to enable the related debugging.

To enable output of debugging messages to the monitor terminal, perform the following tasks:

1. Execute the **terminal monitor** and **terminal debugging** commands.
2. Enable the information center. The information center is enabled by default.
3. Use a debugging command to enable the related debugging.

This command takes effect only for the current connection between the terminal and the device. If a new connection is established, the default is restored.

You can also enable output of debugging messages to the current terminal by executing the **terminal logging level 7** command. The **terminal logging level 7** command and the **terminal debugging** command have the following differences:

- The **terminal logging level 7** command enables log output for all log severity levels (levels 0 through 7).
- The **terminal debugging** command enables log output for the following log severity levels:
  - Debugging level (level **7**).
  - Severity level higher than or equal to the level specified in the **terminal logging level** command.

Examples

Enable output of debugging messages to the current terminal.

```
<Sysname> terminal debugging
The current terminal is enabled to display debugging logs.
```

Related commands

terminal logging level

terminal monitor

terminal logging level

Use **terminal logging level** to set the lowest level of logs that can be output to the current terminal.

Use **undo terminal logging level** to restore the default.

Syntax

terminal logging level *severity*

undo terminal logging level

Default

The lowest level of logs that can be output to the current terminal is 6 (Informational).

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

severity: Specifies a log severity level. Valid values are alert, critical, debugging, emergency, error, informational, notification, warning, and digits from 0 to 7.

Usage guidelines

This command enables the device to output logs with a severity level higher than or equal to the specified level to the current terminal. For example, if you set the *severity* argument to 6, logs with a severity value from 0 to 6 are output to the current terminal.

This command takes effect only for the current connection between the terminal and the device. If a new connection is established, the default is restored.

Examples

Configure the device to output logs with the debugging level and higher levels to the current terminal.

```
<Sysname> terminal logging level 7
```

terminal monitor

Use **terminal monitor** to enable log output to the current terminal.

Use **undo terminal monitor** to disable log output to the current terminal.

Syntax

terminal monitor

undo terminal monitor

Default

Log output to the console is enabled, and log output to the monitor terminal is disabled.

Views

User view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command takes effect only for the current connection between the terminal and the device. If a new connection is established, the default is restored.

Examples

Enable log output to the current terminal.

```
<Sysname> terminal monitor
The current terminal is enabled to display logs.
```

Contents

Flow log commands

display userlog export

Use **display userlog export** to display flow log configuration and statistics.

Syntax

display userlog export

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display flow log configuration and statistics.

```
<Sysname> display userlog export
Flow:
  Export flow log as UDP Packet.
  Version: 3.0
  Source ipv4 address: 2.2.2.2
  Source ipv6 address:
  Log load balance function: Disabled
  Local time stamp: Disabled
  Number of log hosts: 2

  Log host 1:
    Host/Port: 1.2.3.6/2000
    Total logs/UDP packets exported: 112/87

  Log host 2:
    VPN instance:abc
    Host/Port:1.1.1.1/2000
    Total logs/UDP packets exported: 6553665536/409597846
```

Table 1 Command output

Field	Description
Flow	Flow log configuration and statistics.
Export flow log as UDP Packet	Flow log entries were sent to log hosts in UDP.
Version	Flow log feature version.
Source ipv4/ipv6 address	Source IP address of the flow log packets.

Field	Description
Log load balance function	Load balancing status for flow log packets: • **Enabled**—Flow log packets are distributed among available log hosts. • **Disabled**—Every flow log packet is copied and sent to all available log hosts.
Local time stamp	Whether the use of the local time in the flow log timestamp is enabled or disabled.
Number of log hosts	Total number of log hosts.
Log host	Information about the log host.
VPN instance	VPN instance to which the log host belongs.
Host/port	IP address and port number of the log host.
Total logs	Total number of flow log entries successfully exported and those failed to be exported to the log hosts.
UDP packets exported	Total number of UDP packets successfully sent and those failed to be sent to the log hosts. The UDP packets are used to export flow log entries. A UDP packet can contain multiple flow log entries.

Related commands

`userlog flow export`

display userlog host-group

Use **`display userlog host-group`** to display flow log host group information.

Syntax

`display userlog host-group` [**`ipv6`**] [*`host-group-name`*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

`ipv6`: Specifies an IPv6 flow log host group. Do not configure this keyword if you want to specify an IPv4 flow log host group.

`host-group-name`: Specify a flow log host group by its name, a case-sensitive string of 1 to 63 characters. If you do not specify a log host group, this command displays information about all log host groups.

Examples

Display information about IPv4 flow log host group **test**.

```
<Sysname> display userlog host-group test
Userlog host-group test:
  ACL number: 2000

  Flow log host numbers: 1

    Log host 1:
      VPN-instance: test
      Host/port: 1.1.1.2/2000
```

Display information about all IPv4 flow log host groups.

```
<Sysname> display userlog host-group
There are 2 IPv4 host groups.

Userlog host-group test:
  ACL number: 2000

  Flow log host numbers: 1

    Log host 1:
      VPN-instance: test
      Host/Port: 1.2.3.6/0

Userlog host-group test2:
  ACL name: test

  Flow log host numbers: 1

    Log host 1:
      Host/Port: 1.1.1.1/0
```

Table 2 Command output

Field	Description
Userlog host-group test	Information about a flow log host group.
ACL number/ACL name	ACL used by the log host group to match flow log entries.
Flow log host numbers	Number of flow log hosts in the group.
Log host	Information about a flow log host.
VPN-instance	VPN instance to which the log host belongs. This field is not displayed if no VPN instance is specified for the log host.
Host/Port	IP address and port number of the log host.

Related commands

userlog host-group

userlog host-group host flow

reset userlog flow export

Use **reset userlog flow export** to clear flow log statistics.

Syntax

reset userlog flow export

Views

User view

Predefined user roles

network-admin

context-admin

Examples

Clear flow log statistics.

```
<Sysname> reset userlog flow export
```

Related commands

userlog flow export

userlog flow export host

Use **userlog flow export host** to specify a log host to receive flow log entries.

Use **undo userlog flow export host** to remove a log host.

Syntax

userlog flow export [**vpn-instance** *vpn-instance-name*] **host** { *hostname* | *ipv4-address* | **ipv6** *ipv6-address* } **port** *udp-port*

undo userlog flow export [**vpn-instance** *vpn-instance-name*] **host** { *hostname* | *ipv4-address* | **ipv6** *ipv6-address* }

Default

No log hosts are specified.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If the log host is on the public network, do not specify this option.

hostname: Specifies a log host by its name, a case-insensitive string of 1 to 253 characters. The host name can contain letters, digits, and special characters including hyphen (-), underscore (_), and dot (.).

ipv4-address: Specifies a log host by its IPv4 address. The address must be a valid unicast address and cannot be a loopback address.

ipv6 *ipv6-address*: Specifies a log host by its IPv6 address.

port *udp-port*: Specifies the UDP port number of the log host, in the range of 1 to 65535. As a best practice, use UDP port numbers in the range 1025 to 65535 to avoid collision with well-known UDP port numbers.

Examples

Export flow log entries to UDP port 2000 on the log host at 1.2.3.6.

```
<Sysname> system-view
[Sysname] userlog flow export host 1.2.3.6 port 2000
```

Related commands

display userlog export

userlog flow export load-balancing

Use **userlog flow export load-balancing** to enable load balancing for flow log entries.

Use **undo userlog flow export load-balancing** to restore the default.

Syntax

userlog flow export load-balancing

undo userlog flow export load-balancing

Default

Load balancing is disabled. The device sends a copy of each flow log entry to all available log hosts.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

In load balancing mode, flow log entries are distributed among log hosts based on the source IP addresses (before NAT) that are recorded in the entries. The flow log entries generated for the same source IP address are sent to the same log host. If a log host goes down, the flow logs sent to it will be lost.

Examples

Enable load balancing for flow logging.

```
<Sysname> system-view
[Sysname] userlog flow export load-balancing
```

Related commands

userlog flow export host

userlog flow export source-ip

Use **userlog flow export source-ip** to specify a source IP address for flow log packets.

Use **undo userlog flow export source-ip** to restore the default.

Syntax

userlog flow export source-ip { *ipv4-address* | **ipv6** *ipv6-address* }

undo userlog flow export source-ip [**ipv6**]

Default

The source IP address of flow log packets is the IP address of their outgoing interface.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-address: Specifies an IPv4 address.

ipv6 *ipv6-address*: Specifies an IPv6 address.

Examples

Specify 1.2.1.2 as the source IP address for flow log packets.

```
<Sysname> system-view
[Sysname] userlog flow export source-ip 1.2.1.2
```

Related commands

userlog flow export host

userlog flow export timestamp localtime

Use **userlog flow export timestamp localtime** to configure the device to use the local time in the timestamp of flow logs.

Use **undo userlog flow export timestamp localtime** to restore the default.

Syntax

userlog flow export timestamp localtime

undo userlog flow export timestamp localtime

Default

The device uses the UTC time in the timestamp of flow logs.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

The device uses either the local time or the UTC time in the timestamp of flow logs.

- **UTC time**—Standard Greenwich Mean Time (GMT).
- **Local time**—Standard GMT plus or minus the time zone offset.

  The time zone offset can be configured by using the **clock timezone** command. For more information, see *Fundamentals Command Reference*.

Examples

Configure the device to use the local time in the timestamp of flow logs.

```
<Sysname> system-view
[Sysname] userlog flow export timestamp localtime
```

userlog flow export version

Use **userlog flow export version** to set the flow log version.

Use **undo userlog flow export version** to restore the default.

Syntax

userlog flow export version *version-number*

undo userlog flow export version

Default

The flow log version is 1.0.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

version-number: Specifies a flow log version. Available options are 1, 3, and 5, which represent version 1.0, version 3.0, and version 5.0.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the flow log version to 3.0.

```
<Sysname> system-view
[Sysname] userlog flow export version 3
```

Related commands

userlog flow export host

userlog flow syslog

Use **userlog flow syslog** to specify the information center as the destination for flow log export.

Use **undo userlog flow syslog** to restore the default.

Syntax

userlog flow syslog

undo userlog flow syslog

Default

Flow log entries are not exported.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

CAUTION:

The device might generate a lot of session logs in a short time. If the session logs are exported to the information center for processing, the information center might consume too much performance, affecting normal operations of the device.

You can export flow log entries to log hosts or the information center, but not both. If both methods are configured, the system exports flow log entries to the information center.

Flow log entries are converted to the syslog format when they are exported to the information center. Their severity level is informational. With the information center, you can specify multiple log output destinations, including the console, log host, and log file.

Log entries in ASCII format are human readable. However, the log data volume is higher in ASCII format than in binary format.

Examples

Specify the information center as the destination for flow log export.

```
<Sysname> system-view
[Sysname] userlog flow syslog
```

Related commands

userlog flow export host

userlog host-group

Use **userlog host-group** to create a flow log host group and enter its view, or enter the view of an existing flow log host group.

Use **undo userlog host-group** to delete a flow log host group.

Syntax

userlog host-group [**ipv6**] *host-group-name* **acl** { **name** *acl-name* | **number** *acl-number* }

undo userlog host-group [**ipv6**] *host-group-name*

Default

No flow log host groups exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ipv6: Creates an IPv6 flow log host group. Do not configure this keyword if you want to create an IPv4 flow log host group.

host-group-name: Specify a name for the flow log host group, a case-sensitive string of 1 to 63 characters.

acl: Specify an ACL to match the flow log entries to be sent to the flow log host group.

name *acl-name*: Specifies the ACL name, a case-insensitive string of 1 to 63 characters. The ACL name must start with a letter and cannot be **all**.

number *acl-number*: Specifies the ACL number, in the range of 2000 to 3999.

Usage guidelines

The flow log host group feature enables the device to send specific flow logs to specific group of log hosts. This facilitates log filtering and reduces the log sending and processing workload of the device.

A flow log host group uses an ACL to match the flow logs to be sent to it. Make sure the ACL exists and the ACL rules can identify the designated flow logs.

A flow log matches a log host group if it matches the group's ACL, and it is sent only to the log hosts in the matching group.

If a flow log matches multiple log host groups, the device sends the log to the group that comes first in alphabetical order of the matching group names.

If a flow log does not match any log host groups, the device ignores the log host group configuration and sends the log to all configured log hosts.

Examples

Create an IPv4 flow log host group named **test** and specify ACL 2000 for it.

```
<Sysname> system-view
[Sysname] userlog host-group test acl number 2000
[Sysname-userlog-host-group-test]
```

Related commands

display userlog host-group

userlog host-group host flow

userlog host-group host flow

Use **userlog host-group host flow** to assign a log host to a flow log host group.

Use **undo userlog host-group host flow** to remove a log host from a flow log host group.

Syntax

IPv4 flow log host group view:

userlog host-group [**vpn-instance** *vpn-instance-name*] **host flow** { *hostname* | *ipv4-address* }

undo userlog host-group [**vpn-instace** *vpn-instance-name*] **host flow** { *hostname* | *ipv4-address* }

IPv6 flow log host group view:

userlog host-group [**vpn-instance** *vpn-instance-name*] **host flow ipv6** { *hostname* | *ipv6-address* }

undo userlog host-group [**vpn-instance** *vpn-instance-name*] **host flow ipv6** { *hostname* | *ipv6-address* }

Default

No log hosts exist in a flow log host group.

Views

IPv4 flow log host group view

IPv6 flow log host group view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If the log host is on the public network, do not specify this option.

hostname: Specifies a log host by its name, a case-insensitive string of 1 to 253 characters. The host name can contain letters, digits, hyphens (-), underscores (_), and dots (.).

ipv4-address: Specifies a log host by its IPv4 address. The address must be a valid IPv4 unicast address and cannot be a loopback address.

ipv6 *ipv6-address*: Specifies a log host by its IPv6 address. The address must be a valid IPv6 unicast address and cannot be a loopback address or all zeros.

Usage guidelines

A flow log host group can contain multiple log hosts, and a log host can be assigned to multiple flow log host groups.

Before you assign a log host to a flow log host group, make sure the log host has been configured on the device by using **userlog flow export host** the command.

Examples

Assign a log host to flow log host group **test**.

```
<Sysname> system-view
[Sysname] userlog host-group test acl number 2000
[Sysname-userlog-host-group-test] userlog host-group host flow 1.2.3.6
```

Related commands

display userlog host-group

userlog flow export host

userlog host-group

Contents

Fast log output commands

customlog character-encoding utf-8

Use **customlog character-encoding utf-8** to configure fast log output to use the UTF-8 encoding.

Use **undo customlog character-encoding** to restore the default.

Syntax

customlog character-encoding utf-8

undo customlog character-encoding

Default

Fast log output uses the GB18030 encoding.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

For the log host to correctly display Chinese characters in received log messages, make sure the fast log output module uses the same character set encoding as the log host. Fast log output supports using GB18030 and UTF-8 encodings.

Examples

Configure fast log output to use the UTF-8 encoding.

```
<Sysname> system-view
[Sysname] customlog character-encoding utf-8
```

customlog format

Use **customlog format** to enable fast log output.

Use **undo customlog format** to restore the default.

Syntax

customlog format { **aft** | **aft-cmcc** | **aft-telecom** | **aft-unicom** | **attack-defense** | **cntm** | **dns** | **dpi** [**anti-virus** | **audit** | **data-filter** | **file-filter** | **ips** [**sgcc** { **policy-hit** | **signature-update** }] | **netshare** | **sandbox** | **terminal** | **traffic-policy** | **url-filter** [**unicom**]] | **keepalive** **sgcc** | **lb** [**dns-proxy** | **gslb** | **inbound** | **outbound**] | **nat** { **cmcc** | **telecom** | **unicom** } | **packet-filter** [**sgcc**] | **scd** | **security-policy** **sgcc** | **session** | **trusted-access** { **csap** | **iam** [**authorization** | **notification**] } }

undo customlog format { **aft** | **aft-cmcc** | **aft-telecom** | **aft-unicom** | **attack-defense** | **cntm** | **dns** | **dpi** [**anti-virus** | **audit** | **data-filter** | **file-filter** | **ips** | **netshare** | **sandbox** | **terminal** | **traffic-policy** | **url-filter** [**unicom**]] * | **keepalive** | **lb** [**dns-proxy** | **gslb** | **inbound** |

outbound] * | **nat** | **packet-filter** | **scd** | **security-policy** | **session** | **trusted-access** { **csap** | **iam** [**authorization** | **notification**] } } *

Default

Fast log output is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

aft: Enables fast log output for the AFT module.

attack-defense: Enables fast log output for the attack defense module.

dns: Enables fast log output for the DNS module.

dpi: Enables fast log output for a DPI-related module. If you do not specify a DPI module keyword, this command enables fast log output for all the DPI-related modules.

anti-virus: Specifies the anti-virus module.

audit: Specifies the application audit and management module.

ips: Specifies the intrusion protection system module.

sgcc: Specifies the SGCC format for the specified type of IPS logs. If you do not specify this keyword, the standard format is used for fast output of the IPS logs.

policy-hit: Specifies the IPS policy hit logs.

signature-update: Specifies the IPS signature update logs.

netshare: Specifies the netshare control module.

sandbox: Specifies the sandbox module.

traffic-policy: Specifies the bandwidth management module.

url-filter: Specifies the URL filtering module.

unicom: Specifies the UNICOM format for fast output URL filtering logs. If you do not specify this keyword, the standard format is used to output the logs.

keepalive: Enables fast log output of keepalive logs. After this keyword is specified, the device sends keepalive logs to the log host periodically. If the log host cannot receive the keepalive logs in a specific period of time, the log host determines that the device is down.

lb: Enables fast log output for a load balancing module. If you do not specify a load balancing module, this command enables fast log output for all load balancing modules.

- **dns-proxy**: Specifies the transparent DNS proxy module.
- **gslb**: Specifies the global load balancing module.
- **inbound**: Specifies the inbound link load balancing module.
- **outbound**: Specifies the outbound link load balancing module.

nat: Enables fast log output in a specific format for the NAT module.

- **cmcc**: Specifies the CMCC format.
- **telecom**: Specifies the TELECOM format.

- **unicom**: Specifies the UNICOM format.

packet-filter: Enables fast output of packet matching logs for the packet filter and security policy modules.

scd: Enables fast log output for the service connection detection module.

security-policy: Enables fast output of security policy configuration logs for the security policy module.

session: Enables fast log output for the session management module.

sgcc: Specifies the SGCC format for the specified type of logs. If you do not specify this keyword, the standard format is used for fast output of the logs.

Usage guidelines

The fast log output feature enables fast output of logs to log hosts.

Typically, logs generated by a service module are first sent to the information center, which then outputs the logs to the specified destination (such as to log hosts). When fast log output is configured, logs of service modules are sent directly to log hosts instead of to the information center. Compared to outputting logs to the information center, fast log output saves system resources.

Fast log output, flow log, and information center are exclusive from one another. When the **customlog format** command is configured, the specified service module uses only the fast log output method. For more information about flow log, see "Configuring flow log." For more information about the information center, see "Configuring the information center."

To output logs of the NAT module to a log host, you must specify the log format required by the log host in the **customlog format** and **customlog host** commands. Logs of other modules can be output only in one format. You do not need to specify the format for these logs.

Examples

Enable fast log output for the session management module.

```
<Sysname> system
[Sysname] customlog format session
```

customlog host

Use **customlog host** to configure fast log output parameters.

Use **undo customlog host** to remove the fast log output configuration.

Syntax

customlog host [**vpn-instance** *vpn-instance-name*] { *hostname* | *ipv4-address* | **ipv6** *ipv6-address* } [**port** *port-number*] **export** { **aft** | **attack-defense** | **cmcc-sessionlog** | **cmcc-userlog** | **dns** | **dpi** [**anti-virus** | **audit** | **ips** | **netshare** | **sandbox** | **traffic-policy** | **url-filter**] * | **keepalive** | **lb** [**dns-proxy** | **gslb** | **inbound** | **outbound**] *| **packet-filter** | **scd** | **security-policy** | **session** | **telecom-sessionlog** | **telecom-userlog** | **unicom-sessionlog** | **unicom-userlog** } *

undo customlog host [**vpn-instance** *vpn-instance-name*] { *hostname* | *ipv4-address* | **ipv6** *ipv6-address* } [**port** *port-number*]

Default

Fast log output parameters are not configured.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the log host belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the log host is on the public network, do not specify this option.

hostname: Specifies a log host by its name, a case-insensitive string of 1 to 253 characters. The host name can contain letters, digits, hyphens (-), underscores (_), and dots (.).

ipv4-address: Specifies a log host by its IPv4 address.

ipv6 *ipv6-address*: Specifies a log host by its IPv6 address.

port *port-number*: Specifies the port number of the log host. The value range is 1 to 65535, and the default is 514. The setting must be the same as the port number configured on the log host. Otherwise, the log host cannot receive logs.

export: Specifies a source module for fast log output.

aft: Outputs logs of the AFT module to the log host.

attack-defense: Outputs logs of the attack defense module to the log host.

cmcc-sessionlog: Outputs NAT session logs in CMCC format to the log host.

cmcc-userlog: Outputs NAT444 user logs in CMCC format to the log host.

dns: Outputs DNS logs to the log host.

dpi: Outputs logs of a DPI-related module to the log host. If you specify the **dpi** keyword without a DPI module keyword, this command outputs logs of all the DPI-related modules to the log host.

anti-virus: Specifies the anti-virus module.

audit: Specifies the application audit and management module.

ips: Specifies the intrusion protection system module.

netshare: Specifies the netshare control module.

sandbox: Specifies the sandbox module.

traffic-policy: Specifies the bandwidth management module.

url-filter: Specifies the URL filtering module.

keepalive: Outputs keepalive logs to the log host.

lb: Outputs logs of a load balancing module to the log host. If you do not specify a load balancing module, this command outputs logs of all load balancing modules to the log host.

- **dns-proxy**: Specifies the transparent DNS proxy module.
- **gslb**: Specifies the global load balancing module.
- **inbound**: Specifies the inbound link load balancing module.
- **outbound**: Specifies the outbound link load balancing module.

packet-filter: Outputs packtet matching logs of the packet filter and security policy modules to the log host.

scd: Outputs logs of the server connection detection module to the log host.

security-policy: Outputs security policy configuration logs of the security policy module to the log host.

session: Outputs logs of the session management module to the log host.

telecom-sessionlog: Outputs NAT session logs in TELECOM format to the log host.

telecom-userlog: Outputs NAT444 user logs in TELECOM format to the log host.

unicom-sessionlog: Outputs NAT session logs in UNICOM format to the log host.

unicom-userlog: Outputs NAT444 user logs in UNICOM format to the log host.

Usage guidelines

The **customlog host** command takes effect only after the **customlog format** command is configured.

To output NAT logs to a log host, you must specify the log format required by the log host in the **customlog format** and **customlog host** commands.

Examples

Output logs of the session management module to the log host at 1.1.1.1.

```
<Sysname> system-view
[Sysname] customlog host 1.1.1.1 port 1000 export session
```

customlog host source

Use **customlog host source** to specify a source IP address for fast log output.

Use **undo customlog host source** to restore the default.

Syntax

customlog host source *interface-type interface-number*

undo customlog host source

Default

The source IP address of fast output logs is the primary IP address of the outgoing interface.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interface-type interface-number: Specifies a source interface by its type and number. The interface's primary IP address will be used as the source IP address of fast output logs.

Usage guidelines

Configure this command when you need to filter logs according to their source IP addresses on the log host.

The **customlog host source** command takes effect only after the **customlog format** and **customlog host** commands are configured.

Examples

Use the IP address of Loopback 0 as the source IP address of fast output logs.

```
<Sysname> system-view
[Sysname] interface loopback 0
```

```
[Sysname-LoopBack0] ip address 2.2.2.2 32
[Sysname-LoopBack0] quit
[Sysname] customlog host source loopback 0
```

customlog timestamp

Use **customlog timestamp localtime** to configure the timestamp of fast output logs to show the system time.

Use **undo customlog timestamp localtime** to restore the default.

Syntax

customlog timestamp localtime

undo customlog timestamp localtime

Default

The timestamp of fast output logs shows the Greenwich Mean Time (GMT).

Views

System view

Predefined user roles

network-admin

context-admin

Examples

Configure the timestamp of fast output logs to show the system time.

```
<Sysname> system-view
[Sysname] customlog timestamp localtime
```

customlog with-sn

Use **customlog with-sn** to configure the device to carry its serial number in fast output logs.

Use **undo customlog with-sn** to restore the default.

Syntax

customlog with-sn

undo customlog with-sn

Default

The device does not carry its serial number in fast output logs.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This feature enables a device to add a serial number (SN) field to fast output log messages, helping users to identify the devices that sent the log messages.

This feature is not applicable to fast output logs in TELECOM, CMCC, and UNICOM formats.

Examples

Configure the device to carry its serial number in fast output logs.

```
<Sysname> system-view
[Sysname] customlog with-sn
```

Contents

Session-based NetStream commands

display session-based netstream aggregation-cache

Use **display session-based netstream aggregation-cache** to display session-based NetStream statistics.

Syntax

display session-based netstream aggregation-cache { **app** | **app-profile** | **app-user** } *

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

app: Specifies the app aggregation mode.

app-profile: Specifies the app-profile aggregation mode.

app-user: Specifies the app-user aggregation mode.

Usage guidelines

To display session-based NetStream statistics in an aggregation mode, you must enable the aggregation mode by using the **session-based netstream aggregation** command.

Examples

Display statistics about session-based NetStream in app aggregation mode.

```
<Sysname> display session-based netstream aggregation-cache app
Active entries                                 :1
Timeout time for session-based NetStream entries :10
------------------------------------------------------------------------------
AppID      InPkts     InBytes    OutPkts    OutBytes
------------------------------------------------------------------------------
22742      4          240        4          240
Total   Sessions : 1
Current Sessions : 1
SubsCribers      : 1
```

Display statistics about session-based NetStream in app-profile aggregation mode.

```
<Sysname> display session-based netstream aggregation-cache app-profile
Active entries                                 :1
Timeout time for session-based NetStream entries :10
------------------------------------------------------------------------------
AppID      ProfileID  InPkts     InBytes    OutPkts    OutBytes
------------------------------------------------------------------------------
```

```
22742      0          4          240        4          240
Current Sessions : 1
New     Sessions : 0
```

Display statistics about session-based NetStream in app-user aggregation mode.

```
<Sysname> display session-based netstream aggregation-cache app-user
Active entries                                  :1
Timeout time for session-based NetStream entries :10
------------------------------------------------------------------------------
AppID      UserIp           InPkts     InBytes    OutPkts    OutBytes
------------------------------------------------------------------------------
22742      8.8.8.8          4          240        4          240
Total   Sessions : 1
Current Sessions : 1
```

Table 1 Command output

Field	Description
Active entries	Number of active session-based NetStream entries.
Timeout time for session-based NetStream entries	Maximum period of time in minutes a session-based NetStream entry can be cached before being exported to NetStream servers.
App ID	Application layer protocol ID.
UserIP	User IP address.
ProfileID	Traffic rule ID in bandwidth management.
InPkts	Number of upstream packets.
InBytes	Number of upstream bytes.
OutPkts	Number of downstream packets.
OutBytes	Number of downstream bytes.
Total sessions	Total number of sessions.
New sessions	Number of new sessions established in the current statistics collection interval.
Current sessions	Number of concurrent sessions at the time the **display session-based netstream aggregation-cache** command was executed.
SubsCribers	Total number of users in the current statistics collection interval.

Related commands

session-based netstream aggregation

session-based netstream aggregation

Use **session-based netstream aggregation** to enable session-based NetStream aggregation modes.

Use **undo session-based netstream aggregation** to disable session-based NetStream aggregation modes.

Syntax

session-based netstream aggregation { **app** | **app-profile** | **app-user** } *

undo session-based netstream aggregation { **app** | **app-profile** | **app-user** } *

Default

All session-based NetStream aggregation modes are disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

app: Specifies the app aggregation mode, which aggregates traffic by application layer protocol ID.

app-profile: Specifies the app-profile aggregation mode, which aggregates traffic by application layer protocol ID and profile ID.

app-user: Specifies the app-user aggregation mode, which aggregates traffic by application layer protocol ID and user IP address.

Examples

Enable the app aggregation mode for session-based NetStream aggregation.

```
<Sysname> system-view
[Sysname] session-based netstream aggregation app
```

Related commands

display session-based netstream aggregation-cache

session-based netstream enable

Use **session-based netstream enable** to enable session-based NetStream.

Use **undo session-based netstream enable** to disable session-based NetStream.

Syntax

session-based netstream enable

undo session-based netstream enable

Views

System view

Default

Session-based NetStream is disabled.

Predefined user roles

network-admin

context-admin

Examples

Enable session-based NetStream.

```
<Sysname> system-view
```

```
[Sysname] session-based netstream enable
```

session-based netstream export host

Use **session-based netstream export host** to specify a destination host for session-based NetStream data export.

Use **undo session-based netstream export host** to restore the default.

Syntax

session-based netstream export host *ip-address udp-port* [**vpn-instance** *vpn-instance-name*]

undo session-based netstream export host

Default

No destination host is specified for session-based NetStream data export.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the IP address of the destination host.

udp-port: Specifies the destination UDP port number in the range of 0 to 65535.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance to which the destination host belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the destination host is on the public network, do not specify this option.

Examples

Export session-based NetStream data to UDP port 9020 on host 172.16.1.1.

```
<Sysname> system-view
[Sysname] session-based netstream export host 172.16.1.1 9020
```

session-based netstream export source ip

Use **session-based netstream export source ip** to specify a source IP address for session-based NetStream packets.

Use **undo session-based netstream export source ip** to restore the default.

Syntax

session-based netstream export source ip *ip-address*

undo session-based netstream export source ip

Default

The source IP address of session-based NetStream packets is the primary IP address of the output interface.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies an IP address.

Examples

Specify 172.16.1.1 as the source IP address for session-based NetStream packets.

```
<Sysname> system-view
[Sysname] session-based netstream export source ip 172.16.1.1
```

session-based netstream timeout

Use **session-based netstream timeout** to set the aging timer for session-based NetStream entries.

Use **undo session-based netstream timeout** to restore the default.

Syntax

session-based netstream timeout *minutes*

undo session-based netstream timeout

Default

A session-based NetStream entry is automatically aged out and exported after being cached for 5 minutes.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

minutes: Sets the aging timer in minutes. The value range is 1 to 10.

Usage guidelines

When the aging timer for a session-based NetStream entry expires, statistics about the entry is cleared from the cache and exported to the NetStream servers.

Examples

Set the aging timer for session-based NetStream entries to 5 minutes.

```
<Sysname> system-view
[Sysname] session-based netstream timeout 10
```

Contents

Cloud connection commands

The following compatibility matrixes show the support of hardware platforms for cloud connections:

Model	Cloud connection compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	Yes
NFNX3-HDB680, NFNX3-HDB1080	No

cloud-management backup-server domain

Use **cloud-management backup-server domain** to specify a backup cloud server by its domain name.

Use **undo cloud-management backup-server domain** to remove one or all backup cloud servers.

Syntax

cloud-management backup-server domain *domain-name* [**vpn-instance** *vpn-instance-name*] [**source-ip** *ipv4-address*]

undo cloud-management backup-server domain [*domain-name*]

Default

No backup cloud server is specified.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

domain-name: Specifies a backup cloud server by its domain name, a case-sensitive string of 1 to 253 characters. If you do not specify this parameter in the **undo cloud-management backup-server domain** command, all backup cloud servers will be deleted.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the backup cloud server is on the public network.

source-ip *ipv4-address*: Specifies the source IPv4 address for the device that connects to the backup cloud server. It must be the same as the IPv4 address configured on the device. If you do not specify this option, the device uses the primary IPv4 address of the egress interface to connect to the backup cloud server.

Usage guidelines

Before configuring this command, make sure a DNS server is configured to translate domain names.

If you execute this command multiple times to configure a backup cloud server with the same domain name, the most recent configuration takes effect.

You can specify one primary server by using the **cloud-management server domain** command and a maximum of eight backup servers by repeating the **cloud-management backup-server domain** command.

When establishing a cloud connection, the device connects to one of the primary and backup servers according to the sequence in which they are specified. The first specified server has the highest priority. When the connected server fails, the device switches to another server and does not switch back to the original server even if the original server recovers.

To view the connected server, execute the **display cloud-management state** command.

Examples

Specify the server with domain name **123.com** as a backup cloud server.

```
<Sysname> system-view
[Sysname] cloud-management backup-server domain 123.com
```

Related commands

display cloud-management state

cloud-management keepalive

Use **cloud-management keepalive** to set the keepalive interval for the local device to send keepalive packets to the cloud server.

Use **undo cloud-management keepalive** to restore the default.

Syntax

cloud-management keepalive *interval*

undo cloud-management keepalive

Default

The keepalive interval is 180 seconds.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies the keepalive interval in the range of 10 to 600 seconds.

Usage guidelines

If the device does not receive a response from the cloud server within three keepalive intervals, the device sends a registration request to re-establish the cloud connection.

Examples

Set the keepalive interval to 360 seconds.

```
<Sysname> system-view
[Sysname] cloud-management keepalive 360
```

cloud-management ping

Use **cloud-management ping** to set the interval at which the local device sends ping packets to the cloud server.

Use **undo cloud-management ping** to restore the default.

Syntax

cloud-management ping *interval*

undo cloud-management ping

Default

The local device sends ping packets to the cloud server at intervals of 60 seconds.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies the interval at which the local device sends ping packets to the cloud server, in the range of 10 to 600 seconds.

Usage guidelines

After the connection to the cloud server is established, the local device sends ping packets to the server periodically to prevent NAT entry aging. Reduce the interval value if the network condition is poor or the NAT entry aging time is short.

The cloud server does not respond to ping packets.

Examples

Configure the local device to send ping packets to the cloud server at intervals of 120 seconds.

```
<Sysname> system-view
[Sysname] cloud-management ping 120
```

cloud-management server domain

Use **cloud-management server domain** to specify the primary cloud server by its domain name.

Use **undo cloud-management server domain** to restore the default.

Syntax

cloud-management server domain *domain-name* [**vpn-instance** *vpn-instance-name*] [**source-ip** *ipv4-address*]

undo cloud-management server domain

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

domain-name: Specifies the primary cloud server by its domain name, a case-sensitive string of 1 to 253 characters.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the primary cloud server is on the public network.

source-ip *ipv4-address*: Specifies the source IPv4 address for the device that connects to the primary cloud server. It must be the same as the IPv4 address configured on the device. If you do not specify this option, the device uses the primary IPv4 address of the egress interface to connect to the primary cloud server.

Usage guidelines

Before configuring this command, make sure a DNS server is configured to translate domain names.

If you execute the command multiple times, the most recent configuration takes effect.

Examples

Specify the server with domain name **lvzhouv3.**nsfocus.com.cn as the primary cloud server.

```
<Sysname> system-view
[Sysname] cloud-management server domain lvzhouv3.nsfocus.com.cn
```

Related commands

display cloud-management state

cloud-management server password

Use **cloud-management server password** to set the password for establishing cloud connections to the ADWAN server.

Use **cloud-management server password** to restore the default.

Syntax

cloud-management server password { **cipher** | **simple** } *string*

undo cloud-management server password

Default

No password is set for establishing cloud connections to the ADWAN server.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

cipher: Specifies the password in encrypted form.

simple: Specifies the password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. The plaintext form is a case-sensitive string of 1 to 63 characters. The encrypted form is a case-sensitive string of 1 to 117 characters.

Usage guidelines

After you change the password, the device terminates the cloud connections that have been established (if any) and uses the new password to establish cloud connections.

Examples

Set the password for establishing cloud connections to the ADWAN server to **12345678** in plaintext format.

```
<Sysname> system-view
[Sysname] cloud-management server password simple 12345678
```

cloud-management server port

Use **cloud-management server port** to specify the TCP port number used to establish cloud connections.

Use **undo cloud-management server port** to restore the default.

Syntax

cloud-management server port *port-number*

undo cloud-management server port

Default

TCP port number 19443 is used to establish cloud connections.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

port-number: Specifies a TCP port number in the range of 1 to 65535.

Usage guidelines

After you change the port number, the device terminates the cloud connections that have been established (if any) and uses the new port number to establish cloud connections.

Examples

Specify the TCP port number used to establish cloud connections as 80.

```
<Sysname> system-view
[Sysname] cloud-management server port 80
```

cloud-management unbinding-code

Use **cloud-management unbinding-code** to send the verification code for device unbinding to the cloud server.

Syntax

cloud-management unbinding-code *code*

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

code: Specifies the verification code obtained from the cloud server. The verification code is a case-sensitive string of 16 characters.

Usage guidelines

A device can be registered on the cloud server by only one user.

To register a device that has been registered by another user, you need to take the following steps:

1. Obtain a verification code for device unbinding from the cloud server.
2. Execute this command on the device to send the verification code to the cloud server.
3. Register the device on the cloud server.

Examples

Send the verification code for device unbinding to the cloud server.

```
[Sysname] cloud-management unbinding-code A6B9C3C2D5A8Z1S7
```

Related commands

`cloud-management server domain`

display cloud-management state

Use **`display cloud-management state`** to display cloud connection state information.

Syntax

`display cloud-management state`

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display cloud connection state information.

```
<Sysname> display cloud-management state
Cloud connection state                    : Established
Device state                              : Request_success
Cloud server address                      : 10.1.1.1
Cloud server domain name                  : ops.seccloud.nsfocus.com.cn
Cloud connection mode                     : Https
Cloud server port                         : 19443
Connected at                              : Wed Jan 27 14:18:40 2018
Duration                                  : 00d 00h 02m 01s
Process state                             : Message received
```

```
Failure reason                              : N/A
Last down reason                            : socket connection error (Details:N/A)
Last down at                                : Wed Jan 27 13:18:40 2018
Last report failure reason                  : N/A
Last report failure at                      : N/A
Dropped packets after reaching buffer limit : 0
Total dropped packets                       : 1
Last report incomplete reason               : N/A
Last report incomplete at                   : N/A
Buffer full count                           : 0
```

Table 1 Command output

Field	Description
Cloud connection state	Cloud connection state: **Unconnected**, **Request**, and **Established**.
Device state	Local device state: • **Idle**—In idle state. • **Connecting**—Connecting to the cloud server. • **Request_CAS_url**—Sent a central authentication service (CAS) URL request. • **Request_CAS_url_success**—Requesting CAS URL succeeded. • **Request_CAS_TGT**—Sent a ticket granting ticket (TGT) request. • **Request_CAS_TGT_success**—Requesting TGT succeeded. • **Request_CAS_ST**—Sent a service ticket (ST) request. • **Request_CAS_ST_success**—Requesting ST succeeded. • **Request_cloud_auth**—Sent an authentication request. • **Request_cloud_auth_success**—Authentication succeeded. • **Register**—Sent a registration request. • **Register_success**—Registration succeeded. • **Request**—Sent a handshake request. • **Request_success**—Handshake succeeded.
Cloud server address	IP address of the cloud server.
Cloud server domain name	Domain name of the cloud server.
Cloud server port	TCP port number used to establish cloud connections.
Connected at	Time when the cloud connection was established.
Duration	Duration since the establishment of the cloud connection.
Process state	Cloud connection processing state: • DNS not parsed. • DNS parsed. • Message not sent. • Message sent. • Message not received. • Message received.
Failure reason	Cloud connection failure reason: • DNS parse failed. • Socket connection failed. • SSL creation failed. • Sending CAS url request failed.

Field	Description
	• Sending CAS TGT failed. • Sending CAS ST failed. • Sending cloud auth failed. • Sending register failed. • Processing CAS url response failed. • Processing CAS TGT response failed. • Processing CAS ST response failed. • Processing cloud auth response failed. • Processing register response failed. • Sending handshake request failed. • Processing handshake failed. • Sending websocket request failed. • Processing websocket packet failed.
Last down reason	Reason for the most recent cloud connection interruption: • Device or process rebooted. • Socket connection error. • Configuration changed. • Received websocket close packet from cloud. • Keepalive expired. • Packet processing failed. • Main connection went down. • Cloud reset connection. • Memory reached threshold.
Last down at	Time when the cloud connection went down most recently.
Last report failure reason	Reason for the most recent cloud connection packet sending failure: • Tunnel is being deleted. • Tunnel socket is invalid. • Failed to convert string to json. • Failed to convert json to string. • Failed to create message node. • Tunnel is not ready. • Failed to create packet buffer. • SSL sending failure. If the reason is SSL sending failure, one of the following detailed reason will be displayed: • ssl error none. • ssl error ssl. • ssl error read. • ssl error write. • ssl error x509 lookup. • ssl error syscall. • ssl error zero return. • ssl error connect. • ssl error accept.
Last report failure at	Time when the most recent cloud connection packet sending failure occurred.
Dropped packets after reaching buffer limit	Number of packets that are dropped because the CMTNL buffer limit is reached.
Total dropped packets	Total number of dropped packets.

Field	Description
Last report incomplete reason	Reason for the most recent unfinished packet sending: • Interrupted system call. • Socket buffer is full.
Last report incomplete at	Time when the most recent unfinished packet sending occurred.
Buffer full count	Number of times that the buffer becomes full.

Contents

Port mirroring commands

The following compatibility matrixes show the support of hardware platforms for port mirroring:

Models	Feature compatibility
NFNX5-HD6480	Yes only on GE 1/0/0 through GE 1/0/13, XGE 1/0/18, XGE 1/0/19, GE 1/0/22 through GE 1/0/29, and interfaces on cards in four interface card slots
NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280	Yes only on GE 1/0/0 through GE 1/0/23, XGE 1/0/24, and XGE 1/0/25
NFNX3-HDB1780, NFNX3-HDB3080	Yes only on GE 1/0/0 through GE1/0/23, GE 1/0/25, XGE 1/0/26, and XGE 1/0/27
NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	No

display mirroring-group

Use **`display mirroring-group`** to display mirroring group information.

Syntax

`display mirroring-group` { *`group-id`* | **`all`** | **`local`** }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

`group-id`: Specifies a mirroring group by its ID.

The following compatibility matrixes show the value ranges for the mirroring group ID:

Models	Value range
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB680, NFNX3-HDB1080	1 and 2
NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	1

`all`: Specifies all mirroring groups.

`local`: Specifies local mirroring groups.

Usage guidelines

Mirroring group information includes the type, status, and content of a mirroring group. It is sorted by mirroring group number.

Examples

Display information about all mirroring groups.

```
<Sysname> display mirroring-group all
Mirroring group 1:
    Type: Local
    Status: Active
    Mirroring port:
        GigabitEthernet1/0/1  Inbound
    Monitor port: GigabitEthernet1/0/2
```

Table 1 Command output

Field	Description
Mirroring group	ID of the mirroring group.
Type	Type of the mirroring group: Local.
Status	Status of the mirroring group: • **Active**—The mirroring group has taken effect. • **Incomplete**—The mirroring group configuration is not complete and does not take effect.
Mirroring port	Source port.
Monitor port	Destination port.

mirroring-group

Use **mirroring-group** to create a mirroring group.

Use **undo mirroring-group** to delete mirroring groups.

Syntax

mirroring-group *group-id* **local**

undo mirroring-group { *group-id* | **all** | **local** }

Default

No mirroring groups exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

group-id: Specifies a mirroring group ID.

The following compatibility matrixes show the value ranges for the mirroring group ID:

Models	Value range
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280,	1 and 2

Models	Value range
NFNX5-HD5280, NFNX3-HDB680, NFNX3-HDB1080	
NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	1

`local`: Specifies local mirroring groups.

`all`: Specifies all mirroring groups.

Examples

Create local mirroring group 1.

```
<Sysname> system-view
[Sysname] mirroring-group 1 local
```

mirroring-group mirroring-port (interface view)

Use **`mirroring-group mirroring-port`** to configure a port as a source port for a mirroring group.

Use **`undo mirroring-group mirroring-port`** to restore the default.

Syntax

`mirroring-group` *`group-id`* **`mirroring-port`** { **`both`** | **`inbound`** | **`outbound`** }

`undo mirroring-group` *`group-id`* **`mirroring-port`**

Default

A port does not act as a source port for any mirroring groups.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

`group-id`: Specifies a mirroring group by its ID.

The following compatibility matrixes show the value ranges for the mirroring group ID:

Models	Value range
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB680, NFNX3-HDB1080	1 and 2
NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	1

`both`: Mirrors both received and sent packets.

`inbound`: Mirrors only received packets.

`outbound`: Mirrors only sent packets.

Usage guidelines

A Layer 2 or Layer 3 aggregate interface cannot be configured as a source port for a mirroring group.

A source port cannot be used as a monitor port.

Examples

Create local mirroring group 1 to monitor the bidirectional traffic of port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] mirroring-group 1 local
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mirroring-group 1 mirroring-port both
```

Related commands

mirroring-group

mirroring-group mirroring-port (system view)

Use **mirroring-group mirroring-port** to configure source ports for a mirroring group.

Use **undo mirroring-group mirroring-port** to remove source ports from a mirroring group.

Syntax

mirroring-group *group-id* **mirroring-port** *interface-list* { **both** | **inbound** | **outbound** }

undo mirroring-group *group-id* **mirroring-port** *interface-list*

Default

No source port is configured for a mirroring group.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

group-id: Specifies a mirroring group by its ID.

The following compatibility matrixes show the value ranges for the mirroring group ID:

Models	Value range
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB680, NFNX3-HDB1080	1 and 2
NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	1

interface-list: Specifies a space-separated list of up to eight interface items. Each item specifies an interface by its type and number or specifies a range of interfaces in the form of *interface-type interface-number1* **to** *interface-type interface-number2*.

When you specify a range of interfaces, the interfaces must be of the same type and on the same slot. The start interface number must be identical to or lower than the end interface number.

both: Mirrors both received and sent packets.

inbound: Mirrors only received packets.

outbound: Mirrors only sent packets.

Usage guidelines

A Layer 2 or Layer 3 aggregate interface cannot be configured as a source port for a mirroring group.

A source port cannot be used as a monitor port.

Examples

Create local mirroring group 1 to monitor the bidirectional traffic of GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] mirroring-group 1 local
[Sysname] mirroring-group 1 mirroring-port gigabitethernet 1/0/1 both
```

Related commands

mirroring-group

mirroring-group monitor-port (interface view)

Use **mirroring-group monitor-port** to configure a port as the monitor port for a mirroring group.

Use **undo mirroring-group monitor-port** to restore the default.

Syntax

mirroring-group *group-id* **monitor-port**

undo mirroring-group *group-id* **monitor-port**

Default

A port does not act as the monitor port for any mirroring groups.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

group-id: Specifies a mirroring group by its ID.

The following compatibility matrixes show the value ranges for the mirroring group ID:

Models	Value range
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB680, NFNX3-HDB1080	1 and 2
NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	1

Usage guidelines

Do not enable the spanning tree feature on the monitor port of a mirroring group.

A Layer 2 or Layer 3 aggregate interface cannot be configured as the monitor port for a mirroring group.

Use a monitor port only for port mirroring, so the data monitoring device receives and analyzes only the mirrored traffic.

The member port of an existing mirroring group cannot be configured as a monitor port.

Examples

Create local mirroring group 1 and configure GigabitEthernet 1/0/1 as its monitor port.

```
<Sysname> system-view
[Sysname] mirroring-group 1 local
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mirroring-group 1 monitor-port
```

Related commands

mirroring-group

mirroring-group monitor-port (system view)

Use **mirroring-group monitor-port** to configure the monitor ports for a mirroring group.

Use **undo mirroring-group monitor-port** to remove the monitor ports from a mirroring group.

Syntax

mirroring-group *group-id* **monitor-port** *interface-type interface-number*

undo mirroring-group *group-id* **monitor-port** *interface-type interface-number*

Default

No monitor port is configured for a mirroring group.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

group-id: Specifies a mirroring group by its ID.

The following compatibility matrixes show the value ranges for the mirroring group ID:

Models	Value range
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB680, NFNX3-HDB1080	1 and 2
NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	1

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

Do not enable the spanning tree feature on the monitor port of a mirroring group.

Use a monitor port only for port mirroring, so the data monitoring device receives only the mirrored traffic.

The member port of an existing mirroring group cannot be configured as a monitor port.

Examples

Create local mirroring group 1 and configure GigabitEthernet 1/0/1 as its monitor port.

```
<Sysname> system-view
[Sysname] mirroring-group 1 local
[Sysname] mirroring-group 1 monitor-port gigabitethernet 1/0/1
```

Related commands

mirroring-group

Contents

Packet capture commands

display packet-capture status

Use **display packet-capture status** to display packet capture settings and status information.

Syntax

display packet-capture status

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display packet capture settings and status information.

```
<Sysname> display packet-capture status
  Capture status: Started
  Filter: ACL 3000
          Interface GigabitEthernet 1/0/1
```

Table 1 Command output

Field	Description
Capture status	Packet capture status: • **Started**—Packet capture is started. • **Stopped**—Packet capture is stopped. • **Saving**—The device is saving captured packets to a file.
Filter	Filtering settings: • **ACL**—Captures packets permitted by an advanced ACL. • **ACL IPv6**—Captures packets permitted by an IPv6 advanced ACL. • **Interface**—Captures packets received or sent by an interface. If packet capture is not started, the command does not display this field.

Related commands

packet-capture start

packet-capture stop

packet-capture max-bytes

Use **packet-capture max-bytes** to set the maximum packet size for a packet capture record.

Use **undo packet-capture max-bytes** to restore the default.

Syntax

packet-capture max-bytes *bytes*

undo packet-capture max-bytes

Default

The maximum packet size is 1600 bytes for a packet capture record.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

bytes: Specifies the maximum packet size for a packet capture record in bytes. The value range is 512 to 4096.

Usage guidelines

The device captures only the specified maximum number of bytes from a packet. The remaining part of the packet is ignored. To capture all bytes of packets, make sure the maximum packet size for a packet capture record is equal to or greater than the interface MTU.

You can configure packet capture parameters only when packet capture is not started.

Examples

Set the maximum packet size to 1500 bytes for a packet capture record.

```
<Sysname> system-view
[Sysname] packet-capture max-bytes 1500
```

packet-capture max-file-packets

Use **packet-capture max-file-packets** to set the maximum number of packet capture records for a file.

Use **undo packet-capture max-file-packets** to restore the default.

Syntax

packet-capture max-file-packets *number*

undo packet-capture max-file-packets

Default

The maximum number of packet capture records for a file is 100.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

number: Specifies the maximum number of packet capture records for a file. The value range is 100 to 1000.

Usage guidelines

The system first saves packet capture records to memory. After the maximum number of packet capture records for a file is reached, the system saves the records to a file and clears the records in memory.

A greater value for this argument requires more memory space. If the available memory space is limited, decrease the value.

You can configure packet capture parameters only when packet capture is not started.

Examples

Set the maximum number of packet capture records for a file to 500.

```
<Sysname> system-view
[Sysname] packet-capture max-file-packets 500
```

packet-capture start

Use **packet-capture start** to start packet capture.

Syntax

packet-capture start [**acl** { *acl-number* | **ipv6** *acl-number* } | **interface** *interface-type interface-number*] *

Default

Packet capture is not started.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

acl: Captures packets permitted by an advanced ACL.

acl-number: Specifies an IPv4 advanced ACL by its number in the range of 3000 to 3900.

ipv6 *acl-number*: Specifies an IPv6 advanced ACL by its number in the range of 3000 to 3900.

interface *interface-type interface-number*: Captures packets received or sent by an interface.

Usage guidelines

Start packet capture only when necessary. Packet capture affects device performance.

To save .cap files on the device, back up existing .cap files on the device before starting packet capture. The system automatically deletes existing .cap files in the same .cap file directory after you start packet capture.

If you do not specify any options, the device captures all received and sent packets.

On a non-default context, you cannot start packet capture on a shared interface.

Examples

Start packet capture. Use ACL 3000 to identify the packets to be captured.

```
<Sysname> system-view
[Sysname] packet-capture start acl 3000
```

```
The operation will delete .cap files in storage path,continue?[y/n]
```

packet-capture stop

Use **packet-capture stop** to stop packet capture.

Syntax

packet-capture stop [**immediately**]

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

immediately: Stops packet capture and captured-packet saving. If you do not specify this keyword, the device saves captured packets to a file before stopping packet capture.

Usage guidelines

Saving packet capture records to a file takes time. The **packet-capture stop** command without the **immediately** keyword saves all packet capture records to a file before stopping packet capture. If you do not want to use the packet capture records in memory, execute the **packet-capture stop immediately** command.

Examples

Stop packet capture.

```
<Sysname> system-view
[Sysname] packet-capture stop
```

Stop packet capture immediately.

```
<Sysname> system-view
[Sysname] packet-capture stop immediately
```

packet-capture storage

Use **packet-capture storage** to specify the storage directory for the .cap files.

Use **undo packet-capture storage** to restore the default.

Syntax

packet-capture storage { **local** [**limit** *limit-space*] | **remote** *serverpath* [**vpn-instance** *vpn-instance-name*] [**user** *username* [**password** { **cipher** | **simple** } *string*]] }

undo packet-capture storage

Default

The storage directory is the **pcap** directory of the default file system on the master.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

local: Saves the .cap files on the device.

limit *limit-space*: Specifies the maximum storage space for .cap files in KB. The value range is 1024 to 10240. The default is 4096. After the maximum storage space is reached, the system stops capturing packets.

remote: Saves the .cap files to a remote file server.

serverpath: Specifies a directory on an FTP or TFTP server, a case-sensitive string of up to 253 characters. Valid characters include letters, digits, hyphens (-), underscores (_), colons (:), forward slashes (/), and dots (.).

vpn-instance *vpn-instance-name*: Specifies the VPN instance to which the FTP or TFTP server belongs. The *vpn-instance-name* argument specifies the VPN instance name, a case-sensitive string of 1 to 31 characters. If the FTP or TFTP server belongs to the public network, do not specify this option.

user *username*: Specifies the username used to access the FTP server, a case-sensitive string of up to 255 characters. It cannot contain forward slashes (/), backward slashes (\), vertical bars (|), colons (:), asterisks (*), question marks (?), left angle brackets (<), right angle brackets (>), or at signs (@). This option is required if an FTP server is used to save the .cap files.

password: Specifies the password used to access the FTP server.

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password string, case sensitive. A password in encrypted form can have up to 255 characters. A password in plaintext form can have up to 373 characters.

Usage guidelines

The storage space of the storage media on the device is limited. As a best practice, use a remote file server to save the .cap files.

You can configure packet capture parameters only when packet capture is not started.

Examples

Set the storage directory for the .cap files to **ftp://1.1.1.2**. Specify the username and password for accessing the FTP server

```
<Sysname> system-view
[Sysname] packet-capture storage remote ftp://1.1.1.2 user user123 password simple 123
```

Contents

NQA commands

NQA client commands

advantage-factor

Use **advantage-factor** to set the advantage factor to be used for calculating Mean Opinion Scores (MOS) and Calculated Planning Impairment Factor (ICPIF) values.

Use **undo advantage-factor** to restore the default.

Syntax

advantage-factor *factor*

undo advantage-factor

Default

The advantage factor is 0.

Views

Voice operation view

Predefined user roles

network-admin

context-admin

Parameters

factor: Specifies the advantage factor in the range of 0 to 20.

Usage guidelines

The evaluation of voice quality depends on users' tolerance for voice quality. For users with higher tolerance for voice quality, use the **advantage-factor** command to set an advantage factor. When the system calculates the ICPIF value, it subtracts the advantage factor to modify ICPIF and MOS values for voice quality evaluation.

Examples

Set the advantage factor to 10 for the voice operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type voice
[Sysname-nqa-admin-test-voice] advantage-factor 10
```

agent-type

Use **agent-type** to specify the SNMP agent type for the SNMP DCA operation.

Use **undo agent-type** to restore the default.

Syntax

agent-type { **net-snmp** | **user-defined** | **windows** }

undo agent-type

Default

The default SNMP agent type is Net-SNMP.

Views

SNMP DCA template view

Predefined user roles

network-admin

context-admin

Parameters

net-snmp: Specifies the Net-SNMP agent type.

user-defined: Specifies the user-defined agent type.

windows: Specifies the Windows agent type.

Usage guidelines

The SNMP DCA operation monitors the performance of a device running an SNMP agent. It collects the CPU, memory, and disk usage from the SNMP agent and determines the device performance based on the collected object values and their associated thresholds and weights.

Different SNMP agent types use different OIDs for the CPU, memory, and disk usage objects. Make sure the SNMP agent type specified in the SNMP DCA template matches the type of the SNMP agent to be monitored.

For Net-SNMP or Windows SNMP agents, the NQA client has built-in OIDs to collect the CPU, memory, and disk usage objects. You can use the **cpu**, **memory**, and **disk** commands to set the thresholds and weights for these objects. You can also use the **oid** command to configure custom SNMP objects.

For SNMP agents of the user-defined type, the NQA client does not have predefined SNMP objects to collect. You must use the **oid** command to configure the interested SNMP objects and their associated thresholds and weights.

Examples

Set the SNMP agent type to Windows for SNMP DCA template **test**.

```
<Sysname> system-view
[Sysname] nqa template snmpdca test
[Sysname-nqatplt-snmpdca-test] agent-type windows
```

Related commands

cpu

disk

memory

oid

codec-type

Use **codec-type** to configure the codec type for the voice operation.

Use **undo codec-type** to restore the default.

Syntax

codec-type { **g711a** | **g711u** | **g729a** }

undo codec-type

Default

The codec type for the voice operation is G.711 A-law.

Views

Voice operation view

Predefined user roles

network-admin

context-admin

Parameters

g711a: Specifies G.711 A-law codec type.

g711u: Specifies G.711 μ-law codec type

g729a: Specifies G.729 A-law codec type.

Examples

Set the codec type to **g729a** for the voice operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type voice
[Sysname-nqa-admin-test-voice] codec-type g729a
```

community read

Use **community read** to specify the community name for the SNMP operation.

Use **undo community read** to restore the default.

Syntax

community read { **cipher** | **simple** } *community-name*

undo community read

Default

The SNMP operation uses the community name **public**.

Views

SNMP operation view

SNMP template view

SNMP DCA template view

Predefined user roles

network-admin

context-admin

Parameters

cipher: Specifies a community name in encrypted form.

simple: Specifies a community name in plaintext form. For security purposes, the community name specified in plaintext form will be stored in encrypted form.

community-name: Specifies the community name. Its plaintext form is a case-sensitive string of 1 to 32 characters. Its encrypted form is a case-sensitive string of 33 to 73 characters.

Usage guidelines

You must specify the community name for the SNMP operation when both of the following conditions exist:

- The SNMP operation uses the SNMPv1 or SNMPv2c agent.
- The SNMPv1 or SNMPv2c agent is configured with a read-only or read-write community name.

The specified community name must be the same as the community name configured on the SNMP agent.

The community name configuration is not required if the SNMP operation uses the SNMPv3 agent.

For more information about SNMP, see "Configuring SNMP."

Examples

Specify **readaccess** as the community name for the SNMP operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type snmp
[Sysname-nqa-admin-test-snmp] community read simple readaccess
```

cpu

Use **cpu** to specify the threshold and weight for the CPU usage object.

Use **undo cpu** to restore the default.

Syntax

cpu { **threshold** *threshold-value* | **weight** *weight-value* } *

undo cpu

Default

The CPU usage threshold is 80 and the weight is 3.

Views

SNMP DCA template view

Predefined user roles

network-admin

context-admin

Parameters

threshold *threshold-value*: Specifies the CPU usage threshold in the range of 0 to 100. A threshold of 0 means that CPU usage is not used as a metric for measuring the SNMP agent performance.

weight *weight-value*: Specifies the weight of the CPU usage object. The value range is 0 to 100. A weight of 0 means that CPU usage is not used as a metric for measuring the SNMP agent performance.

Usage guidelines

This command takes effect only on SNMP agents of the Net-SNMP or Windows agent type.

The NQA client automatically obtains the CPU usage from the SNMP agent of the Net-SNMP or Windows type in the SNMP DCA operation.

Examples

Set both the threshold and weight of the CPU usage object to 90.

```
<Sysname> system-view
[Sysname] nqa template snmpdca test
[Sysname-nqatplt-snmpdca-test] cpu threshold 90 weight 90
```

Related commands

agent-type

data-fill

Use **data-fill** to configure the payload fill string for probe packets.

Use **undo data-fill** to restore the default.

Syntax

data-fill *string* [**raw**]

undo data-fill

Default

The default payload fill string is the hexadecimal string 00010203040506070809.

Views

ICMP/UDP echo operation view

Path jitter/UDP jitter/voice operation view

ICMP/TCP/UDP template view

TWAMP Light client-session view

Predefined user roles

network-admin

context-admin

Parameters

string: Specifies a case-sensitive string of 1 to 200 characters.

raw: Fills the packet payload with the specified payload fill string without truncation or repetition to fit the payload size. This keyword is available only in UDP template view.

Usage guidelines

How the string is filled depends on the operation type.

- For the ICMP echo operation, the string fills the whole payload of an ICMP echo request.
- For the UDP echo operation, the first five bytes in the payload of a UDP packet are for special purpose. The string fills the remaining part of payload.
- For the UDP jitter operation, the first 68 bytes in the payload of a UDP packet are for special purpose. The string fills the remaining part of the payload.
- For the voice operation, the first 16 bytes in the payload of a UDP packet are for special purpose. The string fills the remaining part of the payload.
- For the path jitter operation, the first four bytes in the payload of an ICMP echo request are for special purpose. The string fills the remaining part of payload.

With the **raw** keyword specified, the payload fill string will be used exactly as specified to fill the packet payload.

Without the **raw** keyword, the payload fill string will be truncated at the end or cyclically repeated to fit the payload size of the probe packet.

For example, if you configure the payload fill string as **abcd**:

- Probe packet with a payload size of 3 bytes will be filled with **abc**.
- Probe packet with a payload size of 6 bytes will be filled with **adcdab**.

In UDP template view, the probe packets without the **raw** keyword specified contain special characters. For a destination device other than an NSFOCUS device, provide the **raw** keyword because it can identify only probe packets without any special characters contained. Make sure the payload fill string specified on the client can be identified by the destination device.

If the destination device is an NSFOCUS device, the **raw** keyword is not a must because the NSFOCUS device can identify the probe packets that contain special characters. As a best practice, do not specify the **raw** keyword.

Examples

Specify **abcd** as the payload fill string for ICMP echo requests.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] data-fill abcd
```

In TCP template view, specify **abcd** as the payload fill string for probe packets.

```
<Sysname> system-view
[Sysname] nqa template tcp tcptplt
[Sysname-nqatplt-tcp-tcptplt] data-fill abcd
```

data-size

Use **data-size** to set the payload size for each probe packet.

Use **undo data-size** to restore the default.

Syntax

data-size *size*

undo data-size

Default

The default payload size of a probe packet for different operations is described in Table 1.

Table 1 Default payload size of a probe packet

Operation type	Codec type	Default size (bytes)
ICMP echo	N/A	100
UDP echo	N/A	100
UDP jitter	N/A	100
UDP tracert	N/A	100
Path jitter	N/A	100
Voice	G.711 A-law	172
Voice	G.711 μ-law	172
Voice	G.729 A-law	32

Operation type	Codec type	Default size (bytes)
TWAMP Light	N/A	142

Views

ICMP/UDP echo operation view

UDP tracert operation view

Path jitter/UDP jitter/voice operation view

ICMP/UDP template view

TWAMP Light client-session view

Predefined user roles

network-admin

context-admin

Parameters

size: Specifies the payload size in bytes. The value range for the *size* argument varies by operation type.

- For the ICMP echo, UDP echo, or UDP tracert operation, the value range is 20 to 65507.
- For the UDP jitter or path jitter operation, the value range is 68 to 65507.
- For the voice operation, the value range is 16 to 65507.
- 44 to 1518 for TWAMP Light tests.

Usage guidelines

In ICMP echo and path jitter operations, the command sets the payload size for each ICMP echo request.

In UDP echo, UDP jitter, UDP tracert, and voice operations, the command sets the payload size for each UDP packet.

In TWAMP Light tests, the payload size cannot be larger than the MTU size of any interface on the test link.

Examples

Set the payload size to 80 bytes for each ICMP echo request.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] data-size 80
```

In ICMP template view, set the payload size to 80 bytes for each probe packet.

```
<Sysname> system-view
[Sysname] nqa template icmp icmptplt
[Sysname-nqatplt-icmp-icmptplt] data-size 80
```

description

Use **description** to configure a description for an NQA operation, such as the operation type or purpose.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

No description is configured for an NQA operation.

Views

ICMP echo/UDP echo/TCP operation view

ARP/DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP tracert operation view

ICMP jitter/UDP jitter/path jitter/voice operation view

TWAMP Light client-session view

Any NQA template view

Predefined user roles

network-admin

context-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 200 characters.

Examples

Configure the description as **icmp-probe** for the ICMP echo operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] description icmp-probe
```

In ICMP template view, configure the description as **icmp-probe** for the NQA operation.

```
<Sysname> system-view
[Sysname] nqa template icmp icmptplt
[Sysname-nqatplt-icmp-icmptplt] description icmp-probe
```

destination ip

Use **destination ip** to configure the destination IPv4 address for the operation.

Use **undo destination ip** to restore the default.

Syntax

destination ip *ip-address*

undo destination ip

Default

No destination IPv4 address is configured for an operation.

Views

ICMP echo/TCP/UDP echo operation view

ARP/DHCP/DLSw/DNS/SNMP operation view

UDP tracert operation view

ICMP jitter/path jitter/UDP jitter/voice operation view

ARP/DNS/ICMP/IMAP/POP3/RADIUS authentication/RADIUS accounting/SMTP/SNMP/SNMP DCA/SSL/TCP/TCP half open/UDP/WAP template view

TWAMP Light client-session view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the destination IPv4 address for the operation.

Examples

Specify 10.1.1.1 as the destination IPv4 address for the ICMP echo operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] destination ip 10.1.1.1
```

In ICMP template view, specify 10.1.1.1 as the destination IPv4 address for the ICMP echo operation.

```
<Sysname> system-view
[Sysname] nqa template icmp icmptplt
[Sysname-nqatplt-icmp-icmptplt] destination ip 10.1.1.1
```

destination ipv6

Use **destination ipv6** to configure the destination IPv6 address for the operation.

Use **undo destination ipv6** to restore the default.

Syntax

destination ipv6 *ipv6-address*

undo destination ipv6

Default

No destination IPv6 address is configured for an operation.

Views

ICMP echo/TCP/UDP echo/UDP jitter operation view

DNS/ICMP/IMAP/POP3/RADIUS authentication/RADIUS accounting/SMTP/SIP/SNMP/SNMP DCA/SSL/TCP/TCP half open/UDP/WAP template view

TWAMP Light client-session view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address: Specifies the destination IPv6 address for the operation. IPv6 link-local addresses are not supported.

Examples

Specify 1::1 as the destination IPv6 address for the ICMP echo operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] destination ipv6 1::1
```

In ICMP template view, specify 1::1 as the destination IPv6 address for the operation.

```
<Sysname> system-view
[Sysname] nqa template icmp icmptplt
[Sysname-nqatplt-icmp-icmptplt] destination ipv6 1::1
```

destination mac

Use **destination mac** to specify the destination MAC address for the operation.

Use **undo destination mac** to restore the default.

Syntax

destination mac *mac-address*

undo destination mac

Default

No destination MAC address is specified.

Views

TWAMP Light client-session view

Predefined user roles

network-admin

context-admin

Parameters

mac-address: Specifies the destination MAC address in the format of H-H-H. For example, to use 000f-00e2-0001 as the destination MAC address, set this argument to f-e2-1.

Usage guidelines

In TWAMP Light client-session view, specify 0001-0002-0003 as the destination MAC address for the TWAMP Light test.

```
<Sysname> system-view
[Sysname] nqa twamp-light client
[Sysname-nqa-twamp-light-client] test-session 1
[Sysname-nqa-twamp-light-client-session1] destination mac 1-2-3
```

destination port

Use **destination port** to configure the destination port number for the operation.

Use **undo destination port** to restore the default.

Syntax

destination port *port-number*

undo destination port

Default

The destination port numbers for NQA operations are as follows:

- 33434 for the UDP tracert operation.
- 161 for the SNMP operation.

No destination port number is configured for other types of operations.

The destination port numbers for NQA templates are as follows:

- 53 for the DNS template.
- 143 for the IMAP template.
- 110 for the POP3 template.
- 1812 for the RADIUS authentication template.
- 1813 for the RADIUS accounting template.
- 5060 for the SIP template.
- 25 for the SMTP template.
- 161 for the SNMP template.
- 161 for the SNMP DCA template.
- 9201 for the WAP template.

No destination port number is configured for other types of NQA templates.

Views

TCP/UDP echo operation view

SNMP operation view

UDP tracert operation view

UDP jitter/voice operation view

DNS/IMAP/POP3/RADIUS authentication/RADIUS accounting/SIP/SMTP/SNMP/SNMP DCA/SSL/TCP/TCP half open /UDP/WAP template view

TWAMP Light client-session view

Predefined user roles

network-admin

context-admin

Parameters

port-number: Specifies the destination port number for the operation, in the range of 1 to 65535.

Usage guidelines

For a TCP half open template, this command is required only if the **port-detect enable** command is configured.

Examples

Set the destination port number to 9000 for the UDP echo operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-echo
[Sysname-nqa-admin-test-udp-echo] destination port 9000
```

In TCP template view, set the destination port number to 9000 for the NQA operation.

```
<Sysname> system-view
```

```
[Sysname] nqa template tcp tcptplt
[Sysname-nqatplt-tcp-tcptplt] destination port 9000
```

Related commands

port-detect enable

disconnect-mode

Use **disconnect-mode** to set a TCP connection termination mode.

Use **undo disconnect-mode** to restore the default.

Syntax

disconnect-mode { **fin** | **rst** }

undo disconnect-mode

Default

The TCP operation uses the RST mode to terminate TCP connections.

Views

TCP template view

Predefined user roles

network-admin

context-admin

Parameters

fin: Sets the FIN mode for TCP connection termination.

rst: Sets the RST mode for TCP connection termination.

Usage guidelines

A TCP operation includes two processes: establishing a TCP connection through the three-way handshake and terminating the TCP connection. When both processes complete, the TCP operation succeeds.

You can use the command to set the connection termination mode for the TCP operation:

- **RST mode**—The server terminates the TCP connection after receiving the RST request from the client.
- **FIN mode**—The server terminates the TCP connection after the four-way handshake between the client and the server.

  Use the FIN mode when the RST mode is not supported on the client.

Examples

In TCP template view, set the FIN mode for TCP connection termination.

```
<Sysname> system-view
[Sysname] nqa template tcp test
[Sysname-nqatplt-tcp-test] disconnect-mode fin
```

disk

Use **disk** to specify the threshold and weight for the disk usage object.

Use **undo disk** to restore the default.

Syntax

disk { **threshold** *threshold-value* | **weight** *weight-value* } *

undo disk

Default

The disk usage threshold is 90 and the weight is 4.

Views

SNMP DCA template view

Predefined user roles

network-admin

context-admin

Parameters

threshold *threshold-value*: Specifies the disk usage threshold in the range of 0 to 100. A threshold of 0 means that disk usage is not used as a metric for measuring the SNMP agent performance.

weight *weight-value*: Specifies the weight of the disk usage object in the range of 0 to 100. A weight of 0 means that disk usage is not used as a metric for measuring the SNMP agent performance.

Usage guidelines

This command takes effect only on SNMP agents of the Net-SNMP or Windows agent type.

The NQA client automatically obtains the disk usage from the SNMP agent of the Net-SNMP or Windows type in the SNMP DCA operation.

Examples

Set both the threshold and weight of the disk usage object to 90.

```
<Sysname> system-view
[Sysname] nqa template snmpdca test
[Sysname-nqatplt-snmpdca-test] disk threshold 90 weight 90
```

Related commands

agent-type

display nqa history

Use **display nqa history** to display the history records of NQA operations.

Syntax

display nqa history [*admin-name operation-tag*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

admin-name operation-tag: Specifies an NQA operation by its administrator name and operation tag. The *admin-name* argument represents the name of the administrator who creates the NQA operation. The *operation-tag* argument represents the operation tag. Each of the arguments is a case-insensitive string of 1 to 32 characters that cannot contain hyphens (-). If you do not specify an NQA operation, the command displays the history records of all NQA operations.

Usage guidelines

The **display nqa history** command does not display the results or statistics of the following operations:

- ICMP jitter.
- Path jitter.
- UDP jitter.
- Voice.

To view the results or statistics of the ICMP jitter, path jitter, UDP jitter, and voice operations, use the **display nqa result** or **display nqa statistics** command.

Examples

Display the history records of the UDP tracert operation with administrator name **administrator** and operation tag **tracert**.

```
<Sysname> display nqa history administrator tracert
NQA entry (admin administrator, tag tracert) history records:
Index      TTL  Response  Hop IP          Status          Time
1          2    328       4.1.1.1         Succeeded       2013-09-09 14:46:06.2
1          2    328       4.1.1.1         Succeeded       2013-09-09 14:46:05.2
1          2    328       4.1.1.1         Succeeded       2013-09-09 14:46:04.2
1          1    328       3.1.1.2         Succeeded       2013-09-09 14:46:03.2
1          1    328       3.1.1.1         Succeeded       2013-09-09 14:46:02.2
1          1    328       3.1.1.1         Succeeded       2013-09-09 14:46:01.2
```

Display the history records of the NQA operation with administrator name **administrator** and operation tag **test**.

```
<Sysname> display nqa history administrator test
NQA entry (admin administrator, tag test) history records:
  Index      Response     Status           Time
  10         329          Succeeded        2011-04-29 20:54:26.5
  9          344          Succeeded        2011-04-29 20:54:26.2
  8          328          Succeeded        2011-04-29 20:54:25.8
  7          328          Succeeded        2011-04-29 20:54:25.5
  6          328          Succeeded        2011-04-29 20:54:25.1
  5          328          Succeeded        2011-04-29 20:54:24.8
  4          328          Succeeded        2011-04-29 20:54:24.5
  3          328          Succeeded        2011-04-29 20:54:24.1
  2          328          Succeeded        2011-04-29 20:54:23.8
  1          328          Succeeded        2011-04-29 20:54:23.4
```

Table 2 Command output

Field	Description
Index	History record ID. The history records in one UDP tracert operation have the same ID.
TTL	If the routing table bypass feature is not enabled in the operation, this field displays the TTL value in the probe packet. If the routing table bypass feature is enabled, the value of this field varies by the **init-ttl** command. However, the actual TTL value in the probe packet is fixed at 1.
Response	Round-trip time if the operation succeeds, timeout time upon timeout, or 0 if the operation cannot be completed, in milliseconds.
Hop IP	IP address of the node that sent the reply packet.
Status	Status of the operation result: • Succeeded. • Unknown error. • Internal error. • Timeout.
Time	Time when the operation was completed.

display nqa reaction counters

Use **display nqa reaction counters** to display the current monitoring results of reaction entries.

Syntax

display nqa reaction counters [*admin-name operation-tag* [*item-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

admin-name operation-tag: Specifies an NQA operation by its administrator name and operation tag. The *admin-name* argument represents the name of the administrator who creates the NQA operation. The *operation-tag* argument represents the operation tag. Each of the arguments is a case-insensitive string of 1 to 32 characters that cannot contain hyphens (-). If you do not specify an NQA operation, the command displays the current monitoring results of reaction entries for all NQA operations.

item-number: Specifies a reaction entry by its ID in the range of 1 to 10. If you do not specify a reaction entry, the command displays the results of all reaction entries.

Usage guidelines

The result fields display hyphens (-) if the threshold type is the average value or if the monitored performance metric is ICPIF or MOS of the voice operation.

The monitoring results of an operation are accumulated, and are not cleared after the operation completes.

Examples

Display the monitoring results of all reaction entries of the ICMP echo operation with administrator name **admin** and operation tag **test**.

```
<Sysname> display nqa reaction counters admin test
NQA entry (admin admin, tag test) reaction counters:
  Index  Checked Element  Threshold Type  Checked Num  Over-threshold Num
  1      probe-duration   accumulate      12           4
  2      probe-duration   average         -            -
  3      probe-duration   consecutive     160          56
  4      probe-fail       accumulate      12           0
  5      probe-fail       consecutive     162          2
```

Table 3 Command output

Field	Description
Index	ID of a reaction entry.
Checked Element	Monitored performance metric. The available performance metrics vary by NQA operation type. For more information, see Table 4 and Table 5.
Threshold Type	Threshold type.
Checked Num	Number of targets that have been monitored for data collection.
Over-threshold Num	Number of threshold violations.

Table 4 Monitored performance metrics for ARP/DHCP/DLSw/DNS/FTP/HTTP/ICMP echo/SNMP/TCP/UDP echo operations

Monitored performance metric	Threshold type	Collect data in	Checked Num	Over-threshold Num
probe-duration	accumulate	Probes after the operation starts.	Number of completed probes.	Number of probes with duration exceeding the threshold.
	average	N/A	N/A	N/A
	consecutive	Probes after the operation starts.	Number of completed probes.	Number of probes with duration exceeding the threshold.
probe-fail	accumulate	Probes after the operation starts.	Number of completed probes.	Number of probe failures.
	consecutive	Probes after the operation starts.	Number of completed probes.	Number of probe failures.

Table 5 Monitored performance metrics for ICMP jitter/UDP jitter/voice operations

Monitored performance metric	Threshold type	Collect data in	Checked Num	Over-threshold Num
RTT	accumulate	Packets sent after the operation starts.	Number of sent packets.	Number of packets with round-trip time exceeding threshold.
	average	N/A	N/A	N/A
jitter-DS/jitter-SD	accumulate	Packets sent after the operation starts.	Number of sent packets.	Number of packets with the one-way jitter exceeding the threshold.
	average	N/A	N/A	N/A
OWD-DS/OWD-SD	N/A	Packets sent after the operation starts.	Number of sent packets.	Number of packets with the one-way delay exceeding the threshold.
packet-loss	accumulate	Packets sent after the operation starts.	Number of sent packets.	Total packet loss.
ICPIF/MOS (available only for the voice operation)	N/A	N/A	N/A	N/A

display nqa result

Use **`display nqa result`** to display the most recent result of an NQA operation.

Syntax

`display nqa result` [*`admin-name operation-tag`*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

`admin-name operation-tag`: Specifies an NQA operation by its administrator name and operation tag. The *`admin-name`* argument represents the name of the administrator who creates the NQA operation. The *`operation-tag`* argument represents the operation tag. Each of the arguments is a case-insensitive string of 1 to 32 characters that cannot contain hyphens (-). If you do not specify an NQA operation, the command displays the most recent results of all NQA operations.

Examples

Display the most recent result of the ARP operation with administrator name **admin** and operation tag **test**.

```
<Sysname> display nqa result admin test
NQA entry (admin admin, tag test) test results:
```

```
    Send operation times: 1              Receive response times: 1
    Min/Max/Average round trip time: 35/35/35
    Square-Sum of round trip time: 1225
    Last succeeded probe time: 2011-05-29 10:50:33.2
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

Display the most recent result of the TCP operation with administrator name **admin** and operation tag **test**.

```
<Sysname> display nqa result admin test
NQA entry (admin admin, tag test) test results:
    Send operation times: 1              Receive response times: 1
    Min/Max/Average round trip time: 35/35/35
    Square-Sum of round trip time: 1225
    Last succeeded probe time: 2011-05-29 10:50:33.2
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to disconnect: 0
    Failures due to no connection: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

Display the most recent result of the ICMP jitter operation with administrator name **admin** and operation tag **test**.

```
<Sysname> display nqa result admin test
NQA entry (admin admin, tag test) test results:
    Send operation times: 10             Receive response times: 10
    Min/Max/Average round trip time: 1/2/1
    Square-Sum of round trip time: 13
    Last packet received time: 2015-03-09 17:40:29.8
  Extended results:
    Packet loss ratio: 0.0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packets out of sequence: 0
    Packets arrived late: 0
  ICMP-jitter results:
   RTT number: 10
    Min positive SD: 0                   Min positive DS: 0
    Max positive SD: 0                   Max positive DS: 0
    Positive SD number: 0                Positive DS number: 0
    Positive SD sum: 0                   Positive DS sum: 0
    Positive SD average: 0               Positive DS average: 0
    Positive SD square-sum: 0            Positive DS square-sum: 0
    Min negative SD: 1                   Min negative DS: 2
```

```
    Max negative SD: 1                      Max negative DS: 2
    Negative SD number: 1                   Negative DS number: 1
    Negative SD sum: 1                      Negative DS sum: 2
    Negative SD average: 1                  Negative DS average: 2
    Negative SD square-sum: 1               Negative DS square-sum: 4
    SD average: 1                           DS average: 2
  One way results:
    Max SD delay: 1                         Max DS delay: 2
    Min SD delay: 1                         Min DS delay: 2
    Number of SD delay: 1                   Number of DS delay: 1
    Sum of SD delay: 1                      Sum of DS delay: 2
    Square-Sum of SD delay: 1               Square-Sum of DS delay: 4
    Lost packets for unknown reason: 0
```

Display the most recent result of the UDP jitter operation with administrator name **admin** and operation tag **test**.

```
<Sysname> display nqa result admin test
NQA entry (admin admin, tag test) test results:
    Send operation times: 10             Receive response times: 10
    Min/Max/Average round trip time: 15/46/26
    Square-Sum of round trip time: 8103
    Last packet received time: 2011-05-29 10:56:38.7
  Extended results:
    Packet loss ratio: 0.0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packets out of sequence: 0
    Packets arrived late: 0
  UDP-jitter results:
   RTT number: 10
    Min positive SD: 8                      Min positive DS: 8
    Max positive SD: 18                     Max positive DS: 8
    Positive SD number: 5                   Positive DS number: 2
    Positive SD sum: 75                     Positive DS sum: 32
    Positive SD average: 15                 Positive DS average: 16
    Positive SD square-sum: 1189            Positive DS square-sum: 640
    Min negative SD: 8                      Min negative DS: 1
    Max negative SD: 24                     Max negative DS: 30
    Negative SD number: 4                   Negative DS number: 7
    Negative SD sum: 56                     Negative DS sum: 99
    Negative SD average: 14                 Negative DS average: 14
    Negative SD square-sum: 946             Negative DS square-sum: 1495
    SD average: 14                          DS average: 14
  One way results:
    Max SD delay: 22                        Max DS delay: 23
    Min SD delay: 7                         Min DS delay: 7
    Number of SD delay: 10                  Number of DS delay: 10
    Sum of SD delay: 125                    Sum of DS delay: 132
```

```
    Square-Sum of SD delay: 1805          Square-Sum of DS delay: 1988
    SD lost packets: 0                    DS lost packets: 0
    Lost packets for unknown reason: 0
```

Display the most recent result of the voice operation with administrator name **admin** and operation tag **test**.

```
<Sysname> display nqa result admin test
NQA entry (admin admin, tag test) test results:
    Send operation times: 1000          Receive response times: 0
    Min/Max/Average round trip time: 0/0/0
    Square-Sum of round trip time: 0
    Last packet received time: 0-00-00 00:00:00.0
  Extended results:
    Packet loss ratio: 100.0%
    Failures due to timeout: 1000
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packets out of sequence: 0
    Packets arrived late: 0
  Voice results:
   RTT number: 0
    Min positive SD: 0                    Min positive DS: 0
    Max positive SD: 0                    Max positive DS: 0
    Positive SD number: 0                 Positive DS number: 0
    Positive SD sum: 0                    Positive DS sum: 0
    Positive SD average: 0                Positive DS average: 0
    Positive SD square-sum: 0             Positive DS square-sum: 0
    Min negative SD: 0                    Min negative DS: 0
    Max negative SD: 0                    Max negative DS: 0
    Negative SD number: 0                 Negative DS number: 0
    Negative SD sum: 0                    Negative DS sum: 0
    Negative SD average: 0                Negative DS average: 0
    Negative SD square-sum: 0             Negative DS square-sum: 0
    SD average: 0                         DS average: 0
  One way results:
    Max SD delay: 0                       Max DS delay: 0
    Min SD delay: 0                       Min DS delay: 0
    Number of SD delay: 0                 Number of DS delay: 0
    Sum of SD delay: 0                    Sum of DS delay: 0
    Square-Sum of SD delay: 0             Square-Sum of DS delay: 0
    SD lost packets: 0                    DS lost packets: 0
    Lost packets for unknown reason: 1000
  Voice scores:
    MOS value: 0.99                       ICPIF value: 87
```

Display the most recent result of the path jitter operation with administrator name **admin** and operation tag **test**.

```
<Sysname> display nqa result admin test
NQA entry (admin admin, tag test) test results:
  Hop IP 192.168.40.210
```

```
    Basic Results:
      Send operation times: 10
      Receive response times: 10
      Min/Max/Average round trip time: 1/1/1
      Square-Sum of round trip time: 10
    Extended Results:
      Packet loss ratio: 0%
      Failures due to timeout: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
      Packets out of sequence: 0
      Packets arrived late: 0
    Path-Jitter Results:
      Jitter number: 9
        Min/Max/Average jitter: 0/0/0
      Positive jitter number: 0
        Min/Max/Average positive jitter: 0/0/0
        Sum/Square-Sum positive jitter: 0/0
      Negative jitter number: 0
        Min/Max/Average negative jitter: 0/0/0
        Sum/Square-Sum negative jitter: 0/0
  Hop IP 192.168.50.209
    Basic Results:
      Send operation times: 10
      Receive response times: 10
      Min/Max/Average round trip time: 1/1/1
      Square-Sum of round trip time: 10
    Extended Results:
      Packet loss ratio: 0%
      Failures due to timeout: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
      Packets out of sequence: 0
      Packets arrived late: 0
    Path-Jitter Results:
      Jitter number: 9
        Min/Max/Average jitter: 0/0/0
      Positive jitter number: 0
        Min/Max/Average positive jitter: 0/0/0
        Sum/Square-Sum positive jitter: 0/0
      Negative jitter number: 0
        Min/Max/Average negative jitter: 0/0/0
        Sum/Square-Sum negative jitter: 0/0
```

Display the most recent result of the UDP tracert operation with administrator name **admin** and operation tag **test**.

```
<Sysname> display nqa result admin test
NQA entry (admin admin, tag test) test results:
    Send operation times: 6              Receive response times: 6
```

```
    Min/Max/Average round trip time: 35/35/35
    Square-Sum of round trip time: 1225
    Last succeeded probe time: 2013-09-09 14:23:24.5
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
  UDP-tracert results:
    TTL    Hop IP             Time
    1      3.1.1.1            2013-09-09 14:23:24.5
    2      4.1.1.1            2013-09-09 14:23:24.5
```

Display the most recent result of the throughput operation with administrator name **admin** and operation tag **test**.

```
<Sysname> display nqa result admin test
NQA entry (admin admin, tag test) test results:
  Basic results     :
    Initial speed(Kbps)    : 100000
    Speed granularity(Kbps): 1000
    Probe duration(s)      : 60
    Probe interval(s)      : 4
    Allowed-loss-ratio     : 1/10000

  Throughput results:
    Frame size(Byte): 64
      Current speed(Kbps): -
      Frame-loss(Loss/Tx): -
      Status             : Failed
      Time               : 2022-01-01 07:20:40.8
    Frame size(Byte): 512
      Current speed(Kbps): 4000
      Frame-loss(Loss/Tx): 0/10000
      Status             : Succeeded
      Time               : 2022-01-01 07:21:40.8
    Frame size(Byte): 1024
      Current speed(Kbps): 8000
      Frame-loss(Loss/Tx): 0/10000
      Status             : Succeeded
      Time               : 2022-01-01 07:22:52.8
    Frame size(Byte): 1280
      Current speed(Kbps): 10000
      Frame-loss(Loss/Tx): 0/10000
      Status             : Succeeded
      Time               : 2022-01-01 07:23:45.8
    Frame size(Byte): 1518
      Current speed(Kbps): 10000
      Frame-loss(Loss/Tx): 0/10000
      Status             : Succeeded
```

```
Time                : 2022-01-01 07:24:45.8
```

Table 6 Command output

Field	Description
NQA entry (admin admin, tag test) test results	NQA operation results.
Data collecting in progress	The operation is in progress.
Path jitter result is not available	No result is generated for the operation.
Send operation times	Number of operations.
Receive response times	Number of response packets received.
Min/Max/Average round trip time	Minimum/maximum/average round-trip time in milliseconds.
Square-Sum of round trip time	Square sum of round-trip time.
Last succeeded probe time	Time when the last successful probe was completed. If no probes are successful in an operation, the field displays **0**. This field is not available for UDP jitter, path jitter, and voice operations.
Last packet received time	Time when the last response packet was received. If no response packets in a probe were received, the field displays **0**. This field is available only for UDP jitter and voice operations.
Extended results	Results of extended items.
Packet loss ratio	Average packet loss ratio. For ICMP jitter, UDP jitter, and voice operations, the accuracy of the field value is 0.1%.
Failures due to timeout	Number of timeout occurrences in an operation.
Failures due to disconnect	Number of disconnections by the peer.
Failures due to no connection	Number of failures to connect with the peer.
Failures due to internal error	Number of failures due to internal errors.
Failures due to other errors	Failures due to other errors.
Packets out of sequence	Number of failures due to out-of-sequence packets.
ICMP-jitter results	ICMP jitter operation results. This field is available only for the ICMP jitter operation.
Packets arrived late	Number of response packets received after a probe times out.
UDP-jitter results	UDP jitter operation results. This field is available only for the UDP jitter operation.
Voice results	Voice operation results. This field is available only for the voice operation.
RTT number	Number of response packets received.
Min positive SD	Minimum positive jitter from source to destination.
Min positive DS	Minimum positive jitter from destination to source.
Max positive SD	Maximum positive jitter from source to destination.
Max positive DS	Maximum positive jitter from destination to source.
Positive SD number	Number of positive jitters from source to destination.
Positive DS number	Number of positive jitters from destination to source.

Field	Description
Positive SD sum	Sum of positive jitters from source to destination.
Positive DS sum	Sum of positive jitters from destination to source.
Positive SD average	Average positive jitters from source to destination.
Positive DS average	Average positive jitters from destination to source.
Positive SD square-sum	Square sum of positive jitters from source to destination.
Positive DS square-sum	Square sum of positive jitters from destination to source.
Min negative SD	Minimum absolute value among negative jitters from source to destination.
Min negative DS	Minimum absolute value among negative jitters from destination to source.
Max negative SD	Maximum absolute value among negative jitters from source to destination.
Max negative DS	Maximum absolute value among negative jitters from destination to source.
Negative SD number	Number of negative jitters from source to destination.
Negative DS number	Number of negative jitters from destination to source.
Negative SD sum	Sum of absolute values of negative jitters from source to destination.
Negative DS sum	Sum of absolute values of negative jitters from destination to source.
Negative SD average	Average absolute value of negative jitters from source to destination.
Negative DS average	Average absolute value of negative jitters from destination to source.
Negative SD square-sum	Square sum of negative jitters from source to destination.
Negative DS square-sum	Square sum of negative jitters from destination to source.
SD average	Average value of jitters from source to destination.
DS average	Average value of jitters from destination to source.
One way results	Unidirectional delay. This field is available only for the ICMP jitter, UDP jitter, and voice operations.
Max SD delay	Maximum delay from source to destination.
Max DS delay	Maximum delay from destination to source.
Min SD delay	Minimum delay from source to destination.
Min DS delay	Minimum delay from destination to source.
Number of SD delay	Number of delays from source to destination.
Number of DS delay	Number of delays from destination to source.
Sum of SD delay	Sum of delays from source to destination.
Sum of DS delay	Sum of delays from destination to source.
Square-Sum of SD delay	Square sum of delays from source to destination.

Field	Description
Square-Sum of DS delay	Square sum of delays from destination to source.
SD lost packets	Number of lost packets from the source to the destination.
DS lost packets	Number of lost packets from the destination to the source.
Lost packets for unknown reason	Number of lost packets for unknown reasons.
Voice scores	Voice parameters. This field is available only for the voice operation.
MOS value	MOS value calculated for the voice operation.
ICPIF value	ICPIF value calculated for the voice operation.
Hop IP	IP address of the hop. This field is available only for the path jitter operation.
Path-jitter results	Path jitter operation results. This field is available only for the path jitter operation.
Jitter number	Number of jitters. This field is available only for the path jitter operation.
Min/Max/Average jitter	Minimum/maximum/average jitter in milliseconds. This field is available only for the path jitter operation.
Positive jitter number	Number of positive jitter. This field is available only for the path jitter operation.
Min/Max/Average positive jitter	Minimum/maximum/average positive jitter in milliseconds. This field is available only for the path jitter operation.
Sum/Square-Sum positive jitter	Sum/square sum of the positive jitter. This field is available only for the path jitter operation.
Negative jitter number	Number of negative jitter. This field is available only for the path jitter operation.
Min/Max/Average negative jitter	Minimum/maximum/average negative jitter in milliseconds. This field is available only for the path jitter operation.
Sum/Square-Sum negative jitter	Sum/square sum of the negative jitter. This field is available only for the path jitter operation.
TTL	If the routing table bypass feature is not enabled in the operation, this field displays the TTL value in the probe packet. If the routing table bypass feature is enabled, the value of this field varies by the **`init-ttl`** command. However, the actual TTL value in the probe packet is fixed at 1.
Hop IP	IP address of the node that sent the reply packet.
Time	Time when the NQA client received the reply packet.

Field	Description
Status	Status of the Y.1564 operation or a test in the Y.1564 operation. The value can be: • **Succeeded**. • **Failed**. • **In progress**. • **Aborted**—The test was manually aborted. • **Timeout**. • **Unknown error**. This field displays two hyphens (**--**) for a test whose status is meaningless..
Last test	Last completed test. The value can be: • **CIR test** • **PIR test** • **Traffic policing test** • **Service performance test**
Estimated total time	Total time that the Y.1564 operation was estimated to take, in seconds.
Actual test time used	Actual time taken to complete the Y.1564 operation, in seconds. **NOTE:** The timer used to measure the test start time and end time is accurate to 1 second. Therefore, a difference of up to 1 second might exist between the value displayed in this field and the time duration between the start and end of the test.
CIR test (with the step of 1)	Information about the CIR test with a step count of 1. The number of steps in a CIR test can be set to any value in the range of 1 to 1000.
Start time	Start time of the test.
End time	End time of the test.
Min/Max/Average IR(Kbps)	Minimum, maximum, and average information rates in kbps.
Min/Max/Average FTD(us)	Minimum, maximum, and average frame transfer delays, in μs.
Min/Max/Average FDV(us)	Minimum, maximum, and average frame delay variations, in μs.
FL count/FLR	Number of lost frames and the frame loss ratio.
Packets out of order	Number of out-of-order packets.
Severely Err Secs/AVAIL	Total number of severely errored seconds (SESs) and the network availability ratio (AVAIL). A severely errored second occurs when the ratio of lost frames during a one-second interval exceeds 50%. AVAIL is calculated as follows: AVAIL = Total seconds in available periods / total seconds taken by the test. • The network is in an unavailable period after 10 consecutive SESs are recorded. The unavailable period ends when 10 consecutive non-SESs are recorded. • The network is in an available period after 10 consecutive non-SESs. The available period ends when 10 consecutive SESs are recorded. By default, the test is considered to start in an available period.
PIR test (color green)	Statistics about the green frames in the PIR test.

Field	Description
PIR test (color yellow)	Statistics about the yellow frames in the PIR test.
PIR test (total)	Summary statistics about the PIR test.
PIR test (color-blind)	Statistics about the PIR test in non-color-aware mode.
Traffic policing test (color green)	Statistics about the green frames in the traffic policing test.
Traffic policing test (color yellow)	Statistics about the yellow frames in the traffic policing test.
Traffic policing test (total)	Summary statistics about the traffic policing test.
Traffic policing test (color-blind)	Statistics about the traffic policing test in non-color-aware mode.
Service performance test	Statistics about the service performance test.
Basic results	Results of basic items.
Throughput results	Throughput operation results.
Frame-loss results	Frame loss operation results.
Latency results	Latency operation results.
Initial speed(Kbps)	Initial rate for sending probe packets, in kbps.
Speed granularity(Kbps)	Granularity of rate adjustment, in kbps.
Probe duration(s)	Duration of a probe, in seconds.
Probe interval(s)	Intervals at which probes are performed, in seconds.
Allowed-loss-ratio	Maximum packet loss rate supported.
Frame size(Byte)	Frame size in bytes.
Current speed(Kbps)	Current rate in kbps.
Frame-loss(Loss/Tx)	Frame loss rate.
Min-latency(us)	Minimum latency in microseconds.
Max-latency(us)	Maximum latency in microseconds.
Avg-latency(us)	Average latency in microseconds.
Min-jitter(ns)	Minimum jitter in nanoseconds.
Max-jitter(ns)	Maximum jitter in nanoseconds.
Avg-jitter(ns)	Average jitter in nanoseconds.
Sent packets	Number of packets sent.
Received packets	Number of packets received.
Status	Probe result: • **Succeeded**. • **Failed**.
Time	Time when the probe was completed.

display nqa statistics

Use **display nqa statistics** to display NQA operation statistics.

Syntax

display nqa statistics [*admin-name operation-tag*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

admin-name operation-tag: Specifies an NQA operation by its administrator name and operation tag. The *admin-name* argument represents the name of the administrator who creates the NQA operation. The *operation-tag* argument represents the operation tag. Each of the arguments is a case-insensitive string of 1 to 32 characters that cannot contain hyphens (-).

Usage guidelines

The statistics are generated after the NQA operation completes. If you execute the **display nqa statistics** command before the operation completes, the statistics are displayed as all 0s.

If a reaction entry is configured, the command displays the monitoring results of the reaction entry in the period specified by the **statistics internal** command. The result fields display hyphens (-) if the threshold type is average value or if the monitored performance metric is ICPIF or MOS for the voice operation.

If you do not specify an NQA operation, this command displays statistics for all NQA operations.

Examples

Display the statistics for the ARP operation with administrator name **admin** and operation tag **test**.

```
<Sysname> display nqa statistics admin test
NQA entry (admin admin, tag test) test statistics:
  NO. : 1
    Start time: 2007-01-01 09:30:20.0
    Life time: 2 seconds
    Send operation times: 1              Receive response times: 1
    Min/Max/Average round trip time: 13/13/13
    Square-Sum of round trip time: 169
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

Display the statistics for the TCP operation with administrator name **admin** and operation tag **test**.

```
<Sysname> display nqa statistics admin test
NQA entry (admin admin, tag test) test statistics:
  NO. : 1
    Start time: 2007-01-01 09:30:20.0
    Life time: 2 seconds
    Send operation times: 1              Receive response times: 1
    Min/Max/Average round trip time: 13/13/13
```

```
    Square-Sum of round trip time: 169
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to disconnect: 0
    Failures due to no connection: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

Display the statistics for the ICMP jitter operation with administrator name **admin** and operation tag **test**.

```
<Sysname> display nqa statistics admin test
NQA entry (admin admin, tag test) test statistics:
  NO. : 1
    Start time: 2015-03-09 17:42:10.7
    Life time: 156 seconds
    Send operation times: 1560           Receive response times: 1560
    Min/Max/Average round trip time: 1/2/1
    Square-Sum of round trip time: 1563
  Extended results:
    Packet loss ratio: 0.0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packets out of sequence: 0
    Packets arrived late: 0
  ICMP-jitter results:
   RTT number: 1560
    Min positive SD: 1                   Min positive DS: 1
    Max positive SD: 1                   Max positive DS: 2
    Positive SD number: 18               Positive DS number: 46
    Positive SD sum: 18                  Positive DS sum: 49
    Positive SD average: 1               Positive DS average: 1
    Positive SD square-sum: 18           Positive DS square-sum: 55
    Min negative SD: 1                   Min negative DS: 1
    Max negative SD: 1                   Max negative DS: 2
    Negative SD number: 24               Negative DS number: 57
    Negative SD sum: 24                  Negative DS sum: 58
    Negative SD average: 1               Negative DS average: 1
    Negative SD square-sum: 24           Negative DS square-sum: 60
   SD average: 1                        DS average: 1
  One way results:
    Max SD delay: 1                      Max DS delay: 2
    Min SD delay: 1                      Min DS delay: 1
    Number of SD delay: 4                Number of DS delay: 4
    Sum of SD delay: 4                   Sum of DS delay: 5
    Square-Sum of SD delay: 4            Square-Sum of DS delay: 7
    Lost packets for unknown reason: 0
  Reaction statistics:
```

```
  Index  Checked Element  Threshold Type  Checked Num  Over-threshold Num
  1      jitter-DS        accumulate      1500         10
  2      jitter-SD        average         -            -
  3      OWD-DS           -               1560         2
  4      OWD-SD           -               1560         0
  5      packet-loss      accumulate      0            0
  6      RTT              accumulate      1560         0
```

Display the statistics for the UDP jitter operation with administrator name **admin** and operation tag **test**.

```
<Sysname> display nqa statistics admin test
NQA entry (admin admin, tag test) test statistics:
  NO. : 1
    Start time: 2007-01-01 09:33:22.3
    Life time: 23 seconds
    Send operation times: 100            Receive response times: 100
    Min/Max/Average round trip time: 1/11/5
    Square-Sum of round trip time: 24360
  Extended results:
    Packet loss ratio: 0.0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packets out of sequence: 0
    Packets arrived late: 0
  UDP-jitter results:
   RTT number: 550
    Min positive SD: 1                   Min positive DS: 1
    Max positive SD: 7                   Max positive DS: 1
    Positive SD number: 220              Positive DS number: 97
    Positive SD sum: 283                 Positive DS sum: 287
    Positive SD average: 1               Positive DS average: 2
    Positive SD square-sum: 709          Positive DS square-sum: 1937
    Min negative SD: 2                   Min negative DS: 1
    Max negative SD: 10                  Max negative DS: 1
    Negative SD number: 81               Negative DS number: 94
    Negative SD sum: 556                 Negative DS sum: 191
    Negative SD average: 6               Negative DS average: 2
    Negative SD square-sum: 4292         Negative DS square-sum: 967
    SD average: 2                        DS average: 2
  One way results:
    Max SD delay: 5                      Max DS delay: 5
    Min SD delay: 1                      Min DS delay: 1
    Number of SD delay: 550              Number of DS delay: 550
    Sum of SD delay: 1475                Sum of DS delay: 1201
    Square-Sum of SD delay: 5407         Square-Sum of DS delay: 3959
    SD lost packets: 0                   DS lost packets: 0
    Lost packets for unknown reason: 0
  Reaction statistics:
```

```
  Index  Checked Element  Threshold Type  Checked Num  Over-threshold Num
  1      jitter-DS        accumulate      90           25
  2      jitter-SD        average         -            -
  3      OWD-DS           -               100          24
  4      OWD-SD           -               100          13
  5      packet-loss      accumulate      0            0
  6      RTT              accumulate      100          52
```

Display the statistics for the voice operation with administrator name **admin** and operation tag **test**.

```
<Sysname> display nqa statistics admin test
NQA entry (admin admin, tag test) test statistics:
  NO. : 1
    Start time: 2007-01-01 09:33:45.3
    Life time: 120 seconds
    Send operation times: 10             Receive response times: 10
    Min/Max/Average round trip time: 1/12/7
    Square-Sum of round trip time: 620
  Extended results:
    Packet loss ratio: 0.0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packets out of sequence: 0
    Packets arrived late: 0
  Voice results:
   RTT number: 10
    Min positive SD: 3                   Min positive DS: 1
    Max positive SD: 10                  Max positive DS: 1
    Positive SD number: 3                Positive DS number: 2
    Positive SD sum: 18                  Positive DS sum: 2
    Positive SD average: 6               Positive DS average: 1
    Positive SD square-sum: 134          Positive DS square-sum: 2
    Min negative SD: 3                   Min negative DS: 1
    Max negative SD: 9                   Max negative DS: 1
    Negative SD number: 4                Negative DS number: 2
    Negative SD sum: 25                  Negative DS sum: 2
    Negative SD average: 6               Negative DS average: 1
    Negative SD square-sum: 187          Negative DS square-sum: 2
    SD average: 6                        DS average: 1
  One way results:
    Max SD delay: 0                      Max DS delay: 0
    Min SD delay: 0                      Min DS delay: 0
    Number of SD delay: 0                Number of DS delay: 0
    Sum of SD delay: 0                   Sum of DS delay: 0
    Square-Sum of SD delay: 0            Square-Sum of DS delay: 0
    SD lost packets: 0                   DS lost packets: 0
    Lost packets for unknown reason: 0
  Voice scores:
    Max MOS value: 4.40                  Min MOS value: 4.40
```

```
    Max ICPIF value: 0                    Min ICPIF value: 0
  Reaction statistics:
    Index  Checked Element  Threshold Type  Checked Num  Over-threshold Num
    1      ICPIF            -               -            -
    2      MOS              -               -            -
```

Display the statistics for the path jitter operation with administrator name **admin** and operation tag **test**.

```
<Sysname> display nqa statistics admin test
NQA entry (admin admin, tag test) test statistics:
  NO. : 1
  Path 1:
  Hop IP 192.168.40.210
    Basic Results:
      Send operation times: 10
      Receive response times: 10
      Min/Max/Average round trip time: 1/1/1
      Square-Sum of round trip time: 10
    Extended Results:
      Packet loss ratio: 0%
      Failures due to timeout: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
      Packets out of sequence: 0
      Packets arrived late: 0
    Path-Jitter Results:
      Jitter number: 9
        Min/Max/Average jitter: 0/0/0
      Positive jitter number: 0
        Min/Max/Average positive jitter: 0/0/0
        Sum/Square-Sum positive jitter: 0/0
      Negative jitter number: 0
        Min/Max/Average negative jitter: 0/0/0
        Sum/Square-Sum negative jitter: 0/0
  Hop IP 192.168.50.209
    Basic Results:
      Send operation times: 10
      Receive response times: 10
      Min/Max/Average round trip time: 1/1/1
      Square-Sum of round trip time: 10
    Extended Results:
      Packet loss ratio: 0%
      Failures due to timeout: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
      Packets out of sequence: 0
      Packets arrived late: 0
    Path-Jitter Results:
      Jitter number: 9
```

```
  Min/Max/Average jitter: 0/0/0
Positive jitter number: 0
  Min/Max/Average positive jitter: 0/0/0
  Sum/Square-Sum positive jitter: 0/0
Negative jitter number: 0
  Min/Max/Average negative jitter: 0/0/0
  Sum/Square-Sum negative jitter: 0/0
```

Table 7 Command output

Field	Description
No.	Statistics group ID.
Start time	Time when the operation started.
Life time	Duration of the operation in seconds.
Send operation times	Number of probe packets sent.
Receive response times	Number of response packets received.
Min/Max/Average round trip time	Minimum/maximum/average round-trip time in milliseconds.
Square-Sum of round trip time	Square sum of round-trip time.
Packet loss ratio	Average packet loss ratio. For ICMP jitter, UDP jitter, and voice operations, the accuracy of the field value is 0.1%.
Failures due to timeout	Number of timeout occurrences in an operation.
Failures due to disconnect	Number of disconnections by the peer.
Failures due to no connection	Number of failures to connect with the peer.
Failures due to internal error	Number of failures due to internal errors.
Failures due to other errors	Failures due to other errors.
Packets out of sequence	Number of failures due to out-of-sequence packets.
Packets arrived late	Number of response packets received after a probe times out.
ICMP-jitter results	ICMP jitter operation results. This field is available only for the ICMP jitter operation.
UDP-jitter results	UDP jitter operation results. This field is available only for the UDP jitter operation.
Voice results	Voice operation results. This field is available only for the voice operation.
RTT number	Number of response packets received.
Min positive SD	Minimum positive jitter from source to destination.
Min positive DS	Minimum positive jitter from destination to source.
Max positive SD	Maximum positive jitter from source to destination.
Max positive DS	Maximum positive jitter from destination to source.
Positive SD number	Number of positive jitters from source to destination.
Positive DS number	Number of positive jitters from destination to source.

Field	Description
Positive SD sum	Sum of positive jitters from source to destination.
Positive DS sum	Sum of positive jitters from destination to source.
Positive SD average	Average positive jitters from source to destination.
Positive DS average	Average positive jitters from destination to source.
Positive SD square-sum	Square sum of positive jitters from source to destination.
Positive DS square-sum	Square sum of positive jitters from destination to source.
Min negative SD	Minimum absolute value among negative jitters from source to destination.
Min negative DS	Minimum absolute value among negative jitters from destination to source.
Max negative SD	Maximum absolute value among negative jitters from source to destination.
Max negative DS	Maximum absolute value among negative jitters from destination to source.
Negative SD number	Number of negative jitters from source to destination.
Negative DS number	Number of negative jitters from destination to source.
Negative SD sum	Sum of absolute values of negative jitters from source to destination.
Negative DS sum	Sum of absolute values of negative jitters from destination to source.
Negative SD average	Average absolute value of negative jitters from source to destination.
Negative DS average	Average absolute value of negative jitters from destination to source.
Negative SD square-sum	Square sum of negative jitters from source to destination.
Negative DS square-sum	Square sum of negative jitters from destination to source.
SD average	Average value of jitters from source to destination.
DS average	Average value of jitters from destination to source.
One way results	Unidirectional delay result. This field is available only for the ICMP jitter, UDP jitter, and voice operations.
Max SD delay	Maximum delay from source to destination.
Max DS delay	Maximum delay from destination to source.
Min SD delay	Minimum delay from source to destination.
Min DS delay	Minimum delay from destination to source.
Number of SD delay	Number of delays from source to destination.
Number of DS delay	Number of delays from destination to source.
Sum of SD delay	Sum of delays from source to destination.

Field	Description
Sum of DS delay	Sum of delays from destination to source.
Square-Sum of SD delay	Square sum of delays from source to destination.
Square-Sum of DS delay	Square sum of delays from destination to source.
SD lost packets	Number of lost packets from the source to the destination.
DS lost packets	Number of lost packets from the destination to the source.
Lost packets for unknown reason	Number of lost packets for unknown reasons.
Voice scores	Voice parameters. This field is available only for the voice operation.
Max MOS value	Maximum MOS value.
Min MOS value	Minimum MOS value.
Max ICPIF value	Maximum ICPIF value.
Min ICPIF value	Minimum ICPIF value.
Reaction statistics	Statistics about the reaction entry in the counting interval.
Index	ID of a reaction entry.
Checked Element	Monitored element.
Threshold Type	Threshold type.
Checked Num	Number of targets that have been monitored for data collection.
Over-threshold Num	Number of threshold violations.
Path	Serial number for the path in the path jitter operation. This field is available only for the path jitter operation.
Hop IP	IP address of the hop. This field is available only for the path jitter operation.
Path-jitter results	Path jitter operation results. This field is available only for the path jitter operation.
Jitter number	Number of jitters. This field is available only for the path jitter operation.
Min/Max/Average jitter	Minimum/maximum/average positive jitter in milliseconds. This field is available only for the path jitter operation.
Positive jitter number	Number of positive jitters. This field is available only for the path jitter operation.
Min/Max/Average positive jitter	Minimum/maximum/average positive jitter in milliseconds. This field is available only for the path jitter operation.
Sum/Square-Sum positive jitter	Sum/square sum of positive jitters. This field is available only for the path jitter operation.
Negative jitter number	Number of negative jitters. This field is available only for the path jitter operation.

Field	Description
Min/Max/Average negative jitter	Minimum/maximum/average negative jitter in milliseconds. This field is available only for the path jitter operation.
Sum/Square-Sum negative jitter	Sum/square sum of negative jitters. This field is available only for the path jitter operation.

Table 8 Monitored performance metrics for ARP/DHCP/DLSw/DNS/FTP/HTTP/ICMP echo/SNMP/TCP/UDP echo operations

Monitored performance metric	Threshold type	Collect data in	Checked Num	Over-threshold Num
probe-duration	accumulate	Probes in the counting interval.	Number of completed probes.	Number of probes of which the duration exceeds the threshold.
	average	N/A	N/A	N/A
	consecutive	Probes in the counting interval.	Number of completed probes.	Number of probes of which the duration exceeds the threshold.
probe-fail	accumulate	Probes in the counting interval.	Number of completed probes.	Number of probe failures.
	consecutive	Probes in the counting interval.	Number of completed probes.	Number of probe failures.

Table 9 Monitored performance metrics for ICMP jitter/UDP jitter/voice operations

Monitored performance metric	Threshold type	Collect data in	Checked Num	Over-threshold Num
RTT	accumulate	Packets sent in the counting interval.	Number of sent packets.	Number of packets of which the round-trip time exceeds the threshold.
	average	N/A	N/A	N/A
jitter-DS/jitter-SD	accumulate	Packets sent in the counting interval.	Number of sent packets.	Number of packets of which the one-way jitter exceeds the threshold.
	average	N/A	N/A	N/A
OWD-DS/OWD-SD	N/A	Packets sent in the counting interval.	Number of sent packets.	Number of packets of which the one-way delay exceeds the threshold.
packet-loss	accumulate	Packets sent in the counting interval.	Number of sent packets.	Number of packet loss.
ICPIF/MOS (available only for the voice operation)	N/A	N/A	N/A	N/A

Related commands

`statistics interval`

display nqa twamp-light client

Use **display nqa twamp-light client** to display test session information on the TWAMP Light client.

Syntax

display nqa twamp-light client [**test-session** *session-id* | **verbose**]

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB1180, NFNX3-HDB1480	No

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

test-session *session-id*: Displays detailed information about a test session by its ID. The value range is 1 to 256.

verbose: Displays detailed information about all TWAMP Light test sessions.

Usage guidelines

If you do not specify any keywords, this command displays brief information about all test sessions.

Examples

Display brief information about all test sessions.

```
<Sysname> display nqa twamp-light client
Brief information about all test sessions:
Total sessions: 1
Active sessions: 1
------------------------------------------------------------------------------
ID    Status     Source IP/Port         Destination IP/Port
1     Active     10.2.2.1/10000         10.2.2.2/20000
```

Display detailed information about all test sessions.

```
<Sysname> display nqa twamp-light client verbose
Session ID                          : 1
  Status                            : Active
  Session type                      : Permanent
  Source interface                  : -
  Service instance                  : -
  Source IP                         : 10.2.2.1
```

```
Source IPv6                      : -
Destination IP                   : 10.2.2.2
Destination IPv6                 : -
Source port                      : 10000
Destination port                 : 20000
Source MAC                       : -
Destination MAC                  : -
VLAN ID                          : -
Service VLAN ID                  : -
Customer VLAN ID                 : -
ToS                              : 0
Padding length                   : 142
Timestamp format                 : PTP
VPN instance                     : -
Priority 802.1p                  : 0
Last start time                  : 2020-01-14 10:57:10.1
Last stop time                   : Never
Packet sending interval(ms)      : 100
Timeout(sec)                     : 5
Duration(sec)                    : -
Packets sent                     : -
Statistics interval(ms)          : 10000
Monitor time(ms)                 : 20000
```

Table 10 Command output

Field	Description
Total sessions	Total number of test sessions.
Active sessions	Number of active sessions.
Session ID	Session ID.
Status	Test status: • **Active**—The TWAMP Light test is active. • **Inactive**—The TWAMP Light test is not active.
Session type	Test session type: • On-demand. • Permanent.
Source interface	Source AC interface of the test session.
Service instance	Ethernet service instance bound to source interface. The Ethernet service instance on the client must be consistent with that on the server.
Source IP	Source IPv4 address of the test session.
Source IPv6	Source IPv6 address of the test session.
Destination IP	Destination IPv4 address of the test session.
Destination IPv6	Destination IPv6 address of the test session.
Source port	Source port number of the test session.
Destination port	Destination port number of the test session.

Field	Description
Source MAC	Source MAC address of the test session.
Destination MAC	Destination MAC address of the test session.
VLAN ID	VLAN ID of the test session.
Service VLAN ID	Outer VLAN ID of the test session.
Customer VLAN ID	Inner VLAN ID of the test session.
ToS	Type of Service of the test session.
Padding length	Padding length of the test session.
Timestamp format	Timestamp format: **NTP** or **PTP**.
VPN instance	MPLS L3VPN instance name.
Priority 802.1p	802.1p priority.
Last start time	Start time of the most recent TWAMP Light test. If the test does not start, this field displays **Never**.
Last stop time	Stop time of the most recent TWAMP Light test. If the test does not complete, this field displays **Never**.
Packet sending interval(ms)	Packet sending interval of the TWAMP Light test, in milliseconds.
Timeout(sec)	Timeout time of the reflected packet within a TWAMP Light test, in seconds.
Duration(sec)	Duration of the TWAMP Light test, in seconds. This field is available only for the on-demand test that is configured with test duration.
Packets sent	Number of sent packets in the TWAMP Light test. This field is available only for the on-demand test that is configured with the number of packets to be sent.
Statistics interval(ms)	Statistics collection interval of the TWAMP Light test, in milliseconds.
Monitor time(ms)	Packet monitoring time of the TWAMP Light test, in milliseconds. The value of this field is specified by the **start** command in TWAMP Light sender view.

Related commands

test-session

display nqa twamp-light client statistics

Use **display nqa twamp-light client statistics** to display test session statistics on the TWAMP Light client, including two-way delay, two-way jitter, and two-way packet loss.

Syntax

display nqa twamp-light client statistics { **two-way-delay** | **two-way-loss** } **test-session** *session-id*

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB1180, NFNX3-HDB1480	No

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

`two-way-delay`: Displays statistics about two-way delay and two-way jitter.

`two-way-loss`: Displays statistics about two-way packet loss.

`session-id`: Specifies a session ID. The value must be an integer, in the range of 1 to 256.

Examples

Display statistics about two-way delay and two-way jitter for the specified TWAMP Light test session.

```
<Sysname> display nqa twamp-light client statistics two-way-delay test-session 1
Latest two-way delay statistics(us):
    Index        Delay(Avg)   Jitter(Avg)   SD-jitter(Avg)   DS-jitter(Avg)
    98           3930         941           2992             3054
    99           4184         1550          3136             2969
    100          3799         1273          3135             3103
    101          3881         1345          2932             2906
    102          3850         1310          3290             3226
    103          4202         1579          3694             3703
    104          3893         1033          2999             3000
    105          3891         1206          2935             2982
    106          3861         1076          2947             2906
    107          3911         1246          3011             2886
    108          4088         1617          3083             2890
    109          3832         1380          3041             2976
    110          4332         1478          3610             3784
    111          3908         1115          2953             2943
    112          4111         1646          3391             3028
    113          3982         1215          2905             2885
    114          3799         1207          2951             2902
    115          4824         2107          3952             3343
    116          4137         1433          3658             3625
    117          3986         1337          2914             2904
    118          3904         1087          3873             3883
    119          3737         1337          4612             4539
```

```
    120          4285         1621          3910            3949
    121          4390         1886          3211            3065
    122          3756         1338          2967            2956
    123          4200         1181          3190            3087
    124          4674         1769          2938            3103
    125          4248         1333          2841            2898
    126          4074         1314          2965            2897
    127          4010         1156          2997            2906
------------------------------------------------------------------------------
Average delay    : 4056           Average jitter   : 1372
Maximum delay    : 28999          Maximum jitter   : 25000
Minimum delay    : 952            Minimum jitter   : 1
Average SD jitter: 3234           Average DS jitter: 3177
Maximum SD jitter: 28115          Maximum DS jitter: 16996
Minimum SD jitter: 0              Minimum DS jitter: 0
```

Table 11 Command output

Field	Description
Latest two-way delay statistics(μs)	Most recent statistics of two-way delay in microseconds.
Index	Serial number of the statistics data.
Delay(Avg)	Average delay.
Jitter(Avg)	Average jitter.
SD jitter(Avg)	Average jitter from source to destination.
DS jitter(Avg)	Average jitter from destination to source.
Average delay	Average delay.
Average jitter	Average jitter.
Maximum delay	Maximum delay.
Maximum jitter	Maximum jitter.
Minimum delay	Minimum delay.
Minimum jitter	Minimum jitter.
Average SD jitter	Average jitter from source to destination.
Average DS jitter	Average jitter from destination to source.
Maximum SD jitter	Maximum jitter from source to destination.
Maximum DS jitter	Maximum jitter from destination to source.
Minimum SD jitter	Minimum jitter from source to destination.
Minimum DS jitter	Minimum jitter from destination to source.

Display the two-way packet loss statistics for the specified TWAMP Light test session.

```
<Sysname> display nqa twamp-light client statistics two-way-loss test-session 1
Latest two-way loss statistics:
    Index         Loss count    Loss ratio    Error count    Error ratio
    104           0             0.0000%       0              0.0000%
    105           0             0.0000%       0              0.0000%
```

```
    106           0             0.0000%       0             0.0000%
    107           0             0.0000%       0             0.0000%
    108           0             0.0000%       0             0.0000%
    109           0             0.0000%       0             0.0000%
    110           0             0.0000%       0             0.0000%
    111           0             0.0000%       0             0.0000%
    112           0             0.0000%       0             0.0000%
    113           0             0.0000%       0             0.0000%
    114           0             0.0000%       0             0.0000%
    115           0             0.0000%       0             0.0000%
    116           0             0.0000%       0             0.0000%
    117           0             0.0000%       0             0.0000%
    118           0             0.0000%       0             0.0000%
    119           0             0.0000%       0             0.0000%
    120           0             0.0000%       0             0.0000%
    121           0             0.0000%       0             0.0000%
    122           0             0.0000%       0             0.0000%
    123           0             0.0000%       0             0.0000%
    124           0             0.0000%       0             0.0000%
    125           0             0.0000%       0             0.0000%
    126           0             0.0000%       0             0.0000%
    127           0             0.0000%       0             0.0000%
    128           0             0.0000%       0             0.0000%
    129           0             0.0000%       0             0.0000%
    130           0             0.0000%       0             0.0000%
    131           0             0.0000%       0             0.0000%
    132           0             0.0000%       0             0.0000%
    133           0             0.0000%       0             0.0000%
--------------------------------------------------------------------------------
Average loss count  : 0              Average loss ratio  : 0.0000%
Maximum loss count  : 0              Maximum loss ratio  : 0.0000%
Minimum loss count  : 0              Minimum loss ratio  : 0.0000%
Average error count : 0              Average error ratio : 0.0000%
Maximum error count : 0              Maximum error ratio : 0.0000%
Minimum error count : 0              Minimum error ratio : 0.0000%
```

Table 12 Command output

Field	Description
Latest two-way loss statistics	Most recent statistics of two-way packet loss.
Loss count	Number of lost packets.
Loss ratio	Packet loss rate.
Error count	Number of error packets.
Error ratio	Packet error rate.
Average loss count	Average number of lost packets.
Average loss ratio	Average packet loss rate.
Maximum loss count	Maximum number of lost packets.

Field	Description
Maximum loss ratio	Maximum packet loss rate.
Minimum loss count	Minimum number of lost packets.
Minimum loss ratio	Minimum packet loss rate.
Average error count	Average number of error packets.
Average error ratio	Average packet error rate.
Maximum error count	Maximum number of error packets.
Maximum error ratio	Maximum packet error rate.
Minimum error count	Minimum number of error packets.
Minimum error ratio	Minimum packet error rate.
Index	ID of a reaction entry.

Related commands

`reset nqa twamp-light statistics`

`test-session` (Twamp Light client view)

display nqa twamp-light client test-session reaction counters

Use **`display nqa twamp-light client test-session reaction counters`** to display the current monitoring results of reaction entries for the TWAMP Light test sessions.

Syntax

`display nqa twamp-light client test-session reaction counters` [*`session-id`* [*`item-number`*]]

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB1180, NFNX3-HDB1480	No

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

`session-id`: Specifies a session by its ID. The value range is 1 to 256. If you do not specify this argument, the command displays all statistics information about the specified session.

item-number: Specifies a reaction entry ID in the range of 1 to 10. If you do not specify a reaction entry, the command displays the current monitoring results of all reaction entries.

Usage guidelines

If you do not specify any parameters, this command displays the monitoring results of reaction entries for all TWAMP Light test sessions.

Examples

Display the current monitoring results of the reaction entries for TWAMP Light test session 1.

```
<Sysname> display nqa twamp-light client test-session reaction counters 1
Reaction counters for session 1:
Index: 1
  Checked element: two-way-delay
  Lower-threshold: 5
  Upper-threshold: 50
  Action type: trap-only
  Check-objects: 1
  Threshold violations: 1
```

Table 13 Command output

Field	Description
Index	ID of a reaction entry.
Checked element	Monitored performance metric.
Lower-threshold	Lower limit of the threshold.
Upper-threshold	Upper limit of the threshold.
Action type	Action for the threshold violation event: • **Trap-only**—Displays results on the terminal display and meanwhile sends SNMP trap messages to the NMS. • **none**—Displays results on the terminal display.
Checked-objects	Number of packets that have been monitored.
Threshold violations	Number of threshold violations.

Related commands

reaction checked-element two-way-delay

reaction checked-element two-way-loss

reaction checked-element two-way-jitter

expect { data | hex-data }

Use **expect** { **data** | **hex-data** } to configure the expected response string to determine a successful NQA operation.

Use **undo expect** { **data** | **hex-data** } to restore the default.

Syntax

expect { **data** | **hex-data** } *string* [{ **offset** | **strict-offset** } *number*]

undo expect { **data** | **hex-data** }

Default

No expected response string is configured to determine a successful NQA operation.

Views

HTTP/HTTPS/TCP/UDP/WAP template view

Predefined user roles

network-admin

context-admin

Parameters

data: Specifies a data string.

hex-data: Specifies a hexadecimal string. This keyword is available only in TCP, UDP and WAP template views.

string: Specifies the string.

- If the **data** keyword is specified, the string is case-sensitive and can contain 1 to 200 characters.
- If the **hex-data** keyword is specified, the string is case-insensitive and can contain any even number of characters in the range of 2 to 200.

offset *number*: Specifies the offset in bytes after which the first match operation starts. The value range for the *number* argument is 0 to 1000, and the default value is 0.

strict-offset *number*: Specifies the strict offset in bytes. The value range for the *number* argument is 0 to 1000, and the default value is 0.

Usage guidelines

Upon receiving a response packet, the NQA client searches the packet payload for the expected string. In whichever cases, the NQA client marks the NQA operation as successful if a match is found. If no match is found, it marks the NQA operation as failed.

- If both the offset and the strict offset are not configured, the NQA client starts the first match operation from the beginning byte of the payload. If no match is found, it starts another match operation from the second byte of the payload. The process continues until a match is found or the last payload byte is tried.
- If an offset is configured, the NQA client starts the first match operation after the specified offset bytes. If no match is found, it continues the match operation as if no offset was configured.
- If a strict offset is configured, the NQA client starts the first match operation after the specified strict offset bytes. If no match is found, it starts another match operation from the second byte after the strict offset bytes. The process continues until a match is found or the last payload byte is tried.

Expected string check takes place in the following conditions:

- For features that use the HTTP or HTTPS template, the NQA client checks for the expected string if the response contains the Content-Length header. The expected string check starts from the Content-Length header field.
- For features that use the TCP or UDP template, the NQA client checks for the expected string if the **data-fill** command is configured.

For features that use the UDP template, the start byte of the offset depends on whether the **raw** keyword is specified in the **data-fill** command:

- If the **raw** keyword is specified, the start byte of the offset is the first byte of the packet payload.
- If the **raw** keyword is not specified, the start byte of the offset is the sixth byte of the packet payload. The first five bytes of the UDP packet payload identify the probe packet type.

For the WAP template that has a destination URL specified, you must configure the expected response data. The system checks for the expected string in the WSP replies (starting from the Headers field) to determine whether the WAP operation is successful.

An NQA operation result varies by the configuration of the expected status code and string that determine a successful NQA operation:

- If both these settings are configured, the NQA operation is successful when the NQA response packet matches both the criteria. Otherwise, the operation fails.
- If either the expected status code or string is configured, the NQA operation is successful when the NQA response packet matches the configured criterion. Otherwise, the operation fails.

For the HTTP or HTTPS template, do not configure both this command and the **expect** { **failed-data** | **hex-failed-data** } command.

For the TCP or UDP template, you can also use the **expect** { **failed-data** | **hex-failed-data** } command to configure the expected string in the response of a failed NQA operation. If both the **expect** { **data** | **hex-data** } and **expect** { **failed-data** | **hex-failed-data** } commands are configured, only the **expect** { **failed-data** | **hex-failed-data** } command takes effect.

Examples

In HTTP template view, specify **welcome!** as expected response string to determine a successful NQA operation.

```
<Sysname> system-view
[Sysname] nqa template http httptplt
[Sysname-nqatplt-http-httptplt] expect data welcome!
```

expect { failed-data | hex-failed-data }

Use **expect** { **failed-data** | **hex-failed-data** } to configure the expected response string to determine a failed NQA operation.

Use **undo expect** { **failed-data** | **hex-failed-data** } to restore the default.

Syntax

expect { **failed-data** | **hex-failed-data** } *string* [{ **offset** | **strict-offset** } *number*]

undo expect { **failed-data** | **hex-failed-data** }

Default

No expected response string is configured to determine a failed NQA operation.

Views

HTTP template view

HTTPS template view

TCP template view

UDP template view

Predefined user roles

network-admin

context-admin

Parameters

failed-data: Specifies a data string.

hex-failed-data: Specifies a hexadecimal string.

string: Specifies the string.

- If the **failed-data** keyword is specified, the string is case-sensitive and can contain 1 to 200 characters.
- If the **hex-failed-data** keyword is specified, the string is case-insensitive and can contain any even number of characters in the range of 2 to 200.

offset *number*: Specifies the offset in bytes after which the first match operation starts. The value range for the *number* argument is 0 to 1000, and the default value is 0. If you do not specify an offset, the match operation starts from the beginning byte of the payload.

strict-offset *number*: Specifies the strict offset in bytes. The value range for the *number* argument is 0 to 1000, and the default value is 0.

Usage guidelines

Upon receiving a response packet, the NQA client performs the match process as follows:

1. It first compares expected failed string with the search scope in the packet payload.
   - If the string is longer than the search scope, the operation is marked as failed.
   - If the string is shorter than the search scope, the NQA client goes to the following step.
2. The client searches for the expected string in the search scope.
   - If a match is found, the operation is marked as failed.
   - If no match is found, the operation is marked as successful.

The NQA client performs the match process only once if no offset is specified or the strict offset is specified. If the offset is specified, the client will start another match process for the whole payload if no match is found for the first round.

This command takes effect only if the **data-fill** command is also configured.

For features that use the UDP template, the start byte of the offset depends on whether the **raw** keyword is specified in the **data-fill** command:

- If the **raw** keyword is specified, the start byte of the offset is the first byte of the packet payload.
- If the **raw** keyword is not specified, the start byte of the offset is the sixth byte of the packet payload. The first five bytes of the UDP packet payload identify the probe packet type.

An NQA operation result varies by the configuration of the expected status code and string that determine a failed NQA operation:

- If both these settings are configured, the NQA operation fails when the NQA response packet matches both the criteria. Otherwise, the operation is successful.
- If either the expected status code or string is configured, the NQA operation fails when the NQA response packet matches the configured criterion. Otherwise, the operation is successful.

For the HTTP or HTTPS template, do not configure both this command and the **expect** { **failed-data** | **hex-failed-data** } command.

For the TCP or UDP template, you can also use the **expect** { **data** | **hex-data** } command to configure the expected string in the response of a successful NQA operation. If both the **expect** { **data** | **hex-data** } and **expect** { **failed-data** | **hex-failed-data** } commands are configured, only the **expect** { **failed-data** | **hex-failed-data** } command takes effect.

Examples

In TCP template view, specify **error** as expected response string to determine a failed NQA operation.

```
<Sysname> system-view
[Sysname] nqa template tcp tcptplt
```

```
[Sysname-nqatplt-tcp-tcptplt] expect failed-data error
```

expect failed-status

Use **expect failed-status** to configure the expected status code to determine a failed NQA operation.

Use **undo expect failed-status** to restore the default.

Syntax

expect failed-status *status-list*

undo expect failed-status [*status-list*]

Default

No expected status code is configured to determine a failed NQA operation.

Views

HTTP/HTTPS template view

Predefined user roles

network-admin

context-admin

Parameters

status-list: Specifies a space-separated list of up to 10 status code items. Each item specifies a status code or a range of status codes in the form of *status-number1* **to** *status-number2*. The value ranges for both the *status-number1* and *status-number2* arguments are 0 to 999. The value for the *status-number2* argument must be equal to or greater than the value for the *status-number1* argument.

Usage guidelines

The status code in the probe packet is a three-digit field in decimal notation which includes the server status information. The first digit defines the class of response.

An NQA operation result varies by the configuration of the expected status code and string that determine a failed NQA operation:

- If both these settings are configured, the NQA operation fails when the NQA response packet matches both the criteria. Otherwise, the operation is successful.
- If either the expected status code or string is configured, the NQA operation fails when the NQA response packet matches the configured criterion. Otherwise, the operation is successful.

Do not configure both this command and the **expect status** command.

Examples

In HTTP template view, set the expected status codes to 300, and 400 to 500.

```
<Sysname> system-view
[Sysname] nqa template http tplt
[Sysname-nqatplt-http-tplt] expect failed-status 300 400 to 500
```

expect ip

Use **expect ip** to specify the expected IPv4 address.

Use **undo expect ip** to restore the default.

Syntax

expect ip *ip-address*

undo expect ip

Default

No expected IPv4 address is specified.

Views

DNS template view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the expected IPv4 address for a DNS echo request.

Usage guidelines

During a DNS operation, the NQA client compares the expected IPv4 address with the IPv4 address resolved by the DNS server. If they are the same, it considers the DNS server legal.

Examples

In DNS template view, specify 1.1.1.1 as the expected IPv4 address.

```
<Sysname> system-view
[Sysname] nqa template dns dnstplt
[Sysname-nqatplt-dns-dnstplt] expect ip 1.1.1.1
```

expect ipv6

Use **expect ipv6** to specify the expected IPv6 address.

Use **undo expect ipv6** to restore the default.

Syntax

expect ipv6 *ipv6-address*

undo expect ipv6

Default

No expected IPv6 address is specified.

Views

DNS template view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the expected IPv6 address for a DNS echo request.

Usage guidelines

During a DNS operation, the NQA client compares the expected IPv6 address with the IPv6 address resolved by the DNS server. If they are the same, it considers the DNS server legal.

Examples

In DNS template view, specify 1::1 as the expected IPv6 address.

```
<Sysname> system-view
[Sysname] nqa template dns dnstplt
[Sysname-nqatplt-dns-dnstplt] expect ipv6 1::1
```

expect status

Use **expect status** to configure the expected status code to determine a successful NQA operation.

Use **undo expect status** to restore the default.

Syntax

expect status *status-list*

undo expect status [*status-list*]

Default

No expected status code is configured to determine a successful NQA operation.

Views

HTTP/HTTPS/RTSP/SIP template view

Predefined user roles

network-admin

context-admin

Parameters

status-list: Specifies a space-separated list of up to 10 status code items. Each item specifies a status code or a range of status codes in the form of *status-num* 1 **to** *status-num 2*. The value ranges for both the *status-num* 1 and *status-num 2* arguments are 0 to 999. The value for the *status-num* 2 argument must be equal to or greater than the value for the *status-num* 1 argument.

Usage guidelines

The status code in the probe packet is a three-digit field in decimal notation which includes the server status information. The first digit defines the class of response.

An NQA operation result varies by the configuration of the expected status code and string that determine a successful NQA operation:

- If both these settings are configured, the NQA operation is successful when the NQA response packet matches both the criteria. Otherwise, the operation fails.
- If either the expected status code or string is configured, the NQA operation is successful when the NQA response packet matches the configured criterion. Otherwise, the operation fails.

For the HTTP or HTTPS template, do not configure both this command and the **expect status** command.

Examples

In HTTP template view, set the expected status codes to 200, 300, and 400 to 500.

```
<Sysname> system-view
[Sysname] nqa template http httptplt
[Sysname-nqatplt-http-httptplt] expect status 200 300 400 to 500
```

filename

Use **filename** to specify a file to be transferred between the FTP server and the FTP client.

Use **undo filename** to restore the default.

Syntax

filename *filename*

undo filename

Default

No file is specified.

Views

FTP operation view

FTP template view

Predefined user roles

network-admin

context-admin

Parameters

filename: Specifies the name of a file, a case-insensitive string of 1 to 200 characters that cannot contain slashes (/).

Examples

Specify **config.txt** as the file to be transferred between the FTP server and the FTP client for the FTP operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type ftp
[Sysname-nqa-admin-test-ftp] filename config.txt
```

In FTP template view, specify **config.txt** as the file to be transferred between the FTP server and the FTP client.

```
<Sysname> system-view
[Sysname] nqa template ftp ftptplt
[Sysname-nqatplt-ftp-ftptplt] filename config.txt
```

frequency

Use **frequency** to specify the interval at which the NQA operation repeats.

Use **undo frequency** to restore the default.

Syntax

frequency *interval*

undo frequency

Default

In NQA operation view, the interval between two consecutive voice or path jitter operations is 60000 milliseconds. The interval between two consecutive operations of other types is 0 milliseconds.

In NQA template view, the interval for two consecutive operations is 5000 milliseconds.

Views

ICMP echo/TCP/UDP echo operation view

ARP/DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP tracert operation view

ICMP jitter/path jitter/UDP jitter/voice operation view

Any NQA template view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies the interval between two consecutive operations, in the range of 0 to 604800000 milliseconds. An interval of 0 milliseconds configures NQA to perform the operation only once, and not to generate any statistics.

Usage guidelines

After an NQA operation starts, it repeats at the specified interval. However, when the interval is reached, but the current operation is not completed or not timed out, the next operation does not start.

Examples

Configure the ICMP echo operation to repeat every 1000 milliseconds.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] frequency 1000
```

In DNS template view, configure the DNS operation to repeat every 1000 milliseconds.

```
<Sysname> system-view
[Sysname] nqa template dns dnstplt
[Sysname-nqatplt-dns-dnstplt] frequency 1000
```

Related commands

probe timeout

frequency-adjustment

Use **frequency-adjustment** to specify the adjusted interval for NQA to start two consecutive NQA operations after a failed operation.

Use **undo frequency-adjustment** to restore the default.

Syntax

frequency-adjustment *adj-interval*

undo frequency-adjustment

Default

No adjusted interval is specified.

Views

Any NQA template view

Predefined user roles

network-admin

context-admin

Parameters

adj-interval: Specifies the adjusted interval in the range of 0 to 604800000 milliseconds.

Usage guidelines

By default, the operation interval is determined by the **frequency** command and does not change regardless of the operation result. This command enables the device to adjust the interval for the next two operations after an NQA operation fails. This mechanism allows for detecting the server status in a timely manner.

The next operation starts only when the last operation is completed and the interval is reached.

Examples

In HTTP template view, set the adjusted interval to 1000 milliseconds.

```
<Sysname> system-view
[Sysname] nqa template http tplt
[Sysname-nqatplt-http-tplt] frequency-adjustment 1000
```

hex-data-fill

Use **hex-data-fill** to configure a hexadecimal string to fill the probe packet payload.

Use **undo hex-data-fill** to restore the default.

Syntax

hex-data-fill *hex* [**raw**]

undo hex-data-fill

Default

The default hexadecimal packet payload fill string is 00010203040506070809.

Views

TCP template view

UDP template view

TWAMP Light client-session view

Predefined user roles

network-admin

context-admin

Parameters

hex: Specifies a hexadecimal string, which is case-insensitive and can contain any even number of characters in the range of 2 to 200.

raw: Fills the payload with the specified hexadecimal string without truncation or repetition to fit the payload size. This keyword is available only in UDP template view.

Usage guidelines

With the **raw** keyword specified, the hexadecimal string will be used exactly as specified to fill the packet payload.

Without the **raw** keyword, the hexadecimal string will be truncated at the end or cyclically repeated to fit the payload size of the probe packet.

For example, if you configure the hexadecimal payload fill string as **abcd**:

- Probe packet with a payload size of 3 bytes will be filled with **abc**.
- Probe packet with a payload size of 6 bytes will be filled with **adcdab**.

In UDP template view, the probe packets without the **raw** keyword specified contain special characters. For a destination device other than an NSFOCUS device, provide the **raw** keyword because it can identify only probe packets without any special characters contained. Make sure the payload fill string specified on the client can be identified by the destination device.

If the destination device is an NSFOCUS device, the **raw** keyword is not a must because the NSFOCUS device can identify the probe packets that contain special characters. As a best practice, do not specify the **raw** keyword.

Examples

In TCP template view, specify **abcd** as the hexadecimal payload fill string.

```
<Sysname> system-view
[Sysname] nqa template tcp tcptplt
[Sysname-nqatplt-tcp-tcptplt] hex-data-fill abcd
```

history-record enable

Use **history-record enable** to enable the saving of history records for the NQA operation.

Use **undo history-record enable** to disable the saving of history records.

Syntax

history-record enable

undo history-record enable

Default

The saving of history records is enabled only for the UDP tracert operation.

Views

ICMP echo/TCP/UDP echo operation view

ARP/DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP tracert operation view

Predefined user roles

network-admin

context-admin

Usage guidelines

To display the history records of the NQA operation, use the **display nqa history** command.

The **undo** form of the command also removes existing history records of an NQA operation.

Examples

Enable the saving of history records for the NQA operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] history-record enable
```

Related commands

display nqa history

history-record keep-time

Use **history-record keep-time** to set the lifetime of history records for an NQA operation.

Use **undo history-record keep-time** to restore the default.

Syntax

history-record keep-time *keep-time*

undo history-record keep-time

Default

The history records of an NQA operation are kept for 120 minutes.

Views

ICMP echo/TCP/UDP echo operation view

ARP/DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP tracert operation view

Predefined user roles

network-admin

context-admin

Parameters

keep-time: Specifies how long the history records can be saved. The value range is 1 to 1440 minutes.

Usage guidelines

When an NQA operation completes, the timer starts. All records are removed when the lifetime is reached.

Examples

Set the lifetime of the history records to 100 minutes for the ICMP echo operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] history-record keep-time 100
```

history-record number

Use **history-record number** to set the maximum number of history records that can be saved for an NQA operation.

Use **undo history-record number** to restore the default.

Syntax

history-record number *number*

undo history-record number

Default

A maximum of 50 history records can be saved for an NQA operation.

Views

ICMP echo/TCP/UDP echo operation view

ARP/DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP tracert operation view

Predefined user roles

network-admin

context-admin

Parameters

number: Specifies the maximum number of history records that can be saved for an NQA operation. The value range is 0 to 50.

Usage guidelines

If the number of history records for an NQA operation exceeds the maximum number, earliest history records are removed.

Examples

Set the maximum number of history records to 10 for the ICMP echo operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] history-record number 10
```

init-ttl

Use **init-ttl** to set the TTL value for UDP packets in the start round of the UDP tracert operation.

Use **undo init-ttl** to restore the default.

Syntax

init-ttl *value*

undo init-ttl

Default

The NQA client sends a UDP packet with the TTL value 1 to start the UDP tracert operation.

Views

UDP tracert operation view

Predefined user roles

network-admin

context-admin

Parameters

value: Specifies the TTL value in the range of 1 to 255.

Examples

Set the TTL value to 5 for the UDP packets in the start round.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-tracert
```

```
[Sysname-nqa-admin-test-udp-tracert] init-ttl 5
```

key

Use **key** to set the shared key for secure RADIUS authentication and accounting.

Use **undo key** to restore the default.

Syntax

key { **cipher** | **simple** } *string*

undo key

Default

No shared key is configured for secure RADIUS authentication or accounting.

Views

RADIUS authentication template view

RADIUS accounting template view

Predefined user roles

network-admin

context-admin

Parameters

cipher: Specifies a key in encrypted form.

simple: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the shared key string. Its plaintext form is a case-sensitive string of 1 to 64 characters. Its encrypted form is a case-sensitive string of 1 to 117 characters.

Usage guidelines

Make sure the NQA client and the RADIUS authentication and accounting server have the same shared key.

Examples

In RADIUS template view, set the shared key to **abc** in plain text for secure RADIUS authentication.

```
<Sysname> system-view
[Sysname] nqa template radius radiustplt
[Sysname-nqatplt-radius-radiustplt] key simple abc
```

lsr-path

Use **lsr-path** to specify a loose source routing (LSR) path.

Use **undo lsr-path** to restore the default.

Syntax

lsr-path *ip-address*&<1-8>

undo lsr-path

Default

No LSR path is configured.

Views

Path jitter operation view

Predefined user roles

network-admin

context-admin

Parameters

ip-address&<1-8>: Specifies a space-separated list of up to eight IP addresses. Each IP address represents a hop on the path.

Usage guidelines

The path jitter operation first uses tracert to detect each hop to the destination. It then sends ICMP echo requests to measure the delay and jitters from the source to each node. If multiple routes exist between the source and destination, the operation uses the path specified by using **lsr-path** command.

Examples

Specify 10.1.1.20 and 10.1.2.10 as the hops on the LSR path for the path jitter operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type path-jitter
[Sysname-nqa-admin-test- path-jitter] lsr-path 10.1.1.20 10.1.2.10
```

mailbox

Use **mailbox** to specify the mailbox name to be used in the IMAP operation.

Use **undo mailbox** to restore the default.

Syntax

mailbox *mailbox-name*

undo mailbox

Default

The IMAP operation uses the mailbox name INBOX.

Views

IMAP template view

Predefined user roles

network-admin

context-admin

Parameters

mailbox-name: Specifies the mailbox name, a case-sensitive string of 1 to 64 characters.

Examples

Set the mailbox name to **fortest1** for IMAP template **imaptplt**.

```
<Sysname> system-view
[Sysname] nqa template imap imaptplt
[Sysname-nqatplt-imap-imaptplt] mailbox fortest1
```

max-failure

Use **max-failure** to set the maximum number of consecutive probe failures in a UDP tracert operation.

Use **undo max-failure** to restore the default.

Syntax

max-failure *times*

undo max-failure

Default

A UDP tracert operation stops and fails when it detects five consecutive probe failures.

Views

UDP tracert operation view

Predefined user roles

network-admin

context-admin

Parameters

times: Specifies the maximum number in the range of 0 to 255. When this argument is set to 0 or 255, the UDP tracert operation does not stop when consecutive probe failures occur.

Usage guidelines

When a UDP tracert operation detects the maximum number of consecutive probe failures, the operation fails and stops probing the path.

Examples

Set the maximum number of consecutive probe failures to 20 in a UDP tracert operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-tracert
[Sysname-nqa-admin-test-udp-tracert] max-failure 20
```

memory

Use **memory** to specify the threshold and weight for the memory usage object.

Use **undo memory** to restore the default.

Syntax

memory { **threshold** *threshold-value* | **weight** *weight-value* } *

undo memory

Default

The memory usage threshold is 70 and the weight is 2.

Views

SNMP DCA template view

Predefined user roles

network-admin

context-admin

Parameters

threshold *threshold-value*: Specifies the memory usage threshold in the range of 0 to 100. A threshold of 0 means that memory usage is not used as a metric for measuring the SNMP agent performance.

weight *weight-value*: Specifies the weight of the memory usage object in the range of 0 to 100. A weight of 0 means that memory usage is not used as a metric for measuring the SNMP agent performance.

Usage guidelines

This command takes effect only on SNMP agents of the Net-SNMP or Windows agent type.

The NQA client automatically obtains the memory usage from the SNMP agent of the Net-SNMP or Windows type in the SNMP DCA operation.

Examples

Set both the threshold and weight of the memory usage object to 90.

```
<Sysname> system-view
[Sysname] nqa template snmpdca test
[Sysname-nqatplt-snmpdca-test] memory threshold 90 weight 90
```

Related commands

agent-type

mode

Use **mode** to set the data transmission mode for the FTP operation.

Use **undo mode** to restore the default.

Syntax

mode { **active** | **passive** }

undo mode

Default

The FTP operation uses the data transmission mode **active**.

Views

FTP operation view

FTP template view

Predefined user roles

network-admin

context-admin

Parameters

active: Sets the data transmission mode to active. The FTP server initiates a connection request.

passive: Sets the data transmission mode to passive. The FTP client initiates a connection request.

Examples

Set the data transmission mode to **passive** for the FTP operation.

```
<Sysname> system-view
```

```
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type ftp
[Sysname-nqa-admin-test-ftp] mode passive
```

In FTP template view, set the data transmission mode to **passive** for the FTP operation.

```
<Sysname> system-view
[Sysname] nqa template ftp ftptplt
[Sysname-nqatplt-ftp-ftptplt] mode passive
```

next-hop ip

Use **next-hop ip** to specify the next hop IPv4 address for probe packets.

Use **undo next-hop ip** to restore the default.

Syntax

next-hop ip *ip-address*

undo next-hop ip

Default

No next hop IPv4 address is specified for probe packets.

Views

ICMP echo operation view

DNS/ICMP/TCP half open template view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the IPv4 address of the next hop.

Usage guidelines

If the next hop IPv4 address is not configured, the device searches the routing table to determine the next hop IPv4 address for the probe packets.

Examples

Specify 10.1.1.1 as the next hop IPv4 address for the ICMP echo operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] next-hop ip 10.1.1.1
```

next-hop ipv6

Use **next-hop ipv6** to specify the next hop IPv6 address for probe packets.

Use **undo next-hop ipv6** to restore the default.

Syntax

next-hop ipv6 *ipv6-address*

undo next-hop ipv6

Default

No next hop IPv6 address is specified for probe packets.

Views

ICMP echo operation view

DNS/ICMP/TCP half open template view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address: Specifies the IPv6 address of the next hop. IPv6 link-local addresses are not supported.

Usage guidelines

If the next hop IPv6 address is not configured, the device searches the routing table to determine the next hop IPv6 address for the probe packets.

Examples

Specify 10::1 as the next hop IPv6 address for the ICMP echo operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] next-hop ipv6 10::1
```

no-fragment enable

Use **no-fragment enable** to enable the no-fragmentation feature.

Use **undo no-fragment enable** to disable the no-fragmentation feature.

Syntax

no-fragment enable

undo no-fragment enable

Default

The no-fragmentation feature is disabled.

Views

UDP tracert operation view

Predefined user roles

network-admin

context-admin

Usage guidelines

The no-fragmentation feature sets the DF field to 1. Packets with the DF field set cannot be fragmented during the forwarding process.

You can use this command to test the path MTU of a link.

Examples

Enable the no-fragmentation feature for the UDP tracert operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-tracert
[Sysname-nqa-admin-test-udp-tracert] no-fragment enable
```

nqa

Use **nqa** to create an NQA operation and enter its view, or enter the view of an existing NQA operation.

Use **undo nqa** to remove the operation.

Syntax

nqa entry *admin-name operation-tag*

undo nqa { **all** | **entry** *admin-name operation-tag* }

Default

No NQA operations exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

admin-name operation-tag: Specifies an NQA operation by its administrator name and operation tag. The *admin-name* argument represents the name of the administrator who creates the NQA operation. The *operation-tag* argument represents the operation tag. Each of the arguments is a case-insensitive string of 1 to 32 characters that cannot contain hyphens (-).

all: Removes all NQA operations, NQA templates, and Y.1564 operation groups that do not contain any Y.1564 operations.

Examples

Create an NQA operation with administrator name **admin** and operation tag **test**, and enter NQA operation view.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test]
```

nqa agent enable

Use **nqa agent enable** to enable the NQA client.

Use **undo nqa agent enable** to disable the NQA client and stop all operations being performed.

Syntax

nqa agent enable

undo nqa agent enable

Default

The NQA client is enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Examples

Enable the NQA client.

```
<Sysname> system-view
[Sysname] nqa agent enable
```

Related commands

nqa server enable

nqa schedule

Use **nqa schedule** to configure scheduling parameters for an NQA operation.

Use **undo nqa schedule** to stop the operation.

Syntax

nqa schedule *admin-name operation-tag* **start-time** { *hh*:*mm*:*ss* [*yyyy/mm/dd* | *mm/dd/yyyy*] | **now** } **lifetime** { *lifetime* | **forever** } [**recurring**]

undo nqa schedule *admin-name operation-tag*

Default

No schedule is configured for an NQA operation.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

admin-name operation-tag: Specifies an NQA operation by its administrator name and operation tag. The *admin-name* argument represents the name of the administrator who creates the NQA operation. The *operation-tag* argument represents the operation tag. Each of the arguments is a case-insensitive string of 1 to 32 characters that cannot contain hyphens (-).

start-time: Specifies the start time and date of the NQA operation.

hh:*mm*:*ss*: Specifies the start time of an NQA operation.

yyyy/mm/dd: Specifies the start date of an NQA operation. The default value is the current system time, and the value for the *yyyy* argument is in the range of 2000 to 2035.

mm/dd/yyyy: Specifies the start date of an NQA operation. The default value is the current system time, and the value for the *yyyy* argument is in the range of 2000 to 2035.

now: Starts the operation immediately.

lifetime: Specifies the duration of an operation.

lifetime: Specifies the duration of an operation in seconds. The value range is 1 to 2147483647.

forever: Performs the operation until you stop it by using the **undo nqa schedule** command.

recurring: Runs the operation automatically at the start time and for the specified duration. If you do not specify this keyword, the NQA operation is performed only once at the specified date and time.

Usage guidelines

You cannot enter the view of a scheduled NQA operation. If you want to enter such a view, use the **undo nqa schedule** command to stop the NQA operation first.

The NQA operation works between the specified start time and the end time (the start time plus operation duration). If the specified start time is ahead of the system time, the operation starts immediately. If both the specified start time and end time are ahead of the system time, the operation does not start. To display the current system time, use the **display clock** command.

Specify a lifetime long enough for an operation to complete.

Examples

Schedule the operation with administrator name **admin** and operation tag **test** to start on 08:08:08 2008/08/08 and last 1000 seconds.

```
<Sysname> system-view
[Sysname] nqa schedule admin test start-time 08:08:08 2008/08/08 lifetime 1000 recurring
```

Related commands

destination ip

display clock (*Fundamentals Command Reference*)

nqa entry

type

nqa template

Use **nqa template** to create an NQA template and enter its view, or enter the view of an existing NQA template.

Use **undo nqa template** to remove an NQA template.

Syntax

nqa template { **arp** | **dns** | **ftp** | **http** | **https** | **icmp** | **imap** | **pop3** | **radius** | **radius-account** | **rtsp** | **sip** | **smtp** | **snmp** | **snmpdca** | **ssl** | **tcp** | **tcphalfopen** | **udp** | **wap** } *name*

undo nqa template { **arp** | **dns** | **ftp** | **http** | **https** | **icmp** | **imap** | **pop3** | **radius** | **radius-account** | **rtsp** | **sip** | **smtp** | **snmp** | **snmpdca** | **ssl** | **tcp** | **tcphalfopen** | **udp** | **wap** } *name*

Default

No NQA templates exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

arp: Specifies the ARP template.

dns: Specifies the DNS template.

ftp: Specifies the FTP template.

http: Specifies the HTTP template.

https: Specifies the HTTPS template.

icmp: Specifies the ICMP template.

imap: Specifies the IMAP template.

pop3: Specifies the POP3 template.

radius: Specifies the RADIUS authentication template.

radius-account: Specifies the RADIUS accounting template.

rtsp: Specifies the RTSP template.

sip: Specifies the SIP template.

smtp: Specifies the SMTP template.

snmp: Specifies the SNMP template.

snmpdca: Specifies the SNMP DCA template.

ssl: Specifies the SSL template.

tcp: Specifies the TCP template.

tcphalfopen: Specifies the TCP half open template.

udp: Specifies the UDP template.

wap: Specifies the WAP template.

name: Specifies the name of the NQA template, a case-insensitive string of 1 to 32 characters.

Examples

Create an ICMP template named **icmptplt**, and enter its view.

```
<Sysname> system-view
[Sysname] nqa template icmp icmptplt
[Sysname-nqatplt-icmp-icmptplt]
```

nqa twamp-light client

Use **nqa twamp-light client** to enable the TWAMP Light client and enter its view, or enter the view of the enabled TWAMP Light client.

Use **undo nqa twamp-light client** to disable the TWAMP Light client.

Syntax

nqa twamp-light client

undo nqa twamp-light client

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB1180, NFNX3-HDB1480	No

Default

The TWAMP Light client is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

The Two-Way Active Measurement Protocol (TWAMP) measures network performance in the complex networks. To create test sessions, you must first use the **nqa twamp-light client** command to enter TWAMP Light client view.

The **undo nqa twamp-light client** command disables the TWAMP Light client and deletes the test sessions on the TWAMP Light client.

Examples

Enable the TWAMP Light client and enter its view.

```
<Sysname> system-view
[Sysname] nqa twamp-light client
[Sysname-nqa-twamp-light-client]
```

nqa twamp-light sender

Use **nqa twamp-light sender** to enable the TWAMP Light sender and enter its view, or enter the view of the enabled TWAMP Light sender.

Use **undo nqa twamp-light sender** to disable the TWAMP Light sender.

Syntax

nqa twamp-light sender

undo nqa twamp-light sender

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB1180, NFNX3-HDB1480	No

Default

The TWAMP Light sender is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

In the TWAMP Light sender view, you can start or stop a TWAMP Light test.

Examples

Enable the TWAMP Light sender and enter its view.

```
<Sysname> system-view
[Sysname] nqa twamp-light sender
[Sysname-nqa-twamp-light-sender]
```

oid

Use **oid** to configure a custom SNMP object and set the threshold and weight for the object.

Use **undo oid** to remove an SNMP object.

Syntax

oid *oid* **threshold** *threshold-value* **weight** *weight-value*

undo oid *oid*

Default

No custom SNMP object is configured.

Views

SNMP DCA template view

Predefined user roles

network-admin

context-admin

Parameters

oid: Specifies the OID. The value is a string of 1 to 255 characters.

threshold *threshold-value*: Specifies the threshold for the object. The value range is 0 to 100. A threshold of 0 means that the object is not used as a metric for measuring the performance of the SNMP agent.

weight *weight-value*: Specifies the weight for the object. The value range is 0 to 100. A weight of 0 means that the object is not used as a metric for measuring the performance of the SNMP agent.

Usage guidelines

For SNMP agents of the user-defined type, the SNMP DCA does not have any predefined SNMP objects to collect. You must use the **oid** command to configure the interested SNMP objects and their associated thresholds and weights. A maximum of eight SNMP objects can be configured.

For SNMP agents of the Net-SNMP and Windows types, the NQA client automatically obtains the values for CPU, memory, and disk usage objects from the SNMP agent during the SNMP DCA operation.

Examples

In SNMP DCA template view, configure an SNMP object and set the threshold and weight for the object.

```
<Sysname> system-view
[Sysname] nqa template snmpdca test
[Sysname-nqatplt-snmpdca-test] oid 1.3.6.1.4.1.2021.11.11.0 threshold 90 weight 90
```

Related commands

agent-type

operation (FTP operation view)

Use **operation** to specify the operation type for the FTP operation.

Use **undo operation** to restore the default.

Syntax

operation { **get** | **put** }

undo operation

Default

The FTP operation type is **get**.

Views

FTP operation view

FTP template view

Predefined user roles

network-admin

context-admin

Parameters

get: Gets a file from the FTP server.

put: Transfers a file to the FTP server.

Usage guidelines

When you perform the **put** operation with the **filename** command configured, make sure the file exists on the NQA client.

If you get a file from the FTP server, make sure the file specified in the URL exists on the FTP server. The NQA client does not save the file obtained from the FTP server.

Use a small file for the FTP operation. A big file might result in transfer failure because of timeout, or might affect other services for occupying much network bandwidth.

Examples

Set the operation type to **put** for the FTP operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type ftp
[Sysname-nqa-admin-test-ftp] operation put
```

In FTP template view, set the operation type to **put** for the FTP operation.

```
<Sysname> system-view
```

```
[Sysname] nqa template ftp ftptplt
[Sysname-nqatplt-ftp-ftptplt] operation put
```

Related commands

password

username

operation (HTTP operation view)

Use **operation** to specify the operation type for the HTTP operation.

Use **undo operation** to restore the default.

Syntax

operation { **get** | **post** | **raw** }

undo operation

Default

The HTTP operation type is **get**.

Views

HTTP operation view

HTTP template view

Predefined user roles

network-admin

context-admin

Parameters

get: Gets data from the HTTP server.

post: Transfers data to the HTTP server.

raw: Sends the RAW request to the HTTP server.

Usage guidelines

The HTTP operation uses HTTP requests as probe packets.

For the **get** or **post** operation, the content in the request is obtained from the URL specified by the **url** command.

For the **raw** operation, the content in the request is configured in raw request view. You can use the **raw-request** command to enter the raw request view.

Examples

Set the operation type to **raw** for the HTTP operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type http
[Sysname-nqa-admin-test-http] operation raw
```

In HTTP template view, set the operation type to **raw** for the HTTP operation.

```
<Sysname> system-view
[Sysname] nqa template http httptplt
[Sysname-nqatplt-http-httptplt] operation raw
```

Related commands

password

raw-request

username

operation (HTTPS template view)

Use **operation** to specify the operation type for the HTTPS operation.

Use **undo operation** to restore the default.

Syntax

operation { **get** | **post** | **raw** }

undo operation

Default

The HTTPS operation type is **get**.

Views

HTTPS template view

Predefined user roles

network-admin

context-admin

Parameters

get: Gets data from the HTTPS server.

post: Transfers data to the HTTPS server.

raw: Sends the RAW request to the HTTPS server.

Usage guidelines

The HTTPS operation uses HTTPS requests as probe packets.

For the **get** or **post** operation, the content in the request is obtained from the URL specified by the **url** command.

For the **raw** operation, the content in the request is configured in raw request view. You can use the **raw-request** command to enter the raw request view.

Examples

In HTTPS template view, set the operation type to **raw** for the HTTPS operation.

```
<Sysname> system-view
[Sysname] nqa template https httptplt
[Sysname-nqatplt-https-httptplt] operation raw
```

Related commands

password

raw-request

username

out interface

Use **out interface** to specify the output interface for probe packets.

Use **undo out interface** to restore the default.

Syntax

out interface *interface-type interface-number*

undo out interface

Default

The output interface for probe packets is not specified. The NQA client determines the output interface based on the routing table lookup.

Views

ICMP echo operation view

DHCP operation view

UDP tracert operation view

UDP jitter operation view

DNS/ICMP/TCP half open template view

Predefined user roles

network-admin

context-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

For successful operation, the specified output interface must be up.

The **out interface** command does not take effect if the **next-hop** command is configured in the ICMP echo operation, DNS template, ICMP template, or TCP half open template.

Examples

password

Use **password** to specify a password.

Use **undo password** to restore the default.

Syntax

password { **cipher** | **simple** } *string*

undo password

Default

No password is specified.

Views

FTP/HTTP operation view

FTP/HTTP/HTTPS/IMAP/POP3/RADIUS authentication template view

Predefined user roles

network-admin

context-admin

Parameters

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. The value of the argument varies as follows:

- For FTP, HTTP, and HTTPS operations, the plaintext form of the password is a case-sensitive string of 1 to 32 characters. The encrypted form of the password is a case-sensitive string of 1 to 73 characters.
- For RADIUS templates, the plaintext form of the password is a case-sensitive string of 1 to 64 characters. The encrypted form of the password is a case-sensitive string of 1 to 117 characters.
- For IMAP and POP3 templates, the plaintext form of the password is a string of 1 to 40 characters. The encrypted form of the password is a string of 1 to 85 characters.

Examples

Set the FTP login password to **ftpuser**.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type ftp
[Sysname-nqa-admin-test-ftp] password simple ftpuser
```

Set the FTP login password to **ftpuser** in FTP template view.

```
<Sysname> system-view
[Sysname] nqa template ftp ftptplt
[Sysname-nqatplt-ftp-ftptplt] password simple ftpuser
```

Related commands

operation

username

port-detect enable

Use **port-detect enable** to enable port detection.

Use **undo port-detect enable** to disable port detection.

Syntax

port-detect enable

undo port-detect enable

Default

Port detection is disabled.

Views

TCP half open/UDP template view

Predefined user roles

network-admin

context-admin

Usage guidelines

In the TCP half open operation, port detection probes whether the listening port of the TCP service on the destination device is available. If the NQA client receives the SYN-ACK packet from the destination device within the probe timeout time after sending a SYN packet, the TCP half open operation succeeds. If the NQA client does not receive the SYN-ACK packet from the destination device within the probe timeout time, the TCP half open operation fails.

In the UDP operation, port detection probes whether the listening port of the UDP service on the destination device is available. If the NQA client does not receive any ICMP port unreachable messages within the probe timeout time, the UDP operation succeeds. If the client receives an ICMP port unreachable message, the UDP operation fails.

If the destination device is an NSFOCUS device, you must also perform the following tasks for the UDP operation:

- Execute the **ip unreachables enable** command on the destination device to enable sending ICMP destination unreachable messages.
- Execute the **data-fill** or **hex-data-fill** command on the NQA client with the **raw** keyword specified.

To set the probe timeout time, execute the **probe timeout** command.

For port detection to take effect, you must use the **destination port** command to configure the destination port.

Examples

Enable port detection in TCP half open template **tplt**.

```
<Sysname> system-view
[Sysname] nqa template tcphalfopen tplt
[Sysname-nqatplt-tcphalfopen-tplt] port-detect enable
```

Related commands

data-fill

destination port

hex-data-fill

ip unreachables enable (*Layer 3—IP Services Command Reference*)

priority 8021p

Use **priority 8021p** to set the 802.1p priority for probe packets.

Use **undo priority 8021p** to restore the default.

Syntax

priority 8021p *value*

undo priority 8021p

Default

The 802.1p priority of probe packets is 0.

Views

TWAMP Light client-session view

Predefined user roles

network-admin

context-admin

Parameters

value: Specifies the 802.1p priority value in the range of 0 to 7.

Usage guidelines

To test the service quality for specific packet priorities in a congested Layer 2 network, you can use this command to specify the priorities.

For more information about 802.1p priority, see QoS in *ACL and QoS Configuration Guide*.

Examples

Set the 802.1p priority to 1 for probe packets in the TWAMP Light test.

```
<Sysname> system-view
[Sysname] nqa twamp-light client
[Sysname-nqa-twamp-light-client] test-session 1
[Sysname-nqa-twamp-light-client-session1] priority 8021p 1
```

probe count

Use **probe count** to specify the probe times.

Use **undo probe count** to restore the default.

Syntax

probe count *times*

undo probe count

Default

In an UDP tracert operation, the NQA client sends three probe packets to each hop along the path. In other types of operations, the NQA client performs one probe to the destination per operation.

Views

ICMP echo/TCP/UDP echo operation view

ARP/DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP tracert operation view

ICMP jitter/UDP jitter operation view

Predefined user roles

network-admin

context-admin

Parameters

times: Specifies the probe times.

- For the UDP tracert operation, this argument specifies the times of probes to each hop along the path. The value range for this argument is 1 to 10.
- For other types of operations, this argument specifies the times of probes to the destination per operation. The value range for this argument is 1 to 15.

Usage guidelines

The following describes how NQA performs different types of operations:

- A TCP or DLSw operation sets up a connection.
- An ICMP jitter or UDP jitter operation sends a number of probe packets. The number of probe packets is set by using the **probe packet-number** command.
- An FTP, HTTP, DHCP, or DNS operation completes an independent task in each probe. For example, an FTP operation uploads or downloads a file in each probe, and an HTTP operation gets a Web page in each probe.
- An ICMP echo operation sends an ICMP echo request.
- An ARP operation sends an ARP request.
- A UDP echo operation sends a UDP packet.
- An SNMP operation sends one SNMPv1 packet, one SNMPv2c packet, and one SNMPv3 packet.
- A path jitter operation is accomplished in the following steps:
  a. The operation uses tracert to obtain the path from the NQA client to the destination. A maximum of 64 hops can be detected.
  b. The NQA client sends ICMP echo requests to each hop along the path. The number of ICMP echo requests is set by using the **probe packet-number** command.
- A UDP tracert operation determines the routing path from the source to the destination. The number of probe packets sent to each hop is set by using the **probe count** command.

If an operation is to perform multiple probes, the NQA client starts a new probe in one of the following conditions:

- The NQA client receives responses to packets sent in the last probe.
- The probe timeout time expires.

This command is not available for the voice or path jitter operations. Each of these operations performs only one probe.

Examples

Configure the ICMP echo operation to perform 10 probes.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] probe count 10
```

probe packet-interval

Use **probe packet-interval** to configure the packet sending interval in the probe.

Use **undo probe packet-interval** to restore the default.

Syntax

probe packet-interval *interval*

undo probe packet-interval

Default

The packet sending interval is 20 milliseconds.

Views

ICMP jitter/path jitter/UDP jitter/voice operation view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies the sending interval in the range of 10 to 60000 milliseconds.

Examples

Configure the UDP jitter operation to send packets every 100 milliseconds.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Sysname-nqa-admin-test-udp-jitter] probe packet-interval 100
```

probe packet-number

Use **probe packet-number** to set the number of packets to be sent in a UDP jitter, path jitter, or voice probe.

Use **undo probe packet-number** to restore the default.

Syntax

probe packet-number *number*

undo probe packet-number

Default

An ICMP jitter, UDP jitter, or path jitter operation sends 10 packets probe and a voice operation sends 1000 packets per probe.

Views

ICMP jitter/path jitter/UDP jitter/voice operation view

Predefined user roles

network-admin

context-admin

Parameters

number: Specifies the number of packets to be sent per probe. Available value ranges include:

- 10 to 1000 for the ICMP jitter, UDP jitter, and path jitter operations.
- 10 to 60000 for the voice operation.

Examples

Configure the UDP jitter probe to send 100 packets.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Sysname-nqa-admin-test-udp-jitter] probe packet-number 100
```

probe packet-timeout

Use **probe packet-timeout** to set the timeout time for waiting for a response in the UDP jitter, path jitter, or voice operation.

Use **undo probe packet-timeout** to restore the default.

Syntax

probe packet-timeout *timeout*

undo probe packet-timeout

Default

The response timeout time for the UDP jitter or path jitter operation is 3000 milliseconds.

The response timeout time for the voice operation is 5000 milliseconds.

Views

ICMP jitter/path jitter/UDP jitter/voice operation view

Predefined user roles

network-admin

context-admin

Parameters

timeout: Specifies the timeout time in milliseconds. The value range is 10 to 3600000.

Examples

Set the response timeout time to 100 milliseconds in the UDP jitter operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Sysname-nqa-admin-test-udp-jitter] probe packet-timeout 100
```

probe timeout

Use **probe timeout** to set the probe timeout time.

Use **undo probe timeout** to restore the default.

Syntax

probe timeout *timeout*

undo probe timeout

Default

The timeout time of a probe is 3000 milliseconds.

Views

ICMP echo/TCP/UDP echo operation view

ARP/DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP tracert operation view

Any NQA template view

Predefined user roles

network-admin

context-admin

Parameters

timeout: Specifies the probe timeout time in milliseconds. The value range for this argument varies as follows:

- For FTP and HTTP operations, the value range is 10 to 86400000.
- For DHCP, DNS, DLSw, ICMP echo, SNMP, TCP, UDP echo, and UDP tracert operations, the value range is 10 to 3600000.
- For FTP, HTTP, and HTTPS templates, the value range is 10 to 86400000.
- For other types of NQA templates, the value range is 10 to 3600000.

Usage guidelines

If a probe does not complete within the period, the probe is timed out.

To make this command to take effect, the interval specified in the **frequency** command must be greater than that specified in this command.

Examples

Set the probe timeout time to 10000 milliseconds for the ICMP echo operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] probe timeout 10000
```

In HTTP template view, set the probe timeout time to 10000 milliseconds for the HTTP operation.

```
<Sysname> system-view
[Sysname] nqa template http httptplt
[Sysname-nqatplt-http-httptplt] probe timeout 10000
```

Related commands

frequency

proxy-url

Use **proxy-url** to specify the URL of the HTTP or HTTPS proxy server.

Use **undo proxy-url** to restore the default.

Syntax

proxy-url *url*

undo proxy-url

Default

The URL of the HTTP or HTTPS proxy server is not specified.

Views

HTTP template view

HTTPS template view

Predefined user roles

network-admin

context-admin

Parameters

url: Specifies the proxy server URL, a case-sensitive string of 1 to 255 characters.

- The URL of the HTTP proxy server is in the format of http://host or http://host:port.
- The URL of the HTTPS proxy server is in the format of https://host or https://host:port.

The *host* parameter in the URL represents the host name of the server, which must meet the following requirements:

- Case sensitive.
- Valid characters are letters, digits, hyphens (-), underscores (_), and dots (.), but consecutive dots (.) are not allowed.
- Must be a dot-separated series of labels. Each label can contain 1 to 63 characters.

Usage guidelines

After the HTTP or HTTPS proxy server URL is specified, the NQA client will send probe packets to the HTTP or HTTPS proxy server, which acts on behalf of the HTTP or HTTPS server.

If proxy servers are required for Internet access, you must specify the URL of the HTTP or HTTPS proxy server for successful HTTP or HTTPS operations.

Examples

In HTTP template view, specify **http://www.company.com** as the URL of the HTTP proxy server.

```
<Sysname> system-view
[Sysname] nqa template http httptplt
[Sysname-nqatplt-http-httptplt] proxy-url http://www.company.com
```

raw-request

Use **raw-request** to enter raw request view and specify the content of an HTTP or HTTPS request.

Use **undo raw-request** to restore the default.

Syntax

raw-request

undo raw-request

Default

The contents of an HTTP or HTTPS raw request are not specified.

Views

HTTP operation view

HTTP/HTTPS template view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command places you in raw request view and deletes the previously configured request content.

If the HTTP or HTTPS operation type is set to **raw**, you must configure this command. In raw request view, use the **text** command to configure the request content to be sent to the HTTP or HTTPS server. For successful HTTP or HTTPS operations, make sure the raw request content is valid and does not contain aliases set by using the **alias** command. For more information about the command, see CLI in *Fundamentals Command Reference*.

Examples

Enter raw request view and specify the content of a GET request for the HTTP operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type http
[Sysname-nqa-admin-test-http] raw-request
[Sysname-nqa-admin-test-http-raw-request] GET /sdn/ui/app/index HTTP/1.0\r\nHost:
172.0.0.2\r\n\r\n
```

In HTTP template view, enter raw request view and specify the content of a POST request for the HTTP operation.

```
<Sysname> system-view
[Sysname] nqa template http httptplt
[Sysname-nqatplt-http-httptplt] raw-request
[Sysname-nqatplt-http-httptplt-raw-request] POST /sdn/ui/app/index HTTP/1.0\r\nHost:
 172.0.0.2\r\nAuthorization: Basic cm9vdDoxMjM0NTY=\r\n\r\n
```

reaction checked-element { jitter-ds | jitter-sd }

Use **reaction checked-element** { **jitter-ds** | **jitter-sd** } to configure a reaction entry for monitoring one-way jitter in the NQA operation.

Use **undo reaction** to delete a reaction entry.

Syntax

reaction *item-number* **checked-element** { **jitter-ds** | **jitter-sd** } **threshold-type** { **accumulate** *accumulate-occurrences* | **average** } **threshold-value** *upper-threshold lower-threshold* [**action-type** { **none** | **trap-only** }]

undo reaction *item-number*

Default

No reaction entries for monitoring one-way jitter exist.

Views

ICMP jitter/UDP jitter/voice operation view

Predefined user roles

network-admin

context-admin

Parameters

item-number: Assigns an ID to the reaction entry, in the range of 1 to 10.

jitter-ds: Specifies the destination-to-source jitter of each probe packet as the monitored element (or performance metric).

jitter-sd: Specifies source-to-destination jitter of each probe packet as the monitored element.

threshold-type: Specifies a threshold type.

accumulate *accumulate-occurrences*: Checks the total number of threshold violations in the operation. The value range is 1 to 14999 for the ICMP jitter and UDP jitter operations, and 1 to 59999 for the voice operation.

average: Checks the average one-way jitter.

threshold-value: Specifies threshold range in milliseconds.

upper-threshold: Specifies the upper limit in the range of 0 to 3600000.

lower-threshold: Specifies the lower limit in the range of 0 to 3600000. It must not be greater than the upper limit.

action-type: Specifies the action to be triggered. The default action is **none**.

none: Specifies the action of displaying results on the terminal display.

trap-only: Specifies the action of displaying results on the terminal display and meanwhile sending SNMP trap messages to the NMS.

Usage guidelines

You cannot edit a reaction entry after it is created. To change the attributes in a reaction entry, use the **undo reaction** command to delete the entry, and then configure a new one.

Only successful probe packets are monitored. Statistics about failed probe packets are not collected.

Examples

Create reaction entry 1 for monitoring the average destination-to-source jitter of UDP jitter packets, and set the upper limit to 50 milliseconds and the lower limit to 5 milliseconds. Before the NQA operation starts, the initial state of the reaction entry is invalid. After the operation, the average destination-to-source jitter is checked against the threshold range. If it exceeds the upper limit, the state of the reaction entry is set to over-threshold. If it is below the lower limit, the state is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the NMS.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Sysname-nqa-admin-test-udp-jitter] reaction 1 checked-element jitter-ds threshold-type average threshold-value 50 5 action-type trap-only
```

Create reaction entry 2 for monitoring the destination-to-source jitter of UDP jitter probe packets, and set the upper limit to 50 milliseconds, and the lower limit to 5 milliseconds. Before the NQA operation starts, the initial state of the reaction entry is invalid. After the operation, the destination-to-source jitter is checked against the threshold range. If the total number of threshold violations reaches or exceeds 100, the state of the entry is set to over-threshold. Otherwise, the state of the entry is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the NMS.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Sysname-nqa-admin-test-udp-jitter] reaction 2 checked-element jitter-ds threshold-type accumulate 100 threshold-value 50 5 action-type trap-only
```

reaction checked-element { owd-ds | owd-sd }

Use **reaction checked-element** { **owd-ds** | **owd-sd** } to configure a reaction entry for monitoring the one-way delay.

Use **undo reaction** to delete a reaction entry.

Syntax

reaction *item-number* **checked-element** { **owd-ds** | **owd-sd** } **threshold-value** *upper-threshold lower-threshold*

undo reaction *item-number*

Default

No reaction entries for monitoring the one-way delay exist.

Views

ICMP jitter/UDP jitter/voice operation view

Predefined user roles

network-admin

context-admin

Parameters

item-number: Assigns an ID to the reaction entry, in the range of 1 to 10.

owd-ds: Specifies the destination-to-source delay of each probe packet as the monitored element.

owd-sd: Specifies the source-to-destination delay of each probe packet as the monitored element.

threshold-value: Specifies threshold range in milliseconds.

upper-threshold: Specifies the upper limit in the range of 0 to 3600000.

lower-threshold: Specifies the lower limit in the range of 0 to 3600000. It must not be greater than the upper limit.

Usage guidelines

You cannot edit a reaction entry after it is created. To change the attributes in a reaction entry, use the **undo reaction** command to delete the entry, and then configure a new one.

Only successful probe packets are monitored. Statistics about failed probe packets are not collected.

No actions can be configured for a reaction entry of monitoring one-way delays. To display the monitoring results and statistics, use the **display nqa reaction counters** and **display nqa statistics** commands.

Examples

Create reaction entry 1 for monitoring the destination-to-source delay of every UDP jitter packet, and set the upper limit to 50 milliseconds and lower limit to 5 milliseconds. Before the NQA operation starts, the initial state of the reaction entry is invalid. The destination-to-source delay is calculated after the response to the probe packet arrives. If the delay exceeds the upper limit, the state of the reaction entry is set to over-threshold. If it is below the lower limit, the state is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the NMS.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Sysname-nqa-admin-test-udp-jitter] reaction 1 checked-element owd-ds threshold-value 50
5
```

reaction checked-element icpif

Use **reaction checked-element icpif** to configure a reaction entry for monitoring the ICPIF value in the voice operation.

Use **undo reaction** to delete a reaction entry.

Syntax

reaction *item-number* **checked-element icpif threshold-value** *upper-threshold lower-threshold* [**action-type** { **none** | **trap-only** }]

undo reaction *item-number*

Default

No reaction entries for monitoring ICPIF values exist.

Views

Voice operation view

Predefined user roles

network-admin

context-admin

Parameters

item-number: Assigns an ID to the reaction entry, in the range of 1 to 10.

threshold-value: Specifies threshold range.

upper-threshold: Specifies the upper limit in the range of 1 to 100.

lower-threshold: Specifies the lower limit in the range of 1 to 100. It must not be greater than the upper limit.

action-type: Specifies what action to be triggered. The default action is **none**.

none: Specifies the action of displaying results on the terminal display.

trap-only: Specifies the action of displaying results on the terminal display and meanwhile sending SNMP trap messages to the NMS.

Usage guidelines

You cannot edit a reaction entry after it is created. To change the attributes in a reaction entry, use the **undo reaction** command to delete the entry, and then configure a new one.

Examples

Create reaction entry 1 for monitoring the ICPIF value in the voice operation, and set the upper limit to 50 and lower limit to 5. Before the voice operation starts, the initial state of the reaction entry is invalid. After the operation, the ICPIF value is checked against the threshold range. If it exceeds the upper limit, the state of the reaction entry is set to over-threshold. If it is below the lower limit, the state is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the NMS.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type voice
[Sysname-nqa-admin-test-voice] reaction 1 checked-element icpif threshold-value 50 5
action-type trap-only
```

reaction checked-element mos

Use **reaction checked-element mos** to configure a reaction entry for monitoring the MOS value in the voice operation.

Use **undo reaction** to delete a reaction entry.

Syntax

reaction *item-number* **checked-element mos threshold-value** *upper-threshold lower-threshold* [**action-type** { **none** | **trap-only** }]

undo reaction *item-number*

Default

No reaction entries for monitoring the MOS value exist.

Views

Voice operation view

Predefined user roles

network-admin

context-admin

Parameters

item-number: Assigns an ID to the reaction entry, in the range of 1 to 10.

threshold-value: Specifies threshold range.

upper-threshold: Specifies the upper limit in the range of 1 to 500.

lower-threshold: Specifies the lower limit in the range of 1 to 500. It must not be greater than the upper limit.

action-type: Specifies what action to be triggered. The default action is **none**.

none: Specifies the action of displaying results on the terminal display.

trap-only: Specifies the action of displaying results on the terminal display and meanwhile sending SNMP trap messages to the NMS.

Usage guidelines

You cannot edit a reaction entry after it is created. To change the attributes in a reaction entry, use the **undo reaction** command to delete the entry, and then configure a new one.

For the MOS threshold, the number is expressed in three digits representing ones, tenths, and hundredths. For example, to express a MOS threshold of 1, enter 100.

Examples

Create reaction entry 1 for monitoring the MOS value of the voice operation, and set the upper limit to 2 and lower limit to 1. Before the NQA operation starts, the initial state of the reaction entry is invalid. After the operation, the MOS value is checked against the threshold range. If it exceeds the upper limit, the state of the reaction entry is set to over-threshold. If it is below the lower limit, the state is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the NMS.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type voice
[Sysname-nqa-admin-test-voice] reaction 1 checked-element mos threshold-value 200 100
action-type trap-only
```

reaction checked-element packet-loss

Use **reaction checked-element packet-loss** to configure a reaction entry for monitoring packet loss in UDP jitter or voice operation.

Use **undo reaction** to delete a reaction entry.

Syntax

reaction *item-number* **checked-element packet-loss threshold-type accumulate** *accumulate-occurrences* [**action-type** { **none** | **trap-only** }]

undo reaction *item-number*

Default

No reaction entries for monitoring packet loss exist.

Views

ICMP jitter/UDP jitter/voice operation view

Predefined user roles

network-admin

context-admin

Parameters

item-number: Assigns an ID to the reaction entry, in the range of 1 to 10.

threshold-type: Specifies a threshold type.

accumulate *accumulate-occurrences*: Specifies the total number of lost packets in the operation. The value range is 1 to 15000 for the ICMP jitter and UDP jitter operations and 1 to 60000 for the voice operation.

action-type: Specifies what action to be triggered. The default action is **none**.

none: Specifies the action of displaying results on the terminal display.

trap-only: Specifies the action of displaying results on the terminal display and meanwhile sending SNMP trap messages to the NMS.

Usage guidelines

You cannot edit a reaction entry after it is created. To change the attributes in a reaction entry, use the **undo reaction** command to delete the entry, and then configure a new one.

Examples

Create reaction entry 1 for monitoring packet loss in the UDP jitter operation. Before the NQA operation starts, the initial state of the reaction entry is invalid. After the operation, the total number of the lost packets is checked against the threshold. If the number reaches or exceeds 100, the state of the reaction entry is set to over-threshold. Otherwise, the state is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the NMS.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Sysname-nqa-admin-test-udp-jitter] reaction 1 checked-element packet-loss
threshold-type accumulate 100 action-type trap-only
```

reaction checked-element probe-duration

Use **reaction checked-element probe-duration** to configure a reaction entry for monitoring the probe duration.

Use **undo reaction** to delete a reaction entry.

Syntax

reaction *item-number* **checked-element probe-duration threshold-type** { **accumulate** *accumulate-occurrences* | **average** | **consecutive** *consecutive-occurrences* } **threshold-value** *upper-threshold lower-threshold* [**action-type** { **none** | **trap-only** }]

undo reaction *item-number*

Default

No reaction entries for monitoring the probe duration exist.

Views

ICMP echo/TCP/UDP echo operation view

ARP/DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

Predefined user roles

network-admin

context-admin

Parameters

item-number: Assigns an ID to the reaction entry, in the range of 1 to 10.

threshold-type: Specifies a threshold type.

accumulate *accumulate-occurrences*: Checks the total number of threshold violations. The value range is 1 to 15.

average: Checks the average probe duration.

consecutive *consecutive-occurrences*: Specifies the number of consecutive threshold violations after the NQA operation starts. The value range is 1 to 16.

threshold-value: Specifies threshold range in milliseconds.

upper-threshold: Specifies the upper limit in the range of 0 to 3600000.

lower-threshold: Specifies the lower limit in the range of 0 to 3600000. It must not be greater than the upper threshold.

action-type: Specifies what action to be triggered. The default action is **none**.

none: Specifies the action of displaying results on the terminal display.

trap-only: Specifies the action of displaying results on the terminal display and meanwhile sending SNMP trap messages to the NMS. This keyword is not available for the DNS operation.

Usage guidelines

You cannot edit a reaction entry after it is created. To change the attributes in a reaction entry, use the **undo reaction** command to delete the entry, and then configure a new one.

Only successful probe packets are monitored. Statistics about failed probe packets are not collected.

Examples

Create reaction entry 1 for monitoring the average probe duration of ICMP echo operation, and set the upper limit to 50 milliseconds and lower limit to 5 milliseconds. Before the NQA operation starts, the initial state of the reaction entry is invalid. After the operation, the average probe duration is checked. If it exceeds the upper limit, the state is set to over-threshold. If it is below the lower limit, the state of the reaction entry is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the NMS.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-duration
threshold-type average threshold-value 50 5 action-type trap-only
```

Create reaction entry 2 for monitoring the probe duration of ICMP echo operation, and set the upper limit to 50 milliseconds and the lower limit to 5 milliseconds. Before the NQA operation starts, the initial state of the reaction entry is invalid. After the operation, the accumulated probe duration is checked against the threshold range. If the total number of threshold violations reaches or exceeds

10, the state of the entry is set to over-threshold. If it is below the lower threshold, the state of the entry is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the NMS.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] reaction 2 checked-element probe-duration
threshold-type accumulate 10 threshold-value 50 5 action-type trap-only
```

Create reaction entry 3 for monitoring the probe duration time of ICMP echo operation, and set the upper limit to 50 milliseconds and the lower limit to 5 milliseconds. Before the NQA operation starts, the initial state of the reaction entry is invalid. After the operation, the consecutive probe duration is checked against the threshold range. If the total number of consecutive threshold violations reaches or exceeds 10, the state of the entry is set to over-threshold. If it is below the lower threshold, the state of the entry is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the NMS.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] reaction 3 checked-element probe-duration
threshold-type consecutive 10 threshold-value 50 5 action-type trap-only
```

reaction checked-element probe-fail (for trap)

Use **reaction checked-element probe-fail** to configure a reaction entry for monitoring the probe failures of the operation.

Use **undo reaction** to delete a reaction entry.

Syntax

reaction *item-number* **checked-element probe-fail threshold-type** { **accumulate** *accumulate-occurrences* | **consecutive** *consecutive-occurrences* } [**action-type** { **none** | **trap-only** }]

undo reaction *item-number*

Default

No reaction entries for monitoring probe failures exist.

Views

ICMP echo/TCP/UDP echo operation view

ARP/DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

Predefined user roles

network-admin

context-admin

Parameters

item-number: Assigns an ID to the reaction entry, in the range of 1 to 10.

threshold-type: Specifies a threshold type.

accumulate *accumulate-occurrences*: Checks the total number of probe failures. The value range is 1 to 15.

consecutive *consecutive-occurrences*: Checks the maximum number of consecutive probe failures. The value range is 1 to 16.

action-type: Specifies what action to be triggered. The default action is **none**.

none: Specifies the action of displaying results on the terminal display.

trap-only: Specifies the action of displaying results on the terminal display and meanwhile sending SNMP trap messages to the NMS. This keyword is not available for the DNS operation.

Usage guidelines

You cannot edit a reaction entry after it is created. To change the attributes in a reaction entry, use the **undo reaction** command to delete the entry, and then configure a new one.

Examples

Create reaction entry 1 for monitoring the probe failures in ICMP echo operation. Before the NQA operation starts, the initial state of the reaction entry is invalid. If the total number of probe failures reaches or exceeds 10, the state of the entry is set to over-threshold. If it is below the threshold, the state of the entry is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the NMS.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail threshold-type accumulate 10 action-type trap-only
```

Create reaction entry 2 for monitoring the probe failures in ICMP echo operation. Before the NQA operation starts, the initial state of the reaction entry is invalid. If the number of consecutive probe failures reaches or exceeds 10, the state of the entry is set to over-threshold. If it is below the threshold, the state of the entry is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the NMS.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] reaction 2 checked-element probe-fail threshold-type consecutive 10 action-type trap-only
```

reaction checked-element probe-fail (for trigger)

Use **reaction checked-element probe-fail** to configure a reaction entry for monitoring probe failures.

Use **undo reaction** to delete a reaction entry.

Syntax

reaction *item-number* **checked-element probe-fail threshold-type consecutive** *consecutive-occurrences* **action-type trigger-only**

undo reaction *item-number*

Default

No reaction entries for monitoring probe failures exist.

Views

ICMP echo/TCP/UDP echo operation view

ARP/DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

Predefined user roles

network-admin

context-admin

Parameters

item-number: Assigns an ID to the reaction entry, in the range of 1 to 10.

threshold-type: Specifies a threshold type.

consecutive *consecutive-occurrences*: Checks the maximum number of consecutive probe failures, in the range of 1 to 16.

action-type: Specifies what action to be triggered.

trigger-only: Triggers other modules to react to certain conditions.

Usage guidelines

You cannot edit a reaction entry after it is created. To change the attributes in a reaction entry, use the **undo reaction** command to delete the entry, and then configure a new one.

Examples

Create reaction entry 1. If the number of consecutive probe failures reaches 3, collaboration is triggered.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type tcp
[Sysname-nqa-admin-test-tcp] reaction 1 checked-element probe-fail threshold-type
consecutive 3 action-type trigger-only
```

Related commands

track

reaction checked-element rtt

Use **reaction checked-element rtt** to configure a reaction entry for monitoring packet round-trip time.

Use **undo reaction** to delete a reaction entry.

Syntax

reaction *item-number* **checked-element rtt threshold-type** { **accumulate** *accumulate-occurrences* | **average** } **threshold-value** *upper-threshold lower-threshold* [**action-type** { **none** | **trap-only** }]

undo reaction *item-number*

Default

No reaction entries for monitoring packet round-trip time exist.

Views

ICMP jitter/UDP jitter/voice operation view

Predefined user roles

network-admin

context-admin

Parameters

item-number: Assigns an ID to the reaction entry, in the range of 1 to 10.

threshold-type: Specifies a threshold type.

accumulate *accumulate-occurrences*: Checks the total number of threshold violations.

The value range for the *accumulate-occurrences* argument varies by operation type:

- 1 to 15000 for the ICMP jitter and UDP jitter operations.
- 1 to 60000 for the voice operation.

average: Checks the packet average round-trip time.

threshold-value: Specifies threshold range in milliseconds.

upper-threshold: Specifies the upper limit in the range of 0 to 3600000.

lower-threshold: Specifies the lower limit in the range of 0 to 3600000. It must not be greater than the upper limit.

action-type: Specifies what action to be triggered. The default action is **none**.

none: Specifies the action of displaying results on the terminal display.

trap-only: Specifies the action of displaying results on the terminal display and meanwhile sending SNMP trap messages to the NMS.

Usage guidelines

You cannot edit a reaction entry after it is created. To change the attributes in a reaction entry, use the **undo reaction** command to delete the entry, and then configure a new one.

Only successful probe packets are monitored. Statistics about failed probe packets are not collected.

Examples

Create reaction entry 1 for monitoring the average round-trip time of UDP jitter probe packets, and set the upper limit to 50 milliseconds and lower limit to 5 milliseconds. Before the NQA operation starts, the initial state of the reaction entry is invalid. After the operation, the average packet round-trip time is checked. If it exceeds the upper limit, the state is set to over-threshold. If it is below the lower limit, the state is set to below-threshold. Once the reaction entry state changes, a trap message is generated and sent to the NMS.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Sysname-nqa-admin-test-udp-jitter] reaction 1 checked-element rtt threshold-type
average threshold-value 50 5 action-type trap-only
```

Create reaction entry 2 for monitoring the round-trip time of UDP jitter probe packets, and set the upper limit to 50 milliseconds and lower limit to 5 milliseconds. Before the NQA operation starts, the initial state of the reaction entry is invalid. After the operation, the packet round-trip time is checked. If the total number of threshold violations reaches or exceeds 100, the state of the entry is set to over-threshold. Otherwise, the state of the entry is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the NMS.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Sysname-nqa-admin-test-udp-jitter] reaction 1 checked-element rtt threshold-type
accumulate 100 threshold-value 50 5 action-type trap-only
```

reaction checked-element two-way-delay

Use **reaction checked-element two-way-delay** to configure a reaction entry for monitoring the two-way delay in the TWAMP Light tests.

Use **undo reaction trap** to delete a reaction entry.

Syntax

reaction *item-number* **checked-element two-way-delay threshold-value** *upper-threshold lower-threshold* [**action-type** { **none** | **trap-only** }]

undo reaction *item-number*

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB1180, NFNX3-HDB1480	No

Default

No reaction entries for monitoring two-way delay exist.

Views

TWAMP Light client-session view

Predefined user roles

network-admin

context-admin

Parameters

item-number: Assigns an ID to the reaction entry, in the range of 1 to 10.

threshold-value: Specifies threshold range in microseconds.

upper-threshold: Specifies the upper limit in the range of 2 to 1000000.

lower-threshold: Specifies the lower limit in the range of 1 to 999999. It must not be greater than the upper limit.

action-type: Specifies the action to be triggered. The default action is **none**.

none: Specifies the action of displaying results on the terminal display.

trap-only: Specifies the action of displaying results on the terminal display and sending SNMP trap messages to the NMS.

Usage guidelines

You cannot edit a reaction entry after it is created. To change the attributes in a reaction entry, use the **undo reaction** command to delete the entry, and then configure a new one.

Only successful probe packets are monitored. Statistics about failed probe packets are not collected.

In a TWAMP test, the device monitors the test result, and starts the monitoring time when either of the following conditions is met:

- The monitoring result goes beyond the threshold upper limit.
- The monitoring result drops below the threshold lower limit from a monitoring result higher than the lower limit.

If either condition is always true during the monitoring time, a threshold violation occurs. To set the monitoring time, use the **monitor-time** keyword in the **start** command.

Examples

Create reaction entry 1 for monitoring the two-way delay of probe packets, and set the upper limit to 50 microseconds and the lower limit to 5 microseconds.

```
<Sysname> system-view
[Sysname] nqa twamp-light client
[Sysname-nqa-twamp-light-client] test-session 1
[Sysname-nqa-twamp-light-client-session1] reaction 1 checked-element two-way-delay
threshold-value 50 5 action-type trap-only
```

Related commands

start (Twamp Light sender view)

reaction checked-element two-way-jitter

Use **reaction checked-element two-way-jitter** to configure a reaction entry for monitoring the two-way jitter in the TWAMP Light tests.

Use **undo reaction** to delete a reaction entry.

Syntax

reaction *item-number* **checked-element two-way-jitter threshold-value** *upper-threshold lower-threshold* [**action-type** { **none** | **trap-only** }]

undo reaction *item-number*

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB1180, NFNX3-HDB1480	No

Default

No reaction entries for monitoring two-way jitter exist.

Views

TWAMP Light client-session view

Predefined user roles

network-admin

context-admin

Parameters

item-number: Assigns an ID to the reaction entry, in the range of 1 to 10.

threshold-value: Specifies threshold range in microseconds.

upper-threshold: Specifies the upper limit in the range of 2 to 1000000.

lower-threshold: Specifies the lower limit in the range of 1 to 999999. It must not be greater than the upper limit.

action-type: Specifies the action to be triggered. The default action is **none**.

none: Specifies the action of displaying results on the terminal display.

trap-only: Specifies the action of displaying results on the terminal display and sending SNMP trap messages to the NMS.

Usage guidelines

You cannot edit a reaction entry after it is created. To change the attributes in a reaction entry, use the **undo reaction** command to delete the entry, and then configure a new one.

Only successful probe packets are monitored. Statistics about failed probe packets are not collected.

In a TWAMP test, the device monitors the test result, and starts the monitoring time when either of the following conditions is met:

- The monitoring result goes beyond the threshold upper limit.
- The monitoring result drops below the threshold lower limit from a monitoring result higher than the lower limit.

If either condition is always true during the monitoring time, a threshold violation occurs. To set the monitoring time, use the **monitor-time** keyword in the **start** command.

Examples

Create reaction entry 1 for monitoring the two-way jitter of probe packets, and set the upper limit to 20 microseconds and the lower limit to 3 microseconds.

```
<Sysname> system-view
[Sysname] nqa twamp-light client
[Sysname-nqa-twamp-light-client] test-session 1
[Sysname-nqa-twamp-light-client-session1] reaction 1 checked-element two-way-jitter
threshold-value 20 3 action-type trap-only
```

Related commands

start (Twamp Light sender view)

reaction checked-element two-way-loss

Use **reaction checked-element two-way-loss** to configure a reaction entry for monitoring the two-way packet loss in the TWAMP Light tests.

Use **undo reaction** to delete a reaction entry.

Syntax

reaction *item-number* **checked-element two-way-loss threshold-value** *upper-threshold lower-threshold* [**action-type** { **none** | **trap-only** }]

undo reaction *item-number*

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB1180, NFNX3-HDB1480	No

Default

No reaction entries for monitoring two-way packet loss exist.

Views

TWAMP Light client-session view

Predefined user roles

network-admin

context-admin

Parameters

item-number: Assigns an ID to the reaction entry, in the range of 1 to 10.

threshold-value: Specifies threshold range.

upper-threshold: Specifies the upper limit in the range of 2 to 1000000.

lower-threshold: Specifies the lower limit in the range of 1 to 999999. It must not be greater than the upper limit.

action-type: Specifies the action to be triggered. The default action is **none**.

none: Specifies the action of displaying results on the terminal display.

trap-only: Specifies the action of displaying results on the terminal display and sending SNMP trap messages to the NMS.

Usage guidelines

You cannot edit a reaction entry after it is created. To change the attributes in a reaction entry, use the **undo reaction** command to delete the entry, and then configure a new one.

In a TWAMP test, the device monitors the test result, and starts the monitoring time when either of the following conditions is met:

- The monitoring result goes beyond the threshold upper limit.
- The monitoring result drops below the threshold lower limit from a monitoring result higher than the lower limit.

If either condition is always true during the monitoring time, a threshold violation occurs. To set the monitoring time, use the **monitor-time** keyword in the **start** command.

Examples

Create reaction entry 1 for monitoring the two-way packet loss of probe packets, and set the upper limit to 1000 and the lower limit to 500.

```
<Sysname> system-view
[Sysname] nqa twamp-light client
[Sysname-nqa-twamp-light-client] test-session 1
[Sysname-nqa-twamp-light-client-session1] reaction 1 checked-element two-way-loss
threshold-value 1000 500 action-type trap-only
```

Related commands

start (Twamp Light sender view)

reaction trap

Use **reaction trap** to configure the sending of traps to the NMS under specific conditions.

Use **undo reaction trap** to restore the default.

Syntax

reaction trap { **path-change** | **probe-failure** *consecutive-probe-failures* | **test-complete** | **test-failure** [*accumulate-probe-failures*] }

undo reaction trap { **path-change** | **probe-failure** | **test-complete** | **test-failure** }

Default

No traps are sent to the NMS.

Views

ICMP echo/TCP/UDP echo operation view

ARP/DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP tracert operation view

ICMP jitter/UDP jitter/voice operation view

Predefined user roles

network-admin

context-admin

Parameters

path-change: Sends a trap when the UDP tracert operation detects a different path to the destination.

probe-failure *consecutive-probe-failures*: Sends a trap to the NMS if the number of consecutive probe failures in an operation is greater than or equal to *consecutive-probe-failures*. The value range for the *consecutive-probe-failures* argument is 1 to 15. The system counts the number of consecutive probe failures for each operation, so multiple traps might be sent.

test-complete: Sends a trap to indicate that the operation is completed. A UDP tracert operation is considered completed when the path to the destination is determined.

test-failure: Sends a trap when an operation fails. For operations other than UDP tracert operation, the system counts the total number of probe failures in an operation. If the number reaches or exceeds the value for the *accumulate-probe-failures* argument, a trap is sent for the operation failure.

accumulate-probe-failures: Specifies the total number of probe failures in an operation. The value range is 1 to 15. This argument is not supported by the UDP tracert operation.

Usage guidelines

The ARP operation supports the **probe-failure**, **test-complete**, and **test-failure** keywords.

The ICMP jitter, UDP jitter, and voice operations support only the **test-complete** keyword.

The following parameters are not available for the UDP tracert operation:

- The **probe-failure** *consecutive-probe-failures* option.
- The *accumulate-probe-failures* argument.

Examples

Configure the system to send a trap if five or more consecutive probe failures occur in an ICMP echo operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] reaction trap probe-failure 5
```

reaction trigger per-probe

Use **reaction trigger per-probe** to configure the probe result sending on a per-probe basis.

Use **undo reaction trigger per-probe** to restore the default.

Syntax

reaction trigger per-probe

undo reaction trigger per-probe

Default

The probe result is sent to the feature that uses the template after three consecutive failed or successful probes.

Views

DNS/ICMP/TCP half open template view

Predefined user roles

network-admin

context-admin

Usage guidelines

The feature enables the NQA client to send the probe result to the feature that uses the NQA template every time a probe is completed.

If you execute this command and the **reaction trigger probe-fail** command multiple times, the most recent configuration takes effect.

If you execute this command and the **reaction trigger probe-pass** command multiple times, the most recent configuration takes effect.

Examples

In ICMP template view, configure the probe result sending on a per-probe basis.

```
<Sysname> system-view
[Sysname] nqa template icmp icmptplt
[Sysname-nqatplt-icmp-icmptplt] reaction trigger per-probe
```

Related commands

reaction trigger probe-fail

reaction trigger probe-pass

reaction trigger probe-fail

Use **reaction trigger probe-fail** to set the number of consecutive probe failures to determine an operation failure.

Use **undo reaction trigger probe-fail** to restore the default.

Syntax

reaction trigger probe-fail *count*

undo reaction trigger probe-fail

Default

The NQA client notifies the feature of the operation failure when the number of consecutive probe failures reaches 3.

Views

Any NQA template view

Predefined user roles

network-admin

context-admin

Parameters

count: Specifies the number of consecutive probe failures, in the range of 1 to 15.

Usage guidelines

If the number of consecutive probe failures is reached, the NQA client notifies the feature that uses the NQA template of the operation failure.

If you execute this command and the **reaction trigger per-probe** command multiple times, the most recent configuration takes effect.

Examples

In HTTP template view, configure the NQA client to notify the feature of the operation failure when the number of consecutive probe failures reaches 5.

```
<Sysname> system-view
[Sysname] nqa template http httptplt
[Sysname-nqatplt-http-httptplt] reaction trigger probe-fail 5
```

Related commands

reaction trigger per-probe

reaction trigger probe-pass

reaction trigger probe-pass

Use **reaction trigger probe-pass** to set the number of consecutive successful probes to determine a successful operation event.

Use **undo reaction trigger probe-pass** to restore the default.

Syntax

reaction trigger probe-pass *count*

undo reaction trigger probe-pass

Default

The NQA client notifies the feature of the successful operation event if the number of consecutive successful probes reaches 3.

Views

Any NQA template view

Predefined user roles

network-admin

context-admin

Parameters

count: Specifies the number of consecutive successful probes, in the range of 1 to 15.

Usage guidelines

If number of consecutive successful probes is reached, the NQA client notifies the feature that uses the template of the successful operation event.

If you execute this command and the **reaction trigger per-probe** command multiple times, the most recent configuration takes effect.

Examples

In HTTP template view, configure the NQA client to notify the feature of the successful operation event if the number of consecutive successful probes reaches 5.

```
<Sysname> system-view
[Sysname] nqa template http httptplt
[Sysname-nqatplt-http-httptplt] reaction trigger probe-pass 5
```

Related commands

reaction trigger per-probe

reaction trigger probe-fail

request-method

Use **request-method** to specify the request method for the RTSP operation.

Use **undo request-method** to restore the default.

Syntax

request-method { **describe** | **options** }

undo request-method

Default

The **options** request method is used.

Views

RTSP template view

Predefined user roles

network-admin

context-admin

Parameters

describe: Specifies the DESCRIBE request method. A DESCRIBE request returns information on a particular object identified by a URL.

options: Specifies the OPTIONS request method. An OPTIONS request returns the request types that the RTSP server will accept.

Usage guidelines

For an RTSP template that uses the DESCRIBE request method, you must use the **url** command to specify the path of a file located on the RTSP server.

Examples

In RTSP template view, set the RTSP request method to DESCRIBE.

```
<Sysname> system-view
[Sysname] nqa template rtsp rtsptplt
[Sysname-nqatplt-rtsp-rtsptplt] request method describe
```

Related commands

url

reset nqa twamp-light statistics

Use **reset nqa twamp-light statistics** to clear the TWAMP Light test sessions.

Syntax

reset nqa twamp-light statistics { **all** | **test-session** *session-id* }

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB1180, NFNX3-HDB1480	No

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

all: Clears statistics about all TWAMP Light test sessions.

test-session *session-id*: Specifies a session by its ID. The value range is 1 to 256.

Usage guidelines

Use the command with caution. Once being cleared, the test session cannot be recovered.

Examples

Clear statistics about all TWAMP Light test sessions.

```
<Sysname> reset nqa twamp-light statistics all
```

Related commands

display nqa twamp-light client statistic

resolve-target

Use **resolve-target** to specify the domain name to be resolved in the DNS operation.

Use **undo resolve-target** to restore the default.

Syntax

resolve-target *domain-name*

undo resolve-target

Default

The domain name to be resolved in the DNS operation is not specified.

Views

DNS operation view

DNS template view

Predefined user roles

network-admin

context-admin

Parameters

domain-name: Specifies the domain name to be resolved. It is a dot-separated case-sensitive string of 1 to 255 characters including letters, digits, hyphens (-), and underscores (_) (for example, aabbcc.com). Each part consists of 1 to 63 characters, and consecutive dots (.) are not allowed.

Examples

Specify **domain1** as the domain name to be resolved.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type dns
[Sysname-nqa-admin-test-dns] resolve-target domain1
```

In DNS template view, specify **domain1** as the domain name to be resolved.

```
<Sysname> system-view
[Sysname] nqa template dns dnstplt
[Sysname-nqatplt-dns-dnstplt] resolve-target domain1
```

resolve-type

Use **resolve-type** to configure the domain name resolution type.

Use **undo resolve-type** to restore the default.

Syntax

resolve-type { **A** | **AAAA** }

undo resolve-type

Default

The domain name resolution type is type A.

Views

DNS template view

Predefined user roles

network-admin

context-admin

Parameters

A: Specifies the type A queries. A type A query resolves a domain name to a mapped IPv4 address.

AAAA: Specifies the type AAAA queries. A type AAAA query resolves a domain name to a mapped IPv6 address.

Examples

In DNS template view, set the domain name resolution type to **A**.

```
<Sysname> system-view
[Sysname] nqa template dns dnstplt
[Sysname-nqatplt-dns-dnstplt] resolve-type A
```

resource-release { data-fill | hex-data-fill }

Use to **resource-release { data-fill | hex-data-fill }** to enable the NQA client to send a resource release notification packet to the NQA server when an NQA operation is complete.

Use **undo resource-release** to restore the default.

Syntax

resource-release { **data-fill** | **hex-data-fill** } *string*

undo resource-release

Default

The NQA client does not send resource release notifications to the NQA server when an NQA operation is complete.

Views

TCP/UDP template view

Predefined user roles

network-admin

context-admin

Parameters

data-fill: Specifies a payload fill string.

hex-data-fill: Specifies a hexadecimal payload fill string.

string: Specifies the payload fill string.

- If the **data-fill** keyword is specified, the payload fill string is case-sensitive and can contain 1 to 200 characters.
- If the **hex-data-fill** keyword is specified, the payload fill string is case-insensitive and can contain any even number of characters in the range of 2 to 200.

Usage guidelines

With this command configured, the NQA client sends a resource release notification packet containing the specified payload to the NQA server when the NQA operation is complete. The NQA server will then terminate the connection for the NQA operation and release the resources assigned to the operation.

Examples

In TCP template view, enable the NQA client to send a resource release notification packet containing payload **abcd** to the NQA server.

```
<Sysname> system-view
[Sysname] nqa template tcp tcptplt
[Sysname-nqatplt-tcp-tcptplt] resource-release data-fill abcd
```

reth-member probe enable

Use **reth-member probe enable** to enable link connectivity probing for a redundant Ethernet (Reth) member interface.

Use **undo reth-member probe enable** to disable link connectivity probing for a Reth member interface.

Syntax

reth-member probe enable

undo reth-member probe enable

Default

The link connectivity probing is disabled for Reth member interfaces.

Views

ICMP echo operation view

Predefined user roles

network-admin

context-admin

Usage guidelines

If you configure an ICMP echo operation for a Reth interface, only Reth interfaces can be configured as the output interface for probe packets by default.

With this command configured, both Reth interfaces and Reth member interfaces can be configured as output interface for probe packets.

- If you configure a Reth interface as the output interface, the device send probe packets out of the Reth interface. The operation tests the link connectivity between the Reth interface and the peer device.
- If you configure a Reth member interface, whatever it is active or inactive, as the output interface, the device sends probe packets out of the configured member interface. The operation tests the link connectivity between the member interface and the peer.

To probe the link connectivity for two Reth member interfaces with their peers respectively, you can configure two ICMP echo operations, each using one Reth member interface as the output interface.

Examples

Enable link connectivity probing between a Reth member interface and its peer.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] reth-member probe enable
```

Related commands

out interface

route-option bypass-route

Use **route-option bypass-route** to enable the routing table bypass feature to test the connectivity to the direct destination.

Use **undo route-option bypass-route** to disable the routing table bypass feature.

Syntax

route-option bypass-route

undo route-option bypass-route

Default

The routing table bypass feature is disabled.

Views

ICMP echo/TCP/UDP echo operation view

DLSw/DNS/FTP/HTTP/SNMP operation view

UDP tracert operation view

ICMP jitter/UDP jitter/voice operation view

Predefined user roles

network-admin

context-admin

Usage guidelines

When the routing table bypass feature is enabled, the following events occur:

- The routing table is not searched. Packets are sent to the destination on a directly connected network.
- The TTL value in the probe packet is set to 1. The TTL set in the **ttl** command does not take effect.

This command does not take effect if the destination address of the NQA operation is an IPv6 address.

Examples

Enable the routing table bypass feature.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] route-option bypass-route
```

source interface (TWAMP Light client-session view)

Use **source interface** to specify the source AC interface for probe frames.

Use **undo source interface** to restore the default.

Syntax

source interface *interface-type interface-number* [**service-instance** *instance-id*]

undo source interface

Default

No source AC interface is specified for probe frames.

Views

TWAMP Light client-session view

Predefined user roles

network-admin

context-admin

Parameters

interface-type interface-number: Specifies a Layer 2 interface by its type and number.

service-instance *instance-id*: Specifies an Ethernet service instance by its ID in the range of 1 to 4096. The AC interface is identified by the combination of the Layer 2 interface and the Ethernet service instance.

Usage guidelines

On an L2VPN network, you can execute this command to bind an Ethernet service instance to the Layer 2 Ethernet interface to create a source AC interface for sending probe packets.

On a Layer 3 network, you can execute this command to use the Layer 3 Ethernet interface as the source interface for sending probe packets.

Follow these guidelines when you configure this command:

- The specified interface must be up.
- If the *interface-type interface-number* argument represents a Layer 2 interface, the **service-instance** *instance-id* option is required.
- If the *interface-type interface-number* argument represents a Layer 3 interface, the following rules apply:
  - In an MPLS L3VPN network, do not specify the **service-instance** *instance-id* option.
  - In an MPLS L2VPN network, the **service-instance** *instance-id* option is optional. This option takes effect if the Layer 3 interface switches to a Layer 2 interface. In this case, you do not have to stop the operation and reconfigure this command. The operation restarts automatically by using the new source AC after the MPLS L2VPN configuration is modified.

Examples

In TWAMP Light client-session view, specify GigabitEthernet 1/0/1 as the source AC interface.

```
<Sysname> system-view
[Sysname] nqa twamp-light client
[Sysname-nqa-twamp-light-client] test-session 1
[Sysname-nqa-twamp-light-client-session1] source interface gigabitethernet 1/0/1
```

Related commands

source ip

source interface

Use **source interface** to specify the IP address of an interface as the source IP address of probe packets.

Use **undo source interface** to restore the default.

Syntax

source interface *interface-type interface-number*

undo source interface

Default

The probe packets take the primary IP address of the outgoing interface as their source IP address.

Views

ICMP echo operation view

UDP tracert operation view

ICMP template view

Predefined user roles

network-admin

context-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

The specified interface must be up. If the interface is down, no probe requests can be sent out.

If you execute this command and the **source ip** or **source ipv6** command for an ICMP echo operation or ICMP template multiple times, the most recent configuration takes effect.

If you execute this command and the **source ip** command for a UDP tracert operation multiple times, the most recent configuration takes effect.

Examples

Specify the IP address of interface GigabitEthernet 1/0/1 as the source IP address of ICMP echo request packets.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] source interface gigabitethernet 1/0/1
```

In ICMP template view, specify the IP address of the interface GigabitEthernet 1/0/1 as the source IP address of ICMP echo request packets.

```
<Sysname> system-view
[Sysname] nqa template icmp icmptplt
[Sysname-nqatplt-icmp-icmptplt] source interface gigabitethernet 1/0/1
```

Related commands

source ip

source ipv6

source ip

Use **source ip** to configure the source IPv4 address for probe packets.

Use **undo source ip** to restore the default.

Syntax

source ip *ip-address*

undo source ip

Default

The probe packets take the primary IP address of their output interface as the source IPv4 address.

Views

ICMP echo/TCP/UDP echo operation view

ARP/DHCP/DLSw/FTP/HTTP/SNMP operation view

UDP tracert operation view

ICMP jitter/path jitter/UDP jitter/voice operation view

TWAMP Light client-session view

Any NQA template view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the source IPv4 address for probe packets.

Usage guidelines

The specified source IP address must be the IPv4 address of a local interface, and the local interface must be up. Otherwise, no probe packets can be sent out.

For an NQA template, if the source and destination addresses have different IP versions, the source address does not take effect.

If you execute the **source interface** and **source ip** commands multiple times for the following types of NQA operations or templates, the most recent configuration takes effect:

- ICMP echo operation.
- UDP tracert operation.
- ICMP template.

Examples

Specify 10.1.1.1 as the source IPv4 address for ICMP echo requests.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] source ip 10.1.1.1
```

In ICMP template view, specify 10.1.1.1 as the source IPv4 address for ICMP echo requests.

```
<Sysname> system-view
[Sysname] nqa template icmp icmptplt
[Sysname-nqatplt-icmp-icmptplt] source ip 10.1.1.1
```

Related commands

source interface

source ipv6

Use **source ipv6** to configure the source IPv6 address for probe packets.

Use **undo source ipv6** to restore the default.

Syntax

source ipv6 *ipv6-address*

undo source ipv6

Default

For the TWAMP Light test, no source IPv6 address is specified. For NQA operations, the probe packets take the IPv6 address of their output interface as the source IPv6 address.

Views

ICMP echo/TCP/UDP echo/UDP jitter operation view

DNS/FTP/HTTP/HTTPS/ICMP/IMAP/POP3/RADIUS authentication/RADIUS accounting/RTSP/SMTP/SNMP/SNMP DCA/SSL/TCP/TCP half open/UDP/WAP template view

TWAMP Light client-session view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address: Specifies the source IPv6 address for probe packets. IPv6 link-local addresses are not supported.

Usage guidelines

The specified source IPv6 address must be the IPv6 address of a local interface. The local interface must be up. Otherwise, no probe packets can be sent out.

For an NQA template, if the source and destination addresses have different IP versions, the source address does not take effect.

If you execute the **source interface** and **source ipv6** commands multiple times for an ICMP echo operation or ICMP template, the most recent configuration takes effect.

Examples

Specify 1::1 as the source IPv6 address for the ICMP echo operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] source ipv6 1::1
```

In ICMP template view, specify 1::1 as the source IPv6 address for ICMP echo requests.

```
<Sysname> system-view
[Sysname] nqa template icmp icmptplt
[Sysname-nqatplt-icmp-icmptplt] source ipv6 1::1
```

Related commands

source interface

source mac

Use **source mac** to specify the source MAC address for probe frames.

Use **undo source mac** to restore the default.

Syntax

source mac *mac-address*

undo source mac

Default

For the TWAMP Light test, no source MAC address is specified.

For supported NQA operations, the probe packets take the MAC address of the egress interface as the source MAC address.

Views

TWAMP Light client-session view

Predefined user roles

network-admin

context-admin

Parameters

mac-address: Specifies the source MAC address in the format of H-H-H. For example, to use 000f-00e2-0001 as the source MAC address, set this argument to f-e2-1.

Examples

In TWAMP Light client-session view, set the source MAC address of probe frames to 1-1-1.

```
<Sysname> system-view
[Sysname] nqa twamp-light client
[Sysname-nqa-twamp-light-client] test-session 1
[Sysname-nqa-twamp-light-client-session1] source mac 1-1-1
```

source port

Use **source port** to configure the source port number for probe packets.

Use **undo source port** to restore the default.

Syntax

source port *port-number*

undo source port

Default

The system automatically selects an unused port number as the source port number.

Views

UDP echo operation view

SNMP operation view

UDP tracert operation view

UDP jitter/voice operation view

TWAMP Light client-session view

DNS template view

Predefined user roles

network-admin

context-admin

Parameters

port-number: Specifies the source port number in the range of 1 to 65535.

Usage guidelines

For TWAMP Light tests, you must configure this command. For other operation types, as a best practice, use the default setting.

For the operation to succeed, make sure the specified port number is not used by any services on the device.

- To obtain the IPv4 addresses and the port numbers in use on this device, see the **Local Addr:port** field in the output from the **display tcp** and **display udp** commands.

- To obtain the IPv6 addresses and the port numbers in use on this device, see the **LAddr->port** field in the output from the **display ipv6 tcp** and **display ipv6 udp** commands.

Examples

Set the source port number to 8000 for probe packets in the UDP echo operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-echo
[Sysname-nqa-admin-test-udp-echo] source port 8000
```

In DNS template view, set the source port number to 8000 for probe packets in the DNS operation.

```
<Sysname> system-view
[Sysname] nqa template dns dnstplt
[Sysname-nqatplt-dns-dnstplt] source port 8000
```

Related commands

display ipv6 tcp (*Layer 3—IP Services Command Reference*)

display ipv6 udp (*Layer 3—IP Services Command Reference*)

display tcp (*Layer 3—IP Services Command Reference*)

display udp (*Layer 3—IP Services Command Reference*)

ssl-client-policy

Use **ssl-client-policy** to specify an SSL client policy for an HTTPS or SSL template.

Use **undo ssl-client-policy** to restore the default.

Syntax

ssl-client-policy *policy-name*

undo ssl-client-policy

Default

No SSL client policy is specified for an HTTPS or SSL template.

Views

HTTPS/SSL template view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies an SSL client policy by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

In the HTTPS or SSL operation, the NQA client uses the specified SSL client policy to establish an SSL connection to the server.

Examples

Specify SSL client policy **policy** for SSL template **ssltplt**.

```
<Sysname> system-view
[Sysname] nqa template ssl ssltplt
```

```
[Sysname-nqatplt-ssl-ssltplt] ssl-client-policy policy
```

start (TWAMP Light sender view)

Use **start** to start the TWAMP Light test.

Syntax

start test-session *session-id* { **permanent** | **duration** *duration* | **packet-count** *count* } [**tx-interval** { **10** | **100** | **1000** | **30000** }] [**time-out** *timeout*] [[**statistics-interval** *statistics-interval*] **monitor-time** *time*]

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB1180, NFNX3-HDB1480	No

Default

The TWAMP Light test is not started.

Views

TWAMP Light sender view

Predefined user roles

network-admin

context-admin

Parameters

test-session *session-id*: Specifies a TWAMP Light test session by its ID. The value range is 1 to 256.

permanent: Runs a TWAMP Light test permanently.

duration *duration*: Specifies the duration for a TWAMP Light test, in the range of 60 to 300 in seconds.

packet-count *count*: Specifies the number of packets to be sent, in the range of 100 to 30000.

tx-interval { **10** | **100** | **1000** | **30000** }: Specifies a list of up to four packet sending intervals. Valid intervals are 10, 100, 1000, and 30000 milliseconds. The default packet sending interval is 100 milliseconds.

time-out *timeout*: Specifies the timeout time of the reflected packet within a TWAMP Light test, in seconds. The value range is 1 to 10. The default timeout time is 5 seconds.

statistics-interval *interval*: Specifies a statistics collection interval for the TWAMP Light test in milliseconds. The value must be an integer multiple of 10 milliseconds. The value range is 1000 to 6000000. The default statistics collection interval varies by packet sending interval. For more information, see Table 14.

monitor-time *time*: Specifies the packet monitoring time for the TWAMP Light test in milliseconds. The packet monitoring time must be an integer multiple of the statistics collection interval. The value range is 1000 to 86400000.

Usage guidelines

The TWAMP Light test includes on-demand test and permanent test.

- The on-demand test is manually scheduled. It allows a single performance measurement.
- A permanent test, once being started, does not stop unless you execute the **stop** command in the Twamp Light sender view to stop it manually.

In a TWAMP test, the device monitors the test result, and starts the monitoring time when either of the following conditions is met:

- The monitoring result goes beyond the threshold upper limit.
- The monitoring result drops below the threshold lower limit from a monitoring result higher than the lower limit.

If either condition is always true during the monitoring time, a threshold violation occurs.

The monitoring time varies by the **monitor-time** *time* option in this command:

- If you specify this option, the monitoring time for packet loss, delay, and jitter uses the specified value.
- If you do not specify this option, the default monitoring time for packet loss, delay, and jitter is used. The default monitoring time varies by the packet sending interval. For more information, see Table 14.

To set the upper and lower limits, use the reaction entry threshold monitoring commands for the TWAMP Light test.

In the TWAMP Light test, a test session is identified by the combination of source IP address, source port number, destination IP address, and destination port number. To ensure the test result, do not specify the same combination for multiple test sessions.

With the **data-fill** command configured, the packet sending interval cannot be 10 or 100 milliseconds.

To prevent empty reported test statistics, set the test interval no less than the packet sending interval.

Table 14 Default values for the statistics collection interval and monitoring time

Packet sending interval (milliseconds)	Default test interval (seconds)	Default monitoring time for two-way packet loss (seconds)	Default monitoring time for two-way delay and jitter (seconds)
10	2	60	2
100	20	60	20
1 s	200	200	200
30 s	600	600	600

Examples

Start the TWAMP Light test and allow the device to send 3000 packets.

```
<Sysname> system-view
[Sysname] nqa twamp-light sender
[Sysname-nqa-twamp-light-sender] start test-session 1 packet-count 3000
```

Related commands

data-fill

stop (Twamp Light sender view)

reaction checked-element two-way-delay

reaction checked-element two-way-loss

reaction checked-element two-way-jitter

statistics hold-time

Use **statistics hold-time** to set the hold time of statistics groups for an NQA operation.

Use **undo statistics hold-time** to restore the default.

Syntax

statistics hold-time *hold-time*

undo statistics hold-time

Default

The hold time of statistics groups for an NQA operation is 120 minutes.

Views

ICMP echo/TCP/UDP echo operation view

ARP/DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

ICMP jitter/path jitter/UDP jitter/voice operation view

Predefined user roles

network-admin

context-admin

Parameters

hold-time: Specifies the hold time in minutes, in the range of 1 to 1440.

Usage guidelines

A statistics group is deleted when its hold time expires.

Examples

Set the hold time to 3 minutes for statistics groups of the ICMP echo operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] statistics hold-time 3
```

statistics interval

Use **statistics interval** to set the statistics collection interval for an NQA operation.

Use **undo statistics interval** to restore the default.

Syntax

statistics interval *interval*

undo statistics interval

Default

The statistics collection interval is 60 minutes.

Views

ICMP echo/TCP/UDP echo operation view

ARP/DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

ICMP jitter/path jitter/UDP jitter/voice operation view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies the interval in minutes, in the range of 1 to 35791394.

Usage guidelines

NQA forms statistics within the same collection interval as a statistics group. To display information about the statistics groups, use the **display nqa statistics** command.

Examples

Configure NQA to collect the ICMP echo operation statistics every 2 minutes.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] statistics interval 2
```

statistics max-group

Use **statistics max-group** to set the maximum number of statistics groups that can be saved.

Use **undo statistics max-group** to restore the default.

Syntax

statistics max-group *number*

undo statistics max-group

Default

A maximum of two statistics groups can be saved.

Views

ICMP echo/TCP/UDP echo operation view

ARP/DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

ICMP jitter/path jitter/UDP jitter/voice operation view

Predefined user roles

network-admin

context-admin

Parameters

number: Specifies the maximum number of statistics groups, in the range of 0 to 100. To disable statistics collection, set the value to 0.

Usage guidelines

When the maximum number of statistics groups is reached and a new statistics group is to be saved, the earliest statistics group is deleted.

Examples

Configure NQA to save a maximum of five statistics groups for the ICMP echo operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] statistics max-group 5
```

stop (TWAMP Light sender view)

Use **stop** to stop the TWAMP Light test.

Syntax

stop { **all** | **test-session** *session-id* }

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB1180, NFNX3-HDB1480	No

Views

TWAMP Light sender view

Predefined user roles

network-admin

context-admin

Parameters

all: Stops the all TWAMP Light test sessions.

test-session *session-id*: Specifies the ID of a TWAMP Light test session. The value range is 1 to 256.

Examples

Stop the TWAMP Light test of the session 1.

```
<Sysname> system-view
[Sysname] nqa twamp-light sender
[Sysname-nqa-twamp-light-sender] stop test-session 1
```

Related commands

start (TWAMP Light sender view)

target-only

Use **target-only** to perform the path jitter operation only on the destination address.

Use **undo target-only** to restore the default.

Syntax

target-only

undo target-only

Default

NQA performs the path jitter operation to the destination hop by hop.

Views

Path jitter operation view

Predefined user roles

network-admin

context-admin

Examples

Perform the path jitter operation only on the destination address.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type path-jitter
[Sysname-nqa-admin-test-path-jitter] target-only
```

test-accuracy

Use **test-accuracy** to set the timing precision level on the TWAMP Light client.

Use **undo test-accuracy** to restore the default.

Syntax

test-accuracy { **microsecond** | **millisecond** }

undo test-accuracy

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB1180, NFNX3-HDB1480	No

Default

The TWAMP Light client uses the microsecond precision.

Views

TWAMP Light client view

Predefined user roles

network-admin

context-admin

Parameters

microsecond: Specifies the microsecond precision.

millisecond: Specifies the millisecond precision.

Usage guidelines

This command controls the timing precision for TWAMP Light client tests. If a device does not support the microsecond precision due to hardware limitation, a measurement error might occur. In this case, you can use this command to adjust the timing precision level.

Before you execute this command, make sure the TWAMP Light client is not performing any TWAMP Light test sessions.

Examples

Set the millisecond precision on the TWAMP Light client.

```
<Sysname> system-view
[Sysname] nqa twamp-light client
[Sysname-nqa-twamp-light-client] test-accuracy millisecond
```

test-session (TWAMP Light client view)

Use **test-session** to create a test session on TWAMP Light client and enter the client-session view, or enter the client-session view of an existing test session on the TWAMP Light client.

Use **undo test-session** to delete a test session on the TWAMP Light client.

Syntax

test-session *session-id*

undo test-session *session-id*

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB1180, NFNX3-HDB1480	No

Default

No test sessions exist on the TWAMP Light client.

Views

TWAMP Light client view

Predefined user roles

network-admin

context-admin

Parameters

session-id: Specifies a test session by its ID. The value range is 1 to 256.

Usage guidelines

To start a TWAMP Light test, perform the following tasks in sequence:

1. Create a test session on the TWAMP Light client and complete the settings.
2. Use the **nqa twamp-light sender** command to enter the TWAMP Light sender view, and start the test session.

Examples

Specify a test session **test-session 1** on the TWAMP Light client and enter the client-session view.

```
<Sysname> system-view
[Sysname] nqa twamp-light client
[Sysname-nqa-twamp-light-client] test-session 1
[Sysname-nqa-twamp-light-client-session1]
```

timestamp-format

Use **timestamp-format** to specify the timestamp format for probe packets in the TWAMP Light test.

Use **undo timestamp-format** to restore the default.

Syntax

timestamp-format { **ntp** | **ptp** }

undo timestamp-format

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB1180, NFNX3-HDB1480	No

Default

The timestamp format for probe packets in the TWAMP Light test is PTP.

Views

TWAMP Light client-session view

Predefined user roles

network-admin

context-admin

Parameters

ntp: Specifies the NTP format.

ptp: Specifies the PTP format.

Usage guidelines

This command allows you to specify a timestamp format for the probe packet in the TWAMP Light test. The time accuracy in the PTP format is higher than that in the NTP format. This makes the TWAMP Light test result more accurate.

If the time is not synchronized through NTP or PTP, or the TWAMP Light test sender and responder use different timestamp formats, the TWAMP Light test can still be performed, but the test result accuracy might be affected.

Examples

Specify the timestamp format as NTP for the TWAMP Light test.

```
<Sysname> system-view
[Sysname] nqa twamp-light client
```

```
[Sysname-nqa-twamp-light-client] test-session 1
[Sysname-nqa-twamp-light-client-session1] timestamp-format ntp
```

tos

Use **tos** to set the ToS value in the IP header for probe packets.

Use **undo tos** to restore the default.

Syntax

tos *value*

undo tos

Default

The ToS value in the IP header of probe packets is 0.

Views

Any operation view

DNS/FTP/HTTP/HTTPS/ICMP/IMAP/POP3/RADIUS authentication/RADIUS accounting/RTSP/SIP/SMTP/SNMP/SNMP DCA/SSL/TCP/TCP half open/UDP/WAP template view

Predefined user roles

network-admin

context-admin

Parameters

value: Specifies the ToS value in the range of 0 to 255.

Examples

In ICMP echo operation view, set the ToS value to 1 in the IP header for probe packets.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] tos 1
```

In ICMP template view, set the ToS value to 1 in the IP header for probe packets.

```
<Sysname> system-view
[Sysname] nqa template icmp icmptplt
[Sysname-nqatplt-icmp-icmptplt] tos 1
```

transport-protocol

Use **transport-protocol** to specify the transport protocol used by the SIP operation.

Use **undo transport-protocol** to restore the default.

Syntax

transport-protocol { **tcp** | **udp** }

undo transport-protocol

Default

UDP is used.

Views

SIP template view

Predefined user roles

network-admin

context-admin

Parameters

tcp: Specifies TCP as the transport protocol.

udp: Specifies UDP as the transport protocol.

Usage guidelines

After you change the transport protocol for a SIP template, the system stops the ongoing SIP operation that uses the template and starts a new SIP operation by using the new transport protocol.

Examples

Specify TCP as the transport protocol for SIP template **siptplt**.

```
<Sysname> system-view
[Sysname] nqa template sip siptplt
[Sysname-nqatplt-sip-siptplt] transport-protocol tcp
```

ttl

Use **ttl** to set the maximum number of hops that the probe packets can traverse.

Use **undo ttl** to restore the default.

Syntax

ttl *value*

undo ttl

Default

The maximum number of hops is 30 for probe packets of the UDP tracert operation, and is 20 for probe packets of other types of operations.

Views

ICMP echo/TCP/UDP echo operation view

DLSw/DNS/FTP/HTTP/SNMP operation view

UDP tracert operation view

ICMP jitter/UDP jitter/voice operation view

DNS/FTP/HTTP/HTTPS/ICMP/IMAP/POP3/RADIUS authentication/RADIUS accounting/RTSP/SIP/SMTP/SNMP/SNMP DCA/SSL/TCP/TCP half open/UDP/WAP template view

Predefined user roles

network-admin

context-admin

Parameters

value: Specifies the TTL value in the range of 1 to 255. For the UDP tracert operation, this setting represents the maximum TTL value that can be carried in the probe packets. For other type of operations, this setting determines the maximum number of hops that the probe packets can traverse.

Usage guidelines

The **route-option bypass-route** command sets the TTL to 1 for probe packets. If you configure both the **route-option bypass-route** and **ttl** commands for an operation, the **ttl** command does not take effect.

For a successful UDP tracert operation, make sure the specified TTL value is not smaller than the value set in the **init-ttl** command.

Examples

Set the maximum number of hops to 16 for probe packets in the ICMP echo operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] ttl 16
```

In ICMP template view, set the maximum number of hops to 16 for probe packets.

```
<Sysname> system-view
[Sysname] nqa template icmp icmptplt
[Sysname-nqatplt-icmp-icmptplt] ttl 16
```

type

Use **type** to specify an NQA operation type and enter its view.

Syntax

type { **arp** | **dhcp** | **dlsw** | **dns** | **ftp** | **http** | **icmp-echo** | **icmp-jitter** | **path-jitter** | **snmp** | **tcp** | **udp-echo** | **udp-jitter** | **udp-tracert** | **voice** }

Default

No operation type is specified.

Views

NQA operation view

Predefined user roles

network-admin

context-admin

Parameters

arp: Specifies the ARP operation type.

dhcp: Specifies the DHCP operation type.

dlsw: Specifies the DLSw operation type.

dns: Specifies the DNS operation type.

ftp: Specifies the FTP operation type.

http: Specifies the HTTP operation type.

icmp-echo: Specifies the ICMP echo operation type.

icmp-jitter: Specifies the ICMP jitter operation type.

path-jitter: Specifies the path jitter operation type.

snmp: Specifies the SNMP operation type.

tcp: Specifies the TCP operation type.

udp-echo: Specifies the UDP echo operation type.

udp-jitter: Specifies the UDP jitter operation type.

udp-tracert: Specifies the UDP tracert operation type.

voice: Specifies the voice operation type.

Usage guidelines

You can specify only one type for an NQA operation. After that, you can configure the operation type-related settings for the NQA operation. To change the type of the NQA operation, remove the NQA operation in system view, and then re-create the NQA operation.

Examples

Specify FTP as the NQA operation type and enter FTP operation view.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type ftp
[Sysname-nqa-admin-test-ftp]
```

url

Use **url** to specify the URL of the destination.

Use **undo url** to restore the default.

Syntax

url *url*

undo url

Default

The destination URL is not specified.

Views

FTP/HTTP operation view

ICMP echo operation view

UDP jitter operation view

FTP/HTTP/HTTPS/RTSP/WAP template view

Predefined user roles

network-admin

context-admin

Parameters

url: Specifies the destination URL, a case-sensitive string of 1 to 255 characters.

Usage guidelines

The following table shows the URL format requirement for different NQA operations:

Operation	URL format	Default port number
HTTP operation	http://*host*/*resource* http://*host*:*port*/*resource*	80
HTTPS operation	https://host/resource https://*host*:*port*/*resource*	443
FTP operation	ftp://*host/filename* ftp://*host*:*port*/*filename*	21
ICMP echo operation	*protocol*://*host*:*port* The *host* paramter is required. The *protocol* and *port* parameters can be unspecified or any values.	N/A
UDP jitter operation	*protocol*://*host*:*port* The *host* and *port* parameters are required. The *protocol* parameter can be unspecified or any value.	N/A
RTSP operation	rtsp*://host/resource* rtsp*://host:port/resource*	554
WAP operation	http*://host/filename* http*://host:port /filename* https*://host/resource* https*://host:port/resource*	N/A

The *host* parameter in the URL represents the host name of the destination server, which must meet the following requirements:

- Case sensitive.
- Valid characters are letters, digits, hyphens (-), underscores (_), and dots (.), but consecutive dots (.) are not allowed.
- Must be a dot-separated series of labels. Each label can contain 1 to 63 characters.

The *port* parameter in the URL, if specified, represents the port number on the destination server that provides the service.

For description about the *filename* parameter, see *Fundamentals Configuration Guide*.

For the **url** command to take effect in the WAP operation, you must configured the **expect** { **data** | **hex-data** } command in WAP template view.

For the ICMP echo operation, the **url** command and the **destination ip** command are mutually exclusive.

For the UDP jitter operation, the **url** command is mutually exclusive with the **destination ip** command and the **destination port** command.

Examples

Configure the URL that the HTTP operation visits as **http://www.company.com/index.html**.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type http
[Sysname-nqa-admin-test-http] url http://www.company.com/index.html
```

In HTTP template view, configure the URL that the HTTP operation visits as **http://www.company.com/index.html**.

```
<Sysname> system-view
[Sysname] nqa template http httptplt
[Sysname-nqatplt-http-httptplt] url http://www.company.com/index.html
```

username

Use **username** to specify a username.

Use **undo username** to restore the default.

Syntax

username *username*

undo username

Default

No username is configured.

Views

FTP/HTTP operation view

FTP/HTTP/HTTPS/IMAP/POP3/RADIUS authentication/RADIUS accounting template view

Predefined user roles

network-admin

context-admin

Parameters

username: Specifies the case-sensitive username.

- The FTP, HTTP, or HTTPS username is a string of 1 to 32 characters.
- The POP3 or IMAP username is a string of 1 to 40 characters in the format of username@domain.com.
- The RADIUS authentication or accounting username is a string of 1 to 253 characters.

Examples

Set the FTP login username to **administrator**.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type ftp
[Sysname-nqa-admin-test-ftp] username administrator
```

Set the FTP login username to **administrator** in FTP template view.

```
<Sysname> system-view
[Sysname] nqa template ftp ftptplt
[Sysname-nqatplt-ftp-ftptplt] username administrator
```

Related commands

operation

password

version (HTTP/HTTPS operation view/HTTPS template view)

Use **version** to specify the version used in the HTTP or HTTPS operation.

Use **undo version** to restore the default.

Syntax

version { **v1.0** | **v1.1** }

undo version

Default

Version 1.0 is used in the HTTP operation or HTTPS operation.

Views

HTTP operation view

HTTP/HTTPS template view

Predefined user roles

network-admin

context-admin

Parameters

v1.0: Uses version 1.0.

v1.1: Uses version 1.1.

Examples

Configure the HTTP operation to use the HTTP version 1.1.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type http
[Sysname-nqa-admin-test-http] version v1.1
```

version (SNMP DCA template view)

Use **version** to specify the SNMP version used in the SNMP DCA operation.

Use **undo version** to restore the default.

Syntax

version { **v1** | **v2c** }

undo version

Default

SNMPv1 is used.

Views

SNMP DCA template view

Predefined user roles

network-admin

context-admin

Parameters

v1: Specifies SNMPv1.

v2c: Specifies SNMPv2c.

Usage guidelines

For the SNMP DCA operation to work correctly, the specified SNMP version must match the version of the SNMP agent to be monitored.

Examples

In SNMP DCA template view, set the SNMP version to SNMPv2c.

```
<Sysname> system-view
[Sysname] nqa template snmpdca test
[Sysname-nqatplt-snmpdca-test] version v2c
```

vlan

Use **vlan** to specify a VLAN for probe frames.

Use **undo vlan** to restore the default.

Syntax

vlan { *vlan-id* | **s-vid** *vlan-id* **c-vid** *vlan-id* }

undo vlan

Default

No VLAN is specified for probe frames.

Views

TWAMP Light client-session view

Predefined user roles

network-admin

context-admin

Parameters

vlan-id: Specifies a VLAN for the probe packet by its ID in the range of 1 to 4094.

s-vid: Specifies an inner VLAN ID.

c-vid: Specifies an outer VLAN ID.

Usage guidelines

After you specify a VLAN for the frame loss, throughput, or latency operation, the operation sends probe frames in the specified VLAN.

You can use this command to specify an inner VLAN ID or outer VLAN ID as needed.

Examples

Configure the TWAMP Light test to send probe frames in VLAN 3.

```
<Sysname> system-view
[Sysname] nqa twamp-light client
[Sysname-nqa-twamp-light-client] test-session 1
[Sysname-nqa-twamp-light-client-session1] vlan 3
```

vpn-instance

Use **vpn-instance** to apply the operation to a VPN instance.

Use **undo vpn-instance** to restore the default.

Syntax

vpn-instance *vpn-instance-name*

undo vpn-instance

Default

The operation is performed on the public network.

Views

ICMP echo/TCP/UDP echo operation view

ARP/DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP tracert operation view

ICMP jitter/path jitter/UDP jitter/voice operation view

TWAMP Light client-session view

Any NQA template view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance-name: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

After you specify a VPN instance, the NQA operation is performed in the specified VPN instance.

Examples

Apply the ICMP echo operation to **vpn1**.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] vpn-instance vpn1
```

In FTP template view, apply the FTP operation to **vpn1**.

```
<Sysname> system-view
[Sysname] nqa template ftp ftptplt
[Sysname-nqatplt-ftp-ftptplt] vpn-instance vpn1
```

NQA server commands

IMPORTANT:

Configure the NQA server only for UDP jitter, TCP, UDP echo, and voice operations.

display nqa server

Use **display nqa server status** to display NQA server status.

Syntax

display nqa server

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display NQA server status.

```
<Sysname> display nqa server
NQA server status: Enabled
TCP connect:
   IP address: 2.2.2.2
   Port: 2000
   ToS:200
   VPN instance: -
UDP echo:
   IP address: 3.3.3.3
   Port: 3000
   ToS: 255
   VPN instance: -
```

Table 15 Command output

Field	Description
NQA server status	Whether the NQA server is enabled.
TCP connect	Information about the TCP listening service on the NQA server.
UDP echo	Information about the UDP listening service on the NQA server.
IP address	IP address specified for the TCP/UDP listening service on the NQA server.
Port	Port number specified for the TCP/UDP listening service on the NQA server.
ToS	ToS value in reply packets sent by the NQA server.
VPN instance	Name of the VPN instance to which the IP address that the NQA server listens on belongs. This field displays a hyphen (-) if the NQA server listens on a public IP address.

display nqa twamp-light responder

Use **display nqa twamp-light responder** to display test sessions on the TWAMP Light responder.

Syntax

display nqa twamp-light responder [**test-session** *session-id*]

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB680, NFNX3-HDB1080	Yes
NFNX3-HDB1180, NFNX3-HDB1480	No

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

test-session *session-id*: Specifies a test session by its ID in the range of 1 to 256. If you do not specify this option, the command displays all test sessions on the TWAMP Light responder.

Examples

Display all test sessions on the TWAMP Light responder.

```
<Sysname> display nqa twamp-light responder
Session ID                      : 1
  Status                        : Active
  Interface                     : -
  Service instance              : -
  Destination IP                : 1.1.1.1
  Destination IPv6              : -
  Source IP                     : 2.2.2.2
  Source IPv6                   : -
  Destination port              : 2001
  Source port                   : 2010
  VPN instance                  : -
  Destination MAC               : 1-1-2
  Source MAC                    : 1-1-1
  VLAN ID                       : -
  Service VLAN ID               : -
  Customer VLAN ID              : -
  Timestamp format              : PTP
  Description                   : -
```

```
Session ID                      : 2
  Status                        : Active
  Interface                     : -
  Service instance              : -
  Destination IP                : 1.1.1.1
  Destination IPv6              : -
  Source IP                     : 3.3.3.3
  Source IPv6                   : -
  Destination port              : 2001
  Source port                   : 2020
  VPN instance                  : -
  Destination MAC               : 1-1-2
  Source MAC                    : 1-1-1
  VLAN ID                       : -
  Service VLAN ID               : -
  Customer VLAN ID              : -
  Timestamp format              : NTP
  Description                   : -
```

Table 16 Command output

Field	Description
Session ID	Test session ID.
Status	TWAMP Light responder status: • **Active**—The TWAMP Light responder is active. • **Inactive**—The TWAMP Light responder is not active.
Interface	Interface that reflects the test packets.
Service instance	Ethernet service instance bound to the interface. The Ethernet service instance on the responder must be consistent with that on the client.
Destination IP	Destination IP address in the reflected packet.
Destination IPv6	Destination IPv6 address in the reflected packet.
Source IP	Source IP address in the reflected packet.
Source IPv6	Source IPv6 address in the reflected packet.
Destination port	Destination port number in the reflected packet.
Source port	Source port number in the reflected packet.
VPN instance	MPLS L3VPN instance name.
Destination MAC	Destination MAC address in the reflected packet.
Source MAC	Source MAC address in the reflected packet.
VLAN ID	VLAN ID in the reflected packet.
Service VLAN ID	Outer VLAN ID or VLAN ID range in the reflected packet.
Customer VLAN ID	Inner VLAN ID or VLAN ID range in the reflected packet.
Timestamp format	Timestamp format: • **AUTO**—The TWAMP Light responder selects a timestamp format

	automatically if you do not set a timestamp format by using the **test-session** command. • **NTP.** • **PTP.**
Description	Description about the test session.

Related commands

nqa reflector

test-session (TWAMP Light responder view)

nqa server enable

Use **nqa server enable** to enable the NQA server.

Use **undo nqa server enable** to disable the NQA server.

Syntax

nqa server enable

undo nqa server enable

Default

The NQA server is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Examples

Enable the NQA server.

```
<Sysname> system-view
[Sysname] nqa server enable
```

nqa server tcp-connect

Use **nqa server tcp-connect** to configure a TCP listening service to enable the NQA server to listen to a port on an IP address.

Use **undo nqa server tcp-connect** to remove a TCP listening service.

Syntax

nqa server tcp-connect { *ipv4-address* | **ipv6** *ipv6-address* } *port-number* [**vpn-instance** *vpn-instance-name*] [**tos** *tos*]

undo nqa server tcp-connect { *ipv4-address* | **ipv6** *ipv6-address* } *port-number* [**vpn-instance** *vpn-instance-name*]

Default

No TCP listening services exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-address: Specifies the IPv4 address for the TCP listening service.

ipv6 *ipv6-address*: Specifies the IPv6 address for the TCP listening service.

port-number: Specifies the port number for the TCP listening service, in the range of 1 to 65535.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the NQA server listens on a public IP address.

tos *tos*: Specifies the ToS value in the IP header for reply packets. The value range is 0 to 255, and the default value is 0.

Usage guidelines

Use this command on the NQA server only for the TCP and DLSw operations. For the DLSw operation, the port number for the TCP listening service on the NQA server must be 2065. Otherwise, the DLSw operation fails.

When you configure the IP address and port number for a TCP listening service on the NQA server, follow these restrictions and guidelines:

- The IP address, port number, and VPN instance must be unique on the NQA server and match the configuration on the NQA client.
- The IP address must be the address of an interface on the NQA server.
- To ensure successful NQA operations and avoid affecting existing services, do not configure the TCP listening service on well-known ports from 1 to 1023.

Examples

Configure a TCP listening service to enable the NQA server to listen to port 9000 on the IP address 169.254.10.2.

```
<Sysname> system-view
[Sysname] nqa server tcp-connect 169.254.10.2 9000
```

Related commands

destination ip

destination port

vpn-instance

nqa server udp-echo

Use **nqa server udp-echo** to configure a UDP listening service to enable the NQA server to listen to a port on an IP address.

Use **undo nqa server udp-echo** to remove the UDP listening service created.

Syntax

nqa server udp-echo { *ipv4-address* | **ipv6** *ipv6-address* } *port-number* [**vpn-instance** *vpn-instance-name*] [**tos** *tos*]

undo nqa server udp-echo { *ipv4-address* | **ipv6** *ipv6-address* } *port-number* [**vpn-instance** *vpn-instance-name*]

Default

No UDP listening services exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-address: Specifies the IPv4 address for the UDP listening service.

ipv6 *ipv6-address*: Specifies the IPv6 address for the UDP listening service.

port-number: Specifies the port number for the UDP listening service, in the range of 1 to 65535.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the NQA server listens on a public IP address.

tos *tos*: Specifies the ToS value in the IP header for reply packets. The value range for this argument is 0 to 255, and the default value is 0.

Usage guidelines

Use this command on the NQA server only for the UDP jitter, UDP echo, and voice operations.

When you configure the IP address and port number for a UDP listening service on the NQA server, follow these restrictions and guidelines:

- The IP address, port number, and VPN instance must be unique on the NQA server and match the configuration on the NQA client.
- The IP address must be the address of an interface on the NQA server.
- To ensure successful NQA operations and avoid affecting existing services, do not configure the UDP listening service on well-known ports from 1 to 1023.

The high performance mode greatly increases the speed at which the NQA server replies to probe packets of the UDP jitter operation. However, the NQA server cannot process probe packets exceeding 100 bytes in this mode. UDP jiiter operations to the NQA server might fail if the probe packet size exceeds 100 bytes.

Examples

Configure a UDP listening service to enable the NQA server to listen to port 9000 on IP address 169.254.10.2.

```
<Sysname> system-view
[Sysname] nqa server udp-echo 169.254.10.2 9000
```

Related commands

destination ip

destination ipv6

destination port

vpn-instance

nqa twamp-light responder

Use **nqa twamp-light responder** to enable the TWAMP Light responder and enter its view, or enter the view of the enabled TWAMP Light responder.

Use **undo nqa twamp-light responder** to disable the TWAMP Light responder.

Syntax

nqa twamp-light responder

undo nqa twamp-light responder

Default

The TWAMP Light responder is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

In TWAMP Light responder view, you can create a test session to interact with the test session on the TWAMP Light client.

The **undo nqa twamp-light responder** command disables the responder and deletes all test sessions on the responder.

Examples

Enable the TWAMP Light responder and enter its view.

```
<Sysname> system-view
[Sysname] nqa twamp-light responder
[Sysname-nqa-twamp-light-responder]
```

test-session (TWAMP Light responder view)

Use **test-session** to create a test session on the TWAMP Light responder.

Use **undo test-session** to delete a test session on the TWAMP Light responder.

Syntax

test-session *session-id* [**interface** *interface-type interface-number* [**service-instance** *instance-id*]] { { **ip** | **ipv6** } **destination** *address* **source** *address* **destination-port** *port-number* **source-port** *port-number* [**vpn-instance** *vpn-instance-name*] | **destination-mac** *mac-address* **source-mac** *mac-address* } * [**vlan** { *vlan-id* | **s-vid** *vlan-id* **c-vid** *vlan-id* } | **timestamp-format** { **ntp** | **ptp** } | **description** *text*] *

undo test-session *session-id*

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB680,	Yes

Models	Command compatibility
NFNX3-HDB1080	
NFNX3-HDB1180, NFNX3-HDB1480	No

Default

No test sessions exist on the TWAMP Light responder.

Views

TWAMP Light responder view

Predefined user roles

network-admin

context-admin

Parameters

session-id: Specifies a test session by its ID. The value range is 1 to 256.

interface *interface-type interface-number*: Specifies a reflecting interface by its type and number.

service-instance *instance-id*: Specifies an Ethernet service instance by its ID, in the range of 1 to 4096.

ip: Specifies an IPv4 address.

ipv6: Specifies an IPv6 address.

destination: Specifies a destination address for the packets to be reflected.

source: Specifies a source address for the packets to be reflected.

destination-port *port-number*: Specifies a destination UDP port number for the packets to be reflected, in the range of 1 to 65535.

source-port *port-number*: Specifies a source UDP port number for the packets to be reflected, in the range of 1 to 65535.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the operation is performed on the public network.

destination-mac: Specifies a destination MAC address for the packets to be reflected.

source-mac: Specifies a source MAC address for the packets to be reflected.

mac-address: Specifies a MAC address in the format H-H-H. For example, to use 000f-00e2-0001 as the destination MAC address, set this argument to f-e2-1.

vlan: Specifies a VLAN, service VLAN ID, or customer VLAN ID for the packets to be reflected.

- *vlan-id*: Specifies a VLAN ID, in the range of 1 to 4094.
- **s-vid**: Specifies a service VLAN ID.
- **c-vid**: Specifies a customer VLAN ID.

timestamp-format: Specifies the timestamp format for the TWAMP Light responder. If you do not specify a timestamp format, the default value AUTO is used and the TWAMP Light responder selects a timestamp format automatically.

- **ntp**: Specifies the NTP format.
- **ptp**: Specifies the PTP format.

timestamp-format: Specifies the timestamp format for the TWAMP Light responder.

- **ntp**: Specifies the NTP format.
- **ptp**: Specifies the PTP format.

description *text*: Specifies a description for the test session, a case-sensitive string of 1 to 200 characters.

Usage guidelines

The test session on the TWAMP Light responder interacts with the test session on the TWAMP Light client.

The following settings specified in this command must be consistent with those on the TWAMP Light client:

- Source IP address.
- Destination IP address.
- Source UDP port number.
- Destination UDP port number.
- VPN instance name.

If the specified test session ID does not exist, this command creates a new test session. If you specify an existing session ID, you are modifying the test session.

You can specify the same interface or Ethernet service instance for different test sessions.

If you want to edit or delete the interface or Ethernet service instance in an existing reflector, you must delete the reflector and reconfigure it.

Except for the interface and Ethernet service instance, you can edit or delete other parameters.

If you do not specify any optional parameters in the **undo** command, you are deleting the test session. If all configurations about the session are deleted, the test session will be deleted.

Examples

Create a test session **test-session 1** on the TWAMP Light responder. Specify source IPv4 address 1.1.1.1, destination IPv4 address 2.2.2.2, source port 3000, destination port 3001, and VPN instance **vpn1** for the test session.

```
<Sysname> system-view
[Sysname] nqa twamp-light responder
[Sysname-nqa-twamp-light-responder] test-session 1 ip destination 2.2.2.2 source 1.1.1.1
destination-port 3001 source-port 3000 vpn-instance vpn1
```

Contents

Track commands

delay

Use **delay** to set the period of time that the Track module must wait before notifying the application module of track entry state changes.

Use **undo delay** to remove the notification delay configuration.

Syntax

delay { **negative** *negative-time* | **positive** *positive-time* } *

undo delay

Default

The Track module notifies the application module immediately when the track entry state changes.

Views

Track view

Predefined user roles

network-admin

context-admin

Parameters

negative *negative-time*: Specifies the delay for notifying the application module that the track entry state has changed to Negative. The *negative-time* argument represents the negative state notification delay in the range of 1 to 300 seconds.

positive *positive-time*: Specifies the delay for notifying the application module that the track entry state has changed to Positive. The *positive-time* argument represents the positive state notification delay in the range of 1 to 300 seconds.

Usage guidelines

If the Track module immediately notifies the application module of a track entry state change but the route convergence is not complete, a communication failure might occur. In such cases, you can set a notification delay to avoid immediate notification of track entry state changes.

The notification delay settings do not take effect if the track entry is not associated with an application module.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the negative state notification delay to 50 seconds and the positive state notification delay to 30 seconds for Boolean OR tracked list 101.

```
<Sysname> system-view
[Sysname] track 101 list boolean or
[Sysname-track-101] delay negative 50 positive 30
```

Related commands

track bfd

track interface

track interface physical

track interface protocol

track ip route reachability

track list boolean

track list threshold percentage

track list threshold weight

track nqa

display track

Use **display track** to display track entry information.

Syntax

display track { *track-entry-number* | **all** [**negative** | **positive**] } [**brief**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

track-entry-number: Specifies a track entry by its ID in the range of 1 to 1024.

all: Specifies all track entries.

negative: Displays information about track entries in Negative state.

positive: Displays information about track entries in Positive state.

brief: Displays brief information about track entries.

Examples

Display information about all track entries.

```
<Sysname> display track all
Track ID: 1
  State: Positive
  Duration: 0 days 0 hours 0 minutes 7 seconds
  Tracked object type: NQA
  Notification delay: Positive 20, Negative 30 (in seconds)
  Tracked object:
    NQA entry: admin test
    Reaction: 10
    Remote IP/URL: 2.2.2.2
    Local IP: 1.1.1.1
    Interface: GigabitEthernet1/0/1
  Tracked by:
    Track-list 6
    Track-list 7
```

```
Track ID: 2
  State: NotReady
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Tracked object type: BFD
  Notification delay: Positive 20, Negative 30 (in seconds)
  Tracked object:
    BFD session mode: Echo
    Outgoing interface: GigabitEthernet1/0/1
    VPN instance name: --
    Remote IP: 192.168.40.1
    Local IP: 192.168.40.2
Track ID: 3
  State: Negative
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Tracked object type: Interface
  Notification delay: Positive 20, Negative 30 (in seconds)
  Tracked object:
    Interface: GigabitEthernet1/0/2
    Protocol: IPv4
  Tracked by:
    Track-list 6
    Track-list 7
Track ID: 5
  State: Positive
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Tracked object type: Route
  Notification delay: Positive 20, Negative 30 (in seconds)
  Tracked object:
    IP route: 0.0.0.0/0 reachability
    VPN instance name: --
    Protocol: Static
    Nexthop interface : GigabitEthernet1/0/3
Track ID: 6
  State: Positive
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Tracked object type: Percentage threshold list
  Notification delay: Positive 20, Negative 30 (in seconds)
  Threshold: Positive 40, Negative 30
  Percentage of positive objects: 50%
  Tracked objects:
    Object 1: Positive
    Object 3: Negative
Track ID: 7
  State: Positive
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Tracked object type: Weight threshold list
  Notification delay: Positive 20, Negative 30 (in seconds)
  Threshold: Positive 50, Negative 30
```

```
  Positive weight/total weight: 50/80
  Tracked objects:
    Object 1: Positive, Weight: 50
Object 3: Negative, Weight: 30
Track ID: 8
  State: Positive
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Tracked object type: Boolean and list
  Notification delay: Positive 20, Negative 30 (in seconds)
  Tracked objects:
    Object 1: Positive
    Object 3: Negative(not)
    Object 10: NotReady(not)
```

Display brief information about track entries in Negative state.

```
<Sysname> display track all negative brief
ID   Status   Type      Remote IP/URL   Local IP        Interface
1    Negative Interface --              --              GE1/0/1
10   Negative Interface --              --              GE1/0/2
12   Negative List      --              --              --
```

Table 1 Command output

Field	Description
Track ID	ID of a track entry.
ID	ID of a track entry.
State	States of a track entry: • **Positive**—The tracked object operates correctly. • **NotReady**—The tracked object is invalid. • **Negative**—The tracked object is abnormal.
Duration	Time period during which the track entry stays in the state.
Type	Tracked object type: • **BFD Echo**—Echo-mode BFD. • **BFDStatic**—Static BFD. • **Interface**. • **Route**. • **NQA**. • **List**—Tracked list. This field is displayed only when the **`display track brief`** command is executed.

Field	Description
Tracked object type	Tracked object type: • **BFD**—Dynamic BFD. • **BFD static**—Static BFD. • **Interface**. • **Route**. • **NQA**. • **Boolean and list**—Boolean AND list. • **Boolean or list**—Boolean OR list. • **Percentage threshold list**. • **Weight threshold list**.
Notification delay: Positive 20, Negative 30 (in seconds)	• The Track module notifies the application modules that the status of the track entry changes to Positive after a delay time of 20 seconds. • The Track module notifies the application modules that the status of the track entry changes to Negative after a delay time of 30 seconds.
Threshold: Positive 40, Negative 30	Positive and negative state thresholds. This field is displayed only when the tracked object type is **Percentage threshold list** or **Weight threshold list**.
Percentage of positive objects	Percentage of Positive objects in the tracked list. This field is displayed only when the tracked object type is **Percentage threshold list**.
Positive weight/total weight: 50/80	Weight of Positive objects to the total weight of all objects in the tracked list. This field is displayed only when the tracked object type is **Weight threshold list**.
Tracked object	Tracked object associated with the track entry.
NQA entry	NQA operation associated with the track entry.
Reaction	Reaction entry associated with the track entry.
BFD session mode	BFD session mode. Only echo mode is supported.
Outgoing interface	Outgoing interface of the packets.
VPN instance name	Name of the VPN instance to which the packets belong. If the packets belong to the public network, two consecutive hyphens (--) are displayed.
Remote IP/URL	Remote IP address or URL. If no remote IP address or URL exists, two consecutive hyphens (--) are displayed.
Local IP	Local IP address. If no local IP address exists, two consecutive hyphens (--) are displayed.
Interface	Interface to be monitored. If no interface is to be monitored, two consecutive hyphens (--) are displayed.
Protocol	Link states or Layer 3 protocol states of the monitored interface: • **None**—Link status of the monitored interface. • **IPv4**—IPv4 protocol status of the monitored Layer 3 interface. • **IPv6**—IPv6 protocol status of the monitored Layer 3 interface.
IP route	Route associated with the track entry.

Field	Description
Protocol	Protocol type of the route. If the route does not exist, **N/A** is displayed.
Nexthop interface	Next hop of the route. If the route does not exist, **N/A** is displayed.
Object 10 : Positive	State of a tracked object: **Positive**, **NotReady**, or **Negative**. If the tracked object type is **Weight threshold list**, the weight of the object is also displayed. If the **(not)** attribute is displayed, the tracked list will negate the state of the object.
Tracked by	Track entries that are tracking the track entry (tracked object).
Track-list 6	Tracked list that is tracking the track entry (tracked object).

Related commands

track bfd

track interface

track interface physical

track interface protocol

track ip route reachability

track nqa

object

Use **object** to add a track entry as an object to a tracked list.

Use **undo object** to remove the object from a tracked list.

Syntax

object *track-entry-number* [**not**] [**weight** *weight*]

undo object *track-entry-number*

Default

A tracked list does not contain any objects.

Views

Track view

Predefined user roles

network-admin

context-admin

Parameters

track-entry-number: Specifies a track entry by its ID in the range of 1 to 1024.

not: Negates the state of the object. For example, the tracked list regards the object as Negative when the object is in Positive state. This keyword is supported only by a Boolean list.

weight *weight*: Assigns a weight in the range of 1 to 255 to the object. This keyword is supported only by a weight threshold list. The default weight is 10.

Usage guidelines

The track entry ID of the object cannot be the same as the ID of the tracked list to which the object is added.

You can add a maximum of 16 objects to a tracked list.

Loops between track entries are not allowed. For example, after you add track entry 1 (object 1) to tracked list 2 and track entry 2 (object 2) to tracked list 3, you cannot add track entry 3 (object 3) to tracked list 1 because a loop will be created.

Examples

Create Boolean AND list 100 and add track entries 1 and 2 as tracked objects to the list.

```
<Sysname> system-view
[Sysname] track 100 list boolean and
[Sysname-track-100] object 1
[Sysname-track-100] object 2 not
```

Related commands

track list boolean

track list threshold percentage

track list threshold weight

threshold percentage

Use **threshold percentage** to set the threshold values used to determine the state of a percentage threshold list.

Use **undo threshold percentage** to restore the default.

Syntax

threshold percentage { **negative** *negative-threshold* | **positive** *positive-threshold* } *

undo threshold percentage

Default

The negative state threshold is 0% and the positive state threshold is 1%.

Views

Track view

Predefined user roles

network-admin

context-admin

Parameters

negative *negative-threshold*: Specifies the negative state threshold in the range of 0 to 100. The percentage of Positive objects must be equal to or smaller than the configured negative state threshold for the tracked list to be set to the Negative state.

positive *positive-threshold*: Specifies the positive state threshold in the range of 0 to 100. The percentage of Positive objects must be equal to or greater than the configured positive state threshold for the tracked list to be set to the Positive state. The *positive-threshold* must be greater than the *negative-threshold.*

Usage guidelines

The state of a percentage threshold list remains unchanged if the percentage of Positive objects is below the positive state threshold and above the negative state threshold.

This command is supported only by a percentage threshold list.

Examples

Set the negative state threshold to 30% and the positive state threshold to 50% for percentage threshold list 1.

```
<Sysname> system-view
[Sysname] track 1 list threshold percentage
[Sysname-track-1] threshold percentage negative 30 positive 50
```

Related commands

track list threshold percentage

threshold weight

Use **threshold weight** to set the threshold values used to determine the state of a weight threshold list.

Use **undo threshold weight** to restore the default.

Syntax

threshold weight { **negative** *negative-threshold* | **positive** *positive-threshold* } *

undo threshold weight

Default

The negative state threshold is 0 and the positive state threshold is 1.

Views

Track view

Predefined user roles

network-admin

context-admin

Parameters

negative *negative-threshold*: Specifies the negative state threshold in the range of 0 to 255. The total weight of Positive objects must be equal to or smaller than the configured negative state threshold for the tracked list to be set to the Negative state.

positive *positive-threshold*: Specifies the positive state threshold in the range of 0 to 255. The total weight of Positive objects must be equal to or greater than the configured positive state threshold for the tracked list to be set to the Positive state. The *positive-threshold* must be greater than the *negative-threshold.*

Usage guidelines

The state of a weight threshold list remains unchanged if the total weight of Positive objects is below the positive state threshold and above the negative state threshold.

This command is supported only by a weight threshold list.

Examples

Set the negative state threshold to 30 and the positive state threshold to 50 for weight threshold list 1.

```
<Sysname> system-view
[Sysname] track 1 list threshold weight
[Sysname-track-1] threshold weight negative 30 positive 50
```

Related commands

track list threshold weight

track bfd

Use **track bfd** to create a track entry associated with a BFD session and enter track entry view, or enter the view of an existing track entry.

Use **undo track** to remove the track entry and all configurations from its view.

Syntax

track *track-entry-number* **bfd echo interface** *interface-type interface-number* **remote ip** *remote-ip-address* **local ip** *local-ip-address*

undo track *track-entry-number*

Default

No track entries exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

track-entry-number: Specifies the track entry ID in the range of 1 to 1024.

interface *interface-type interface-number*: Specifies the outgoing interface by its type and number of the BFD echo packets.

remote ip *remote-ip-address*: Specifies the destination IP address of the BFD echo packets.

local ip *local-ip-address*: Specifies the source IP address of the BFD echo packets.

Usage guidelines

To create a track entry, you must specify the tracked object type, which is **bfd** in this command.

To enter the view of an existing track entry, use the **track** *track-entry-number* command. The tracked object type is not required.

To modify the settings of a track entry, execute the **undo track** command to remove the track entry, and then create the track entry again.

When you associate Track with BFD, the virtual IP address of a VRRP group cannot be the local or remote address of a BFD session.

Examples

Associate track entry 1 with BFD to monitor the link between local IP address 192.168.40.2 and remote IP address 192.168.40.1 by sending BFD echo packets through GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] track 1 bfd echo interface gigabitethernet 1/0/1 remote ip 192.168.40.1 local ip 192.168.40.2
[Sysname-track-1]
```

Related commands

delay

display track

track interface

Use **track interface** to create a track entry associated with the link state of an interface and enter track entry view, or enter the view of an existing track entry.

Use **undo track** to remove the track entry and all configurations from its view.

Syntax

track *track-entry-number* **interface** *interface-type interface-number*

undo track *track-entry-number*

Default

No track entries exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

track-entry-number: Specifies the track entry ID in the range of 1 to 1024.

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

To create a track entry, you must specify the tracked object type, which is **interface** in this command.

To enter the view of an existing track entry, use the **track** *track-entry-number* command. The tracked object type is not required.

When you associate Track with interface management to monitor the link status of an interface, the track entry state changes as follows:

- The track entry state is Positive if the link state of the interface is up.
- The track entry state is Negative if the link state of the interface is down.

To display the link state of an interface, use the **display ip interface brief** command.

To modify the settings of a track entry, execute the **undo track** command to remove the track entry, and then create the track entry again.

Examples

Create track entry 1 and associate it with the link state of interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] track 1 interface gigabitethernet 1/0/1
```

```
[Sysname-track-1]
```

Related commands

delay

display ip interface brief (*Layer 3—IP Services Command Reference*)

display track

track interface physical

Use **track interface physical** to create a track entry associated with the physical state of an interface and enter track entry view, or enter the view of an existing track entry.

Use **undo track** to remove the track entry and all configurations from its view.

Syntax

track *track-entry-number* **interface** *interface-type interface-number* **physical**

undo track *track-entry-number*

Default

No track entries exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

track-entry-number: Specifies the track entry ID in the range of 1 to 1024.

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

To create a track entry, you must specify the tracked object type, which is **interface physical** in this command.

To enter the view of an existing track entry, use the **track** *track-entry-number* command. The tracked object type is not required.

To modify the settings of a track entry, execute the **undo track** command to remove the track entry, and then create the track entry again.

Examples

Create track entry 1 and associate it with the physical state of GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] track 1 interface gigabitethernet 1/0/1 physical
[Sysname-track-1]
```

track interface protocol

Use **track interface protocol** to create a track entry associated with the protocol state of an interface and enter track entry view, or enter the view of an existing track entry.

Use **undo track** to remove the track entry and all configurations from its view.

Syntax

track *track-entry-number* **interface** *interface-type interface-number* **protocol** { **ipv4** | **ipv6** }

undo track *track-entry-number*

Default

No track entries exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

track-entry-number: Specifies the track entry ID in the range of 1 to 1024.

interface-type interface-number: Specifies an interface by its type and number.

ipv4: Monitors the IPv4 protocol state. When the IPv4 protocol state of an interface is up, the state of the track object is Positive. When the IPv4 protocol state of an interface is down, the state of the track object is Negative. To display the IPv4 protocol state of an interface, use the **display ip interface brief** command.

ipv6: Monitors the IPv6 protocol state. When the IPv6 protocol state of an interface is up, the state of the track object is Positive. When the IPv6 protocol state of an interface is down, the state of the track object is Negative. To display the IPv6 protocol state of an interface, use the **display ipv6 interface brief** command.

Usage guidelines

To create a track entry, you must specify the tracked object type, which is **interface protocol** in this command.

To enter the view of an existing track entry, use the **track** *track-entry-number* command. The tracked object type is not required.

To modify the settings of a track entry, execute the **undo track** command to remove the track entry, and then create the track entry again.

Examples

Create track entry 1 and associate it with the IPv4 protocol state of interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] track 1 interface gigabitethernet 1/0/1 protocol ipv4
[Sysname-track-1]
```

Related commands

delay

display ip interface brief (*Layer 3—IP Services Command Reference*)

display ipv6 interface brief (*Layer 3—IP Services Command Reference*)

display track

track ip route reachability

Use **track ip route reachability** to create a track entry associated with a route entry and enter track entry view, or enter the view of an existing track entry.

Use **undo track** to remove the track entry and all configurations from its view.

Syntax

track *track-entry-number* **ip route** [**vpn-instance** *vpn-instance-name*] *ip-address* { *mask-length* | *mask* } **reachability**

undo track *track-entry-number*

Default

No track entries exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

track-entry-number: Specifies the track entry ID in the range of 1 to 1024.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, this command creates the track entry for routes on the public network.

ip-address: Specifies the IP address of the route entry associated with the track entry in dotted decimal notation.

mask-length: Specifies the mask length in the range of 0 to 32.

mask: Specifies the mask of the IP address, in dotted decimal notation.

Usage guidelines

To create a track entry, you must specify the tracked object type, which is **ip route reachability** in this command.

To enter the view of an existing track entry, use the **track** *track-entry-number* command. The tracked object type is not required.

To modify the settings of a track entry, execute the **undo track** command to remove the track entry, and then create the track entry again.

Route management does not immediately notify the Track module of the route status changes when the following conditions are met:

- An active/standby device switchover or a RIB process switchover has occurred.
- The status of the monitored route entry is changed before the routing protocol completes the graceful restart.

You can resolve the problem by configuring the nonstop routing feature.

Examples

Create track entry 1 to monitor the status of the route entry 10.1.1.0/24.

```
<Sysname> system-view
[Sysname] track 1 ip route 10.1.1.0 24 reachability
```

```
[Sysname-track-1]
```

Related commands

delay

display ip routing-table (*Layer 3—IP Routing Command Reference*)

display track

track list boolean

Use **track list boolean** to create a Boolean tracked list and enter its view, or enter the view of an existing tracked list.

Use **undo track** to remove the tracked list and all configurations from its view.

Syntax

track *track-entry-number* **list boolean** { **and** | **or** }

undo track *track-entry-number*

Default

No tracked lists exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

track-entry-number: Specifies an ID for the tracked list in the range of 1 to 1024.

and: Calculates the tracked list state by using the Boolean AND operation.

or: Calculates the tracked list state by using the Boolean OR operation.

Usage guidelines

The state of a Boolean list is determined by the tracked object states based on the Boolean AND or Boolean OR operation.

- **Boolean AND list**—The tracked list is set to the Positive state only when all objects are in Positive state. If one or more objects are in Negative state, the tracked list is set to the Negative state.
- **Boolean OR list**—The tracked list is set to the Positive state if any object is in Positive state. If all objects are in Negative state, the tracked list is set to the Negative state.

To create a track entry, you must specify the tracked object type, which is **list boolean** in this command.

To enter the view of an existing track entry, use the **track** *track-entry-number* command. The tracked object type is not required.

To modify the settings of a track entry, execute the **undo track** command to remove the track entry, and then create the track entry again.

Examples

Create Boolean OR list 101 and enter its view.

```
<Sysname> system-view
```

```
[Sysname] track 101 list boolean or
[Sysname-track-101]
```

Related commands

delay

object

track list threshold percentage

Use **track list threshold percentage** to create a percentage threshold tracked list and enter its view, or enter the view of an existing tracked list.

Use **undo track** to remove the tracked list and all configurations from its view.

Syntax

track *track-entry-number* **list threshold percentage**

undo track *track-entry-number*

Default

No tracked lists exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

track-entry-number: Specifies an ID for the tracked list in the range of 1 to 1024.

Usage guidelines

The state of a percentage threshold list is determined by comparing the percentage of Positive objects in the list with the percentage thresholds configured for the list.

To configure the threshold values used to determine the state of a percentage threshold list, use the **threshold percentage** command.

To create a track entry, you must specify the tracked object type, which is **list threshold percentage** in this command.

To enter the view of an existing track entry, use the **track** *track-entry-number* command. The tracked object type is not required.

To modify the settings of a track entry, execute the **undo track** command to remove the track entry, and then create the track entry again.

Examples

Create percentage threshold list 101 and enter its view.

```
<Sysname> system-view
[Sysname] track 101 list threshold percentage
[Sysname-track-101]
```

Related commands

delay

object

threshold percentage

track list threshold weight

Use **track list threshold weight** to create a weight threshold tracked list and enter its view, or enter the view of an existing tracked list.

Use **undo track** to remove the tracked list and all configurations from its view.

Syntax

track *track-entry-number* **list threshold weight**

undo track *track-entry-number*

Default

No tracked lists exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

track-entry-number: Specifies an ID for the tracked list in the range of 1 to 1024.

Usage guidelines

The state of a weight threshold list is determined by comparing the weight of Positive objects in the list with the weight thresholds configured for the list.

To configure the threshold values used to determine the state of a weight threshold list, use the **threshold weight** command.

To create a track entry, you must specify the tracked object type, which is **list threshold weight** in this command.

To enter the view of an existing track entry, use the **track** *track-entry-number* command. The tracked object type is not required.

To modify the settings for a track entry, execute the **undo track** command to remove the track entry, and then execute the **track list threshold weight** command again.

Examples

Create weight threshold tracked list 101 and enter its view.

```
<Sysname> system-view
[Sysname] track 101 list threshold weight
[Sysname-track-101]
```

Related commands

delay

object

threshold weight

track nqa

Use **track nqa** to create a track entry associated with the reaction entry of an NQA operation and enter track entry view, or enter the view of an existing track entry.

Use **undo track** to remove the track entry and all configurations from its view.

Syntax

track *track-entry-number* **nqa entry** *admin-name operation-tag* **reaction** *item-number*

undo track *track-entry-number*

Default

No track entries exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

track-entry-number: Specifies the track entry ID in the range of 1 to 1024.

entry *admin-name operation-tag*: Specifies the NQA operation to be associated with the track entry. The *admin-name* argument specifies the name of the NQA operation administrator who creates the NQA operation, and is a case-insensitive string of 1 to 32 characters. The *operation-tag* argument specifies the NQA operation tag, and is a case-insensitive string of 1 to 32 characters.

reaction *item-number*: Specifies the reaction entry to be associated with the track entry. The *item-number* argument is the reaction entry ID in the range of 1 to 10.

Usage guidelines

To create a track entry, you must specify the tracked object type, which is **nqa** in this command.

To enter the view of an existing track entry, use the **track** *track-entry-number* command. The tracked object type is not required.

To modify the settings of a track entry, execute the **undo track** command to remove the track entry, and then create the track entry again.

Examples

Create track entry 1 and associate it with reaction entry 3 of NQA operation **admin-test**.

```
<Sysname> system-view
[Sysname] track 1 nqa entry admin test reaction 3
[Sysname-track-1]
```

Related commands

delay

display track

Contents

BFD commands

Basic BFD commands

bfd authentication-mode

Use **bfd authentication-mode** to configure the BFD authentication mode for single-hop BFD control packets.

Use **undo bfd authentication-mode** to restore the default.

Syntax

bfd authentication-mode { **hmac-md5** | **hmac-mmd5** | **hmac-msha1** | **hmac-sha1** | **m-md5** | **m-sha1** | **md5** | **sha1** | **simple** } *key-id* { **cipher** | **plain** } *string*

undo bfd authentication-mode

Default

Single-hop BFD control packets are not authenticated.

Views

Interface view

BFD template view

Static BFD session view

Predefined user roles

network-admin

context-admin

Parameters

hmac-md5: Specifies the HMAC MD5 algorithm.

hmac-mmd5: Specifies the HMAC Meticulous MD5 algorithm.

hmac-msha1: Specifies the HMAC Meticulous SHA1 algorithm.

hmac-sha1: Specifies the HMAC SHA1 algorithm.

m-md5: Specifies the Meticulous MD5 algorithm.

m-sha1: Specifies the Meticulous SHA1 algorithm.

md5: Specifies the MD5 algorithm.

sha1: Specifies the SHA1 algorithm.

simple: Specifies the simple authentication mode.

key-id: Sets the authentication key ID in the range of 1 to 255.

cipher: Specifies a key in encrypted form.

plain: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. Its plaintext form is a case-sensitive string of 1 to 16 characters. Its encrypted form is a case-sensitive string of 33 to 53 characters.

Usage guidelines

Use this command to enhance BFD session security.

If this command is executed in static BFD session view, it takes effect only on static BFD sessions used for single-hop detection.

BFD version 0 does not support this command. The configuration does not take effect.

Examples

Configure GigabitEthernet 1/0/1 to perform simple authentication for single-hop BFD control packets, setting the authentication key ID to **1** and plaintext key to **123456**.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] bfd authentication-mode simple 1 plain 123456
```

Related commands

bfd static

bfd demand enable

Use **bfd demand enable** to enable the Demand BFD session mode.

Use **undo bfd demand enable** to restore the default.

Syntax

bfd demand enable

undo bfd demand enable

Default

The BFD session is in Asynchronous mode.

Views

Interface view

Static BFD session view

Predefined user roles

network-admin

context-admin

Usage guidelines

In Demand mode, the device periodically sends BFD control packets. If the peer end is operating in Asynchronous mode (default), the peer end stops sending BFD control packets. If the peer end is operating in Demand mode, both ends stop sending BFD control packets. As a best practice, configure the **bfd echo enable** command together with this command to detect connectivity by sending Echo packets. If the device does not receive any Echo packets from the peer end, it considers the session down.

In Asynchronous mode, the device periodically sends BFD control packets. The device considers that the session is down if it does not receive any BFD control packets within a specific interval.

If this command is executed in static BFD session view, it takes effect only on static BFD sessions used for single-hop detection.

BFD version 0 does not support this command. The configuration does not take effect.

Examples

Enable the Demand BFD session mode on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] bfd demand enable
```

Related commands

bfd echo enable

bfd detect-interface first-fail-timer

Use **bfd detect-interface first-fail-timer** to configure the timer that delays reporting the first BFD session establishment failure to the data link layer.

Use **undo bfd detect-interface first-fail-timer** to restore the default.

Syntax

bfd detect-interface first-fail-timer *seconds*

undo bfd detect-interface first-fail-timer

Default

The first BFD session establishment failure is not reported to the data link layer.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies the timeout time that reports the first BFD session establishment failure to the data link layer. The value range for this argument is 1 to 10000 seconds.

Usage guidelines

If the BFD session fails to be established when the timer expires, BFD reports the failure to the data link layer and sets the data link layer state of the interface to DOWN(BFD). This behavior rapidly identifies the interfaces for which BFD sessions fail to be established. In this case, the BFD session state is displayed as Down in the **display bfd session** command output. The line protocol state of the interface is displayed as DOWN(BFD) in the **display interface** command output.

If you execute the **bfd detect-interface source-ip** command on the local end, the BFD session for detecting the local interface state fails to be established when the following conditions exist:

- The **bfd detect-interface source-ip** command is not executed on the remote end.
- The local and remote ends have mismatching BFD authentication settings.

Examples

Configure the timer that delays reporting the first BFD session establishment failure as 10 seconds for GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] bfd detect-interface first-fail-timer 10
```

Related commands

bfd detect-interface source-ip

display interface (*Interface Command Reference*)

bfd detect-interface source-ip

Use **bfd detect-interface source-ip** to associate the interface state with BFD and specify the source IP address for BFD control packets.

Use **undo bfd detect-interface** to remove the association between the interface state and BFD.

Syntax

bfd detect-interface source-ip *ip-address* [**discriminator local** *local-value* **remote** *remote-value*] [**template** *template-name*]

undo bfd detect-interface

Default

The interface state is not associated with BFD. BFD does not set the link layer protocol of the interface to DOWN(BFD) state when detecting a failure.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the source IP address for BFD control packets, in dotted decimal notation.

discriminator: Specifies BFD session discriminators. If you do not specify discriminators, the device obtains BFD session discriminators through autonegotiation.

local *local-value*: Specifies the local discriminator. The value range for the *local-value* argument is 1 to 32768.

remote *remote-value*: Specifies the remote discriminator in the range of 1 to 4294967295.

template *template-name*: Specifies a template by its name, a case-sensitive string of 1 to 63 characters. If you specify a nonexistent template or do not specify a template, the BFD session uses the BFD parameters configured in interface view. If you first specify a nonexistent template and then create the template, the BFD session uses the parameters configured in the template.

Usage guidelines

By creating a BFD session for single-hop detection through exchange of BFD control packets, this feature implements fast link detection. When BFD detects a link fault, it sets the link layer protocol state to DOWN(BFD). This behavior helps applications relying on the link layer protocol state achieve fast convergence.

The source IP address of control packets is specified manually, and the destination IP address is fixed at 224.0.0.184. As a best practice, specify the IP address of the interface as the source IP address. If the interface does not have an IP address, specify a unicast IP address other than 0.0.0.0 as the source IP address.

You can associate the state of the following interfaces with BFD:

- Layer 3 Ethernet interfaces and subinterfaces. For BFD detection to take effect, do not execute this command on both a Layer 3 Ethernet interface and its subinterface.
- Layer 3 aggregate interfaces, Layer 3 aggregate subinterfaces, and member ports (Layer 3 Ethernet interfaces only) in a Layer 3 aggregation group.

To configure this command on the preceding interfaces at the same time, you must manually specify the local and remote discriminators on each of the interfaces. As a best practice, do not configure this command on these interfaces at the same time.

- VLAN interfaces.

If the peer device does not support obtaining BFD session discriminators through autonegotiation, you must specify the discriminators on both the local and peer devices. Without the discriminators, the BFD session cannot come up.

The BFD session discriminators must match on the local and peer devices. For example, if you configure **bfd detect-interface source-ip** 20.1.1.1 **discriminator local** 513 **remote** 514 on the local device, you must configure **bfd detect-interface source-ip** 20.1.1.2 **discriminator local** 514 **remote** 513 on the peer device.

The local discriminators of BFD sessions for interfaces on the same device must be different.

To modify your configuration, remove it by using the **undo** form of the command and then execute the **bfd detect-interface source-ip** command again.

The echo function does not take effect on BFD sessions associated with interface states.

If you specify an existing template for this command, the **bfd demand enable** command cannot take effect.

Examples

Associate GigabitEthernet 1/0/1 with BFD to detect the interface state, and specify the source IP address as 20.1.1.1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] bfd detect-interface source-ip 20.1.1.1
```

Related commands

bfd demand enable

bfd echo enable

bfd template

bfd detect-interface special-processing

Use **bfd detect-interface special-processing** to enable special processing for BFD sessions.

Use **undo bfd detect-interface special-processing** to disable special processing for BFD sessions.

Syntax

bfd detect-interface special-processing [**admin-down** | **authentication-change** | **session-up**] *

undo bfd detect-interface special-processing [**admin-down** | **authentication-change** | **session-up**] *

Default

All types of special processing for BFD sessions are disabled.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

admin-down: Notifies a session down event to the data link layer upon receipt of a BFD packet with the State field as AdminDown. This keyword helps rapidly discover interfaces on which BFD sessions are manually shut down. If you do not specify this keyword, the device sets the BFD session state to Down, but does not notify the session down event to the data link layer.

authentication-change: Immediately sets the session to down state upon a local authentication information change. This keyword helps rapidly discover interfaces with authentication information changes. If you do not specify this keyword, the device sets the session to down state if authentication information inconsistency still persists after a period of time.

session-up: Ignores authentication information inconsistency when the local session is up. If a large number of BFD sessions exist, examining authentication information consistency affects device performance. If you do not specify this keyword, the device examines authentication information in incoming BFD packets when the local session state is up. If the authentication information does not match on the two ends, the BFD session is declared down.

Usage guidelines

If you do not specify any parameters, this command enables or disables all types of special processing.

Examples

Enable all types of special processing for BFD sessions on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] bfd detect-interface special-processing admin-down
authentication-change session-up
```

bfd detect-multiplier

Use **bfd detect-multiplier** to set the single-hop detection time multiplier for control packet mode and echo packet mode.

Use **undo bfd detect-multiplier** to restore the default.

Syntax

bfd detect-multiplier *value*

undo bfd detect-multiplier

Default

The single-hop detection time multiplier is 5 for control packet mode and echo packet mode.

Views

Interface view

BFD template view

Static BFD session view

Predefined user roles

network-admin

context-admin

Parameters

value: Specifies a detection time multiplier. The value range for this argument is 3 to 50.

Usage guidelines

The detection time multiplier determines the maximum number of concurrent BFD packets (including control packets and echo packets) that can be discarded.

Table 1 Detection interval calculation method

Mode	Detection interval
Echo packet mode	Detection time multiplier of the sender × actual packet sending interval of the sender
Control packet mode BFD session in asynchronous mode	Detection time multiplier of the receiver × actual packet sending interval of the receiver
Control packet mode BFD session in demand mode	Detection time multiplier of the sender × actual packet sending interval of the sender

If this command is executed in static BFD session view, it takes effect only on static BFD sessions used for single-hop detection.

Examples

Set the single-hop detection time multiplier for control packet mode and the detection time multiplier for echo packet mode to 6 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] bfd detect-multiplier 6
```

bfd echo enable

Use **bfd echo enable** to enable the echo function.

Use **undo bfd echo enable** to disable the echo function.

Syntax

bfd echo [**receive** | **send**] **enable**

undo bfd echo [**receive** | **send**] **enable**

Default

The echo function is disabled.

Views

Interface view

Static BFD session view

Predefined user roles

network-admin

context-admin

Parameters

receive: Specifies the echo packet receiving capability.

send: Specifies the echo packet sending capability.

Usage guidelines

If you enable the echo function for a BFD session in which control packets are sent and the session comes up, BFD performs the following operations:

- Periodically sends echo packets to detect link connectivity.
- Decreases the control packet receiving rate at the same time.

To enable only the echo packet receiving capability, use the **bfd echo receive enable** command.

To enable only the echo packet sending capability, use the **bfd echo send enable** command.

If you do not specify the **receive** or **send** keyword, the command enables both the echo packet receiving and sending capabilities.

The echo function does not take effect on BFD sessions associated with interface states.

The echo function does not take effect on control-mode BFD sessions established with IPv6 link-local addresses.

If this command is executed in static BFD session view, it takes effect only on static BFD sessions used for single-hop detection.

BFD version 0 does not support this command. The configuration does not take effect.

Examples

Enable the echo function on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] bfd echo enable
```

bfd echo-source-ip

Use **bfd echo-source-ip** to configure the source IP address of BFD echo packets.

Use **undo bfd echo-source-ip** to remove the configured source IP address of BFD echo packets.

Syntax

bfd echo-source-ip *ip-address*

undo bfd echo-source-ip

Default

No source IP address is configured for BFD echo packets.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the source IP address of BFD echo packets. The source IP address must be a valid unicast IPv4 address in dotted decimal notation.

Usage guidelines

Make sure the source IP address is not on the same network segment as any local interfaces. This avoids the following situations:

- A large number of ICMP redirect packets might be sent from the peer, resulting in link congestion.
- With malformed packet attack detection and prevention enabled, the local end might filter echo packets sent from the peer as malformed packets, resulting in BFD session establishment failure. For more information about malformed packet attack detection and prevention, see attack detection and prevention in *Security Configuration Guide*.

Examples

Configure the source IP address of BFD echo packets as 8.8.8.8.

```
<Sysname> system-view
[Sysname] bfd echo-source-ip 8.8.8.8
```

bfd echo-source-ipv6

Use **bfd echo-source-ipv6** to configure the source IPv6 address of BFD echo packets.

Use **undo bfd echo-source-ipv6** to remove the configured source IPv6 address of BFD echo packets.

Syntax

bfd echo-source-ipv6 *ipv6-address*

undo bfd echo-source-ipv6

Default

No source IPv6 address is configured for BFD echo packets.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address: Specifies the source IPv6 address for BFD echo packets.

Usage guidelines

The source IPv6 address of echo packets can only be a global unicast address.

Make sure the source IPv6 address is not on the same network segment as any local interfaces. This avoids the following situations:

- A large number of ICMPv6 redirect packets might be sent from the peer, resulting in link congestion.
- With malformed packet attack detection and prevention enabled, the local end might filter echo packets sent from the peer as malformed packets, resulting in BFD session establishment failure. For more information about malformed packet attack detection and prevention, see attack detection and prevention in *Security Configuration Guide*.

Examples

Configure the source IPv6 address of BFD echo packets as 80::2.

```
<Sysname> system-view
[Sysname] bfd echo-source-ipv6 80::2
```

bfd init-fail timer

Use **bfd init-fail-timer** to set the delay timer for BFD to notify upper-layer protocols of session establishment failures.

Use **undo bfd init-fail-timer** to restore the default.

Syntax

bfd init-fail-timer *seconds*

undo bfd init-fail-timer

Default

BFD does not notify upper-layer protocols of session establishment failures.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies the delay time in the range of 5 to 600 seconds. After the delay time, BFD notifies the upper-layer protocol of session establishment failures.

Usage guidelines

CAUTION:

For session establishment failures caused by configuration mismatches at the two ends, this command can cause the upper-layer protocol to act incorrectly. Therefore, use this command with caution. BFD status mismatch and BFD authentication configuration mismatch are examples of configuration mismatches.

This command takes effect only for control packet mode.

In some cases, for an upper-layer protocol to act correctly, BFD must notify the upper-layer protocol of session establishment failures.

Examples

Set the delay timer to 10 seconds for BFD to notify upper-layer protocols of session establishment failures.

```
<Sysname> system-view
[Sysname] bfd init-fail-timer 10
```

bfd min-echo-receive-interval

Use **bfd min-echo-receive-interval** to set the minimum interval for receiving BFD echo packets.

Use **undo bfd min-echo-receive-interval** to restore the default.

Syntax

bfd min-echo-receive-interval *interval*

undo bfd min-echo-receive-interval

Default

The minimum interval for receiving BFD echo packets is 400 milliseconds.

Views

Interface view

BFD template view

Static BFD session view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies the minimum interval for receiving BFD echo packets, in milliseconds. The value takes 0 or is in the range of 100 to 1000.

Usage guidelines

This command sets the BFD echo packet receiving interval, which is the actual BFD echo packet sending interval.

The local end stops sending echo packets after autonegotiation with the remote end if the following conditions are met:

- The echo function is enabled on the local end.
- The minimum interval for receiving BFD echo packets is set to 0 milliseconds on the remote end.

If this command is executed in static BFD session view, it takes effect only on static BFD sessions used for single-hop detection.

Examples

Set the minimum interval for receiving BFD echo packets to 500 milliseconds on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] bfd min-echo-receive-interval 500
```

bfd min-receive-interval

Use **bfd min-receive-interval** to set the minimum interval for receiving single-hop BFD control packets.

Use **undo bfd min-receive-interval** to restore the default.

Syntax

bfd min-receive-interval *interval*

undo bfd min-receive-interval

Default

The minimum interval for receiving single-hop BFD control packets is 400 milliseconds.

Views

Interface view

BFD template view

Static BFD session view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies the minimum interval for receiving single-hop BFD control packets, in milliseconds. The value range for this argument is 100 to 1000.

Usage guidelines

Use this command to prevent the control packet sending rate of the peer end from exceeding the control packet receiving rate of the local end.

The actual control packet sending interval of the peer end takes the greater value between the following values:

- Minimum interval for transmitting BFD control packets on the peer end.
- Minimum interval for receiving BFD control packets on the local end.

If this command is executed in static BFD session view, it takes effect only on static BFD sessions used for single-hop detection.

Examples

Set the minimum interval for receiving single-hop BFD control packets to 500 milliseconds on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] bfd min-receive-interval 500
```

bfd min-transmit-interval

Use **bfd min-transmit-interval** to set the minimum interval for transmitting single-hop BFD control packets.

Use **undo bfd min-transmit-interval** to restore the default.

Syntax

bfd min-transmit-interval *interval*

undo bfd min-transmit-interval

Default

The minimum interval for transmitting single-hop BFD control packets is 400 milliseconds.

Views

Interface view

BFD template view

Static BFD session view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies the minimum interval for transmitting single-hop BFD control packets, in milliseconds. The value range for this argument is 100 to 1000.

Usage guidelines

Use this command to prevent the BFD packet sending rate from exceeding the device capability.

The actual BFD control packet transmitting interval on the local end is the greater value between the following values:

- Minimum interval for transmitting BFD control packets on the local end.
- Minimum interval for receiving BFD control packets on the peer end.

If this command is executed in static BFD session view, it takes effect only on static BFD sessions used for single-hop detection.

Examples

Set the minimum interval for transmitting single-hop BFD control packets to 500 milliseconds on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] bfd min-transmit-interval 500
```

bfd multi-hop authentication-mode

Use **bfd multi-hop authentication-mode** to configure the authentication mode for multihop BFD control packets.

Use **undo bfd multi-hop authentication-mode** to restore the default.

Syntax

bfd multi-hop authentication-mode { **hmac-md5** | **hmac-mmd5** | **hmac-msha1** | **hmac-sha1** | **m-md5** | **m-sha1** | **md5** | **sha1** | **simple** } *key-id* { **cipher** | **plain** } *string*

undo bfd multi-hop authentication-mode

Default

No authentication is performed.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

hmac-md5: Specifies the HMAC MD5 algorithm.

hmac-mmd5: Specifies the HMAC Meticulous MD5 algorithm.

hmac-msha1: Specifies the HMAC Meticulous SHA1 algorithm.

hmac-sha1: Specifies the HMAC SHA1 algorithm.

m-md5: Specifies the Meticulous MD5 algorithm.

m-sha1: Specifies the Meticulous SHA1 algorithm.

md5: Specifies the MD5 algorithm.

sha1: Specifies the SHA1 algorithm.

simple: Specifies the simple authentication mode.

key-id: Sets the authentication key ID in the range of 1 to 255.

cipher: Specifies a key in encrypted form.

plain: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. Its plaintext form is a case-sensitive string of 1 to 16 characters. Its encrypted form is a case-sensitive string of 33 to 53 characters.

Usage guidelines

Use this command to enhance BFD session security.

BFD version 0 does not support this command. The configuration does not take effect.

Examples

Configure the simple authentication mode for multihop BFD control packets, setting the authentication key ID to 1 and key to **123456**.

```
<Sysname> system-view
[Sysname] bfd multi-hop authentication-mode simple 1 plain 123456
```

bfd multi-hop destination-port

Use **bfd multi-hop destination-port** to configure the destination port number for multihop BFD control packets.

Use **undo bfd multi-hop destination-port** to restore the default.

Syntax

bfd multi-hop destination-port *port-number*

undo bfd multi-hop destination-port

Default

The destination port number for multihop BFD control packets is 4784.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

port-number: Specifies the destination port number of multihop BFD control packets, 3784 or 4784.

Usage guidelines

IANA assigned port number 4784 to BFD for multihop BFD detection in control packet mode. By default, NSFOCUS devices use 4784 as the destination port number for multihop BFD control packets, while devices from other vendors might use 3784. To avoid BFD session establishment failures, make sure the devices on both ends of the BFD session use the same destination port number for multihop BFD control packets.

This command applies to only new multihop BFD sessions in control packet mode.

Examples

Specify the destination port number for multihop BFD control packets as 3784.

```
<Sysname> system-view
[Sysname] bfd multi-hop destination-port 3784
```

bfd multi-hop detect-multiplier

Use **bfd multi-hop detect-multiplier** to set the multihop detection time multiplier for control packet mode and echo packet mode.

Use **undo bfd multi-hop detect-multiplier** to restore the default.

Syntax

bfd multi-hop detect-multiplier *value*

undo bfd multi-hop detect-multiplier

Default

The multihop detection time multiplier is 5 for control packet mode and echo packet mode.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

value: Specifies the multihop detection time multiplier in the range of 3 to 50.

Usage guidelines

The detection time multiplier determines the maximum number of concurrent BFD control packets that can be discarded.

Table 2 Detection interval calculation method

Mode	Detection interval
Echo packet mode	Detection time multiplier of the sender × actual packet sending interval of the sender
Control packet mode BFD session in asynchronous mode	Detection time multiplier of the receiver × actual packet sending interval of the receiver
Control packet mode BFD session in demand mode	Detection time multiplier of the sender × actual packet sending interval of the sender

Examples

Set the multihop detection time multiplier to 6.

```
<Sysname> system-view
[Sysname] bfd multi-hop detect-multiplier 6
```

bfd multi-hop min-echo-receive-interval

Use **bfd multi-hop min-echo-receive-interval** to set the minimum interval for receiving multihop BFD echo packets.

Use **undo bfd multi-hop min-echo-receive-interval** to restore the default.

Syntax

bfd multi-hop min-echo-receive-interval *interval*

undo bfd multi-hop min-echo-receive-interval

Default

The minimum interval for receiving multihop BFD echo packets is 400 milliseconds.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies the minimum interval for receiving multihop BFD echo packets, in milliseconds. The value takes 0 or is in the range of 100 to 1000.

Usage guidelines

The interval for receiving multihop BFD echo packets is also the interval for sending multihop BFD echo packets. By executing this command, you can control both the receiving interval and sending interval for multihop BFD echo packets.

This command takes effect only on static BFD sessions for multihop detection with echo packets.

Examples

Set the minimum interval for receiving multihop BFD echo packets to 500 milliseconds.

```
<Sysname> system-view
[Sysname] bfd multi-hop min-echo-receive-interval 500
```

Related commands

bfd static

bfd multi-hop min-receive-interval

Use **bfd multi-hop min-receive-interval** to set the minimum interval for receiving multihop BFD control packets.

Use **undo bfd multi-hop min-receive-interval** to restore the default.

Syntax

bfd multi-hop min-receive-interval *interval*

undo bfd multi-hop min-receive-interval

Default

The minimum interval for receiving multihop BFD control packets is 400 milliseconds.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies the minimum interval for receiving multihop BFD control packets, in milliseconds. The value range for this argument is 100 to 1000.

Usage guidelines

Use this command to prevent the packet sending rate of the peer end from exceeding the packet receiving capability (minimum control packet receiving interval) of the local end. If the receiving capability is exceeded, the peer end dynamically adjusts the BFD control packet sending interval to the minimum control packet receiving interval of the local end.

Examples

Set the minimum interval for receiving multihop BFD control packets to 500 milliseconds.

```
<Sysname> system-view
[Sysname] bfd multi-hop min-receive-interval 500
```

bfd multi-hop min-transmit-interval

Use **bfd multi-hop min-transmit-interval** to set the minimum interval for transmitting multihop BFD control packets.

Use **undo bfd multi-hop min-transmit-interval** to restore the default.

Syntax

bfd multi-hop min-transmit-interval *interval*

undo bfd multi-hop min-transmit-interval

Default

The minimum interval for transmitting multihop BFD control packets is 400 milliseconds.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies the minimum interval for transmitting multihop BFD control packets, in milliseconds. The value range for this argument is 100 to 1000.

Usage guidelines

Use this command to prevent the BFD packet sending rate from exceeding the device capability.

The actual BFD control packet transmitting interval on the local end is the greater value between the following values:

- Minimum interval for transmitting BFD control packets on the local end.
- Minimum interval for receiving BFD control packets on the peer end.

Examples

Set the minimum interval for transmitting multihop BFD control packets to 500 milliseconds.

```
<Sysname> system-view
[Sysname] bfd multi-hop min-transmit-interval 500
```

bfd session init-mode

Use **bfd session init-mode** to configure the mode for establishing a BFD session.

Use **undo bfd session init-mode** to restore the default.

Syntax

bfd session init-mode { **active** | **passive** }

undo bfd session init-mode

Default

BFD uses the **active** mode.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

active: Specifies the active mode. In active mode, BFD actively transmits BFD control packets to the remote device, regardless of whether it receives a BFD control packet from the remote device.

passive: Specifies the passive mode. In passive mode, BFD does not actively transmit a BFD control packet to the remote end; it transmits a BFD control packet only after receiving a BFD control packet from the remote end.

Usage guidelines

A minimum of one end must operate in active mode for a BFD session to be established.

BFD version 0 does not support this command. The configuration does not take effect.

Examples

Configure the session establishment mode as **passive**.

```
<Sysname> system-view
[Sysname] bfd session init-mode passive
```

bfd static

Use **bfd static** to create a static BFD session and enter its view, or enter the view of an existing static BFD session.

Use **undo bfd static** to delete a static BFD session and all its settings.

Syntax

Static BFD session for single-hop detection with IPv4 control packets:

bfd static *session-name* [**peer-ip** *ipv4-address* **interface** *interface-type interface-number* **source-ip** *ipv4-address* **discriminator local** *local-value* **remote** *remote-value*]

undo bfd static *session-name*

Static BFD session for multihop detection with IPv4 control packets:

bfd static *session-name* [**peer-ip** *ipv4-address* [**vpn-instance** *vpn-instance-name*] **source-ip** *ipv4-address* **discriminator local** *local-value* **remote** *remote-value*]

undo bfd static *session-name*

Static BFD session for single-hop detection with IPv4 echo packets:

bfd static *session-name* [**peer-ip** *ipv4-address* **interface** *interface-type interface-number* **destination-ip** *ipv4-address* [**source-ip** *ipv4-address*] **one-arm-echo discriminator** { **local** *local-value* | **auto** }]

undo bfd static *session-name*

Static BFD session for multihop detection with IPv4 echo packets:

bfd static *session-name* [**peer-ip** *ipv4-address* [**vpn-instance** *vpn-instance-name*] **destination-ip** *ipv4-address* [**source-ip** *ipv4-address*] **one-arm-echo discriminator** { **local** *local-value* | **auto** }]

undo bfd static *session-name*

Static BFD session for single-hop detection with IPv6 control packets:

bfd static *session-name* [**peer-ipv6** *ipv6-address* **interface** *interface-type interface-number* **source-ipv6** *ipv6-address* **discriminator local** *local-value* **remote** *remote-value*]

undo bfd static *session-name*

Static BFD session for multihop detection with IPv6 control packets:

bfd static *session-name* [**peer-ipv6** *ipv6-address* [**vpn-instance** *vpn-instance-name*] **source-ipv6** *ipv6-address* **discriminator local** *local-value* **remote** *remote-value*]

undo bfd static *session-name*

Static BFD session for single-hop detection with IPv6 echo packets:

bfd static *session-name* [**peer-ipv6** *ipv6-address* **interface** *interface-type interface-number* **destination-ipv6** *ipv6-address* [**source-ipv6** *ipv6-address*] **one-arm-echo discriminator** { **local** *local-value* | **auto** }]

undo bfd static *session-name*

Static BFD session for multihop detection with IPv6 echo packets:

bfd static *session-name* [**peer-ipv6** *ipv6-address* [**vpn-instance** *vpn-instance-name*] **destination-ipv6** *ipv6-address* [**source-ipv6** *ipv6-address*] **one-arm-echo discriminator** { **local** *local-value* | **auto** }]

undo bfd static *session-name*

Static BFD session for single-hop detection with IPv4 echo packets (the peer address is fixed at 224.0.0.184):

bfd static *session-name* [**peer-ip default-ip interface** *interface-type interface-number* **source-ip** *ip-address* **discriminator local** *discr-value* **remote** *discr-value*]

undo bfd static *session-name*

Default

No static BFD sessions exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

session-name: Specifies a static BFD session name, a case-sensitive string of 1 to 64 characters.

peer-ip *ipv4-address*: Specifies the peer IPv4 address in dotted decimal notation. It must be a valid unicast IPv4 address. For a static BFD session in control packet mode, the peer IPv4 address and the source IPv4 address determine the path to be detected. For a static BFD session in echo packet mode, the peer IPv4 address and the destination IPv4 address determine the path to be detected.

peer-ipv6 *ipv6-address*: Specifies the peer IPv6 address. For a static BFD session in control packet mode, the peer IPv6 address and the source IPv6 address determine the path to be detected. For a static BFD session in echo packet mode, the peer IPv6 address and the destination IPv6 address determine the path to be detected.

default-ip: Specifies the peer IPv4 address as 224.0.0.184.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the static BFD session belongs to the public network.

interface *interface-type interface-number*: Specifies an interface by its type and number. BFD uses the specified interface as the outgoing interface for outgoing packets.

destination-ip *ipv4-address*: Specifies the destination IPv4 address for echo packets, in dotted decimal notation. It must be a valid unicast IPv4 address of the local end.

destination-ipv6 *ipv6-address*: Specifies the destination IPv6 address for echo packets. It must be the IPv6 address of the local end.

source-ip *ipv4-address*: Specifies the source IPv4 address for BFD packets, in dotted decimal notation. It must be a valid unicast IPv4 address.

source-ipv6 *ipv6-address*: Specifies the source IPv6 address for BFD packets.

one-arm-echo: Specifies the static BFD session mode as echo packet mode.

discriminator: Specifies BFD session discriminators.

local *local-value*: Specifies the local discriminator in the range of 1 to 32768.

remote *remote-value*: Specifies the remote discriminator in the range of 1 to 4294967295.

auto: Enables the device to automatically assign local discriminator values to static BFD sessions.

Usage guidelines

By working with Track, a static BFD session can provide fast failure detection. For more information about Track association with BFD, see Track in *Network Management and Monitoring Configuration Guide*.

If a static BFD session in control packet mode is created on the peer device, you must use this command to create a static BFD session on the local device. The BFD session discriminators must match on the local and peer devices. For example, if you configure **bfd static** abc **peer-ip** 20.1.1.1 **vpn-instance** vpn1 **source-ip** 20.1.1.2 **discriminator local** 513 **remote** 514 on the local device, you must configure **bfd static** bcd **peer-ip** 20.1.1.2 **vpn-instance** vpn1 **source-ip** 20.1.1.1 **discriminator local** 514 **remote** 513 on the peer device.

When creating a static BFD session, you must specify a peer IP address. The system checks only the format of the IP address but not its correctness. If the peer IPv4 or IPv6 address is incorrect, the static BFD session cannot be established.

You need to create a static BFD session on only the local device if you use the echo packet mode to perform detection. As a best practice, specify the source IP address for echo packets when creating a static BFD session. Make sure the specified source IP address does not belong to the subnet where a local interface resides. Without a source IP address specified, the device uses the IP address specified in the **bfd echo-source-ip** or **bfd echo-source-ipv6** command as the source IP address of echo packets.

To use a static BFD session in control packet for single-hop detection, you must perform the following configuration:

- Specify the IP address of the peer interface for the **peer-ip**/**peer-ipv6** parameter.
- Specify the IP address of the local interface for the **source-ip**/**source-ipv6** parameter.

The **bfd static** *session-name* command without any parameters specified can only be used to enter the view of an existing static BFD session.

To modify a static BFD session, delete it and then configure a new static BFD session.

If you do not specify a VPN instance or an interface, the device performs multihop detection in the public network.

To detect network layer connectivity, execute the following commands:

- **bfd static** *session-name* **peer-ip** *ipv4-address* **interface** *interface-type interface-number* **source-ip** *ipv4-address* **discriminator local** *local-value* **remote** *remote-value*

  For the static BFD session to be successfully established, make sure the IPv4 addresses of the local and peer interfaces where the static BFD session resides are used as the source and peer IPv4 addresses, respectively.
- **bfd static** *session-name* **peer-ipv6** *ipv6-address* **interface** *interface-type interface-number* **source-ipv6** *ipv6-address* **discriminator local** *local-value* **remote** *remote-value*

  For the static BFD session to be successfully established, make sure the IPv6 addresses of the local and peer interfaces where the static BFD session resides are used as the source and peer IPv6 addresses, respectively.

To detect data link layer connectivity, execute the following command:

- **bfd static** *session-name* **peer-ip default-ip interface** *interface-type interface-number* **source-ip** *ip-address* **discriminator local** *discr-value* **remote** *discr-value*

  If the **process-interface-status** command is also executed, BFD sets the interface state to DOWN(BFD) when detecting a link failure. Specify the IP address of the interface as the source IP address. If the interface does not have an IP address, specify a unicast IP address other than 0.0.0.0 as the source IP address. An interface can use only one static BFD session to detect data link layer connectivity.

For a static BFD session in control packet mode, the source IP address of BFD packets is the IP address specified for the **source-ip**/**source-ipv6** keyword, and the destination IP address is the IP address specified for the **peer-ip**/**peer-ipv6** keyword.

For a static BFD session in echo packet mode, the source IP address of BFD packets is the IP address specified for the **source-ip**/**source-ipv6** keyword, and the destination IP address is the IP address specified for the **destination-ip**/**destination-ipv6** keyword.

BFD supports detecting data link connectivity for the following interface types:

- Layer 3 Ethernet interfaces and subinterfaces. For BFD detection to take effect, do not execute this command on both a Layer 3 Ethernet interface and its subinterface.

- Layer 3 aggregate interfaces, Layer 3 aggregate subinterfaces, and member ports in a Layer 3 aggregation group. For BFD detection to take effect, do not execute this command on any two of the interface types at the same time.
- VLAN interfaces.

Different static BFD sessions cannot have the same local discriminator.

Examples

Create a static BFD session and enter its view. The static BFD session detects the path between 1.1.1.1 and 1.1.1.2 and uses GigabitEthernet 1/0/1 to send BFD packets with source IP address 1.1.1.1 and destination IP address is 1.1.1.2. The local discriminator is 1537, and the remote discriminator is 2048.

```
<Sysname> system-view
[Sysname] bfd static aaaa peer-ip 1.1.1.2 interface gigabitethernet 1/0/1 source-ip
1.1.1.1 discriminator local 1537 remote 2048
[Sysname-bfd-static-session-abc]
```

Create a static BFD session and enter its view. The static BFD session detects the path between 1.1.1.1 and 1.1.1.2 and uses GigabitEthernet 1/0/1 to send BFD packets with source IP address 9.9.9.9 and destination IP address is 1.1.1.2.

```
<Sysname> system-view
[Sysname] bfd static abc peer-ip 1.1.1.1 interface gigabitethernet 1/0/1 destination-ip
1.1.1.2 source-ip 9.9.9.9 one-arm-echo discriminator auto
[Sysname-bfd-static-session-abc]
```

Related commands

bfd echo-source-ip

process-interface-status

bfd template

Use **bfd template** to create a BFD template and enter its view, or enter the view of an existing BFD template.

Use **undo bfd template** to delete the BFD template.

Syntax

bfd template *template-name*

undo bfd template *template-name*

Default

No BFD templates exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

template-name: Specifies the template name, a case-sensitive string of 1 to 63 characters.

Examples

Create BFD template **bfd1** and enter BFD template view.

```
<Sysname> system-view
[Sysname] bfd template bfd1
[Sysname-bfd-template-bfd1]
```

display bfd session

Use **display bfd session** to display BFD session information.

Syntax

display bfd session [**discriminator local** *local-value* | **static name** *session-name* | **verbose**]

display bfd session [[**dynamic**] [**control** | **echo**] [**ip**] [**state** { **down** | **admin-down** | **init** | **up** }] [**discriminator remote** *remote-value*] [**peer-ip** *ipv4-address* [**vpn-instance** *vpn-instance-name*]] [**verbose**]]

display bfd session [[**dynamic**] [**control** | **echo**] [**ipv6**] [**state** { **down** | **admin-down** | **init** | **up** }] [**discriminator remote** *remote-value*] [**peer-ipv6** *ipv6-address* [**vpn-instance** *vpn-instance-name*]] [**verbose**]]

display bfd session [[**dynamic**] [**control** | **echo**] [**state** { **down** | **admin-down** | **init** | **up** }] [**discriminator remote** *remote-value*] [[**peer-ip** *ipv4-address* [**vpn-instance** *vpn-instance-name*]] | [**peer-ipv6** *ipv6-address* [**vpn-instance** *vpn-instance-name*]]] [**verbose**]]

display bfd session [[**static**] [**ip**] [**state** { **down** | **admin-down** | **init** | **up** }] [**discriminator remote** *remote-value*] [**peer-ip** *ipv4-address* [**vpn-instance** *vpn-instance-name*]] [**verbose**]

display bfd session [[**static**] [**ipv6**] [**state** { **down** | **admin-down** | **init** | **up** }] [**discriminator remote** *remote-value*] [**peer-ipv6** *ipv6-address* [**vpn-instance** *vpn-instance-name*]] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

discriminator local *local-value*: Specifies a BFD session by its local discriminator in the range of 1 to 4294967295.

name *session-name*: Specifies a static BFD session by its name, a case-sensitive string of 1 to 64 characters.

dynamic: Specifies dynamic BFD sessions.

static: Specifies static BFD sessions.

control: Specifies BFD sessions in control mode.

echo: Specifies BFD sessions in echo mode.

ip: Specifies BFD sessions used to detect IPv4 links.

ipv6: Specifies BFD sessions used to detect IPv6 links.

state: Displays BFD sessions by session state.

down: Specifies BFD sessions in Down state.

admin-down: Specifies BFD sessions in AdminDown state.

init: Specifies BFD sessions in Init state.

up: Specifies BFD sessions in Up state.

discriminator remote *remote-value*: Specifies a BFD session by its remote discriminator in the range of 1 to 4294967295.

peer-ip *ipv4-address*: Specifies a BFD session by the peer IPv4 address in dotted decimal notation.

peer-ipv6 *ipv6-address*: Specifies a BFD session by the peer IPv6 address.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command displays information for the BFD sessions of the public network.

verbose: Displays detailed BFD session information.

Usage guidelines

If you do not specify the **dynamic** or **static** keyword, this command displays all dynamic and static BFD sessions.

Examples

Display brief information about all BFD sessions.

```
<Sysname> display bfd session
 Total sessions: 9        Up sessions: 9        Init mode: Active

 IPv4 session working in control packet mode:

 LD/RD           SourceIP        DestinationIP   State   Holdtime    Interface
 513/513         1.1.1.1         1.1.1.2         Up      2297ms      GE1/0/1

 IPv6 session working in control packet mode:

      Local discr: 513                  Remote discr: 513
        Source IP: FE80::20C:29FF:FED4:7171
   Destination IP: FE80::20C:29FF:FE72:AC4D
    Session state: Up                      Interface: GE1/0/1
        Hold time: 2142ms

 IPv4 static session working in control packet mode:

 LD/RD           SourceIP        DestinationIP   State   Holdtime    Interface
 1017/7101       2.1.1.1         2.1.1.2         Up      4988ms      GE1/0/1

 IPv6 static session working in control packet mode:

      Local discr: 1226                 Remote discr: 6221
        Source IP: 12::1
   Destination IP: 12::2
```

```
     Session state: Up                     Interface: GE1/0/1
         Hold time: 4812ms

IPv4 static session working in echo mode:

 LD              SourceIP        DestinationIP   State   Holdtime    Interface
 1226            192.168.51.1    192.168.51.5    Up      4238ms      GE1/0/1

 IPv6 static session working in echo mode:

       Local discr: 2012
         Source IP: 15::1
    Destination IP: 15::5
     Session state: Up                     Interface: GE1/0/1
         Hold time: 4626ms
```

Table 3 Command output

Field	Description
Total sessions	Total number of BFD sessions.
Up sessions	Total number of active BFD sessions.
Init mode	BFD operating mode: **Active** or **Passive**.
IPv4 session working in control packet mode	BFD session type and operating mode: • **IPv4 session working in control packet mode**. • **IPv4 session working in echo mode**. • **IPv6 session working in control packet mode**. • **IPv6 session working in echo mode**. • **IPv4 static session working in control packet mode**. • **IPv4 static session working in echo mode**. • **IPv6 static session working in control packet mode**. • **IPv6 static session working in echo mode.**
LD/RD	Local discriminator/Remote discriminator of the session.
Source IP	Source IPv4 address of the session.
Destination IP	Destination IPv4 address of the session.
State	Session state: **Down**, **Init**, **Adown**, or **Up**.
Holdtime	Length of time before session detection timer expires. For a BFD session in **Down** state, this field displays **0ms**.
Interface	Name of the interface of the session.
Local discr	Local discriminator of the session.
Remote discr	Remote discriminator of the session.
Session state	Session state: **Down**, **Adown**, **Init**, or **Up**.
Hold time	Length of time before session detection timer expires. For a BFD session in **Down** state, this field displays **0ms**.

Display detailed information about all BFD sessions.

```
<Sysname> display bfd session verbose
```

```
Total sessions: 9        Up sessions: 9        Init mode: Active

IPv4 session working in control packet mode:
         Local discr: 33793                     Remote discr: 33793
           Source IP: 23.1.1.2                Destination IP: 23.1.1.3
       Session state: Up
           Interface: GigabitEthernet1/0/1
     Min Tx interval: 1000ms              Actual Tx interval: 1000ms
     Min Rx interval: 1000ms                  Detection time: 5000ms
            Rx count: 133                           Tx count: 142
     Connection type: Direct                    Up duration: 00:02:01
           Hold time: 4571ms                      Auth mode: None
      Detection mode: Async                           Slot: 0
            Protocol: OSPF
             Version: 1
           Diag info: No Diagnostic


IPv6 session working in control packet mode:
         Local discr: 33794                     Remote discr: 33794
           Source IP: FE80::5457:A5FF:FE0F:306
      Destination IP: FE80::5457:A1FF:FEB5:206
       Session state: Up
           Interface: GigabitEthernet1/0/1
     Min Tx interval: 1000ms              Actual Tx interval: 1000ms
     Min Rx interval: 1000ms                  Detection time: 5000ms
            Rx count: 3262                          Tx count: 3048
     Connection type: Direct                    Up duration: 00:44:26
           Hold time: 4409ms                      Auth mode: None
      Detection mode: Async                           Slot: 0
            Protocol: OSPFv3
             Version: 1
           Diag info: No Diagnostic


IPv4 static session working in control packet mode:
        Session name: abc
         Local discr: 1017                      Remote discr: 7101
           Source IP: 2.1.1.1                 Destination IP: 2.1.1.2
       Session state: Up
           Interface: GigabitEthernet1/0/1
     Min Tx interval: 1000ms              Actual Tx interval: 1000ms
     Min Rx interval: 1000ms                  Detection time: 5000ms
            Rx count: 1012                          Tx count: 1064
     Connection type: Direct                    Up duration: 00:14:41
           Hold time: 4438ms                      Auth mode: None
      Detection mode: Async                           Slot: 0
            Protocol: STATIC_IPv4
```

```
            Version: 1
          Diag info: No Diagnostic


IPv6 static session working in control packet mode:
       Session name: blue
        Local discr: 1226                     Remote discr: 6221
          Source IP: 12::1
     Destination IP: 12::2
      Session state: Up
          Interface: GigabitEthernet1/0/1
    Min Tx interval: 1000ms              Actual Tx interval: 1000ms
    Min Rx interval: 1000ms                  Detection time: 5000ms
           Rx count: 225                           Tx count: 266
    Connection type: Direct                     Up duration: 00:03:13
          Hold time: 4371ms                       Auth mode: None
     Detection mode: Async                             Slot: 0
           Protocol: STATIC_IPv6
            Version: 1
          Diag info: No Diagnostic


IPv4 static session working in echo mode:
       Session name: aa
        Local discr: 1226
          Source IP: 192.168.51.1            Destination IP: 192.168.51.5
      Session state: Up
          Interface: GigabitEthernet1/0/1
          Hold time: 4965ms              Actual Tx interval: 1000ms
    Min Rx interval: 1000ms                  Detection time: 5000ms
           Rx count: 308                           Tx count: 308
    Connection type: Direct                     Up duration: 00:04:28
     Detection mode: Async                             Slot: 0
           Protocol: STATIC_IPv4
            Version: 1
          Diag info: No Diagnostic


IPv6 static session working in echo mode:
       Session name: bb
        Local discr: 2012
          Source IP: 15::1                   Destination IP: 15::5
      Session state: Up
          Interface: GigabitEthernet1/0/1
          Hold time: 4426ms              Actual Tx interval: 1000ms
    Min Rx interval: 1000ms                  Detection time: 5000ms
           Rx count: 193                           Tx count: 193
    Connection type: Direct                     Up duration: 00:02:46
```

```
Detection mode: Async                              Slot: 0
      Protocol: STATIC_IPv6
       Version: 1
     Diag info: No Diagnostic
```

Table 4 Command output

Field	Description
Total sessions	Total number of BFD sessions.
Up sessions	Total number of active BFD sessions.
Init mode	BFD operating mode: Active or Passive.
IPv4 session working in control packet mode	BFD session type and operating mode: • **IPv4 session working in control packet mode**. • **IPv4 session working in echo mode**. • **IPv6 session working in control packet mode**. • **IPv6 session working in echo mode**. • **IPv4 static session working in control packet mode**. • **IPv4 static session working in echo mode**. • **IPv6 static session working in control packet mode**. • **IPv6 static session working in echo mode**.
Local discr	Local ID of the session.
Remote discr	Remote ID of the session.
Source IP	Source IP address of the session.
Destination IP	Destination IP address of the session.
Session state	Session state: **Down**, **Init**, or **Up**.
Interface	Name of the interface of the session.
Min Tx interval	Minimum transmit interval.
Min Rx interval	Minimum receive interval.
Actual Tx interval	Actual transmit interval.
Detection time	Actual session detection timer.
Rx count	Number of packets received.
Tx count	Number of packets sent.
Connection type	Connection type of the interface: Direct or indirect.
Up duration	Time period for which the session has been up.
Hold time	Length of time before session detection timer expires. For a BFD session in down state, this field displays **0ms**.
Auth mode	Session authentication mode.
Connect type	Connection type of the interface: Direct or indirect.
Up duration	Time period for which the session has been up.

Field	Description
Detection mode	Detection mode: • **Async**—Asynchronous mode. • **Demand**—Demand mode. • **Async/Echo**—Asynchronous mode with echo function enabled. • **Demand/Echo**—Demand mode with echo function enabled.
Slot	Slot number of the card where the BFD session resides.
Protocol	Protocol associated with BFD: • **OSPF**. • **ISIS_BR_L1**—IS-IS with the network type as broadcast and the router type as Level 1. • **ISIS_BR_L2**—IS-IS with the network type as broadcast and the router type as Level 2. • **ISIS_P2P**—IS-IS with the network type as P2P. • **ISIS6_BR_L1**—IPv6 IS-IS with the network type as broadcast and the router type as Level 1. • **ISIS6_BR_L2**—IPv6 IS-IS with the network type as broadcast and the router type as Level 2. • **ISIS6_P2P**—IPv6 IS-IS with the network type as P2P. • **BGP**. • **STATIC4**—IPv4 static routing. • **TRACK**—Track. • **RIP**. • **IPFRR**—FIB IP FRR. • **MAD**. • **OSPFv3**. • **BGP4+**. • **PIM**. • **STATIC6**—IPv6 static routing. • **RIPNG**—RIPng. • **Interface**—Interface state. • **TUNNEL**. • **STATIC_IPv4**—IPv4 static BFD session. • **STATIC_IPv6**—IPv6 static BFD session.
Diag info	Diagnostic information about the session: • **No Diagnostic**. • **Control Detection Time Expired**—A control-mode BFD session goes down because local detection times out. • **Echo Function Failed**—An echo-mode BFD session goes down, because local detection times out or the source IP address of echo packets is deleted. • **Neighbor Signaled Session Down**—The remote end notifies the local end of BFD session down. • **Administratively Down**—The local system prevents a BFD session from being established.

first-fail-timer

Use **first-fail-timer** to configure the timer that delays reporting the first BFD session establishment failure to the data link layer.

Use **undo first-fail-timer** to restore the default.

Syntax

first-fail-timer *seconds*

undo first-fail-timer

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080	No
NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	Yes

Default

The first BFD session establishment failure is not reported to the data link layer.

Views

Static BFD session view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Specifies the timeout time that reports the first BFD session establishment failure to the data link layer. The value range for this argument is 1 to 10000 seconds.

Usage guidelines

This command takes effect only on static BFD sessions after you configure the **process-interface-status** command.

If the static BFD session fails to be established when the timer expires, BFD reports the failure to the data link layer and sets the data link layer state of the interface to DOWN(BFD). This behavior rapidly identifies the interfaces for which BFD sessions fail to be established. In this case, the BFD session state is displayed as Down in the **display bfd session** command output. The line protocol state of the interface is displayed as DOWN(BFD) in the **display interface** command output.

If you execute the command on the local end, the BFD session for detecting the local interface state fails to be established when the following conditions exist:

- The command is not executed on the remote end.
- The local and remote ends have mismatching BFD authentication settings.

Examples

Configure the timer that delays reporting the first BFD session establishment failure as 100 seconds.

```
<Sysname> system-view
[Sysname] bfd static abc peer-ip default-ip interface gigabitethernet 1/0/1 source-ip
10.1.1.1 discriminator local 1 remote 1
[Sysname-bfd-static-session-1] first-fail-timer 100
```

Related commands

bfd static

display interface (*Interface Command Reference*)

processing-interface-status

process-interface-status

Use **process-interface-status** to associate the interface state with a static BFD session.

Use **undo process-interface-status** to restore the default.

Syntax

process-interface-status

undo process-interface-status

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080	No
NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	Yes

Default

The state of a static BFD session does not affect the state of the data link layer of the interface.

Views

Static BFD session view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command enables a static BFD session with peer address 224.0.0.184 to set the link layer protocol of the interface to DOWN(BFD) when detecting a link failure. To display information about the link layer protocol state, use the **display interface** command.

Examples

Associate the state of GigabitEthernet 1/0/1 with static BFD session **abc**.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname] bfd static abc peer-ip default-ip interface gigabitethernet 1/0/1 source-ip
10.1.1.1 discriminator local 1 remote 1
[Sysname-bfd-static-session-abc] process-interface-status
```

Related commands

bfd static

display interface

reset bfd session statistics

Use **reset bfd session statistics** to clear the BFD session statistics.

Syntax

reset bfd session statistics

Views

User view

Predefined user roles

network-admin

context-admin

Examples

Clear the BFD session statistics.

```
<Sysname> reset bfd session statistics
```

snmp-agent trap enable bfd

Use **snmp-agent trap enable bfd** to enable SNMP notifications for BFD.

Use **undo snmp-agent trap enable bfd** to disable SNMP notifications for BFD.

Syntax

snmp-agent trap enable bfd

undo snmp-agent trap enable bfd

Default

All SNMP notifications are enabled for BFD.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

To report critical BFD events to an NMS, enable SNMP notifications for BFD. For BFD event notifications to be sent correctly, you must also configure SNMP as described in the network management and monitoring configuration guide for the device.

Examples

Disable SNMP notifications for BFD.

```
<Sysname> system-view
[Sysname] undo snmp-agent trap enable bfd
```

special-processing

Use **special-processing** to enable special processing for a static BFD session used to detect data link layer connectivity.

Use **undo special-processing** to disable special processing for the static BFD session.

Syntax

special-processing [**admin-down** | **authentication-change** | **session-up**] *

undo special-processing [**admin-down** | **authentication-change** | **session-up**] *

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080	No
NFNX3-HDB1180, NFNX3-HDB1480, NFNX3-HDB680, NFNX3-HDB1080	Yes

Default

All types of special processing are disabled for a static BFD session used to detect data link layer connectivity.

Views

Static BFD session view

Predefined user roles

network-admin

context-admin

Parameters

admin-down: Notifies a session down event to the data link layer upon receipt of a BFD packet with the State field as AdminDown. This keyword helps rapidly discover interfaces on which BFD sessions are manually shut down. If you do not specify this keyword, the device sets the BFD session state to Down, but does not notify the session down event to the data link layer.

authentication-change: Immediately sets the session to down state upon a local authentication information change. This keyword helps rapidly discover interfaces with authentication information changes. If you do not specify this keyword, the device sets the session to down state if authentication information inconsistency still persists after a period of time.

session-up: Ignores authentication information inconsistency when the local session is up. If a large number of BFD sessions exist, examining authentication information consistency affects device performance. If you do not specify this keyword, the device examines authentication information in incoming BFD packets when the local session state is up. If the authentication information does not match on the two ends, the BFD session is declared down.

Usage guidelines

If you do not specify any parameters, this command enables or disables all types of special processing.

Examples

Enable all types of special processing for a static BFD session whose outgoing interface is GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] bfd static abc peer-ip default-ip interface gigabitethernet 1/0/1 source-ip 10.1.1.1 discriminator local 1 remote 1
[Sysname-bfd-static-session-1] special-processing
```

Related commands

bfd static

process-interface-status

Contents

Monitor Link commands

display monitor-link group

Use **display monitor-link group** to display information about monitor link groups.

Syntax

display monitor-link group { *group-id* | **all** }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

group-id: Specifies a monitor link group by its ID. The value range for this argument is 1 to 16.

all: Specifies all monitor link groups.

Usage guidelines

This command does not display information about ports that belong to a link aggregation group.

Examples

Display information about all monitor link groups.

```
<Sysname> display monitor-link group all
Monitor link protocol status: Disabled
Monitor link group 1 information:
  Group status     : N/A
  Downlink up-delay: 0(s)
  Last-up-time     : -
  Last-down-time   : -

  Member                    Role       Status
  ------------------------------------------------
  GE1/0/1                   UPLINK     UP
  GE1/0/2                   DOWNLINK   UP
```

Table 1 Command output

Field	Description
Monitor link protocol status	Whether Monitor Link is enabled: • Enabled. • Disabled.

Field	Description
Group status	Monitor link group status: • **DOWN**. • **UP**. • **N/A**—Monitor Link is disabled globally. The monitor link group does not operate.
Downlink up-delay	Switchover delay of the downlink interfaces in the monitor link group, in seconds.
Last-up-time	Last time when the monitor link group came up.
Last-down-time	Last time when the monitor link group went down.
Member	Member interfaces of the monitor link group.
Role	Interface role, which can be uplink interface or downlink interface.
Status	Member interface state: • **DOWN**. • **DOWN (Monitor Link)**—The member interface is shut down by Monitor Link. • **UP**.

downlink up-delay

Use **`downlink up-delay`** to set the switchover delay for the downlink interfaces in a monitor link group.

Use **`undo downlink up-delay`** to restore the default.

Syntax

`downlink up-delay` *`delay`*

`undo downlink up-delay`

Default

The switchover delay is 0 seconds. The downlink interfaces come up as soon as an uplink interface in the monitor link group comes up.

Views

Monitor link group view

Predefined user roles

network-admin

context-admin

Parameters

`delay`: Sets the switchover delay in the range of 1 to 300 seconds.

Usage guidelines

To avoid frequent state changes of downlink interfaces in the event that the uplink interfaces in the monitor link group flap, you can configure a switchover delay. The switchover delay is the time that the downlink interfaces wait before they come up following an uplink interface.

Examples

Set the switchover delay to 50 seconds for the downlink interfaces in monitor link group 1.

```
<Sysname> system-view
[Sysname] monitor-link group 1
[Sysname-mtlk-group1] downlink up-delay 50
```

monitor-link disable

Use **monitor-link disable** to disable Monitor Link globally.

Use **undo monitor-link disable** to enable Monitor Link globally.

Syntax

monitor-link disable

undo monitor-link disable

Default

Monitor Link is enabled globally.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

All monitor link groups can operate only after you enable Monitor Link globally. When you disable Monitor Link globally, all monitor link groups cannot operate and the downlink interfaces brought down by the monitor link groups resume their original states.

Examples

Disable Monitor Link globally.

```
<Sysname> system-view
[Sysname] monitor-link disable
```

monitor-link group

Use **monitor-link group** to create a monitor link group and enter its view, or enter the view of an existing monitor link group.

Use **undo monitor-link group** to remove a monitor link group.

Syntax

monitor-link group *group-id*

undo monitor-link group *group-id*

Default

No monitor link groups exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

group-id: Specifies a monitor link group ID. The value range for this argument is 1 to 16.

Examples

Create monitor link group 1 and enter its view.

```
<Sysname> system-view
[Sysname] monitor-link group 1
[Sysname-mtlk-group1]
```

port

Use **port** to assign an interface to a monitor link group.

Use **undo port** to remove an interface from a monitor link group.

Syntax

port *interface-type* { *interface-number* | *interface-number.subnumber* } { **downlink** | **uplink** }

undo port *interface-type interface-number*

Default

No member interfaces exist in a monitor link group.

Views

Monitor link group view

Predefined user roles

network-admin

context-admin

Parameters

interface-type: Specifies an interface by its type.

interface-number: Specifies an interface by its number.

interface-number.subnumber: Specifies an existing subinterface by its number.

downlink: Specifies a downlink interface.

uplink: Specifies an uplink interface.

Usage guidelines

You can assign an interface to only one monitor link group.

You can also assign an interface to a monitor link group by using the **port monitor-link group** command in interface view.

If you have configured an interface as the downlink interface of a monitor link group, do not configure its subinterfaces as the uplink interfaces of any monitor link group.

Because the state of subinterfaces is associated with the state of the interface, do not add them to the same monitor link group.

If you have configured a Selected port of an aggregation group as the downlink interface of a monitor link group, do not configure an Unselected port of the aggregation group as the uplink interface of the monitor link group.

Do not assign an aggregate interface and member ports of the aggregate group to the same monitor link group.

Examples

Configure GigabitEthernet 1/0/1 as an uplink interface and GigabitEthernet 1/0/2 as a downlink interface for monitor link group 1.

```
<Sysname> system-view
[Sysname] monitor-link group 1
[Sysname-mtlk-group1] port gigabitethernet 1/0/1 uplink
[Sysname-mtlk-group1] port gigabitethernet 1/0/2 downlink
```

Related commands

port monitor-link group

port monitor-link group

Use **port monitor-link group** to assign an interface to a monitor link group.

Use **undo port monitor-link group** to remove an interface from a monitor link group.

Syntax

port monitor-link group *group-id* { **downlink** | **uplink** }

undo port monitor-link group *group-id*

Default

An interface is not a monitor link group member.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface/subinterface view

Layer 2 aggregate interface view

Layer 3 aggregate interface/subinterface view

Predefined user roles

network-admin

context-admin

Parameters

group-id: Specifies a monitor link group by its ID. The value range for this argument is 1 to 16.

downlink: Specifies a downlink interface.

uplink: Specifies an uplink interface.

Usage guidelines

You can assign an interface to only one monitor link group.

You can also assign an interface to a monitor link group by using the **port** command in monitor link group view.

If you have configured an interface as the downlink interface of a monitor link group, do not configure its subinterfaces as the uplink interfaces of any monitor link group.

Because the state of subinterfaces is associated with the state of the interface, do not add the interface and its subinterfaces to the same monitor link group.

If you have configured a Selected port of an aggregation group as the downlink interface of a monitor link group, do not configure an Unselected port of the aggregation group as the uplink interface of the monitor link group.

Do not assign an aggregate interface and member ports of the aggregate group to the same monitor link group.

Examples

Configure GigabitEthernet 1/0/1 as an uplink interface and GigabitEthernet 1/0/2 as a downlink interface for monitor link group 1.

```
<Sysname> system-view
[Sysname] monitor-link group 1
[Sysname-mtlk-group1] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port monitor-link group 1 uplink
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] port monitor-link group 1 downlink
```

Related commands

port

Contents

Smart Link commands

display smart-link flush

Use **display smart-link flush** to display information about the received flush messages.

Syntax

display smart-link flush

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display information about the received flush messages.

```
<Sysname> display smart-link flush
 Received flush packets                          : 10
 Receiving interface of the last flush packet    : GigabitEthernet1/0/1
 Receiving time of the last flush packet         : 19:19:03 2012/04/21
 Device ID of the last flush packet              : 000f-e200-8500
 Control VLAN of the last flush packet           : 1
```

Table 1 Command output

Field	Description
Received flush packets	Total number of received flush messages.
Receiving interface of the last flush packet	Port that received the last flush message.
Receiving time of the last flush packet	Time when the last flush message was received.
Device ID of the last flush packet	Device ID carried in the last flush message.
Control VLAN of the last flush packet	Control VLAN ID carried in the last flush message.

Related commands

reset smart-link statistics

display smart-link group

Use **display smart-link group** to display information about the specified or all smart link groups.

Syntax

display smart-link group { *group-id* | **all** }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

group-id: Specifies a smart link group by its ID. The value range for this argument is 1 to 48.

all: Displays information about all smart link groups.

Examples

Display information about smart link group 1.

```
<Sysname> display smart-link group 1
Smart link group 1 information:
  Device ID       : 0011-2200-0001
  Preemption mode : None
  Preemption delay: 1(s)
  Control VLAN    : 1
  Protected VLAN  : Reference Instance 2, 4

  Member                  Role      State   Flush-count     Last-flush-time
  ------------------------------------------------------------------------------
  GE1/0/1                 PRIMARY   ACTIVE  1               16:45:20 2012/04/21
  GE1/0/2                 SECONDARY STANDBY 2               16:37:20 2012/04/21
```

Table 2 Command output

Field	Description
Preemption mode	Preemption mode: • **None**—Preemption disabled. • **Role**—Role preemption mode. • **Speed**—**Speed preemption mode.**
Preemption delay	Preemption delay time, in seconds.
Control-VLAN	Control VLAN ID.
Protected VLAN	Protected VLANs of the smart link group. Referenced Multiple Spanning Tree Instances (MSTIs) are displayed. To view the VLANs mapped to the referenced MSTIs, use the **display stp region-configuration** command.
Member	Member port of the smart link group.
Role	Port role: primary or secondary.
State	Port state: active, down, or standby.
Flush-count	Number of transmitted flush messages.
Last-flush-time	Time when the last flush message was transmitted (NA indicates that no flush message has been transmitted).

flush enable

Use **flush enable** to enable flush update.

Use **undo flush enable** to disable flush update.

Syntax

flush enable [**control-vlan** *vlan-id*]

undo flush enable

Default

Flush update is enabled for smart link groups, and VLAN 1 is used for flush message transmission.

Views

Smart link group view

Predefined user roles

network-admin

context-admin

Parameters

control-vlan *vlan-id*: Specifies the control VLAN used for transmitting flush messages. The *vlan-id* argument represents the control VLAN ID and is in the range of 1 to 4094.

Usage guidelines

You must configure different control VLANs for different smart link groups.

- Make sure the configured control VLAN already exists, and assign the smart link group member ports to the control VLAN.
- The control VLAN of a smart link group must also be one of its protected VLANs. Do not remove the control VLAN. Otherwise, flush messages cannot be sent correctly.

Examples

Disable flush update for smart link group 1.

```
<Sysname> system-view
[Sysname] smart-link group 1
[Sysname-smlk-group1] undo flush enable
```

Related commands

smart-link flush enable

port

Use **port** to assign a port to a smart link group and specify the port role.

Use **undo port** to remove a port from a smart link group.

Syntax

port *interface-type interface-number* { **primary** | **secondary** }

undo port *interface-type interface-number*

Default

No member ports exist in a smart link group.

Views

Smart link group view

Predefined user roles

network-admin

context-admin

Parameters

interface-type interface-number: Specifies a port by its type and number, which can be a Layer 2 Ethernet interface or Layer 2 aggregate interface.

primary: Specifies a port as the primary port.

secondary: Specifies a port as the secondary port.

Usage guidelines

Before configuring member ports for a smart link group, you must configure protected VLANs for the smart link group.

Disable the spanning tree feature on the ports you want to add to the smart link group. You cannot enable the spanning tree feature on a smart link group member port.

If you configure a port as both an aggregation group member and a smart link group member, only the aggregation group member configuration takes effect. The port is not shown in the output from the **display smart-link group** command. The smart link group member configuration takes effect after the port leaves the aggregation group.

You can also assign a port to a smart link group by using the **port smart-link group** command in interface view.

Examples

Configure GigabitEthernet 1/0/1 as the secondary port of smart link group 1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo stp enable
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] smart-link group 1
[Sysname-smlk-group1] protected-vlan reference-instance 0
[Sysname-smlk-group1] port gigabitethernet 1/0/1 secondary
```

Related commands

port smart-link group

port smart-link group

Use **port smart-link group** to assign a port to a smart link group and specify the port role.

Use **undo port smart-link group** to remove a port from a smart link group.

Syntax

port smart-link group *group-id* { **primary** | **secondary** }

undo port smart-link group *group-id*

Default

A port is not a smart link group member.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

context-admin

Parameters

group-id: Specifies a smart link group by its ID. The value range for this argument is 1 to 48.

primary: Specifies the port as the primary port.

secondary: Specifies the port as the secondary port.

Usage guidelines

Before configuring member ports for a smart link group, you must configure protected VLANs for the smart link group.

Disable the spanning tree feature on the ports you want to add to the smart link group. You cannot enable the spanning tree feature on a smart link group member port.

If you configure a port as both an aggregation group member and a smart link group member, only the aggregation group member configuration takes effect. The port is not shown in the output from the **display smart-link group** command. The smart link group member configuration takes effect after the port leaves the aggregation group.

You can assign a port to a smart link group by using the **port** command in smart link group view.

Examples

Configure GigabitEthernet 1/0/1 as the primary port of smart link group 1.

```
<Sysname> system-view
[Sysname] smart-link group 1
[Sysname-smlk-group1] protected-vlan reference-instance 0
[Sysname-smlk-group1] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo stp enable
[Sysname-GigabitEthernet1/0/1] port smart-link group 1 primary
```

Configure Layer 2 aggregate interface 1 as the primary port of smart link group 1.

```
<Sysname> system-view
[Sysname] smart-link group 1
[Sysname-smlk-group1] protected-vlan reference-instance 0
[Sysname-smlk-group1] quit
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] undo stp enable
[Sysname-Bridge-Aggregation1] port smart-link group 1 primary
```

Related commands

port

preemption delay

Use **preemption delay** to set the preemption delay.

Use **undo preemption delay** to restore the default.

Syntax

preemption delay *delay*

undo preemption delay

Default

The preemption delay is 1 second.

Views

Smart link group view

Predefined user roles

network-admin

context-admin

Parameters

delay: Specifies the preemption delay in the range of 0 to 300 seconds.

Usage guidelines

Preemption delay is the period of time that the primary port waits before taking over to collaborate with the switchover of upstream devices.

The preemption delay configuration takes effect only after a preemption mode is configured.

Examples

Enable role preemption and set the preemption delay to 10 seconds.

```
<Sysname> system-view
[Sysname] smart-link group 1
[Sysname-smlk-group1] preemption mode role
[Sysname-smlk-group1] preemption delay 10
```

Related commands

preemption mode

preemption mode

Use **preemption mode** to configure a preemption mode for a smart link group.

Use **undo preemption mode** to restore the default.

Syntax

preemption mode { **role** | **speed** [**threshold** *threshold-value*] }

undo preemption mode

Default

No preemption mode is configured for a smart link group.

Views

Smart link group view

Predefined user roles

network-admin

context-admin

Parameters

role: Specifies the role preemption mode, which enables the primary port to transition to forwarding state after the primary link recovers.

speed: Specifies the speed preemption mode.

threshold *threshold-value*: Specifies the speed preemption threshold in percentage. The value range for the *threshold-value* argument is 1 to 10000.

Usage guidelines

If you specify the speed preemption mode, the following conditions occur when the primary link recovers:

- If you specify the **threshold** *threshold-value* option, the primary port transitions to forwarding state when the following condition is met:

  The difference between the primary port speed and the secondary port speed equals or exceeds the threshold value (in percentage) of the secondary port speed.
- If you do not specify the **threshold** *threshold-value* option, the primary port transitions to forwarding state when the primary port speed exceeds the secondary port speed.

Examples

Configure the role preemption mode.

```
<Sysname> system-view
[Sysname] smart-link group 1
[Sysname-smlk-group1] preemption mode role
```

Configure the speed preemption mode and specify the speed preemption threshold as 1000.

```
<Sysname> system-view
[Sysname] smart-link group 1
[Sysname-smlk-group1] preemption mode speed threshold 1000
```

protected-vlan

Use **protected-vlan** to configure protected VLANs for a smart link group.

Use **undo protected-vlan** to remove the protected VLAN of a smart link group.

Syntax

protected-vlan reference-instance *instance-id-list*

undo protected-vlan [**reference-instance** *instance-id-list*]

Default

A smart link group does not have protected VLANs.

Views

Smart link group view

Predefined user roles

network-admin

context-admin

Parameters

reference-instance *instance-id-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI ID or a range of MSTI IDs in the form of *instance-id 1* **to** *instance-id 2*. The value range for MSTI IDs is 0 to 4094. 0 represents the common internal

spanning tree (CIST). The *instance-id 2* must be equal to or greater than *instance-id 1*. You can use the **display stp region-configuration** command to display instance-to-VLAN mappings.

Usage guidelines

You must configure all VLANs to which the member ports of a smart link group belongs as protected VLANs.

If the VLAN-to-MSTI mappings change, the protected VLANs change.

To remove protected VLAN configuration, follow these restrictions and guidelines:

- If you specify the **reference-instance** *instance-id-list* option, the **undo protected-vlan** command removes configuration of VLANs mapped to the specified MSTIs. If you do not specify the **reference-instance** *instance-id-list* option, the command removes configuration of all protected VLANs.
- If a smart link group has member ports, you cannot remove protected VLAN configuration. If a smart link group does not have member ports, you can remove protected VLAN configuration.

Examples

Map VLANs 1 through 30 to MSTI 1, and activate the MST region configuration. Configure the VLANs mapped to MSTI 1 as the protected VLANs of smart link group 1.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] instance 1 vlan 1 to 30
[Sysname-mst-region] active region-configuration
[Sysname-mst-region] quit
[Sysname] smart-link group 1
[Sysname-smlk-group1] protected-vlan reference-instance 1
```

Related commands

display stp region-configuration (*Layer 2—LAN Switching Command Reference*)

smart-link group

reset smart-link statistics

Use **reset smart-link statistics** to clear statistics about flush messages.

Syntax

reset smart-link statistics

Views

User view

Predefined user roles

network-admin

context-admin

Examples

Clear statistics about flush messages.

```
<Sysname> reset smart-link statistics
```

Related commands

display smart-link flush

smart-link flush enable

Use **smart-link flush enable** to enable flush message receiving.

Use **undo smart-link flush enable** to disable flush message receiving.

Syntax

smart-link flush enable [**control-vlan** *vlan-id-list*]

undo smart-link flush enable [**control-vlan** *vlan-id-list*]

Default

Flush message receiving is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

context-admin

Parameters

control-vlan *vlan-id-list*: Specifies a space-separated list of up to 10 control VLAN items. Each item specifies a control VLAN ID or a range of control VLAN IDs in the form of *vlan-id1* **to** *vlan-id2*. The value range for the *vlan-id* argument is 1 to 4094. The *vlan-id2* must be greater than or equal to *vlan-id1*. The default value for the *vlan-id-list* argument is 1.

Examples

Enable GigabitEthernet 1/0/1 to receive flush messages.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] smart-link flush enable
```

Enable Layer 2 aggregate interface 1 to receive flush messages.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] smart-link flush enable
```

Related commands

flush enable

smart-link group

Use **smart-link group** to create a smart link group and enter its view, or enter the view of an existing smart link group.

Use **undo smart-link group** to remove a smart link group.

Syntax

smart-link group *group-id*

undo smart-link group *group-id*

Default

No smart link groups exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

group-id: Specifies a smart link group ID. The value range for this argument is 1 to 48.

Usage guidelines

You cannot remove a smart link group with member ports.

Examples

Create smart link group 1 and enter its view.

```
<Sysname> system-view
[Sysname] smart-link group 1
[Sysname-smlk-group1]
```

Contents

Interface backup commands

backup interface

Use **backup interface** to specify a backup interface for an interface.

Use **undo backup interface** to remove a backup interface.

Syntax

backup interface *interface-type interface-number* [*priority*]

undo backup interface *interface-type interface-number*

Default

An interface does not have backup interfaces.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

interface-type interface-number: Specifies a backup interface by its type and number.

priority: Assigns a priority to the backup interface. The value range is 0 to 255, and the default is 0. The greater the value, the higher the priority.

Usage guidelines

Use this command on the primary interface to specify its backup interfaces. If you also configure the traffic thresholds, the primary and backup interfaces operate in load balancing mode. If you do not configure the traffic thresholds, the primary and backup interfaces operate in strict active/standby mode.

Backup interface priority is used for interface backup to make interface activation or deactivation decisions when the primary interface fails or is overloaded. Backup interfaces are activated in descending order of priority, with the highest-priority interface deactivated first. In contrast, they are deactivated in ascending order of priority, with the lowest-priority interface deactivated first.

Once a backup interface is activated to forward traffic, only the primary interface can preempt it. A higher-priority backup interface cannot preempt a lower-priority backup interface that has taken over the primary interface.

Use Table 1 when you configure primary and backup interfaces.

Table 1 Restrictions on the primary and backup interfaces

Item	Restrictions
Maximum number of primary interfaces/device	10.
Backup interfaces/primary interface	3.

Item	Restrictions
Configuration restrictions	• An interface can only be the backup of one interface. • A primary interface cannot be configured as a backup interface at the same time. • A main interface and its subinterfaces cannot be the backup of each other. • The primary and backup interfaces cannot be members of a logical link. For example, they cannot be members of a Layer 3 aggregation group.

This command and the **backup track** command are mutually exclusive.

- If you have configured the **backup interface** command on the primary interface, you cannot configure the **backup track** command on the primary or backup interface.
- If you have associated a backup interface with a track entry, you cannot configure the **backup interface** command on it or specify it as a backup interface by using the **backup interface** command.

Examples

Specify GigabitEthernet 1/0/2 as a backup interface of GigabitEthernet 1/0/1, with a priority of 50.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] backup interface gigabitethernet 1/0/2 50
```

Related commands

backup track

backup threshold

Use **backup threshold** to configure traffic thresholds on a primary interface for load sharing.

Use **undo backup threshold** to restore the default.

Syntax

backup threshold *upper-threshold lower-threshold*

undo backup threshold

Default

No traffic thresholds are configured.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

upper-threshold: Specifies the upper threshold as a percentage of bandwidth available on the primary interface. The value range is 1 to 99.

lower-threshold: Specifies the lower threshold as a percentage of bandwidth available on the primary interface. The value range is 1 to 99.

NOTE:

To set the bandwidth used for load sharing calculation in this command, use the **bandwidth** command on the primary interface.

Usage guidelines

Before you can use this command on an interface, you must specify a minimum of one backup interface for the interface.

This command enables a primary interface and its backup interfaces to be load shared. In load sharing mode, interface backup regularly compares the amount of traffic with the thresholds.

- When the amount of traffic on the primary interface exceeds the upper threshold, the backup interfaces are activated to share load in descending order of backup priority.
- When the total amount of traffic on all the load-shared interfaces drops below the lower threshold, the backup interfaces are deactivated in ascending order of priority. As a best practice, configure the lower threshold smaller than half of the upper threshold to prevent link flapping from causing frequent interface switchovers.
- When the primary interface goes down, the active/standby mode applies. Only the highest-priority interface is activated.

You can configure the traffic polling interval by using the **backup timer flow-check** command.

NOTE:

- "Traffic" on an interface refers to the amount of incoming or outgoing traffic, whichever is higher.
- If two backup interfaces have the same priority, the one configured first has preference.

Examples

On GigabitEthernet 1/0/1, set the upper and lower traffic thresholds to 80 and 20, respectively.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] backup threshold 80 20
```

Related commands

backup interface

backup timer flow-check

backup timer delay

Use **backup timer delay** to set interface state switchover delay timers on a primary interface.

Use **undo backup timer delay** to restore the default.

Syntax

backup timer delay *up-delay down-delay*

undo backup timer delay

Default

Both up and down delay timers are 5 seconds.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

up-delay: Specifies the number of seconds that the primary or backup interface must wait before it can come up. The value range is 1 to 65535 seconds.

down-delay: Specifies the number of seconds that the active primary or backup interface must wait before it is set to down state. The value range is 1 to 65535 seconds.

Usage guidelines

Before you can use this command on an interface, you must specify at least one backup interface for the interface.

The switchover delay mechanism prevents link flapping from causing frequent interface switchovers. When the link of the active interface fails, the interface state does not change immediately. Instead, a down delay timer starts. If the link recovers before the timer expires, the interface state does not change. If the link is still down when the timer expires, the interface state changes to down.

Examples

Specify GigabitEthernet 1/0/2 as a backup of GigabitEthernet 1/0/1, and set both up and down delay timers to 10 seconds.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] backup interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/1] backup timer delay 10 10
```

Related commands

backup interface

backup timer flow-check

Use **backup timer flow-check** to configure the traffic polling interval on a primary interface.

Use **undo backup timer flow-check** to restore the default.

Syntax

backup timer flow-check *interval*

undo backup timer flow-check

Default

The traffic polling interval is 30 seconds.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies a traffic polling interval in the range of 30 to 600 seconds.

Usage guidelines

Before you can use this command on an interface, you must specify at least one backup interface for the interface.

This command takes effect when the primary and backup interfaces operate in load sharing mode. Interface backup compares the amount of traffic with the thresholds at this interval to determine whether to activate or deactivate a backup interface.

Examples

Set the traffic polling interval to 60 seconds on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] backup timer flow-check 60
```

Related commands

backup interface

backup track

Use **backup track** to associate a backup interface with a track entry.

Use **undo backup track** to restore the default.

Syntax

backup track *track-entry-number*

undo backup track

Default

An interface is not associated with a track entry.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

track-entry-number: Specifies a track entry ID in the range of 1 to 1024.

Usage guidelines

To change the state of a backup interface response to the link state of the primary interface, use this command. For the setting to work, you must configure the track entry to monitor the state of the primary link. For more information about configuring a track entry, see *Network Management and Monitoring Configuration Guide*.

You can associate an interface with only one track entry. If you execute this command multiple times, the most recent configuration takes effect.

You can create the associated track entry before or after the association. The association takes effect after the track entry is created.

To maintain performance, limit the number of associations to 64.

This command and the **backup interface** command are mutually exclusive.

- If you have configured the **backup interface** command on the primary interface, you cannot configure the **backup track** command on the primary or backup interface.

- If you have associated a backup interface with a track entry, you cannot configure the **backup interface** command on it or specify it as a backup interface by using the **backup interface** command.

Examples

Associate GigabitEthernet 1/0/1 with track entry 1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] backup track 1
```

Related commands

backup interface

display interface-backup state

Use **display interface-backup state** to display state information for primary and backup interfaces.

Syntax

display interface-backup state

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display state information for primary and backup interfaces.

```
<Sysname> display interface-backup state
Interface: GE1/0/1
  UpDelay: 10 s
  DownDelay: 5 s
  Upper threshold: 80
  Lower threshold: 20
State: DOWN
  Backup interfaces:
    GE1/0/2             Priority: 30   State: UP_DELAY
    GE1/0/3             Priority: 20   State: STANDBY

IB Track Information:
  GE1/0/4             Track: 1  State: STANDBY
  GE1/0/5             Track: 2  State: UP
```

Table 2 Command output

Field	Description
Interface	Name of the primary interface.

Field	Description
UpDelay	The number of seconds that elapse after the primary interface goes down before the backup interface is activated.
DownDelay	The number of seconds that elapse after the primary interface comes up before the backup interface is deactivated.
Upper threshold	The upper traffic threshold specified as a percentage of bandwidth available on the primary interface. When the traffic on the primary interface exceeds the upper threshold, the backup interfaces are activated to share load in descending order of backup priority.
Lower threshold	The lower traffic threshold specified as a percentage of bandwidth available on the primary interface. When the total amount of traffic on all the load-shared interfaces drops below the lower threshold, the backup interfaces are deactivated in ascending order of priority.
State	State of the primary interface: • **UP**—The interface is both administratively and physically up. • **DOWN**—The interface is administratively up, but its physical state is down (possibly because no physical link exists or the link has failed). • **UP_DELAY**—The interface has recovered, and it is waiting to preempt the active backup interface. • **DOWN_DELAY**—The interface has failed, and it is waiting to be taken over by a backup interface. During this period, packet loss occurs on the primary interface. The interface can forward traffic only when it is in UP state.
Backup interfaces	Backup interfaces assigned to the primary interface.
Priority	Priority of the backup interface.
State	State of the backup interface: • **UP**—The interface is both administratively and physically up. • **DOWN**—The interface is administratively up, but its physical state is down (possibly because no physical link exists or the link has failed). • **UP_DELAY**—The backup interface is waiting to take over the primary interface. • **DOWN_DELAY**—The interface is waiting to be preempted by the primary interface that has recovered. • **STANDBY**—The interface is on standby while the primary interface is operating correctly. The interface can forward traffic only when it is in UP state.
IB Track Information	Associations of backup interfaces and track entries.
Track	Track entry ID associated with the backup interface.
State	State of the backup interface associated with a track entry: • **INVALID**—The backup role of the interface has not taken effect, for example, because the track entry has not been created. • **UP**—The interface is both administratively and physically up. • **DOWN**—The interface is administratively up, but its physical state is down (possibly because no physical link exists or the link has failed). • **STANDBY**—The backup interface is on standby while the primary link is operating correctly.

display interface-backup statistics

Use **display interface-backup statistics** to display traffic statistics for load-shared interfaces.

Syntax

display interface-backup statistics

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display traffic statistics for load-shared interfaces.

```
<Sysname> display interface-backup statistics
Interface: GigabitEthernet1/0/2
  Statistics interval: 30 s
  Bandwidth: 100000000 bps
  ActiveTotalIn: 102 bytes
  ActiveTotalOut: 108 bytes
  ActiveIntervalIn: 102 bytes
  ActiveIntervalOut: 108 bytes
  Active used bandwidth: 28 bps
  TotalIn: 102 bytes
  TotalOut: 108 bytes
  TotalIntervalIn: 102 bytes
  TotalIntervalOut: 108 bytes
  Total used bandwidth: 28 bps
```

Table 3 Command output

Field	Description
Interface	Name of the primary interface.
Statistics interval	Traffic polling interval, in seconds.
Bandwidth	Expected bandwidth (in bps) of the primary interface. This bandwidth is used for load sharing computation. You can use the **bandwidth** command in interface view to set its value.
PrimaryTotalIn	Cumulative sum of incoming bytes on the primary interface at the most recent traffic polling.
PrimaryTotalOut	Cumulative sum of outgoing bytes on the primary interface at the most recent traffic polling.
PrimaryIntervalIn	Number of incoming bytes on the primary interface for the most recent polling interval.
PrimaryIntervalOut	Number of outgoing bytes on the primary interface for the most recent polling interval.

Field	Description
Primary used bandwidth	The primary interface's used bandwidth that was counted in load sharing computation.
TotalIn	Cumulative sum of incoming bytes on the load-shared primary and backup interfaces at the most recent traffic polling.
TotalOut	Cumulative sum of outgoing bytes on the load-shared primary and backup interfaces at the most recent traffic polling.
TotalIntervalIn	Number of incoming bytes on the load-shared primary and backup interfaces for the most recent polling interval.
TotalIntervalOut	Number of outgoing bytes on the load-shared primary and backup interfaces for the most recent polling interval.
Total used bandwidth	Total used bandwidth (in bps) of the load-shared primary and backup interfaces for the most recent polling interval.

Contents

Interface collaboration commands

collaboration-group

Use **collaboration-group** to create a collaboration group and enter its view, or enter the view of an existing collaboration group.

Use **undo collaboration-group** to delete a collaboration group.

Syntax

collaboration-group *group-id*

undo collaboration-group *group-id*

Default

No collaboration groups exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

group-id: Specifies a collaboration group ID. The value range for this argument is 1 to 16.

Usage guidelines

Interface collaboration assigns different interfaces on a device to a collaboration group and associates the states of these interfaces. All member interfaces in a collaboration group can or cannot transmit packets.

Collaboration groups take effect only when Monitor Link is enabled globally.

You must remove all member interfaces from a collaboration group before deleting the collaboration group.

Examples

Create collaboration group 1 and enter its view.

```
<Sysname> system-view
[Sysname] collaboration-group 1
[Sysname-collaboration-group1]
```

collaboration-group clean

Use **collaboration-group clean** to remove ineffective member interfaces from all collaboration groups.

Syntax

collaboration-group clean

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

A member interface in a collaboration group becomes ineffective when the card that hosts the interface is removed or changed to another slot or the ID of the IRF member device that hosts the interface changes. This command prevents an ineffective interface from causing all other member interfaces in the same collaboration group to go down.

An ineffective interface cannot be automatically assigned to the original collaboration group when its hosting card is reinstalled or changed back to the original slot or the IRF member ID is changed back to the original ID. You must assign it to the original collaboration group manually.

Examples

Remove ineffective member interfaces from all collaboration groups.

```
<Sysname> system-view
[Sysname] collaboration-group clean
```

display collaboration-group

Use **display collaboration-group** to display information about collaboration groups.

Syntax

display collaboration-group { *group-id* | **all** } [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

group-id: Specifies a collaboration group by its ID. The value range for this argument is 1 to 16.

all: Specifies all collaboration groups.

verbose: Displays detailed information. If you do not specify this keyword, the command displays brief information.

Examples

Display brief information about all collaboration groups.

```
<Sysname> display collaboration-group all
  Group ID                Group status
  1                       DOWN
  2                       DOWN
```

Display detailed information about all collaboration groups.

```
<Sysname> display collaboration-group all verbose
Collaboration group protocol status: Enabled
Collaboration group 1 information:
```

```
Group status     : DOWN
Member up delay  : 0 seconds
Last up time     : 16:55:34 2017/04/05
Last down time   : 16:57:22 2017/04/05
Member                    Status
GE1/0/1                   DOWN
GE1/0/2                   Collaboration-down
```

Table 1 Command output

Field	Description
Group status	Collaboration group status: • **DOWN**. • **UP**. • **N/A**—Monitor Link is disabled globally. The collaboration group does not take effect. • **UP-Pending**—The collaboration group is transitioning from **DOWN** to **UP**. It takes 10 seconds for the system to determine the collaboration group state (**DOWN** or **UP**).
Collaboration group protocol status	Whether interface collaboration is enabled globally: • Enabled. • Disabled.
Member up delay	Delay time for the member interfaces in the collaboration group to come up after a device restart, in seconds.
Last up time	Last time when the collaboration group came up.
Last down time	Last time when the collaboration group went down.
Member	Member interfaces of the collaboration group.
Status	Member interface status: • **UP**—The interface is up. • **DOWN**—The interface is down. To identify cause, use the **display interface** command. • **Collaboration-down**—The interface is shut down by interface collaboration. • **Not available**—The interface is ineffective because the hosting card is not in position.

port

Use **port** to assign an interface to a collaboration group.

Use **undo port** to remove an interface from a collaboration group.

Syntax

port *interface-type interface-number*

undo port *interface-type interface-number*

Default

No member interfaces exist in a collaboration group.

Views

Collaboration group view

Predefined user roles

network-admin

context-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

You can assign an interface to only one collaboration group.

For a collaboration group to work correctly, do not assign its member interfaces to a redundancy group.

Do not add both Selected ports and Unselected ports in a dynamic aggregation group to the same collaboration group.

If you have configured a member interface as the uplink/downlink interface of a monitor link group, do not configure any other member interface in the same collaboration group as the downlink/uplink interface of any monitor link group.

You can also assign an interface to a collaboration group by using the **port collaboration-group** command in interface view.

Examples

Assign GigabitEthernet 1/0/1 to collaboration group 1.

```
<Sysname> system-view
[Sysname] collaboration-group 1
[Sysname-collaboration-group1] port gigabitethernet 1/0/1
```

Related commands

port collaboration-group

port collaboration-group

Use **port collaboration-group** to assign the current interface to a collaboration group.

Use **undo port collaboration-group** to remove the current interface from a collaboration group.

Syntax

port collaboration-group *group-id*

undo collaboration-group *group-id*

Default

The interface is not a collaboration group member.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Layer 2 aggregate interface view

Layer 3 aggregate interface view

Predefined user roles

network-admin

context-admin

Parameters

group-id: Specifies a collaboration group by its ID. The value range for this argument is 1 to 16.

Usage guidelines

You can assign an interface to only one collaboration group.

To assign an interface to a collaboration group by using this command, make sure the collaboration group have been created.

For a collaboration group to work correctly, do not assign its member interfaces to a redundancy group.

Do not add both Selected ports and Unselected ports in a dynamic aggregation group to the same collaboration group.

If you have configured a member interface as the uplink/downlink interface of a monitor link group, do not configure any other member interface in the same collaboration group as the downlink/uplink interface of any monitor link group.

You can also assign an interface to a collaboration group by using the **port** command in collaboration group view.

Examples

Assign GigabitEthernet 1/0/1 to collaboration group 1.

```
<Sysname> system-view
[Sysname] collaboration-group 1
[Sysname-collaboration-group1] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port collaboration-group 1
```

Related commands

port

up-delay

Use **up-delay** to set the delay time for the member interfaces in a collaboration group to come up after a device restart.

Use **undo up-delay** to restore the default.

Syntax

up-delay *delay*

undo up-delay

Default

The delay time is 0 seconds. The member interfaces come up as soon as the device restarts.

Views

Collaboration group view

Predefined user roles

network-admin

context-admin

Parameters

delay: Specifies the delay time in the range of 1 to 3600 seconds.

Usage guidelines

This command enables the member interfaces to come up after a configurable delay time upon a device restart.

Examples

Set the delay time to 10 seconds for the member interfaces in collaboration group 1.

```
<Sysname> system-view
[Sysname] collaboration-group 1
[Sysname-collaboration-group1] up-delay 10
```

Contents

Ping, tracert, and system debugging commands

debugging

Use **debugging** to enable debugging for a module.

Use **undo debugging** to disable debugging for a module or for all modules.

Syntax

debugging *module-name* [*option*]

undo debugging { **all** | *module-name* [*option*] }

Default

Debugging is disabled for all modules.

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

module-name: Specifies a module by its name, such as **arp** or **device**. For a list of supported modules, use the **debugging ?** command.

option: Specifies the debugging option for a module. Available options vary by module. To display the debugging options supported by a module, use the **debugging** *module-name* **?** command.

all: Specifies all modules.

Usage guidelines

CAUTION:

Output of excessive debugging messages increases the CPU usage and downgrades the system performance. To guarantee system performance, enable debugging only for modules that are in an exceptional condition.

The system sends generated debug messages to the device information center, which then sends the messages to appropriate destinations based on the log output configuration. For more information about the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Enable debugging for the device management module.

```
<Sysname> debugging dev
This command is CPU intensive and might affect ongoing services. Are you sure you want to continue? [Y/N]:Y
```

Related commands

display debugging

debugging-auto-off enable cpu-usage-alarm

Use **debugging-auto-off enable cpu-usage-alarm** to enable the debugging-auto-off feature to automatically disable all types of debugging when the CPU usage reaches or exceeds the lowest CPU usage alarm threshold.

Use **undo debugging enable cpu-usage-alarm** to disable the debugging-auto-off feature from automatically disabling all types of debugging when the CPU usage reaches or exceeds the lowest CPU usage alarm threshold.

Syntax

debugging-auto-off enable cpu-usage-alarm

undo debugging-auto-off enable cpu-usage-alarm

Default

The debugging-auto-off feature is disabled.

Views

User view

Predefined user roles

network-admin

context-admin

Usage guidelines

Excessive output from debugging commands might affect system performance. To guarantee system performance, enable the debugging-auto-off feature to automatically disable all types of debugging when the CPU usage reaches or exceeds the lowest CPU usage alarm threshold. The CPU usage alarm thresholds are set by using the **monitor cpu-usage threshold** command.

The device does not automatically enable all types of debugging after the CPU usage drops to or below the CPU usage recovery threshold. To enable debugging for a module or all modules, use the **debugging** command.

Examples

Enable the debugging-auto-off feature to automatically disable all types of debugging when the CPU usage reaches or exceeds the lowest CPU usage alarm threshold.

```
<Sysname> debugging-auto-off enable cpu-usage-alarm
```

Related commands

display debugging-auto-off

monitor cpu-usage threshold (*Fundamentals Command Reference*)

display debugging

Use **display debugging** to display the enabled debugging features for a module or for all modules.

Syntax

display debugging [*module-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

module-name: Specifies a module by its name. For a list of supported modules, use the **display debugging ?** command. If you do not specify a module name, this command displays the enabled debugging features for all modules.

Examples

Display all enabled debugging features.

```
<Sysname> display debugging
DEV debugging switch is on
```

Related commands

debugging

display debugging-auto-off

Use **display debugging-auto-off** to display the enabling status of the debugging-auto-off feature.

Syntax

display debugging-auto-off

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Usage guidelines

To conserve system resources, the device automatically disables all types of debugging in the following situations:

- All users have gone offline.
- The CPU usage reaches or exceeds the lowest CPU usage alarm threshold.

The device always automatically disables all types of debugging when all users have gone offline. This mechanism is not user configurable.

To enable the device to automatically disable all types of debugging when the CPU usage reaches or exceeds the lowest CPU usage alarm threshold, use the **debugging-auto-off enable cpu-usage-alarm** command.

Examples

Display the enabling status of the debugging-auto-off feature.

```
<Sysname> display debugging-auto-off
```

```
Occasions for the system to automatically turn off all debugging:
 When all users log out: Enabled
 When the CPU usage reaches or exceeds the CPU usage alarm threshold: Disabled
```

Table 1 Command output

Field	Description
Occasions for the system to automatically turn off all debugging	Situations where the device automatically disables all types of debugging.
When all users log out: Enabled	The debugging-auto-off feature is always enabled for the situation where all users have gone offline.
The CPU usage reaches or exceeds the CPU usage alarm threshold: Enabled	The debugging-auto-off feature is enabled for the situation where the CPU usage reaches or exceeds the lowest CPU usage alarm threshold.
The CPU usage reaches or exceeds the CPU usage alarm threshold: Disabled	The debugging-auto-off feature is disabled for the situation where the CPU usage reaches or exceeds the lowest CPU usage alarm threshold.

Related commands

debugging-auto-off enable cpu-usage-alarm

ping

Use **ping** to test the reachability of the destination IP address and display ping statistics.

Syntax

ping [**ip**] [**-a** *source-ip* | **-c** *count* | **-f** | **-h** *ttl* | **-i** *interface-type interface-number* | **-m** *interval* | **-n** | **-p** *pad* | **-q** | **-r** | **-s** *packet-size* | **-t** *timeout* | **-tos** *tos* | **-v** | **-vpn-instance** *vpn-instance-name*] * *host*

Views

Any view

Predefined user roles

network-admin

context-admin

Parameters

ip: Distinguishes between a destination host name and the **ping** command keywords if the name of the destination host is **i**, **ip**, **ipv**, **ipv6**, **l**, **ls**, or **lsp**. For example, you must use the command in the form of **ping ip ip** instead of **ping ip** if the destination host name is **ip**.

-a *source-ip*: Specifies an IP address of the device as the source IP address of ICMP echo requests. If you do not specify this option, the source IP address of ICMP echo requests is the primary IP address of the outbound interface.

-c *count*: Specifies the number of ICMP echo requests that are sent to the destination. The value range is 1 to 4294967295, and the default is 5.

-f: Sets the "Don't Fragment" bit in the IP header.

-h *ttl*: Specifies the TTL value of ICMP echo requests. The value range is 1 to 255, and the default is 255.

-i *interface-type interface-number*: Specifies the source interface of ICMP echo requests. If you do not specify this option, the system looks up the routing table or forwarding table

for a matching route and uses the output interface of that route as the source interface of ICMP echo requests.

-m *interval*: Specifies the interval (in milliseconds) to send ICMP echo requests. The value range is 1 to 65535, and the default is 200.

-n: Disables domain name resolution for the *host* argument. If the *host* argument represents the host name of the destination, and if this keyword is not specified, the device translates *host* into an address.

-p *pad*: Specifies the value of the **pad** field in an ICMP echo request, in hexadecimal format, 1 to 8 bits. The *pad* argument is in the range of 0 to ffffffff. If the specified value is less than 8 bits, 0s are added in front of the value to extend it to 8 bits. For example, if *pad* is configured as 0x2f, then the packets are padded with 0x0000002f to make the total length of the packet meet the requirements of the device. By default, the padded value starts from 0x01 up to 0xff, where another round starts again if necessary, such as 0x010203…feff01….

-q: Displays only the summary statistics. If this keyword is not specified, the system displays all the ping statistics.

-r: Records the addresses of the hops (up to 9) the ICMP echo requests passed. If this keyword is not specified, the addresses of the hops that the ICMP echo requests passed are not recorded.

-s *packet-size*: Specifies the length (in bytes) of ICMP echo requests (excluding the IP packet header and the ICMP packet header). The value range for the *packet-size* argument is 20 to 8100. The default setting is 56 bytes.

-t *timeout*: Specifies the timeout time (in milliseconds) of an ICMP echo reply. The value range is 0 to 65535, and the default is 2000. If the source does not receive an ICMP echo reply within the timeout, it considers the ICMP echo reply timed out.

-tos *tos*: Specifies the ToS value of ICMP echo requests. The value range is 0 to 255, and the default is 0.

-v: Displays non-ICMP echo reply packets. If this keyword is not specified, the system does not display non-ICMP echo reply packets.

-vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance to which the destination belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the destination is on the public network, do not specify this option.

host: Specifies the IP address or host name of the destination. The host name is a case-insensitive string of 1 to 253 characters. It can contain letters, digits, and special characters such as hyphen (-), underscore (_), and dot (.).

Usage guidelines

To ping a device identified by its host name, configure the DNS settings on the device first. If the DNS settings are not configured, the ping operation fails.

To abort the ping operation during the execution of the command, press **Ctrl+C**.

Examples

Test whether the device with an IP address of 1.1.2.2 is reachable.

```
<Sysname> ping 1.1.2.2
Ping 1.1.2.2 (1.1.2.2): 56 data bytes, press CTRL+C to break
56 bytes from 1.1.2.2: icmp_seq=0 ttl=254 time=2.137 ms
56 bytes from 1.1.2.2: icmp_seq=1 ttl=254 time=2.051 ms
56 bytes from 1.1.2.2: icmp_seq=2 ttl=254 time=1.996 ms
56 bytes from 1.1.2.2: icmp_seq=3 ttl=254 time=1.963 ms
56 bytes from 1.1.2.2: icmp_seq=4 ttl=254 time=1.991 ms
```

```
--- Ping statistics for 1.1.2.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.963/2.028/2.137/0.062 ms
```

Test whether the device with an IP address of 1.1.2.2 in VPN instance **vpn1** is reachable.

```
<Sysname> ping -vpn-instance vpn1 1.1.2.2
Ping 1.1.2.2 (1.1.2.2): 56 data bytes, press CTRL+C to break
56 bytes from 1.1.2.2: icmp_seq=0 ttl=254 time=2.137 ms
56 bytes from 1.1.2.2: icmp_seq=1 ttl=254 time=2.051 ms
56 bytes from 1.1.2.2: icmp_seq=2 ttl=254 time=1.996 ms
56 bytes from 1.1.2.2: icmp_seq=3 ttl=254 time=1.963 ms
56 bytes from 1.1.2.2: icmp_seq=4 ttl=254 time=1.991 ms

--- Ping statistics for 1.1.2.2 in VPN instance vpn1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.963/2.028/2.137/0.062 ms
```

Test whether the device with an IP address of 1.1.2.2 is reachable. Only results are displayed.

```
<Sysname> ping -q 1.1.2.2
Ping 1.1.2.2 (1.1.2.2): 56 data bytes, press CTRL+C to break

--- Ping statistics for 1.1.2.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.962/2.196/2.665/0.244 ms
```

Test whether the device with an IP address of 1.1.2.2 is reachable. The IP addresses of the hops that the ICMP packets passed in the path are displayed.

```
<Sysname> ping -r 1.1.2.2
Ping 1.1.2.2 (1.1.2.2): 56 data bytes, press CTRL+C to break
56 bytes from 1.1.2.2: icmp_seq=0 ttl=254 time=4.685 ms
RR:      1.1.2.1
         1.1.2.2
         1.1.1.2
         1.1.1.1
56 bytes from 1.1.2.2: icmp_seq=1 ttl=254 time=4.834 ms  (same route)
56 bytes from 1.1.2.2: icmp_seq=2 ttl=254 time=4.770 ms  (same route)
56 bytes from 1.1.2.2: icmp_seq=3 ttl=254 time=4.812 ms  (same route)
56 bytes from 1.1.2.2: icmp_seq=4 ttl=254 time=4.704 ms  (same route)

--- Ping statistics for 1.1.2.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 4.685/4.761/4.834/0.058 ms
```

The output shows the following information:

- The destination is reachable.
- The route is 1.1.1.1 <-> {1.1.1.2; 1.1.2.1} <-> 1.1.2.2.

Table 2 Command output

Field	Description
Ping 1.1.2.2 (1.1.2.2): 56 data bytes, press CTRL+C to break	Test whether the device with IP address 1.1.2.2 is reachable. There are 56 bytes in each ICMP echo request. Press escape key **Ctrl+C** to abort the ping operation. The escape key is configurable by using the **escape-key** command. For more information about this command, see login management commands in *Fundamentals Command Reference*.
56 bytes from 1.1.2.2: icmp_seq=0 ttl=254 time=4.685 ms	Received ICMP echo replies from the device whose IP address is 1.1.2.2. If no echo reply is received within the timeout period, no information is displayed. • **bytes**—Number of bytes in the ICMP echo reply. • **icmp_seq**—Packet sequence, used to determine whether a segment is lost, disordered or repeated. • **ttl**—TTL value in the ICMP echo reply. • **time**—Response time.
RR:	Routers through which the ICMP echo request passed. They are displayed in inversed order, which means the router with a smaller distance to the destination is displayed first.
--- Ping statistics for 1.1.2.2 ---	Statistics on data received and sent in the ping operation.
--- Ping statistics for 1.1.2.2 in VPN instance vpn1 ---	Ping statistics for a device in a VPN instance.
5 packet(s) transmitted	Number of ICMP echo requests sent.
5 packet(s) received	Number of ICMP echo replies received.
0.0% packet loss	Percentage of unacknowledged packets to the total packets sent.
round-trip min/avg/max/std-dev = 4.685/4.761/4.834/0.058 ms	Minimum/average/maximum/standard deviation response time, in milliseconds.

ping ipv6

Use **ping ipv6** to test the reachability of the destination IPv6 address and display IPv6 ping statistics.

Syntax

ping ipv6 [**-a** *source-ipv6* | **-c** *count* | **-i** *interface-type interface-number* | **-m** *interval* | **-q** | **-s** *packet-size* | **-t** *timeout* | **-tc** *traffic-class*| **-v** | **-vpn-instance** *vpn-instance-name*] * *host*

Views

Any view

Predefined user roles

network-admin

context-admin

Parameters

-a *source-ipv6*: Specifies an IPv6 address of the device as the source IP address of ICMP echo requests. If you do not specify this option, the source IPv6 address of ICMP echo requests is the IPv6 address of the outbound interface. See RFC 3484 for information about the address selection rule.

-c *count*: Specifies the number of ICMPv6 echo requests that are sent to the destination. The value range is 1 to 4294967295, and the default is 5.

-i *interface-type interface-number*: Specifies the source interface of ICMPv6 echo requests. If you do not specify this option, the system looks up the routing table or forwarding table for a matching route and uses the output interface of that route as the source interface of ICMPv6 echo requests. You must specify this option if the destination address is a multicast address or a link-local address.

-m *interval*: Specifies the interval (in milliseconds) to send an ICMPv6 echo reply. The value range is 1 to 65535, and the default is 1000.

-q: Displays only the summary statistics. If you do not specify this keyword, the system displays all the ping statistics.

-s *packet-size*: Specifies the length (in bytes) of ICMPv6 echo requests (excluding the IPv6 packet header and the ICMPv6 packet header). The value range for the *packet-size* argument is 20 to 8100. The default setting is 56 bytes.

-t *timeout*: Specifies the timeout time (in milliseconds) of an ICMPv6 echo reply. The value range is 0 to 65535, and the default is 2000.

-tc *traffic-class*: Specifies the traffic class value in an ICMPv6 packet. The value range is 0 to 255 and the default is 0.

-v: Displays detailed information (including the **dst** field and the **idx** field) about ICMPv6 echo replies. If this keyword is not specified, the system only displays brief information (not including the **dst** field and the **idx** field) about ICMPv6 echo replies.

-vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance to which the destination belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the destination is on the public network, do not specify this option.

host: Specifies the IPv6 address or host name of the destination. The host name is a case-insensitive string of 1 to 253 characters. It can contain letters, digits, and special characters such as hyphen (-), underscore (_), and dot (.).

Usage guidelines

To ping a device identified by its host name, configure the DNS settings on the device first. If the DNS settings are not configured, the IPv6 ping operation fails.

To abort the IPv6 ping operation during the execution of the command, press **Ctrl+C**.

Examples

Test whether the IPv6 address (2001::2) is reachable.

```
<Sysname> ping ipv6 2001::2
Ping6(56 data bytes) 2001::1 --> 2001::2, press CTRL+C to break
56 bytes from 2001::2, icmp_seq=0 hlim=64 time=62.000 ms
56 bytes from 2001::2, icmp_seq=1 hlim=64 time=23.000 ms
56 bytes from 2001::2, icmp_seq=2 hlim=64 time=20.000 ms
56 bytes from 2001::2, icmp_seq=3 hlim=64 time=4.000 ms
56 bytes from 2001::2, icmp_seq=4 hlim=64 time=16.000 ms

--- Ping6 statistics for 2001::2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 4.000/25.000/62.000/20.000 ms
```

Test whether the IPv6 address (2001::2) is reachable. Only the statistics are displayed.

```
<Sysname> ping ipv6 –q 2001::2
```

```
Ping6(56 data bytes) 2001::1 --> 2001::2, press CTRL+C to break

--- Ping6 statistics for 2001::2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 4.000/25.000/62.000/20.000 ms
```

Test whether the IPv6 address (2001::2) is reachable. Detailed ping information is displayed.

```
<Sysname> ping ipv6 –v 2001::2
Ping6(56 data bytes) 2001::1 --> 2001::2, press CTRL+C to break
56 bytes from 2001::2, icmp_seq=0 hlim=64 dst=2001::1 idx=3 time=62.000 ms
56 bytes from 2001::2, icmp_seq=1 hlim=64 dst=2001::1 idx=3 time=23.000 ms
56 bytes from 2001::2, icmp_seq=2 hlim=64 dst=2001::1 idx=3 time=20.000 ms
56 bytes from 2001::2, icmp_seq=3 hlim=64 dst=2001::1 idx=3 time=4.000 ms
56 bytes from 2001::2, icmp_seq=4 hlim=64 dst=2001::1 idx=3 time=16.000 ms

--- Ping6 statistics for 2001::2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 4.000/25.000/62.000/20.000 ms
```

Table 3 Command output

Field	Description
Ping6(56 data bytes) 2001::1 --> 2001::2, press CTRL+C to break	An ICMPv6 echo reply with a data length of 56 bytes is sent from 2001::1 to 2001::2. Press escape key **Ctrl+C** to abort the IPv6 ping operation. The escape key is configurable by using the **escape-key** command. For more information about this command, see login management commands in *Fundamentals Command Reference*.
56 bytes from 2001::2, icmp_seq=1 hlim=64 dst=2001::1 idx=3 time=62.000 ms	Received ICMPv6 echo replies from the device whose IPv6 address is 2001::2. • The number of data bytes is 56. • The packet sequence is 1. • The hop limit value is 64. • The destination address is 2001::1. Specify the **-v** keyword to display this field. • The index for the packet inbound interface is 3. Specify the **-v** keyword to display this field. • The response time is 62 milliseconds.
--- Ping6 statistics for 2001::2 ------	Statistics on data received and sent in an IPv6 ping operation.
5 packet(s) transmitted	Number of ICMPv6 echo requests sent.
5 packet(s) received	Number of ICMPv6 echo replies received.
0.0% packet loss	Percentage of unacknowledged packets to the total packets sent.
round-trip min/avg/max/ std-dev =4.000/25.000/62.000/20.000 ms	Minimum/average/maximum/standard deviation response time, in milliseconds.

tracert

Use **tracert** to trace the path that the IPv4 packets traverse from source to destination.

Syntax

tracert [**-a** *source-ip* | **-f** *first-ttl* | **-i** *interface-type interface-number* | **-m** *max-ttl* | **-p** *port* | **-q** *packet-number* | **-t** *tos* | **-vpn-instance** *vpn-instance-name* [**-resolve-as** { **global** | **none** | **vpn** }] | **-w** *timeout*] * *host*

Views

Any view

Predefined user roles

network-admin

context-admin

Parameters

-a *source-ip*: Specifies an IP address of the device as the source IP address of probe packets. If you do not specify this option, the source IP address of probe packets is the primary IP address of the outbound interface.

-f *first-ttl*: Specifies the TTL of the first packet sent to the destination. The value range is 1 to 255, and the default is 1. It must be no greater than the value of the *max-ttl* argument.

-i *interface-type interface-number*: Specifies the source interface of probe packets. If you do not specify this option, the system looks up the routing table or forwarding table for a matching route and uses the output interface of that route as the source interface of probe packets.

-m *max-ttl*: Specifies the maximum number of hops allowed for a probe packet. The value range is 1 to 255, and the default is 30. It must be no smaller than the value of the *first-ttl* argument.

-p *port*: Specifies an invalid UDP port of the destination. The value range is 1 to 65535, and the default is 33434.

-q *packet-number*: Specifies the number of probe packets to send per hop. The value range is 1 to 65535, and the default is 3.

-t *tos*: Specifies the ToS value of probe packets. The value range is 0 to 255, and the default is 0.

-vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance to which the destination belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the destination is on the public network, do not specify this option.

-resolve-as: Specifies a routing table for autonomous system (AS) resolution. Tracert searches the specified routing table for the AS that each hop along the path belongs to. If you do not specify this keyword, the global routing table is used. If the AS information is found, this command displays the AS number next to the address of the hop in the probe result.

- **global**: Specifies the global routing table.
- **none**: Disables AS resolution.
- **vpn**: Specifies the VPN routing table.

-w *timeout*: Specifies the timeout time in milliseconds of the reply packet for a probe packet. The value range is 1 to 65535, and the default is 5000.

host: Specifies the IP address or host name of the destination. The host name is a case-insensitive string of 1 to 253 characters. It can contain letters, digits, and special characters such as hyphen (-), underscore (_), and dot (.).

Usage guidelines

After identifying network failure with the **ping** command, use the **tracert** command to locate failed nodes.

If the destination address is on the public network, you do not need to specify the **-resolve-as** keyword to obtain the AS information. The device automatically uses the global routing table for AS resolution.

If the destination address is on a private network, address information of intermediate hops might be stored in either the global routing table or the VPN routing table. To learn the AS path that the packets traverse, execute the **tracert** command twice, once with the **-resolve-as global** keywords and again with the **-resolve-as vpn** keywords.

The output from the **tracert** command includes IP addresses of all the Layer 3 devices that the packets traverse from source to destination. Asterisks (* * *) are displayed if the device cannot reply with an ICMP error message. The reason might be the destination is unreachable or sending ICMP timeout/destination unreachable packets is disabled.

Before starting a tracert operation, you must enable sending of ICMP destination unreachable messages on the intermediate devices between the source and destination. The tracert operation stops if any of the following ICMP destination unreachable messages is received:

- **!N**—Network unreachable.
- **!H**—Destination host unreachable.
- !**P**—Protocol unreachable. The protocol number is unknown.
- **!F**—Fragmentation needed. This message indicates that packet fragmentation is needed but the "Don't Fragment" bit is set on an immediate device.
- **!W**—Destination host unknown.
- **!Q**—Network unreachable for ToS.
- **!T**—Host unreachable for ToS.
- **!X**—Communication administratively prohibited by filtering policies.
- **!V**—Host precedence violation.
- **!C**—Precedence cutoff in effect.

To abort the tracert operation during the execution of the command, press **Ctrl+C**.

Examples

Display the path that the packets traverse from source to destination (1.1.2.2).

```
<Sysname> tracert 1.1.2.2
traceroute to 1.1.2.2 (1.1.2.2), 30 hops at most, 40 bytes each packet, press CTRL+C to break
 1  1.1.1.2 (1.1.1.2) 673 ms 425 ms 30 ms
 2  1.1.2.2 (1.1.2.2) [AS 100] 580 ms 470 ms 80 ms
```

Display the path that the packets traverse from source to destination (1.1.3.2) in VPN instance vpn1, as well as the AS information of the hops along the path.

```
<Sysname> tracert –vpn-instance vpn1 –resolve-as vpn 1.1.3.2
traceroute to 1.1.3.2 (1.1.3.2), 30 hops at most, 40 bytes each packet, press CTRL+C to break
 1  1.1.1.2 (1.1.1.2) 673 ms 425 ms 30 ms
 2  1.1.2.2 (1.1.2.2) 580 ms 470 ms 80 ms
 3  1.1.3.2 (1.1.3.2) [AS 65535] 530 ms 472 ms 380 ms
```

Table 4 Command output

Field	Description
traceroute to 1.1.2.2 (1.1.2.2)	Display the route that the IP packets traverse from the current device to the device whose IP address is 1.1.2.2.

Field	Description
hops at most	Maximum number of hops of the probe packets, which can be set by the **-m** keyword.
bytes each packet	Number of bytes of a probe packet.
press CTRL+C to break	During the execution of the command, press escape key **Ctrl+C** to abort the tracert operation. The escape key is configurable by using the **escape-key** command. For more information about this command, see login management commands in *Fundamentals Command Reference*.
2 1.1.2.2 (1.1.2.2) [AS 100] 580 ms 470 ms 80 ms	Probe result of the probe packets that contain a TTL value of 2, including the following information about the second hop: • Domain name of the hop. If no domain name is configured, the IP address is displayed as the domain name. • IP address of the hop. The IP address is displayed in parentheses. • Number of the AS that the hop belongs to. The AS number appears only when it is found for the hop in the specified routing table. • The round-trip time of the probe packets. The number of packets that can be sent in each probe can be set by using the **-q** keyword.

tracert ipv6

Use **tracert ipv6** to display the path that the IPv6 packets traverse from source to destination.

Syntax

tracert ipv6 [**-f** *first-hop* | **-i** *interface-type interface-number* | **-m** *max-hops* | **-p** *port* | **-q** *packet-number* | **-t** *traffic-class* | **-vpn-instance** *vpn-instance-name* [**-resolve-as** { **global** | **none** | **vpn** }] | **-w** *timeout*] * *host*

Views

Any view

Predefined user roles

network-admin

context-admin

Parameters

-f *first-hop*: Specifies the TTL value of the first packet. The value range is 1 to 255, and the default is 1. The value must be no greater than the value of the *max-hops* argument.

-i *interface-type interface-number*: Specifies the source interface of probe packets. If you do not specify this option, the system looks up the routing table or forwarding table for a matching route and uses the output interface of that route as the source interface of probe packets. You must specify this option if the destination address is a multicast address or a link-local address.

-m *max-hops*: Specifies the maximum number of hops allowed for a packet. The value range is 1 to 255, and the default is 30. The value must be no smaller than the value of the *first-hop* argument.

-p *port*: Specifies an invalid UDP port of the destination. The value range is 1 to 65535, and the default is 33434.

-q *packet-number*: Specifies the number of probe packets sent each time. The value range is 1 to 65535, and the default is 3.

-t *traffic-class*: Specifies the traffic class value in an IPv6 probe packet. The value range is 0 to 255, and the default is 0.

-vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance to which the destination belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the destination is on the public network, do not specify this option.

-resolve-as: Specifies a routing table for AS resolution. Tracert searches the specified routing table for the AS that each hop along the path belongs to. If you do not specify this keyword, the global routing table is used. If the AS information is found, this command displays the AS number next to the address of the hop in the probe result.

- **global**: Specifies the global routing table.
- **none**: Disables AS resolution.
- **vpn**: Specifies the VPN routing table.

-w *timeout*: Specifies the timeout time (in milliseconds) of the reply packet of a probe packet. The value range is 1 to 65535, and the default is 5000.

host: Specifies the IPv6 address or host name of the destination. The host name is a case-insensitive string of 1 to 253 characters. It can contain letters, digits, and special characters such as hyphen (-), underscore (_), and dot (.).

Usage guidelines

After identifying network failure with the **ping ipv6** command, you can use the **tracert ipv6** command to locate failed nodes.

If the destination address is on the public network, you do not need to specify the **-resolve-as** keyword to obtain the AS information. The device automatically uses the global routing table for AS resolution.

If the destination address is on a private network, address information of intermediate hops might be stored in either the global routing table or the VPN routing table. To learn the AS path that the packets traverse, execute the **tracert ipv6** command twice, once with the **-resolve-as global** keywords and again with the **-resolve-as vpn** keywords.

The output from the **tracert ipv6** command includes IPv6 addresses of all the Layer 3 devices that the packets traverse from source to destination. Asterisks (* * *) are displayed if the device cannot reply with an ICMP error message. The reason might be the destination is unreachable or sending ICMP timeout/destination unreachable packets is disabled.

Before starting an IPv6 tracert operation, you must enable sending of ICMPv6 destination unreachable messages on the intermediate devices between the source and destination. The IPv6 tracert operation stops if any of the following ICMPv6 destination unreachable messages is received:

- **!N**—No route to destination.
- **!P**—Communication with destination administratively prohibited by filtering policies.
- **!A**—Address unreachable. The unreachable reason is unknown.
- **!S**—Beyond scope of source address. This message is displayed if the probe packet has a link-local source address and a non-link-local destination address. Such a packet cannot be delivered to the destination without leaving the scope of the source address.

To abort the tracert operation during the execution of the command, press **Ctrl+C**.

Examples

Display the path that the packets traverse from source to destination (2001:3::2).

```
<Sysname> tracert ipv6 2001:3::2
traceroute to 2001:3::2(2001:3::2), 30 hops at most, 60 byte packets, press CTRL+C to break
 1  2001:1::2  0.661 ms  0.618 ms  0.579 ms
```

```
 2  2001:2::2 [AS 100]  0.861 ms  0.718 ms  0.679 ms
 3  2001:3::2 [AS 200]  0.822 ms  0.731 ms  0.708 ms
```

Display the path that the packets traverse from source to destination (2001:3::2) in VPN instance vpn1, as well as the AS information of the hops along the path.

```
<Sysname> tracert ipv6 –vpn-instance vpn1 –resolve-as vpn 2001:3::2
traceroute to 2001:3::2(2001:3::2), 30 hops at most, 60 byte packets , press CTRL+C to
break
1  2001:1::2  0.661 ms  0.618 ms  0.579 ms
2  2001:2::2  0.861 ms  0.718 ms  0.679 ms
3  2001:3::2 [AS 65535]  0.822 ms  0.731 ms  0.708 ms
```

Table 5 Command output

Field	Description
traceroute to 2001:3::2	Display the route that the IPv6 packets traverse from the current device to the device whose IP address is 2001:3:2.
hops at most	Maximum number of hops of the probe packets, which can be set by the **-m** keyword.
byte packets	Number of bytes of a probe packet.
press CTRL+C to break	During the execution of the command, press escape key **Ctrl+C** to abort the IPv6 tracert operation. The escape key is configurable by using the **escape-key** command. For more information about this command, see login management commands in *Fundamentals Command Reference*.
2 2001:2::2 [AS 100] 0.861 ms 0.718 ms 0.679 ms	Probe result of the probe packets that contain a hoplimit value of 2, including the following information about the second hop: • IPv6 address of the hop. • Number of the AS the hop belongs to. The AS number appears only when it is found for the hop in the specified routing table. • The round-trip time of the probe packets. The number of packets that can be sent in each probe can be set by using the **-q** keyword.

Contents

NTP commands

The device is inadequate in clock precision. As a best practice, do not use the device as a time server to synchronize the time of the other devices.

NTP is supported only on the following Layer 3 interfaces:

- Layer 3 Ethernet interfaces.
- Layer 3 Ethernet subinterfaces.
- Layer 3 aggregate interfaces.
- Layer 3 aggregate subinterfaces.
- VLAN interfaces.
- Tunnel interfaces.

display ntp-service ipv6 sessions

Use **display ntp-service ipv6 sessions** to display information about all IPv6 NTP associations.

Syntax

display ntp-service ipv6 sessions [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

verbose: Displays detailed information about all IPv6 NTP associations. If you do not specify this keyword, the command displays only brief information about the IPv6 NTP associations.

Examples

Display brief information about all IPv6 NTP associations.

```
<Sysname> display ntp-service ipv6 sessions
Notes: 1 source(master), 2 source(peer), 3 selected, 4 candidate, 5 configured.

 Source:   [125]3000::32
 Reference: 127.127.1.0          Clock stratum: 2
 Reachabilities: 1               Poll interval: 64
 Last receive time: 6            Offset: -0.0
 Roundtrip delay: 0.0            Dispersion: 0.0

 Total sessions : 1
```

Table 1 Command output

Field	Description
[12345]	• **1**—Clock source selected by the system (the current reference source). • **2**—The stratum level of the clock source is less than or equal to 15. • **3**—The clock source has survived the clock selection algorithm. • **4**—The clock source is a candidate clock source. • **5**—The clock source was created by a command.
Source	IPv6 address of the NTP server. If this field displays **::**, the IPv6 address of the NTP server has not been resolved successfully.

Reference	Reference clock ID of the NTP server:
	• If the reference clock is the local clock, the value of this field is related to the value of the **Clock stratum** field:
	  ◦ When the value of the **Clock stratum** field is 0 or 1, this field displays **LOCL**.
	  ◦ When the **Clock stratum** field has another value, this field displays the MD5 digest value of the first 32 bits of the IPv6 address. The MD5 digest value is in dotted decimal format.
	• If the reference clock is the clock of another device on the network, this field displays the MD5 digest value of the first 32 bits of the IPv6 address. The MD5 digest value is in dotted decimal format. If this field displays **INIT**, the local device has not established a connection with the NTP server.

Clock stratum	Stratum level of the NTP server, which determines the clock accuracy. The value is in the range of 1 to 16. A lower stratum level represents higher clock accuracy. A stratum 16 clock is not synchronized and cannot be used as a reference clock.
Reachabilities	Reachability count of the NTP server. 0 indicates that the NTP server is unreachable.
Poll interval	Polling interval in seconds. It is the maximum interval between successive NTP messages.
Last receive time	Length of time from when the last NTP message was received or when the local clock was last updated to the current time. Time is in seconds by default. • If the time length is greater than 2048 seconds, it is displayed in minutes (m). • If the time length is greater than 300 minutes, it is displayed in hours (h). • If the time length is greater than 96 hours, it is displayed in days (d). • If the time length is greater than 999 days, it is displayed in years (y). If the time when the most recent NTP message was received or when the local clock was updated most recently is behind the current time, this field displays a hyphen (-).
Offset	Offset of the system clock relative to the reference clock, in milliseconds.
Roundtrip delay	Roundtrip delay from the local device to the clock source, in milliseconds.
Dispersion	Maximum error of the system clock relative to the reference source.
Total sessions	Total number of associations.

Display detailed information about all IPv6 NTP associations.

```
<Sysname> display ntp-service ipv6 sessions verbose
```

```
Clock source: 1::1
Session ID: 36144
Clock stratum: 16
Clock status:  configured, insane, valid, unsynced
Reference clock ID: INIT
VPN instance: Not specified
Local mode: sym_active, local poll interval: 6
Peer mode: unspec, peer poll interval: 10
Offset: 0.0000ms, roundtrip delay: 0.0000ms, dispersion:  15937ms
Root roundtrip delay: 0.0000ms, root dispersion: 0.0000ms
Reachabilities:0, sync distance: 15.938
Precision: 2^-18, version: 4, source interface: Not specified
Reftime: 00000000.00000000  Thu, Feb  7 2036  6:28:16.000
Orgtime: d17cbb21.0f318106  Tue, May 17 2011  9:15:13.059
Rcvtime: 00000000.00000000  Thu, Feb  7 2036  6:28:16.000
Xmttime: 00000000.00000000  Thu, Feb  7 2036  6:28:16.000
Roundtrip delay samples: 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000
Offset samples: 0.00  0.00  0.00  0.00  0.00  0.00  0.00  0.00
Filter order: 0     1     2     3     4     5     6     7

Total sessions: 1
```

Table 2 Command output

Field	Description
Clock source	IPv6 address of the clock source. If this field displays **::**, the IPv6 address of the NTP server has not been resolved successfully.
Clock stratum	Stratum level of the NTP server, which determines the clock precision. The value is in the range of 1 to 16. A lower stratum level represents higher clock accuracy. A stratum 16 clock is not synchronized and cannot be used as a reference clock.

Clock status	Status of the clock source corresponding to this association:
	• **configured**—The association was created at the CLI.
	• **dynamic**—The association is established dynamically.
	• **master**—The clock source is the primary NTP server of the current system.
	• **selected**—The clock source has survived the clock selection algorithm.
	• **candidate**—The clock source is the candidate reference source.
	• **sane**—The clock source has passed authentication and its clock will be used as the reference clock.
	• **insane**—The clock source has not passed authentication, or it has passed authentication but its clock will not be used as the reference clock.
	• **valid**—The clock source is valid, which means the clock source meets the following requirements:
	  ○ It has been authenticated and synchronized.
	  ○ Its stratum level is valid.
	  ○ Its root delay and root dispersion values are within their ranges.
	• **invalid**—The clock source is invalid.
	• **unsynced**—The clock source has not been synchronized or the value of the stratum level is invalid.

Field	Description

Reference clock ID	• If the reference clock is the local clock, the value of this field is related to the value of the Clock stratum field:
	  ○ When the value of the Clock stratum field is 0 or 1, this field displays **LOCL**.
	  ○ When the Clock stratum field has another value, this field displays the MD5 digest value of the first 32 bits of the IPv6 address. The MD5 digest value is in dotted decimal format.
	• If the reference clock is the clock of another device on the network, this field displays the MD5 digest value of the first 32 bits of the IPv6 address. The MD5 digest value is in dotted decimal format. If this field displays **INIT**, the local device has not established a connection with the NTP server.

VPN instance	VPN instance of the NTP server. If the NTP server is in a public network, this field displays **Not specified**.
Local mode	Operation mode of the local device: • **unspec**—The mode is unspecified. • **sym_active**—Active mode. • **sym_passive**—Passive mode. • **client**—Client mode. • **server**—Server mode. • **broadcast**—Broadcast or multicast server mode. • **bclient**—Broadcast or multicast client mode.
local poll interval	Polling interval for the local device, in seconds. The value displayed is a power of 2. For example, if the displayed value is 6, the poll interval of the local device is 2^6, or 64 seconds.
peer mode	Operation mode of the peer device: • **unspec**—The mode is unspecified. • **sym_active**—Active mode. • **sym_passive**—Passive mode. • **client**—Client mode. • **server**—Server mode. • **broadcast**—Broadcast or multicast server mode. • **bclient**—Broadcast or multicast client mode.
peer poll interval	Polling interval for the peer device, in seconds. The value displayed is a power of 2. For example, if the displayed value is 6, the polling interval of the local device is 2^6, or 64 seconds.
Offset	Offset of the system clock relative to the reference clock, in milliseconds.
roundtrip delay	Roundtrip delay from the local device to the clock source, in milliseconds.
dispersion	Maximum error of the system clock relative to the reference clock.
Root roundtrip delay	Roundtrip delay from the local device to the primary NTP server, in milliseconds.
root dispersion	Maximum error of the system clock relative to the primary reference clock, in milliseconds.
Reachabilities	Reachability count of the clock source. 0 indicates that the clock source is unreachable.
sync distance	Synchronization distance relative to the upper-level clock, in seconds, and calculated from dispersion and roundtrip delay values.
Precision	Accuracy of the system clock.
version	NTP version in the range of 1 to 4.

Field	Description
source interface	Source interface. If the source interface is not specified, this field displays **Not specified**.
Reftime	Reference timestamp in the NTP message.
Orgtime	Originate timestamp in the NTP message.
Rcvtime	Receive timestamp in the NTP message.
Xmttime	Transmit timestamp in the NTP message.
Filter order	Dispersion information.
Reference clock status	Status of the local clock. The field is displayed only when you use the **ntp-service refclock-master** command to set the local clock as a reference clock. When the reach field of the local clock is 255, the field is displayed as **working normally**. Otherwise, the field is displayed as **working abnormally**.
Total sessions	Total number of associations.

display ntp-service sessions

Use **display ntp-service sessions** to display information about all IPv4 NTP associations.

Syntax

display ntp-service sessions [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

verbose: Displays detailed information about all IPv4 NTP associations. If you do not specify this keyword, the command displays only brief information about the NTP associations.

Usage guidelines

When a device is operating in NTP broadcast or multicast server mode, the **display ntp-service sessions** command does not display the IPv4 NTP association information corresponding to the broadcast or multicast server. However, the associations are counted in the total number of associations.

Examples

Display brief information about all IPv4 NTP associations.

```
<Sysname> display ntp-service sessions
       source          reference       stra reach poll  now offset  delay disper
**************************************************************************
[12345]LOCAL(0)        LOCL               0     1   64    - 0.0000 0.0000 7937.9
    [5]0.0.0.0         INIT              16     0   64    - 0.0000 0.0000 0.0000
```

```
Notes: 1 source(master), 2 source(peer), 3 selected, 4 candidate, 5 configured.
 Total sessions: 1
```

Table 3 Command output

Field	Description
source	• When the reference clock is the local clock, the field displays **LOCAL** (*number*). It indicates that the IP address of the local clock is 127.127.1.*number*, where *number* represents the NTP process number in the range of 0 to 3. • When the reference clock is the clock of another device, the field displays the IP address of the NTP server. If this field displays **0.0.0.0**, the IP address of the NTP server has not been resolved successfully.

reference	Reference clock ID of the NTP server:
	• If the reference clock is the local clock, the value of this field is related to the value of the **stra** field:
	  ○ When the value of the **stra** field is 0 or 1, this field displays **LOCL**.
	  ○ When the **stra** field has another value, this field displays the IP address of the local clock.
	• If the reference clock is the clock of another device on the network, this field displays the IP address of the device. If the device supports IPv6, this field displays the MD5 digest of the first 32 bits of the IPv6 address of the device. If this field displays **INIT**, the local device has not established a connection with the NTP server.

stra	Stratum level of the clock source, which determines the clock accuracy. The value is in the range of 1 to 16. The clock accuracy decreases from stratum 1 to stratum 16. A stratum 1 clock has the highest precision, and a stratum 16 clock is not synchronized and cannot be used as a reference clock.
reach	Reachability count of the clock source. 0 indicates that the clock source is unreachable.
poll	Polling interval in seconds. It is the maximum interval between successive NTP messages.
now	Length of time from when the last NTP message was received or when the local clock was last updated to the current time. Time is in seconds by default. • If the time length is greater than 2048 seconds, it is displayed in minutes (m). • If the time length is greater than 300 minutes, it is displayed in hours (h). • If the time length is greater than 96 hours, it is displayed in days (d). • If the time length is greater than 999 days, it is displayed in years (y). If the time when the most recent NTP message was received or when the local clock was updated most recently is behind the current time, this field displays a hyphen (-).
offset	Offset of the system clock relative to the reference clock, in milliseconds.
delay	Roundtrip delay from the local device to the NTP server, in milliseconds.
disper	Maximum error of the system clock relative to the reference source, in milliseconds.
[12345]	• **1**—Clock source selected by the system (the current reference source). • **2**—The stratum level of the clock source is less than or equal to 15. • **3**—The clock source has survived the clock selection algorithm. • **4**—The clock source is a candidate clock source. • **5**—The clock source was created by a configuration command.
Total sessions	Total number of associations.

Display detailed information about all IPv4 NTP associations.

```
<Sysname> display ntp-service sessions verbose
 Clock source: 192.168.1.40
 Session ID: 35888
 Clock stratum: 2
 Clock status:  configured, master, sane, valid
 Reference clock ID: 127.127.1.0
 VPN instance: Not specified
 Local mode: client, local poll interval: 6
 Peer mode: server, peer poll interval: 6
 Offset: 0.2862ms, roundtrip delay: 3.2653ms, dispersion: 4.5166ms
 Root roundtrip delay: 0.0000ms, root dispersion: 10.910ms
 Reachabilities:31, sync distance: 0.0194
 Precision: 2^-18, version: 3, source interface: Not specified
 Reftime: d17cbba5.1473de1e  Tue, May 17 2011  9:17:25.079
 Orgtime: 00000000.00000000  Thu, Feb  7 2036  6:28:16.000
 Rcvtime: d17cbbc0.b1959a30  Tue, May 17 2011  9:17:52.693
 Xmttime: d17cbbc0.b1959a30  Tue, May 17 2011  9:17:52.693
 Roundtrip delay samples: 0.007 0.010 0.006 0.011 0.010 0.005 0.007 0.003
 Offset samples: 5629.55 3913.76 5247.27 6526.92 31.99 148.72 38.27 0.29
 Filter order: 7     5     2     6     0     4     1     3

 Total sessions: 1
```

Table 4 Command output

Field	Description
Clock source	IP address of the NTP server. If this field displays **0.0.0.0**, the IP address of the NTP server has not been resolved successfully.
Clock stratum	Stratum level of the NTP server, which determines the clock accuracy. The value is in the range of 1 to 16. A lower stratum level represents greater clock accuracy. A stratum 16 clock is not synchronized and cannot be used as a reference clock.

Clock status	Status of the clock source corresponding to this association:
	• **configured**—The association was created by a configuration command.
	• **dynamic**—The association is established dynamically.
	• **master**—The clock source is the primary NTP server of the current system.
	• **selected**—The clock source has survived the clock selection algorithm.
	• **candidate**—The clock source is the candidate reference source.
	• **sane**—The clock source has passed authentication and its clock will be used as the reference clock.
	• **insane**—The clock source has not passed authentication, or it has passed authentication but its clock will not be used as the reference clock.
	• **valid**—The clock source is valid, which means the clock source meets the following requirements:
	  ○ It has been authenticated and synchronized.
	  ○ Its stratum level is valid.
	  ○ Its root delay and root dispersion values are within their ranges.
	• **invalid**—The clock source is invalid.
	• **unsynced**—The clock source has not been synchronized or the value of the stratum level is invalid.

Field	Description

Reference clock ID	Reference clock ID of the NTP server:
	• If the reference clock is the local clock, the value of this field is related to the value of the **Clock** stratum field:
	  ○ When the value of the **Clock** stratum field is 0 or 1, this field displays **LOCL**.
	  ○ When the **Clock** stratum field has another value, this field displays the IP address of the local clock.
	• If the reference clock is the clock of another device on the network, this field displays the IP address of the device. If the device supports IPv6, this field displays the MD5 digest of the first 32 bits of the IPv6 address of the device. If this field displays **INIT**, the local device has not established a connection with the NTP server.

VPN instance	VPN instance to which the NTP server belongs. If the NTP server is in a public network, the field displays **Not specified**.
Local mode	Operation mode of the local device: • **unspec**—The mode is unspecified. • **active**—Active mode. • **passive**—Passive mode. • **client**—Client mode. • **server**—Server mode. • **broadcast**—Broadcast or multicast server mode. • **bclient**—Broadcast or multicast client mode.
local poll interval	Polling interval of the local device, in seconds. The value displayed is a power of 2. For example, if the displayed value is 6, the poll interval of the local device is 2^6, or 64 seconds.
Peer mode	Operation mode of the peer device: • **unspec**—The mode is unspecified. • **active**—Active mode. • **passive**—Passive mode. • **client**—Client mode. • **server**—Server mode. • **broadcast**—Broadcast or multicast server mode. • **bclient**—Broadcast or multicast client mode.
peer poll interval	Polling interval of the peer device, in seconds. The value displayed is a power of 2. For example, if the displayed value is 6, the poll interval of the local device is 2^6, or 64 seconds.
Offset	Offset of the system clock relative to the reference clock, in milliseconds.
roundtrip delay	Roundtrip delay from the local device to the NTP server, in milliseconds.
dispersion	Maximum error of the system clock relative to the reference clock.
Root roundtrip delay	Roundtrip delay from the local device to the primary NTP server, in milliseconds.
root dispersion	Maximum error of the system clock relative to the primary reference clock, in milliseconds.
Reachabilities	Reachability count of the clock source. 0 indicates that the clock source is unreachable.
sync distance	Synchronization distance relative to the upper-level clock, in seconds, and calculated from dispersion and roundtrip delay values.
Precision	Accuracy of the system clock.

Field	Description
version	NTP version in the range of 1 to 4.
source interface	Source interface. If the source interface is not specified, this field is **Not specified**.
Reftime	Reference timestamp in the NTP message.
Orgtime	Originate timestamp in the NTP message.
Rcvtime	Receive timestamp in the NTP message.
Xmttime	Transmit timestamp in the NTP message.
Filter order	Sample information order.
Reference clock status	Status of the local clock. The field is displayed only when you use the **ntp-service refclock-master** command to set the local clock as a reference clock. When the reach field of the local clock is 255, the field is displayed as **working normally**. Otherwise, the field is displayed as **working abnormally**.
Total sessions	Total number of associations.

display ntp-service status

Use **display ntp-service status** to display NTP service status.

Syntax

display ntp-service status

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display NTP service status after time synchronization.

```
<Sysname> display ntp-service status
 Clock status: synchronized
 Clock stratum: 2
 System peer: LOCAL(0)
 Local mode: client
 Reference clock ID: 127.127.1.0
 Leap indicator: 00
 Clock jitter: 0.000977 s
 Stability: 0.000 pps
 Clock precision: 2^-18
 Root delay: 0.00000 ms
 Root dispersion: 3.96367 ms
 Reference time: d0c5fc32.92c70b1e  Wed, Dec 29 2010 18:28:02.573
```

```
System poll interval: 64 s
```

Display the NTP service status when time is not synchronized.

```
<Sysname> display ntp-service status
 Clock status: unsynchronized
 Clock stratum: 16
 Reference clock ID: none
 Clock jitter: 0.000000 s
 Stability: 0.000 pps
 Clock precision: 2^-18
 Clock precision:
 Root delay: 0.00000 ms
 Root dispersion: 0.00002 ms
 Reference time: d0c5fc32.92c70b1e  Wed, Dec 29 2010 18:28:02.573
 System poll interval: 8 s
```

Table 5 Command output

Field	Description
Clock status	Status of the system clock: • **synchronized**—The system clock has been synchronized. • **unsynchronized**—The system clock has not been synchronized.
Clock stratum	Stratum level of the system clock.
System peer	IP address of the selected NTP server.
Local mode	Operation mode of the local device: • **unspec**—The mode is unspecified. • **active**—Active mode. • **passive**—Passive mode. • **client**—Client mode. • **server**—Server mode. • **broadcast**—Broadcast or multicast server mode. • **bclient**—Broadcast or multicast client mode.
Reference clock ID	For an IPv4 NTP server: The field represents the IP address of the remote server when the local device is synchronized to a remote NTP server. The field represents the local clock when the local device uses the local clock as the reference source. • When the local clock has a stratum level of 1, this field displays **LOCL**. • When the local clock has any other stratum, this field displays the IP address of the local clock. For an IPv6 NTP server: The field represents the MD5 digest of the first 32 bits of the IPv6 address of the remote server when the local device is synchronized to a remote IPv6 NTP server. The field represents the local clock when the local device uses the local clock as the reference source. • When the local clock has a stratum level of 1, this field displays **LOCL**. • When the local clock has any other stratum, this field displays the MD5 digest of the first 32 bits of the IPv6 address of the local clock.

Field	Description
Leap indicator	Alarming status: • **00**—Normal. • **01**—Leap second, indicates that the last minute in a day has 61 seconds. • **10**—Leap second, indicates that the last minute in a day has 59 seconds. • **11**—Time is not synchronized.
Clock jitter	Difference between the system clock and reference clock, in seconds.
Stability	Clock frequency stability. A lower value represents better stability.
Clock precision	Accuracy of the system clock.
Root delay	Roundtrip delay from the local device to the primary NTP server, in milliseconds.
Root dispersion	Maximum error of the system clock relative to the primary NTP server, in milliseconds.
Reference time	Reference timestamp.
System poll interval	System polling interval in seconds.

display ntp-service trace

Use **display ntp-service trace** to display brief information about each NTP server from the local device back to the primary NTP server.

Syntax

display ntp-service trace [**source** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

source *interface-type interface-number*: Specifies the source interface for sending NTP packets to trace each NTP server from the local device back to the primary NTP server. The source IP address of the NTP packets is the IPv4 address/IPv6 address of the specified source interface. If the IP address of an NTP server is a link-local address, the link-local address of the outgoing interface of NTP packets is used as the source IP address of the NTP packets. If you do not specify this option, the interface that sends the tracing NTP packets acts as the source interface.

Usage guidelines

To trace back to the primary NTP server from the source interface, make sure the source interface and the NTP servers from the local device to the primary NTP server are reachable to each other.

Examples

Display brief information about each NTP server from the local device back to the primary NTP server.

```
<Sysname> display ntp-service trace
Server     127.0.0.1
```

```
Stratum    3, jitter  0.000, synch distance 0.0000.
Server     3000::32
Stratum    2 , jitter 790.00, synch distance 0.0000.
RefID      127.127.1.0
```

The output shows that server 127.0.0.1 is synchronized to server 3000::32, and server 3000::32 is synchronized to the local clock.

Table 6 Command output

Field	Description
Server	IP address of the NTP server.
Stratum	Stratum level of the NTP server.
jitter	Root mean square (RMS) value of the clock offset relative to the upper-level clock, in milliseconds.
synch distance	Synchronization distance relative to the upper-level NTP server, in seconds, calculated from dispersion and roundtrip delay values.
RefID	Identifier of the primary NTP server. When the stratum level of the primary reference clock is 0, it is displayed as **LOCL**. Otherwise, it is displayed as the IP address of the primary reference clock.

Related commands

ntp-service ipv6 source

ntp-service ipv6 unicast-peer

ntp-service ipv6 unicast-server

ntp-service source

ntp-service unicast-peer

ntp-service unicast-server

ntp-service acl

Use **ntp-service acl** to configure the right for peer devices to access the IPv4 NTP services on the local device.

Use **undo ntp-service** to remove the configured IPv4 NTP service access right.

Syntax

ntp-service { **peer** | **query** | **server** | **synchronization** } **acl** *ipv4-acl-number*

undo ntp-service { **peer** | **query** | **server** | **synchronization** } [**acl** *ipv4-acl-number*]

Default

The right for the peer devices to access the IPv4 NTP services on the local device is **peer**.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

peer: Allows time requests and NTP control queries (such as alarms, authentication status, and time server information) from a peer device and allows the local device to synchronize itself to a peer device.

query: Allows only NTP control queries from a peer device to the local device.

server: Allows time requests and NTP control queries from a peer device, but does not allow the local device to synchronize itself to a peer device.

synchronization: Allows only time requests from a peer device.

acl *ipv4-acl-number*: Specifies an IPv4 ACL by its number. The peer devices that match the IPv4 ACL have the access right specified in the command. The *ipv4-acl-number* argument represents an IPv4 basic ACL number in the range of 2000 to 2999 or an IPv4 advanced ACL number in the range of 3000 to 3999.

Usage guidelines

When the device receives an IPv4 NTP request, it matches the request against the access rights in order from the least restrictive to the most restrictive: **peer**, **server**, **synchronization**, and **query**.

- If no IPv4 NTP access control is configured, the **peer** access right applies.
- If the IP address of the peer device matches a **permit** statement in an IPv4 ACL, the access right is granted to the peer device. If a **deny** statement or no IPv4 ACL is matched, no access right is granted.
- If no IPv4 ACL is specified for an access right or the IPv4 ACL specified for the access right is not created, the access right is not granted.
- If none of the IPv4 ACLs specified for the access rights is created, the **peer** access right applies.
- If none of the IPv4 ACLs specified for the access rights contains rules, no access right is granted.

The **ntp-service acl** command provides minimal security for a system running NTP. A more secure method is NTP authentication.

Examples

Configure the peer devices on subnet 10.10.0.0/16 to have full access to the local device.

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 10.10.0.0 0.0.255.255
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] ntp-service peer acl 2001
```

Related commands

ntp-service authentication enable

ntp-service authentication-keyid

ntp-service reliable authentication-keyid

ntp-service authentication enable

Use **ntp-service authentication enable** to enable NTP authentication.

Use **undo ntp-service authentication enable** to disable NTP authentication.

Syntax

ntp-service authentication enable

undo ntp-service authentication enable

Default

NTP authentication is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

Enable NTP authentication in networks that require time synchronization security to make sure NTP clients are synchronized only to authenticated NTP servers.

To authenticate an NTP server, set an authentication key and specify it as a trusted key.

Examples

Enable NTP authentication.

```
<Sysname> system-view
[Sysname] ntp-service authentication enable
```

Related commands

ntp-service authentication-keyid

ntp-service reliable authentication-keyid

ntp-service authentication-keyid

Use **ntp-service authentication-keyid** to set an NTP authentication key.

Use **undo ntp-service authentication-keyid** to remove an NTP authentication key.

Syntax

ntp-service authentication-keyid *keyid* **authentication-mode md5** { **cipher** | **simple** } *string* [**acl** *ipv4-acl-number* | **ipv6 acl** *ipv6-acl-number*] *

undo ntp-service authentication-keyid *keyid*

Default

No NTP authentication key exists.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

keyid: Specifies an authentication key ID in the range of 1 to 4294967295.

authentication-mode md5: Specifies the MD5 authentication algorithm.

cipher: Specifies an authentication key in encrypted form.

simple: Specifies an authentication key in plaintext form. For security purposes, the authentication key specified in plaintext form will be stored in encrypted form.

string: Specifies a case-sensitive authentication key. Its plaintext form is a string of 1 to 32 characters. Its encrypted form is a string of 1 to 73 characters.

acl *ipv4-acl-number*: Specifies an IPv4 basic ACL by its number in the range of 2000 to 2999. Only the devices permitted by the ACL can use the key ID for authentication.

ipv6 acl *ipv6-acl-number*: Specifies an IPv6 basic ACL by its number in the range of 2000 to 2999. Only the devices permitted by the ACL can use the key ID for authentication.

Usage guidelines

NTP authentication must be enabled on an NTP network that requires time synchronization security. NTP authentication ensures that NTP clients are synchronized only to authenticated NTP time servers.

The key ID in the message from the peer device identifies the key used for authentication. The **acl** *ipv4-acl-number* or **acl** *ipv6-acl-number* option is used to identify the peer device that can use the key ID.

- If the specified IPv4 or IPv6 ACL does not exist, any device can use the key ID for authentication.
- If the specified IPv4 or IPv6 ACL does not contain any rules, no device can use the key ID for authentication.

To ensure a successful NTP authentication, configure the same key ID and key on the time server and client. Make sure the peer device is allowed to use the key ID for authentication on the local device.

After you specify an NTP authentication key, use the **ntp-service reliable authentication-keyid** command to configure the key as a trusted key. The key automatically changes to untrusted after you delete the key. In this case, you do not need to execute the **undo ntp-service reliable authentication-keyid** command.

You can set a maximum of 128 authentication keys by executing the command.

Examples

Set a plaintext MD5 authentication key, with the key ID of **10** and key value of **BetterKey**.

```
<Sysname> system-view
[Sysname] ntp-service authentication enable
[Sysname] ntp-service authentication-keyid 10 authentication-mode md5 simple BetterKey
```

Related commands

ntp-service authentication enable

ntp-service reliable authentication-keyid

ntp-service broadcast-client

Use **ntp-service broadcast-client** to configure the device to operate in NTP broadcast client mode and use the current interface to receive NTP broadcast packets.

Use **undo ntp-service broadcast-client** to remove the configuration.

Syntax

ntp-service broadcast-client

undo ntp-service broadcast-client

Default

The device does not operate in any NTP association mode.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

After you configure the command, the device listens to NTP messages sent by the NTP broadcast server and is synchronized based on the received NTP messages.

If you have configured the device to operate in broadcast client mode on an interface with the command, do not add the interface to any aggregate group. To add the interface to an aggregate group, remove the configuration of the command.

Examples

Configure the device to operate in broadcast client mode and receive NTP broadcast messages on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ntp-service broadcast-client
```

Related commands

ntp-service broadcast-server

ntp-service broadcast-server

Use **ntp-service broadcast-server** to configure the device to operate in NTP broadcast server mode and use the current interface to send NTP broadcast packets.

Use **undo ntp-service broadcast-server** to remove the configuration.

Syntax

ntp-service broadcast-server [**authentication-keyid** *keyid* | **version** *number*] *

undo ntp-service broadcast-server

Default

The device does not operate in any NTP association mode.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

authentication-keyid *keyid*: Specifies the key ID to be used for sending broadcast messages to broadcast clients. The value range for the *keyid* argument is 1 to 4294967295. If you do not specify this option, the local device cannot synchronize broadcast clients enabled with NTP authentication.

version *number*: Specifies the NTP version. The value range for the *number* argument is 1 to 4, and the default is 4.

Usage guidelines

After you configure the command, the device periodically sends NTP messages to the broadcast address 255.255.255.255.

If you have configured the device to operate in broadcast server mode on an interface with the command, do not add the interface to any aggregate group. To add the interface to an aggregate group, remove the configuration of the command.

Examples

Configure the device to operate in broadcast server mode and send NTP broadcast messages on GigabitEthernet 1/0/1, using key 4 for encryption. Set the NTP version to 4.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ntp-service broadcast-server authentication-keyid 4
version 4
```

Related commands

ntp-service broadcast-client

ntp-service dscp

Use **ntp-service dscp** to set a DSCP value for IPv4 NTP packets.

Use **undo ntp-service dscp** to restore the default.

Syntax

ntp-service dscp *dscp-value*

undo ntp-service dscp

Default

The DSCP value for IPv4 NTP packets is 48.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

dscp-value: Sets a DSCP value in the range of 0 to 63 for IPv4 NTP packets.

Usage guidelines

The DSCP value is included in the ToS field of an IPv4 packet to identify the packet priority.

Examples

Set the DSCP value for IPv4 NTP packets to **30**.

```
<Sysname> system-view
[Sysname] ntp-service dscp 30
```

ntp-service enable

Use **ntp-service enable** to enable the NTP service.

Use **undo ntp-service enable** to disable the NTP service.

Syntax

ntp-service enable

undo ntp-service enable

Default

The NTP service is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Examples

Enable the NTP service.

```
<Sysname> system-view
[Sysname] ntp-service enable
```

ntp-service inbound enable

Use **ntp-service inbound enable** to enable an interface to receive NTP messages.

Use **undo ntp-service inbound enable** to disable an interface from receiving NTP messages.

Syntax

ntp-service inbound enable

undo ntp-service inbound enable

Default

An interface receives NTP messages.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

Execute the **undo ntp-service inbound enable** command on an interface in the following cases:

- You do not want the interface to synchronize the peer device in the corresponding subnet.
- You do not want the device to be synchronized by the peer device in the subnet corresponding to the interface.

Examples

Disable GigabitEthernet 1/0/1 from receiving NTP messages.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo ntp-service inbound enable
```

ntp-service ipv6 acl

Use **ntp-service ipv6 acl** to configure the right for the peer devices to access the IPv6 NTP services of the local device.

Use **undo ntp-service ipv6** to remove the configured IPv6 NTP service access right.

Syntax

ntp-service ipv6 { **peer** | **query** | **server** | **synchronization** } **acl** *ipv6-acl-number*

undo ntp-service ipv6 { **peer** | **query** | **server** | **synchronization** } [**acl** *ipv6-acl-number*]

Default

The right for the peer devices to access the IPv6 NTP services on the local device is **peer**.

Views

System view

Predefined user roes

network-admin

context-admin

Parameters

peer: Allows time requests and NTP control queries (such as alarms, authentication status, and time server information) and allows the local device to synchronize itself to a peer device.

query: Allows only NTP control queries from a peer device to the local device.

server: Allows time requests and NTP control queries, but does not allow the local device to synchronize itself to a peer device.

synchronization: Allows only time requests from a system whose address passes the access list criteria.

ipv6-acl-number: Specifies an IPv6 ACL by its number. The peer devices that match the IPv6 ACL have the access right specified in the command. The *ipv6-acl-number argument* represents a basic IPv6 ACL number in the range of 2000 to 2999 or an advanced IPv6 ACL number in the range of 3000 to 3999.

Usage guidelines

When the device receives an IPv6 NTP request, it matches the request against the access rights in order from the least restrictive to the most restrictive: **peer**, **server**, **synchronization**, and **query**.

- If no IPv6 NTP access control is configured, the **peer** access right applies.
- If the IP address of the peer device matches a **permit** statement in an IPv6 ACL, the access right is granted to the peer device. If a **deny** statement or no IPv6 ACL is matched, no access right is granted.
- If no IPv6 ACL is specified for an access right or the IPv6 ACL specified for the access right is not created, the access right is not granted.

- If none of the IPv6 ACLs specified for the access rights is created, the **peer** access right applies.
- If none of the IPv6 ACLs specified for the access rights contains rules, no access right is granted.

The **ntp-service ipv6 acl** command provides a minimum security method. NTP authentication is more secure.

Examples

Configure the peer devices on subnet 2001::1 to have full access to the local device.

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2001
[Sysname-acl-ipv6-basic-2001] rule permit source 2001::1 64
[Sysname-acl-ipv6-basic-2001] quit
[Sysname] ntp-service ipv6 peer acl 2001
```

Related commands

ntp-service authentication enable

ntp-service authentication-keyid

ntp-service reliable authentication-keyid

ntp-service ipv6 dscp

Use **ntp-service ipv6 dscp** to set a DSCP value for IPv6 NTP packets.

Use **undo ntp-service ipv6 dscp** to restore the default.

Syntax

ntp-service ipv6 dscp *dscp-value*

undo ntp-service ipv6 dscp

Default

The DSCP value for IPv6 NTP packets is 56.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

dscp-value: Specifies a DSCP value in the range of 0 to 63 for IPv6 NTP packets.

Usage guidelines

The DSCP value is included in the Traffic Class field of an IPv6 packet to identify the packet priority.

Examples

Set the DSCP value for IPv6 NTP packets to **30**.

```
<Sysname> system-view
[Sysname] ntp-service ipv6 dscp 30
```

ntp-service ipv6 inbound enable

Use **ntp-service ipv6 inbound enable** to enable an interface to receive IPv6 NTP messages.

Use **undo ntp-service ipv6 inbound enable** to disable an interface from receiving IPv6 NTP messages.

Syntax

ntp-service ipv6 inbound enable

undo ntp-service ipv6 inbound enable

Default

An interface receives IPv6 NTP messages.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

Execute the **undo ntp-service ipv6 inbound enable** command on an interface in the following cases:

- You do not want the interface to synchronize the peer devices in the corresponding subnet.
- You do not want the device to be synchronized by the peer devices in the subnet corresponding to the interface.

Examples

Disable GigabitEthernet 1/0/1 from receiving IPv6 NTP messages.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo ntp-service ipv6 inbound enable
```

ntp-service ipv6 multicast-client

Use **ntp-service ipv6 multicast-client** to configure the device to operate in IPv6 NTP multicast client mode and use the current interface to receive IPv6 NTP multicast packets.

Use **undo ntp-service ipv6 multicast-client** to remove the configuration.

Syntax

ntp-service ipv6 multicast-client *ipv6-address*

undo ntp-service ipv6 multicast-client *ipv6-address*

Default

The device does not operate in any NTP association mode.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address: Specifies an IPv6 multicast address. An IPv6 broadcast client and an IPv6 broadcast server must be configured with the same multicast address.

Usage guidelines

After you configure the command, the device listens to IPv6 NTP messages using the specified multicast address as the destination address. It is synchronized based on the received IPv6 NTP messages.

If you have configured the device to operate in IPv6 multicast client mode on an interface by using the command, do not add the interface to any aggregate group. To add the interface to an aggregate group, remove the configuration of the command.

Examples

Configure the device to operate in IPv6 multicast client mode and receive IPv6 NTP multicast messages with the destination FF21::1 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ntp-service ipv6 multicast-client ff21::1
```

Related commands

ntp-service ipv6 multicast-server

ntp-service ipv6 multicast-server

Use **ntp-service ipv6 multicast-server** to configure the device to operate in IPv6 NTP multicast server mode and use the current interface to send IPv6 NTP multicast packets.

Use **undo ntp-service ipv6 multicast-server** to remove the configuration.

Syntax

ntp-service ipv6 multicast-server *ipv6-address* [**authentication-keyid** *keyid* | **ttl** *ttl-number*] *

undo ntp-service ipv6 multicast-server *ipv6-address*

Default

The device does not operate in any NTP association mode.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ipv6-address: Specifies an IPv6 multicast address. An IPv6 multicast client and server must be configured with the same multicast address.

authentication-keyid *keyid*: Specifies the key ID to be used for sending multicast messages to multicast clients. The value range for the *keyid* argument is 1 to 4294967295. If you do not specify this option, the local device cannot synchronize clients enabled with NTP authentication.

ttl *ttl-number*: Specifies the TTL of NTP multicast messages. The value range for the *ttl-number* argument is 1 to 255, and the default is 16.

Usage guidelines

After you configure the command, the device periodically sends NTP messages to the specified IPv6 multicast address.

If you have configured the device to operate in IPv6 multicast server mode on an interface with the command, do not add the interface to any aggregate group. To add the interface to an aggregate group, remove the configuration of the command.

Examples

Configure the device to operate in IPv6 multicast server mode and send IPv6 NTP multicast messages on GigabitEthernet 1/0/1 to the multicast address FF21::1, using key 4 for encryption.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ntp-service ipv6 multicast-server ff21::1
```

Related commands

ntp-service ipv6 multicast-client

ntp-service ipv6 source

Use **ntp-service ipv6 source** to specify a source interface for IPv6 NTP messages.

Use **undo ntp-service ipv6 source** to restore the default.

Syntax

ntp-service ipv6 source *interface-type interface-number*

undo ntp-service ipv6 source

Default

No source interface is specified for IPv6 NTP messages. The device automatically selects the source IP address for IPv6 NTP messages. For more information, see *RFC 3484*.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

If you specify a source interface for IPv6 NTP messages, the device uses the IPv6 address of the source interface as the source address to send IPv6 NTP messages. Consequently, the destination address of the IPv6 NTP response messages is the address of the source interface.

When the device responds to an IPv6 NTP request, the source IPv6 address of the NTP response is always the IPv6 address of the interface that has received the IPv6 NTP request.

If you do not want the IPv6 address of an interface on the local device to become the destination address for response messages, use the command to specify another interface as the source interface for IPv6 NTP messages.

The source interface for IPv6 NTP messages can also be specified in the following ways:

- In NTP client/server mode, if you have specified the source interface for IPv6 NTP messages in the **ntp-service ipv6 unicast-server** command, the specified interface acts as the source interface for IPv6 NTP messages.
- In NTP symmetric active/passive mode, if you have specified the source interface for IPv6 NTP messages in the **ntp-service ipv6 unicast-peer** command, the specified interface acts as the source interface for IPv6 NTP messages.
- In NTP multicast mode, if you have configured the **ntp-service ipv6 multicast-server** command on an interface, the interface acts as the source interface for NTP multicast messages.

If the specified source interface is down, the device does not send IPv6 NTP messages.

Examples

Specify the source interface of IPv6 NTP messages as GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] ntp-service ipv6 source gigabitethernet 1/0/1
```

ntp-service ipv6 unicast-peer

Use **ntp-service ipv6 unicast-peer** to specify an IPv6 symmetric-passive peer for the device.

Use **undo ntp-service ipv6 unicast-peer** to remove the IPv6 symmetric-passive peer specified for the device.

Syntax

ntp-service ipv6 unicast-peer { *peer-name* | *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**authentication-keyid** *keyid* | **maxpoll** *maxpoll-interval* | **minpoll** *minpoll-interval* | **priority** | **source** *interface-type interface-number*] *

undo ntp-service ipv6 unicast-peer { *peer-name* | *ipv6-address* } [**vpn-instance** *vpn-instance-name*]

Default

No IPv6 symmetric-passive peer is specified.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

peer-name: Specifies a symmetric-passive peer by its host name, a case-insensitive string of 1 to 253 characters. Valid characters are letters, digits, hyphens (-), underscores (_), and periods (.).

ipv6-address: Specifies a symmetric-passive peer by its IPv6 address. It must be a unicast address, rather than a multicast address.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the symmetric-passive peer belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the symmetric-passive peer is on the public network, do not specify this option.

authentication-keyid *keyid*: Specifies the key ID to be used for sending NTP messages to the peer. The value range for the *keyid* argument is 1 to 4294967295. If you do not specify this option, the local device and the peer do not authenticate each other.

maxpoll *maxpoll-interval*: Specifies the maximum polling interval. The value range for the *maxpoll-interval* argument is 4 to 17, to which base 2 is raised to get the interval in seconds. The maximum polling interval is in the range of 2^4 to 2^{17} (16 to 131072) seconds. The default value for the *maxpoll-interval* argument is 6 and the default maximum polling interval is 2^6 (64) seconds.

minpoll *minpoll-interval*: Specifies the minimum polling interval. The value range for the *minpoll-interval* argument is 4 to 17, to which base 2 is raised to get the interval in seconds. The minimum polling interval is in the range of 2^4 to 2^{17} (16 to 131072) seconds. The default value for the *minpoll-interval* argument is 6 and the default minimum polling interval is 2^6 (64) seconds.

priority: Specifies the peer specified by *ipv6-address* or *peer-name* as the first choice under the same condition.

source *interface-type interface-number*: Specifies the source interface for IPv6 NTP messages. If the specified passive peer address is not a link local address, the source IPv6 address for IPv6 NTP messages sent by the local device is the IPv6 address of the specified source interface. If the specified passive peer address is a link local address, the IPv6 NTP messages are sent from the specified source interface, and the source address of the messages is the link local address of the interface. The *interface-type interface-number* argument represents the interface type and number. If you do not specify an interface, the device automatically selects the source IPv6 address of IPv6 NTP messages. For more information, see *RFC 3484*.

Usage guidelines

When you specify an IPv6 passive peer for the device, the device and its IPv6 passive peer can be synchronized to each other. If their clocks are in synchronized state, the clock with a high stratum level is synchronized to the clock with a lower stratum level.

To synchronize the PE to a PE or CE in a VPN instance, provide the **vpn-instance** *vpn-instance-name* option in the command.

If you include the **vpn-instance** *vpn-instance-name* option in the **undo ntp-service ipv6 unicast-peer** command, the command removes the symmetric-passive peer in the specified VPN instance. If you do not include the **vpn-instance** *vpn-instance-name* option in the command, the command removes the symmetric-passive peer on the public network.

If the specified IPv6 address of the passive peer is a link local address, you must specify the source interface for NTP messages and cannot specify a VPN instance for the passive peer.

If the specified IPv6 address of the passive peer is a link local address, you must specify the source interface for NTP messages and cannot specify a VPN instance for the passive peer.

After you specify an IPv6 symmetric-passive peer for a device, the device polls and synchronize its time with the peer device at the minimum polling interval. If the time discrepancy between the two remains in the acceptable range, the system gradually increases the polling interval until the maximum polling interval is reached. If the time discrepancy exceeds the acceptable range repeatedly, the polling interval decreases gradually.

The polling interval configuration takes effect when the next polling starts.

Examples

Specify the device with the IPv6 address of 2001::1 as the symmetric-passive peer of the local device, and specify the source interface for IPv6 NTP messages as GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] ntp-service ipv6 unicast-peer 2001::1 source gigabitethernet 1/0/1
```

Related commands

ntp-service authentication enable

ntp-service authentication-keyid

ntp-service reliable authentication-keyid

ntp-service ipv6 unicast-server

Use **ntp-service ipv6 unicast-server** to specify an IPv6 NTP server for the device.

Use **undo ntp-service ipv6 unicast-server** to remove an IPv6 NTP server specified for the device.

Syntax

ntp-service ipv6 unicast-server { *server-name* | *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**authentication-keyid** *keyid* | **maxpoll** *maxpoll-interval* | **minpoll** *minpoll-interval* | **priority** | **source** *interface-type interface-number*] *

undo ntp-service ipv6 unicast-server { *server-name* | *ipv6-address* } [**vpn-instance** *vpn-instance-name*]

Default

No IPv6 NTP server is specified.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

server-name: Specifies an NTP server by its host name, a case-insensitive string of 1 to 253 characters. Valid characters are letters, digits, hyphens (-), underscores (_), and periods (.).

ipv6-address: Specifies an NTP server by its IPv6 address. It must be a unicast address, rather than a multicast address.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the NTP server belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the NTP server is on the public network, do not specify this option.

authentication-keyid *keyid*: Specifies the key ID to be used for sending NTP messages to the NTP server. The value range for the *keyid* argument is 1 to 4294967295. If you do not specify this option, the local device and NTP server do not authenticate each other.

maxpoll *maxpoll-interval*: Specifies the maximum polling interval. The value range for the *maxpoll-interval* argument is 4 to 17, to which base 2 is raised to get the interval in seconds. The maximum polling interval is in the range of 2^4 to 2^{17} (16 to 131072) seconds. The default value for the *maxpoll-interval* argument is 6 and the default maximum polling interval is 2^6 (64) seconds.

minpoll *minpoll-interval*: Specifies the minimum polling interval. The value range for the *minpoll-interval* argument is 4 to 17, to which base 2 is raised to get the interval in seconds. The minimum polling interval is in the range of 2^4 to 2^{17} (16 to 131072) seconds. The default value for the *minpoll-interval* argument is 6 and the default minimum polling interval is 2^6 (64) seconds.

priority: Specifies this NTP server as the first choice under the same condition.

source *interface-type interface-number*: Specifies the source interface for IPv6 NTP messages. If the specified IPv6 NTP server address is not a link local address, the source IPv6

address for IPv6 NTP messages sent by the local device to the NTP server is the IPv6 address of the specified source interface. If the specified IPv6 NTP server address is a link local address, the IPv6 NTP messages are sent from the specified source interface, and the source address of the messages is the link local address of the interface. The *interface-type interface-number* argument represents the interface type and number. If you do not specify an interface, the device automatically selects the source IPv6 address of IPv6 NTP messages. For more information, see *RFC 3484*.

Usage guidelines

When you specify an IPv6 NTP server for the device, the device is synchronized to the IPv6 NTP server, but the IPv6 NTP server is not synchronized to the device.

To synchronize the PE to a PE or CE in a VPN instance, specify the **vpn-instance** *vpn-instance-name* option in the command.

If you include the **vpn-instance** *vpn-instance-name* option in the **undo ntp-service unicast-server** command, the command removes the NTP server in the specified VPN. If you do not include the **vpn-instance** *vpn-instance-name* option in the command, the command removes the NTP server on the public network.

If the specified IPv6 address of the NTP server is a link local address, you must specify the source interface for NTP messages and cannot specify a VPN instance for the NTP server.

After you specify an IPv6 NTP server for a device, the device polls and synchronizes its time with the server at the minimum polling interval. If the time discrepancy between the two remains in the acceptable range, the system gradually increases the polling interval until the maximum polling interval is reached. If the time discrepancy exceeds the acceptable range repeatedly, the polling interval decreases gradually.

The polling interval configuration takes effect when the next polling starts.

Examples

Specify the IPv6 NTP server 2001::1 for the device.

```
<Sysname> system-view
[Sysname] ntp-service ipv6 unicast-server 2001::1
```

Related commands

ntp-service authentication enable

ntp-service authentication-keyid

ntp-service reliable authentication-keyid

ntp-service max-dynamic-sessions

Use **ntp-service max-dynamic-sessions** to set the maximum number of dynamic NTP sessions.

Use **undo ntp-service max-dynamic-sessions** to restore the default.

Syntax

ntp-service max-dynamic-sessions *number*

undo ntp-service max-dynamic-sessions

Default

The maximum number of dynamic NTP sessions is 100.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

number: Sets the maximum number of dynamic NTP associations, in the range of 0 to 100.

Usage guidelines

A device can have a maximum of 128 concurrent associations, including static associations and dynamic associations. A static association refers to an association that a user has manually created by using an NTP command. A dynamic association is a temporary association created by the system during operation.

This command limits the number of dynamic NTP associations and prevents dynamic NTP associations from occupying too many system resources.

Examples

Set the maximum number of dynamic NTP associations to 50.

```
<Sysname> system-view
[Sysname] ntp-service max-dynamic-sessions 50
```

Related commands

display ntp-service sessions

ntp-service multicast-client

Use **ntp-service multicast-client** to configure the device to operate in NTP multicast client mode and use the current interface to receive NTP multicast packets.

Use **undo ntp-service multicast-client** to remove the configuration.

Syntax

ntp-service multicast-client [*ip-address*]

undo ntp-service multicast-client [*ip-address*]

Default

The device does not operate in any NTP association mode.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies a multicast IP address. The default is 224.0.1.1. A multicast server and client must be configured with the same multicast IP address.

Usage guidelines

After you configure the command, the device listens to NTP messages using the specified multicast address as the destination address.

If you have configured the device to operate in multicast client mode on an interface with the command, do not add the interface to any aggregate group. To add the interface to an aggregate group, remove the configuration of the command.

Examples

Configure the device to operate in multicast client mode and receive NTP multicast messages on GigabitEthernet 1/0/1, and set the multicast address to 224.0.1.1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ntp-service multicast-client 224.0.1.1
```

Related commands

ntp-service multicast-server

ntp-service multicast-server

Use **ntp-service multicast-server** to configure the device to operate in NTP multicast server mode and use the current interface to send NTP multicast packets.

Use **undo ntp-service multicast-server** to remove the configuration.

Syntax

ntp-service multicast-server [*ip-address*] [**authentication-keyid** *keyid* | **ttl** *ttl-number* | **version** *number*] *

undo ntp-service multicast-server [*ip-address*]

Default

The device does not operate in any NTP association mode.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies a multicast IP address. The default is 224.0.1.1. A multicast server and client must be configured with the same multicast IP address.

authentication-keyid *keyid*: Specifies the key ID to be used for sending multicast messages to multicast clients. The value range for the *keyid* argument is 1 to 4294967295. If you do not specify this option, the local device cannot synchronize multicast clients enabled with NTP authentication.

ttl *ttl-number*: Specifies the TTL of NTP multicast messages. The value range for the *ttl-number* argument is 1 to 255. The default value is 16.

version *number*: Specifies the NTP version. The value range for the *number* argument is 1 to 4. The default value is 4.

Usage guidelines

After you configure the command, the device periodically sends NTP messages to the specified multicast address.

If you have configured the device to operate in multicast server mode on an interface with the command, do not add the interface to any aggregate group. To add the interface to an aggregate group, remove the configuration of the command.

Examples

Configure the device to operate in multicast server mode and send NTP multicast messages on GigabitEthernet 1/0/1 to the multicast address 224.0.1.1, using key 4 for encryption. Set the NTP version to 4.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ntp-service multicast-server 224.0.1.1 version 4
authentication-keyid 4
```

Related commands

ntp-service multicast-client

ntp-service refclock-master

Use **ntp-service refclock-master** to configure the local clock as the reference source.

Use **undo ntp-service refclock-master** to remove the configuration.

Syntax

ntp-service refclock-master [*ip-address*] [*stratum*]

undo ntp-service refclock-master [*ip-address*]

Default

The device does not use its local clock as the reference clock.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: IP address of the local clock, 127.127.1.*u*, where *u* is the NTP process ID in the range of 0 to 3. The default value is 127.127.1.0.

stratum: Stratum level of the local clock, in the range of 1 to 15. The default value is 8. A lower stratum level represents higher clock accuracy.

Usage guidelines

Typically an NTP server that gets its time from an authoritative time source, such as an atomic clock has stratum 1 and operates as the primary time server to provide time synchronization for other devices in the network. The accuracy of each server is the stratum, with the topmost level (primary servers) assigned as one and each level downwards (secondary servers) in the hierarchy assigned as one greater than the preceding level.

If the devices in a network cannot synchronize to an authoritative time source, you can perform the following tasks:

- Select a device that has a relatively accurate clock from the network.
- Use the local clock of the device as the reference clock to synchronize other devices in the network.

Use the command with caution to avoid time errors. As a best practice, set the local clock time to a correct value before you execute the command.

Examples

Specify the local clock as the reference source, with the stratum level 2.

```
<Sysname> system-view
[Sysname] ntp-service refclock-master 2
```

ntp-service reliable authentication-keyid

Use **ntp-service reliable authentication-keyid** to specify an authentication key as a trusted key.

Use **undo ntp-service reliable authentication-keyid** to remove the configuration.

Syntax

ntp-service reliable authentication-keyid *keyid*

undo ntp-service reliable authentication-keyid *keyid*

Default

No trusted key is specified.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

keyid: Specifies an authentication key by its ID in the range of 1 to 4294967295.

Usage guidelines

When NTP authentication is enabled, a client can be synchronized only to a server that can provide a trusted authentication key.

Before you use the command, make sure NTP authentication is enabled and an authentication key is configured. The key automatically changes to untrusted after you delete the key. In this case, you do not need to execute the **undo ntp-service reliable authentication-keyid** command.

You can set a maximum of 128 keys by executing the command.

Examples

Enable NTP authentication, specify the MD5 algorithm, with the key ID of 37 and key value of **BetterKey**.

```
<Sysname> system-view
[Sysname] ntp-service authentication enable
[Sysname] ntp-service authentication-keyid 37 authentication-mode md5 simple BetterKey
```

Specify this key as a trusted key.

```
[Sysname] ntp-service reliable authentication-keyid 37
```

Related commands

ntp-service authentication enable

ntp-service authentication-keyid

ntp-service source

Use **ntp-service source** to specify a source interface for NTP messages.

Use **undo ntp-service source** to restore the default.

Syntax

ntp-service source *interface-type interface-number*

undo ntp-service source

Default

No source interface is specified for NTP messages. The device performs the following operations:

- Searches the routing table for the outbound interface of NTP messages.
- Uses the primary IP address of the outbound interface as the source IP address for NTP messages.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

If you specify a source interface for NTP messages, the device uses the primary IP address of the specified interface as the source IP address to send NTP messages. Consequently, the destination address of the NTP response messages is the primary IP address of the source interface.

When the device responds to an NTP request, the source IP address of the NTP response is always the IP address of the interface that has received the NTP request.

If you do not want the IP address of an interface on the local device to become the destination address for response messages, use the command to specify another interface as the source interface for NTP messages.

If you have specified the source interface for NTP messages in the **ntp-service unicast-server** or **ntp-service unicast-peer** command, the specified source interface is used as the source interface for NTP messages.

If you have configured the **ntp-service broadcast-server** or **ntp-service multicast-server** command in an interface view, the interface is used as the source interface for broadcast or multicast NTP messages.

If the specified source interface is down, the device does not send NTP messages.

Examples

Specify the source interface for NTP messages as GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] ntp-service source gigabitethernet 1/0/1
```

ntp-service time-offset-threshold

Use **ntp-service time-offset-threshold** to set the time offset thresholds for outputting logs and traps during time synchronization.

Use **undo ntp-service time-offset-threshold** to restore the default.

Syntax

ntp-service time-offset-threshold { **log** *log-threshold* | **trap** *trap-threshold* }*

undo ntp-service time-offset-threshold

Default

No time offset thresholds are set for outputting logs and traps during time synchronization.

Views

System view

Predefined user roles

network-admin

Parameters

log *log-threshold*: Specifies the time offset threshold for outputting logs during time synchronization, in the range of 128 to 60000 milliseconds.

trap *trap-threshold*: Specifies the time offset threshold for outputting traps during time synchronization, in the range of 128 to 60000 milliseconds.

Usage guidelines

By default, the system synchronizes the NTP client's time to the server and outputs a log and a trap when the time offset exceeds 128 ms for multiple times.

After you set the thresholds, the system synchronizes the client's time to the server when the time offset exceeds 128 ms, but outputs logs and traps only when the time offset exceeds the specified thresholds, respectively.

Examples

Set the NTP time-offset thresholds for outputting logs and traps to 500 ms and 600 ms, respectively.

```
<Sysname> system-view
[Sysname] ntp-service time-offset-threshold log 500 trap 600
```

ntp-service unicast-peer

Use **ntp-service unicast-peer** to specify a symmetric-passive peer for the device.

Use **undo ntp-service unicast-peer** to remove the symmetric-passive peer specified for the device.

Syntax

ntp-service unicast-peer { *peer-name* | *ip-address* } [**vpn-instance** *vpn-instance-name*] [**authentication-keyid** *keyid* | **maxpoll** *maxpoll-interval* | **minpoll** *minpoll-interval* | **priority** | **source** *interface-type interface-number* | **version** *number*] *

undo ntp-service unicast-peer { *peer-name* | *ip-address* } [**vpn-instance** *vpn-instance-name*]

Default

No symmetric-passive peer is specified.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

peer-name: Specifies a symmetric-passive peer by its host name, a case-insensitive string of 1 to 253 characters. Valid characters are letters, digits, hyphens (-), underscores (_), and periods (.).

ip-address: Specifies a symmetric-passive peer by its IP address. It must be a unicast address, rather than a broadcast address, a multicast address, or the IP address of the local clock.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the symmetric-passive peer belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the symmetric-passive peer is on the public network, do not specify this option.

authentication-keyid *keyid*: Specifies the key ID to be used for sending NTP messages to the peer. The value range for the *keyid* argument is 1 to 4294967295. If you do not specify this option, the local device and the peer do not authenticate each other.

maxpoll *maxpoll-interval*: Specifies the maximum polling interval. The value range for the *maxpoll-interval* argument is 4 to 17, to which base 2 is raised to get the interval in seconds. The maximum polling interval is in the range of 2^4 to 2^{17} (16 to 131072) seconds. The default value for the *maxpoll-interval* argument is 6 and the default maximum polling interval is 2^6 (64) seconds.

minpoll *minpoll-interval*: Specifies the minimum polling interval. The value range for the *minpoll-interval* argument is 4 to 17, to which base 2 is raised to get the interval in seconds. The minimum polling interval is in the range of 2^4 to 2^{17} (16 to 131072) seconds. The default value for the *minpoll-interval* argument is 6 and the default minimum polling interval is 2^6 (64) seconds.

priority: Specifies the peer specified by *ip-address* or *peer-name* as the first choice under the same condition.

source *interface-type interface-number*: Specifies the source interface for NTP messages. In an NTP message the local device sends to its peer, the source IP address is the primary IP address of this interface. The *interface-type interface-number* argument represents the interface type and number. If you do not specify this option, the device searches the routing table for the outgoing interface and uses the primary IP address of the outgoing interface as the source IP address of the NTP messages.

version *number*: Specifies the NTP version. The value range for the *number* argument is 1 to 4. The default value is 4.

Usage guidelines

When you specify a passive peer for the device, the device and its passive peer can be synchronized to each other. If their clocks are in synchronized state, the clock with a high stratum level is synchronized to the clock with a lower stratum level.

To synchronize the PE to a PE or CE in a VPN instance, provide **vpn-instance** *vpn-instance-name* in your command.

If you include **vpn-instance** *vpn-instance-name* in the **undo ntp-service unicast-peer** command, the command removes the symmetric-passive peer in the specified VPN instance. If you do not include **vpn-instance** *vpn-instance-name* in the command, the command removes the symmetric-passive peer on the public network.

After you specify a symmetric-passive peer for a device, the device polls and synchronizes its time with the peer device at the minimum polling interval. If the time discrepancy between the two remains in the acceptable range, the system gradually increases the polling interval until the maximum polling interval is reached. If the time discrepancy exceeds the acceptable range repeatedly, the polling interval decreases gradually.

The polling interval configuration takes effect when the next polling starts.

Examples

Specify the device with the IP address of 10.1.1.1 as the symmetric-passive peer of the local device, and configure the local device to run NTP version 4. Specify the source interface of NTP messages as GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] ntp-service unicast-peer 10.1.1.1 version 4 source gigabitethernet 1/0/1
```

Related commands

ntp-service authentication enable

ntp-service authentication-keyid

ntp-service reliable authentication-keyid

ntp-service unicast-server

Use **ntp-service unicast-server** to specify an NTP server for the device.

Use **undo ntp-service unicast-server** to remove an NTP server specified for the device.

Syntax

ntp-service unicast-server { *server-name* | *ip-address* } [**vpn-instance** *vpn-instance-name*] [**authentication-keyid** *keyid* | **maxpoll** *maxpoll-interval* | **minpoll** *minpoll-interval* | **priority** | **source** *interface-type interface-number* | **version** *number*] *

undo ntp-service unicast-server { *server-name* | *ip-address* } [**vpn-instance** *vpn-instance-name*]

Default

No NTP server is specified.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

server-name: Specifies an NTP server by its host name, a case-insensitive string of 1 to 253 characters. Valid characters are letters, digits, hyphens (-), underscores (_), and periods (.).

ip-address: Specifies an NTP server by its IP address. It must be a unicast address, rather than a broadcast address, a multicast address, or the IP address of the local clock.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the NTP server belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the NTP server is on the public network, do not specify this option.

authentication-keyid *keyid*: Specifies the key ID to be used for sending NTP messages to the NTP server. The value range for the *keyid* argument is 1 to 4294967295. If you do not specify this option, the local device and NTP server do not authenticate each other.

maxpoll *maxpoll-interval*: Specifies the maximum polling interval. The value range for the *maxpoll-interval* argument is 4 to 17, to which base 2 is raised to get the interval in seconds. The maximum polling interval is in the range of 2^4 to 2^{17} (16 to 131072) seconds. The default value for the *maxpoll-interval* argument is 6 and the default maximum polling interval is 2^6 (64) seconds.

minpoll *minpoll-interval*: Specifies the minimum polling interval. The value range for the *minpoll-interval* argument is 4 to 17, to which base 2 is raised to get the interval in seconds. The minimum polling interval is in the range of 2^4 to 2^{17} (16 to 131072) seconds. The default value for the *minpoll-interval* argument is 6 and the default minimum polling interval is 2^6 (64) seconds.

priority: Specifies this NTP server as the first choice under the same condition.

source *interface-type interface-number*: Specifies the source interface for NTP messages. For an NTP message the local device sends to the NTP server, the source IP address is the primary IP address of this interface. The *interface-type interface-number* argument represents the interface type and number. If you do not specify this option, the device searches the routing table for the outgoing interface and uses the primary IP address of the outgoing interface as the source IP address of the NTP messages.

version *number*: Specifies the NTP version. The value range for the *number* argument is 1 to 4. The default value is 4.

Usage guidelines

When you specify an NTP server for the device, the device is synchronized to the NTP server, but the NTP server is not synchronized to the device.

To synchronize the PE to a PE or CE in a VPN instance, provide **vpn-instance** *vpn-instance-name* in your command.

If you include the **vpn-instance** *vpn-instance-name* option in the **undo ntp-service unicast-server** command, the command removes the NTP server in the specified VPN instance. If you do not include the **vpn-instance** *vpn-instance-name* option in the command, the command removes the NTP server on the public network.

After you specify an NTP server for a device, the device polls and synchronizes its time with the server at the minimum polling interval. If the time discrepancy between the two remains in the acceptable range, the system gradually increases the polling interval until the maximum polling interval is reached. If the time discrepancy exceeds the acceptable range repeatedly, the polling interval decreases gradually.

The polling interval configuration takes effect when the next polling starts.

Examples

Specify NTP server 10.1.1.1 for the device, and configure the device to run NTP version 4.

```
<Sysname> system-view
[Sysname] ntp-service unicast-server 10.1.1.1 version 4
```

Related commands

ntp-service authentication enable

ntp-service authentication-keyid

ntp-service reliable authentication-keyid

SNTP commands

display sntp ipv6 sessions

Use **display sntp ipv6 sessions** to display information about all IPv6 SNTP associations.

Syntax

display sntp ipv6 sessions

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display information about all IPv6 SNTP associations.

```
<Sysname> display sntp ipv6 sessions
SNTP server: 2001::1
Stratum: 16
Version: 4
Last receive time: No packet was received.

SNTP server: 2001::100
Stratum: 3
Version: 4
Last receive time: Fri, Oct 21 2011 11:28:28.058 (Synced)
```

Table 7 Command output

Field	Description
SNTP server	SNTP server (NTP server). If this field displays **::**, the IPv6 address of the NTP server has not been resolved successfully.
Stratum	Stratum level of the NTP server, which determines the clock accuracy. It is in the range of 1 to 16. A lower stratum level represents a higher clock accuracy. A clock with stratum level 16 is not synchronized.
Version	SNTP version.
Last receive time	Time when the last message was received: • **Synced**—The local clock is synchronized to the NTP server. • **No packet was received**—The device has not received any SNTP session information from the server.

display sntp sessions

Use **display sntp sessions** to display information about all IPv4 SNTP associations.

Syntax

display sntp sessions

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display information about all IPv4 SNTP associations.

```
<Sysname> display sntp sessions
SNTP server     Stratum   Version    Last receive time
1.0.1.11        2         4          Tue, May 17 2011  9:11:20.833 (Synced)
```

Table 8 Command output

Field	Description
SNTP server	SNTP server (NTP server). If this field displays **0.0.0.0**, the IP address of the NTP server has not been resolved successfully.
Stratum	Stratum level of the NTP server, which determines the clock accuracy. It is in the range of 1 to 16. A lower stratum level represents higher clock accuracy. A clock with stratum level 16 is not synchronized.
Version	SNTP version.
Last receive time	Time when the last message was received. Synced means the local clock is synchronized to the NTP server.

sntp authentication enable

Use **sntp authentication enable** to enable SNTP authentication.

Use **undo sntp authentication enable** to disable SNTP authentication.

Syntax

sntp authentication enable

undo sntp authentication enable

Default

SNTP authentication is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

You need to enable SNTP authentication in networks that require time synchronization security to make sure SNTP clients are synchronized only to authenticated NTP servers.

To authenticate an NTP server, set an authentication key and specify it as a trusted key.

Examples

Enable SNTP authentication.

```
<Sysname> system-view
[Sysname] sntp authentication enable
```

Related commands

sntp authentication-keyid

sntp reliable authentication-keyid

sntp authentication-keyid

Use **sntp authentication-keyid** to set an SNTP authentication key.

Use **undo sntp authentication-keyid** to remove an SNTP authentication key.

Syntax

sntp authentication-keyid *keyid* **authentication-mode md5** { **cipher** | **simple** } *string* [**acl** *ipv4-acl-number* | **ipv6 acl** *ipv6-acl-number*] *

undo sntp authentication-keyid *keyid*

Default

No SNTP authentication key exists.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

keyid: Specifies an authentication key ID in the range of 1 to 4294967295.

authentication-mode md5: Specifies the MD5 authentication algorithm.

cipher: Specifies an authentication key in encrypted form.

simple: Specifies an authentication key in plaintext form. For security purposes, the authentication key specified in plaintext form will be stored in encrypted form.

string: Specifies a case-sensitive authentication key. Its plaintext form is a string of 1 to 32 characters. Its encrypted form is a string of 1 to 73 characters.

acl *ipv4-acl-number*: Specifies an IPv4 basic ACL by its number in the range of 2000 to 2999. Only the devices permitted by the ACL can use the key ID for authentication.

ipv6 acl *ipv6-acl-number*: Specifies an IPv6 basic ACL by its number in the range of 2000 to 2999. Only the devices permitted by the ACL can use the key ID for authentication.

Usage guidelines

SNTP authentication must be enabled on an SNTP network that requires time synchronization security. SNTP authentication ensures that SNTP clients are synchronized only to authenticated NTP time servers.

The key ID in the message from the peer device identifies the key used for authentication. The **acl** *ipv4-acl-number* or **acl** *ipv6-acl-number* option is used to identify the peer device that can use the key ID.

- If the specified IPv4 or IPv6 ACL does not exist, any device can use the key ID for authentication.
- If the specified IPv4 or IPv6 ACL does not contain any rules, no device can use the key ID for authentication.

To ensure a successful authentication, configure the same key ID and key on the time server and client. Make sure the peer device is allowed to use the key ID for authentication on the local device.

After you configure an SNTP authentication key, use the **sntp reliable authentication-keyid** command to set it as a trusted key. The key automatically changes to untrusted after you delete the key. In this case, you do not need to execute the **undo sntp-service reliable authentication-keyid** command.

You can set a maximum of 128 authentication keys by executing the command.

Examples

Set an MD5 authentication key, with the key ID of **10** and key value of **BetterKey**. Input the key in plain text.

```
<Sysname> system-view
[Sysname] sntp authentication enable
[Sysname] sntp authentication-keyid 10 authentication-mode md5 simple BetterKey
```

Related commands

sntp authentication enable

sntp reliable authentication-keyid

sntp enable

Use **sntp enable** to enable the SNTP service.

Use **undo sntp enable** to disable the SNTP service.

Syntax

sntp enable

undo sntp enable

Default

The SNTP service is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Examples

Enable the SNTP service.

```
<Sysname> system-view
[Sysname] sntp enable
```

sntp ipv6 unicast-server

Use **sntp ipv6 unicast-server** to specify an IPv6 NTP server for the device.

Use **undo sntp ipv6 unicast-server** to remove the IPv6 NTP server specified for the device.

Syntax

sntp ipv6 unicast-server { *server-name* | *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**authentication-keyid** *keyid* | **source** *interface-type interface-number*] *

undo sntp ipv6 unicast-server { *server-name* | *ipv6-address* } [**vpn-instance** *vpn-instance-name*]

Default

No IPv6 NTP server is specified.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

server-name: Specifies an NTP server by its host name, a case-insensitive string of 1 to 253 characters. Valid characters are letters, digits, hyphens (-), underscores (_), and periods (.).

ipv6-address: Specifies an NTP server by its IPv6 address.

vpn-instance *vpn-instance-name*: Specifies MPLS L3VPN instance to which the NTP server belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the NTP server is on the public network, do not specify this option.

authentication-keyid *keyid*: Specifies the key ID to be used for sending NTP messages to the NTP server. The value range for the *keyid* argument is 1 to 4294967295. If you do not specify this option, the local device and NTP server do not authenticate each other.

source *interface-type interface-number*: Specifies the source interface for IPv6 NTP messages. If the specified IPv6 NTP server address is not a link local address, the source IPv6 address for IPv6 NTP messages sent by the local device to the NTP server is the IPv6 address of the specified source interface. If the specified IPv6 NTP server address is a link local address, the IPv6 NTP messages are sent from the specified source interface, and the source address of the messages is the link local address of the interface. The *interface-type interface-number* argument represents the interface type and number. If you do not specify an interface, the device automatically selects the source IPv6 address of IPv6 NTP messages. For more information, see *RFC 3484*.

Usage guidelines

When you specify an IPv6 NTP server for the device, the device is synchronized to the NTP server, but the NTP server is not synchronized to the device.

To synchronize the PE to a PE or CE in a VPN instance, provide the **vpn-instance** *vpn-instance-name* option in your command.

If you include the **vpn-instance** *vpn-instance-name* option in the **undo ntp-service unicast-server** command, the command removes the NTP server in the specified VPN instance. If you do not include the **vpn-instance** *vpn-instance-name* option in the command, the command removes the NTP server on the public network.

If the specified IPv6 address of the NTP server is a link local address, you must specify the source interface for NTP messages and cannot specify a VPN instance for the NTP server.

Examples

Specify the IPv6 NTP server 2001::1 for the device.

```
<Sysname> system-view
[Sysname] sntp ipv6 unicast-server 2001::1
```

Related commands

sntp authentication enable

sntp authentication-keyid

sntp reliable authentication-keyid

sntp reliable authentication-keyid

Use **sntp reliable authentication-keyid** to specify a trusted key.

Use **undo sntp reliable authentication-keyid** to remove the trusted key.

Syntax

sntp reliable authentication-keyid *keyid*

undo sntp reliable authentication-keyid *keyid*

Default

No trusted key is specified.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

keyid: Specifies an authentication key by its ID in the range of 1 to 4294967295.

Usage guidelines

If SNTP is enabled, the SNTP client is synchronized only to an NTP server that provides a trusted key.

Before you use the command, make sure SNTP authentication is enabled and an authentication key is configured. The key automatically changes to untrusted after you delete the key. In this case, you do not need to execute the **undo sntp-service reliable authentication-keyid** command.

Examples

Enable NTP authentication, and specify the MD5 encryption algorithm, with the key ID of 37 and key value of **BetterKey**.

```
<Sysname> system-view
[Sysname] sntp authentication enable
[Sysname] sntp authentication-keyid 37 authentication-mode md5 simple BetterKey
```

Specify this key as a trusted key.

```
[Sysname] sntp reliable authentication-keyid 37
```

Related commands

sntp authentication-keyid

sntp authentication enable

sntp time-offset-threshold

Use **sntp time-offset-threshold** to set the time offset thresholds for outputting logs and traps during time synchronization.

Use **undo sntp-service time-offset-threshold** to restore the default.

Syntax

sntp time-offset-threshold { **log** *log-threshold* | **trap** *trap-threshold* }*

undo sntp time-offset-threshold

Default

No time offset thresholds are set for outputting logs and traps during time synchronization.

Views

System view

Predefined user roles

network-admin

Parameters

log *log-threshold*: Specifies the time offset threshold for outputting logs during time synchronization, in the range of 128 to 60000 milliseconds.

trap *trap-threshold*: Specifies the time offset threshold for outputting traps during time synchronization, in the range of 128 to 60000 milliseconds.

Usage guidelines

After you set the thresholds, the system synchronizes the client's time to the server when the time offset exceeds 128 ms, but outputs logs and traps only when the time offset exceeds the specified thresholds, respectively.

Examples

Set the time offset thresholds for outputting logs and traps during time synchronization of 500 ms and 600 ms, respectively.

```
<Sysname> system-view
[Sysname] sntp time-offset-threshold log 500 trap 600
```

sntp unicast-server

Use **sntp unicast-server** to specify an NTP server for the device.

Use **undo sntp unicast-server** to remove an NTP server specified for the device.

Syntax

sntp unicast-server { *server-name* | *ip-address* } [**vpn-instance** *vpn-instance-name*] [**authentication-keyid** *keyid* | **source** *interface-type interface-number* | **version** *number*] *

undo sntp unicast-server { *server-name* | *ip-address* } [**vpn-instance** *vpn-instance-name*]

Default

No NTP server is specified.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

server-name: Specifies an NTP server by its host name, a case-insensitive string of 1 to 253 characters. Valid characters are letters, digits, hyphens (-), underscores (_), and periods (.).

ip-address: Specifies an NTP server by its IP address. It must be a unicast address, rather than a broadcast address, a multicast address, or the IP address of the local clock.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance VPN to which the NTP server belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the NTP server is on the public network, do not specify this option.

authentication-keyid *keyid*: Specifies the key ID to be used for sending NTP messages to the NTP server. The value range for the *keyid* argument is 1 to 4294967295. If you do not specify this option, the local device and NTP server do not authenticate each other.

source *interface-type interface-number*: Specifies the source interface for NTP messages. In an NTP message the local device sends to the NTP server, the source IP address is the primary IP address of this interface. The *interface-type interface-number* argument represents the interface type and number.

version *number*: Specifies the NTP version. The value range for the *number* argument is 1 to 4. The default value is 4.

Usage guidelines

When you specify an NTP server for the device, the device is synchronized to the NTP server, but the NTP server is not synchronized to the device.

To synchronize the PE to a PE or CE in a VPN instance, provide **vpn-instance** *vpn-instance-name* in your command.

If you include the **vpn-instance** *vpn-instance-name* option in the **undo ntp-service unicast-server** command, the command removes the NTP server in the specified VPN instance. If you do not include the **vpn-instance** *vpn-instance-name* option in the command, the command removes the NTP server on the public network.

Examples

Specify NTP server 10.1.1.1 for the device, and configure the device to run NTP version 4.

```
<Sysname> system-view
[Sysname] sntp unicast-server 10.1.1.1 version 4
```

Related commands

sntp authentication enable

sntp authentication-keyid

sntp reliable authentication-keyid

Contents

EAA commands

action cli

Use **action cli** to add a CLI action to a monitor policy.

Use **undo action** to remove an action.

Syntax

action *number* **cli** *command-line*

undo action *number*

Default

A monitor policy does not contain any actions.

Views

CLI-defined policy view

Predefined user roles

network-admin

context-admin

Parameters

number: Specifies an action ID in the range of 0 to 231.

cli *command-line*: Specifies the command line to be executed when the event occurs. You can enter abbreviated forms of command keywords, but you must make sure the forms can uniquely identify the command keywords. For example, you can enter **dis cu** for the **display current-configuration** command.

Usage guidelines

You can configure a series of actions to be executed in response to the event specified in a monitor policy. EAA executes the actions in ascending order of action IDs. When you add actions to a policy, you must make sure the execution order is correct. If two actions have the same ID, the most recent one takes effect.

To execute a command in a view other than user view, you must define actions required for accessing the target view before defining the command execution action. In addition, you must number the actions in the order they should be executed, starting with entering system view.

For example, to shut down an interface, you must create the following actions in order:

1. Action to enter system view.
2. Action to enter interface view.
3. Action to shut down the interface.

When you define an action, you can specify a value or specify a variable name for an argument. For more information about using EAA environment variables, see "rtm environment."

Examples

Configure a CLI action for the CLI-defined policy **test** to shut down GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] rtm cli-policy test
[Sysname-rtm-test] action 1 cli system-view
[Sysname-rtm-test] action 2 cli interface gigabitethernet 1/0/1
```

```
[Sysname-rtm-test] action 3 cli shutdown
```

action reboot

Use **action reboot** to add a reboot action to a monitor policy.

Use **undo action** to remove an action.

Syntax

action *number* **reboot** [**slot** *slot-number*]

undo action *number*

Default

A monitor policy does not contain any actions.

Views

CLI-defined policy view

Predefined user roles

network-admin

context-admin

Parameters

number: Specifies an action ID in the range of 0 to 231.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, the command reboots the IRF fabric.

Usage guidelines

The reboot action configured with this command reboots devices or cards without saving the running configuration. If you want to save the running configuration, use the **action cli** command to configure reboot actions.

You can configure a series of actions to be executed in response to the event specified in a monitor policy. EAA executes the actions in ascending order of action IDs. When you add actions to a policy, you must make sure the execution order is correct. If two actions have the same ID, the most recent one takes effect.

When you define an action, you can specify a value or specify a variable name for an argument. For more information about using EAA environment variables, see "rtm environment."

Examples

Configure an action for the CLI-defined policy **test** to reboot the specified slot.

<Sysname> system-view

```
[Sysname] rtm cli-policy test
[Sysname-rtm-test] action 3 reboot slot 1
```

action switchover

Use **action switchover** to add an active/standby switchover action to a monitor policy.

Use **undo action** to remove an action.

Syntax

action *number* **switchover**

undo action *number*

Default

A monitor policy does not contain any actions.

Views

CLI-defined policy view

Predefined user roles

network-admin

context-admin

Parameters

number: Specifies an action ID in the range of 0 to 231.

Usage guidelines

You can configure a series of actions to be executed in response to the event specified in a monitor policy. EAA executes the actions in ascending order of action IDs. When you add actions to a policy, you must make sure the execution order is correct. If two actions have the same ID, the most recent one takes effect.

This command does not trigger a master/subordinate switchover in either of the following situations:

- No subordinate device is configured.
- The subordinate device is not in up state.

Examples

Configure an action for the CLI-defined policy **test** to perform an active/standby switchover.

```
<Sysname> system-view
[Sysname] rtm cli-policy test
[Sysname-rtm-test] action 3 switchover
```

action syslog

Use **action syslog** to add a Syslog action to a monitor policy.

Use **undo action** to remove an action.

Syntax

action *number* **syslog priority** *priority* **facility** *local-number* **msg** *msg-body*

undo action *number*

Default

A monitor policy does not contain any actions.

Views

CLI-defined policy view

Predefined user roles

network-admin

context-admin

Parameters

number: Specifies an action ID in the range of 0 to 231.

priority *priority*: Specifies the log severity level in the range of 0 to 7. A lower value represents a higher severity level.

facility *local-number*: Specifies a logging facility by its facility number in the range of local0 to local7. Facility numbers are used by a log host to identify log creation facilities for filtering log messages.

msg *msg-body*: Configures the log message body.

Usage guidelines

EAA sends log messages to the information center. You can configure the information center to output these messages to certain destinations. For more information about the information center, see "Configuring the information center."

You can configure a series of actions to be executed in response to the event specified in a monitor policy. EAA executes the actions in ascending order of action IDs. When you add actions to a policy, you must make sure the execution order is correct. If two actions have the same ID, the most recent one takes effect.

When you define an action, you can specify a value or specify a variable name for an argument. For more information about using EAA environment variables, see "rtm environment."

Examples

Configure an action for the CLI-defined policy **test** to send a log message "hello" with a severity of 7 from the facility device **local3**.

```
<Sysname> system-view
[Sysname] rtm cli-policy test
[Sysname-rtm-test] action 3 syslog priority 7 facility local3 msg hello
```

commit

Use **commit** to enable a CLI-defined monitor policy.

Syntax

commit

Default

No CLI-defined monitor policies are enabled.

Views

CLI-defined policy view

Predefined user roles

network-admin

context-admin

Usage guidelines

You must execute this command for a CLI-defined monitor policy to take effect.

After changing the settings in a policy that has been enabled, you must re-execute this command for the changes to take effect.

Examples

Enable CLI-defined monitor policy **test**.

```
<Sysname> system-view
[Sysname] rtm cli-policy test
[Sysname-rtm-test] commit
```

display rtm environment

Use **display rtm environment** to display user-defined EAA environment variables and their values.

Syntax

display rtm environment [*var-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

var-name: Specifies a user-defined EAA environment variable by its name, a case-sensitive string of 1 to 63 characters. The name can contain digits, letters, and the underscore sign (_), but its leading character cannot be the underscore sign. If you do not specify a variable, this command displays all user-defined EAA environment variables.

Examples

Display all user-defined EAA environment variables.

```
<Sysname> display rtm environment
Name              Value
save_cmd          save main force
show_run_cmd      display current-configuration
```

Table 1 Command output

Field	Description
Name	Name of a user-defined EAA environment variable. This field displays a maximum of 30 characters. To display a user-defined EAA environment variable name of more than 30 characters, use the **display current-configuration** command.
Value	Value of the user-defined EAA environment variable. This field displays a maximum of 30 characters. To display a user-defined EAA environment variable value of more than 30 characters, use the **display current-configuration** command.

display rtm policy

Use **display rtm policy** to display information about EAA monitor policies.

Syntax

display rtm policy { **active** | **registered** [**verbose**] } [*policy-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

active: Specifies policies that are executing the actions.

registered: Specifies policies that have been created.

verbose: Displays detailed information about monitor policies.

policy-name: Specifies a policy by its name, a case-sensitive string of 1 to 63 characters. If you do not specify a policy, the command displays information about all monitor policies.

Usage guidelines

To display the running configuration of CLI-defined monitor policies, execute the **display current-configuration** command in any view or execute the **display this** command in CLI-defined monitor policy view.

Examples

Display monitor policies that are executing the actions.

```
<Sysname> display rtm policy active
JID   Type  Event      TimeActive           PolicyName
507   CLI   INTERFACE  Aug 29 14:55:55 2013 test
```

Table 2 Command output

Field	Description
JID	Job ID, displayed only when you specify the **active** keyword.
Type	Policy creation method: • **TCL**—The policy was configured by using Tcl. • **CLI**—The policy was configured from the CLI.
Event	Event type, including CLI, hotplug, interface, process, SNMP, SNMP-Notification, Syslog, and track.
TimeActive	Time when the monitor policy was triggered.
PolicyName	Name of the monitor policy.

Display brief information about all created monitor policies.

```
<Sysname> display rtm policy registered
Total number: 1
Type  Event      TimeRegistered       PolicyName
CLI              Aug 29 14:54:50 2013 test
```

Table 3 Command output

Field	Description
Total number	Total number of the monitor policies.
Type	Policy creation method: • **TCL**—The policy was configured by using Tcl. • **CLI**—The policy was configured from the CLI.
Event	Event type, including CLI, hotplug, interface, process, SNMP, SNMP-Notification, Syslog, and track.

Field	Description
TimeRegistered	Time when the monitor policy was created.
PolicyName	Name of the monitor policy.

Display detailed information about all monitor policies.

```
<Sysname> display rtm policy registered verbose
  Total number: 1

   Policy Name: test
   Policy Type: CLI
    Event Type:
TimeRegistered: Aug 29 14:54:50 2013
     User-role: network-operator
                network-admin
```

Table 4 Command output

Field	Description
Total number	Total number of the monitor polices.
PolicyName	Name of the monitor policy.
Policy Type	Policy creation method: • **TCL**—The policy was configured by using Tcl. • **CLI**—The policy was configured from the CLI.
Event Type	Event type, including CLI, hotplug, interface, process, SNMP, SNMP-Notification, Syslog, and track.
TimeRegistered	Time when the policy was created.
User-role	User roles for executing the monitor policy. To execute the monitor policy, an administrator must have a minimum of one of the displayed user roles.

event cli

Use **event cli** to configure a CLI event for a CLI-defined monitor policy.

Use **undo event** to delete the event in a CLI-defined monitor policy.

Syntax

event cli { **async** [**skip**] | **sync** } **mode** { **execute** | **help** | **tab** } **pattern** *regular-exp*

undo event

Default

No CLI event is configured.

Views

CLI-defined policy view

Predefined user roles

network-admin

context-admin

Parameters

async [**skip**]: Enables or disables the system to execute the command that triggers the policy. If you specify the **skip** keyword, the system executes the actions in the policy without executing the command that triggers the policy. If you do not specify the **skip** keyword, the system executes both the actions in the policy and the command entered at the CLI.

sync: Enables the system to execute the command that triggers the event only if the policy has been executed successfully.

mode { **execute** | **help** | **tab** }: Specifies the CLI operation to monitor:

- **execute**: Triggers the policy when a matching command is entered.
- **help**: Triggers the policy when a question mark (?) is entered at a matching command line.
- **tab**: Triggers the policy when the **Tab** key is pressed to complete a parameter in a matching command line.

pattern *regular-exp*: Specifies a regular expression for matching commands that trigger the policy. For more information about using regular expressions, see CLI in *Fundamentals Configuration Guide*.

Usage guidelines

Use CLI event monitor policies to monitor operations performed at the CLI.

You can configure only one event for a monitor policy. If the monitor policy already contains an event, the new event replaces the old event.

Examples

Configure a CLI-defined policy to monitor execution of commands that contain the **display interface brief** string. Enable the system to execute the actions in the policy without executing the command that triggers the policy.

```
<Sysname>system-view
[Sysname] rtm cli-policy test
[Sysname-rmt-test] event cli async skip mode execute pattern display interface brief
```

Configure a CLI-defined policy to monitor the use of the **Tab** key at command lines that contain the **display interface brief** string. Enable the system to execute the actions in the policy and display the complete parameter when **Tab** is pressed at a policy-matching command line.

```
<Sysname> system-view
[Sysname] rtm cli-policy test
[Sysname-rmt-test] event cli async mode tab pattern display interface brief
```

Configure a CLI-defined policy to monitor the use of the question mark (?) at command lines that contain the **display interface brief** string. Enable the system to execute a policy-matching command line only if the actions in the policy are executed successfully when a question mark is entered at the command line.

```
<Sysname>system-view
[Sysname] rtm cli-policy test
[Sysname-rmt-test] event cli sync mode help pattern display interface brief
```

event hotplug

Use **event hotplug** to configure an IRF member device join or leave event.

Use **undo event** to delete the event in a CLI-defined monitor policy.

Syntax

event hotplug [**insert** | **remove**] **slot** *slot-number*

undo event

Default

No hotplug event is configured.

Views

CLI-defined policy view

Predefined user roles

network-admin

context-admin

Parameters

insert: Specifies the IRF member device join event.

remove: Specifies the IRF member device leave event.

slot *slot-number*: Specifies an IRF member device by its member ID.

Usage guidelines

After you configure the event, the monitor policy is triggered when the member device joins or leaves the IRF fabric. If you do not specify the **insert** or **remove** keyword, EAA monitors the member device for joining or leaving the IRF fabric.

You can configure only one event entry for a monitor policy. If the monitor policy already contains an event entry, the new event entry replaces the old event entry.

Examples

Configure a CLI-defined policy to monitor the member device for joining or leaving the IRF fabric.

```
<Sysname> system-view
[Sysname] rtm cli-policy test
[Sysname-rtm-test] event hotplug slot 1
```

event interface

Use **event interface** to configure an interface event for a CLI-defined monitor policy.

Use **undo event** to delete the event in a CLI-defined monitor policy.

Syntax

event interface *interface-type interface-number* **monitor-obj** *monitor-obj* **start-op** *start-op* **start-val** *start-val* **restart-op** *restart-op* **restart-val** *restart-val* [**interval** *interval*]

undo event

Default

No interface event is configured.

Views

CLI-defined policy view

Predefined user roles

network-admin

context-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

monitor-obj *monitor-obj*: Specifies the traffic statistic to be monitored on the interface. For keywords available for the *monitor-obj* argument, see Table 5.

start-op *start-op*: Specifies the operator for comparing the monitored traffic statistic with the start threshold. The start threshold is crossed if the comparison result meets the condition. For keywords available for the *start-op* argument, see Table 6.

start-val *start-val*: Specifies the start threshold to be compared with the monitored traffic statistic. The value range is 0 to 4294967295.

restart-op *restart-op*: Specifies the operator for comparing the monitored traffic statistic with the restart threshold. The restart threshold is crossed if the comparison result meets the condition. For keywords available for the *restart-op* argument, see Table 6.

restart-val *restart-val*: Specifies the restart threshold to be compared with the monitored traffic statistic. The value range is 0 to 4294967295.

interval *interval*: Specifies the interval to sample the monitored traffic statistic for a comparison. The value range is 1 to 4294967295, in seconds. The default value is 300.

Table 5 Monitored objects

Monitored traffic statistic	Description
input-drops	Number of discarded incoming packets during the sampling interval
input-errors	Number of incoming error packets during the sampling interval
output-drops	Number of discarded outgoing packets during the sampling interval
output-errors	Number of outgoing error packets during the sampling interval
rcv-bps	Receive rate, in bps during the sampling interval
rcv-broadcasts	Number of incoming broadcasts during the sampling interval
rcv-pps	Receive rate, in packets per second
tx-bps	Transmit rate, in bps
tx-pps	Transmit rate, in packets per second

Table 6 Comparison operators

Comparison operator	Description
eq	Equal to
ge	Greater than or equal to
gt	Greater than
le	Less than or equal to
lt	Less than
ne	Not equal to

Usage guidelines

Use interface event monitor policies to monitor traffic statistics on an interface.

You can configure only one event for a monitor policy. If the monitor policy already contains an event, the new event replaces the old event.

EAA executes an interface event policy when the monitored interface traffic statistic crosses the start threshold in the following situations:

- The statistic crosses the start threshold for the first time.
- The statistic crosses the start threshold each time after it crosses the restart threshold.

The following is the interface event monitor process of EAA:

1. Compares the traffic statistic sample with the start threshold at sampling intervals until the start threshold is crossed.
2. Executes the policy.
3. Compares the traffic statistic sample with the restart threshold at sampling intervals until the restart threshold is crossed.
4. Compares the traffic statistic sample with the start threshold at sampling intervals until the start threshold is crossed.
5. Executes the policy again.

This process cycles for the monitor policy to be executed and re-executed.

Examples

Configure a CLI-defined policy to monitor the incoming error packet statistic on GigabitEthernet 1/0/1 every 60 seconds. Set the start threshold to 1000 and the restart threshold to 50. Enable EAA to execute the policy when the statistic exceeds 1000 for the first time. Enable EAA to re-execute the policy if the statistic exceeds 1000 each time after the statistic has dropped below 50.

```
<Sysname> system-view
[Sysname] rtm cli-policy test
[Sysname-rtm-test] event interface gigabitethernet 1/0/1 monitor-obj input-errors
start-op gt start-val 1000 restart-op lt restart-val 50 interval 60
```

event process

Use **event process** to configure a process event for a CLI-defined monitor policy.

Use **undo event** to delete the event in a CLI-defined monitor policy.

Syntax

event process { **exception** | **restart** | **shutdown** | **start** } [**name** *process-name* [**instance** *instance-id*]] [**slot** *slot-number*]

undo event

Default

No process event is configured.

Views

CLI-defined policy view

Predefined user roles

network-admin

context-admin

Parameters

exception: Monitors the specified process for exceptional events. EAA executes the policy when an exception occurs to the monitored process.

restart: Monitors the specified process for restart events. EAA executes the policy when the monitored process restarts.

shutdown: Monitors the specified process for shutdown events. EAA executes the policy when the monitored process is shut down.

start: Monitors the specified process for start events. EAA executes the policy when the monitored process starts.

name *process-name*: Specifies a user-mode process by its name. The process can be one that is running or not running. If you do not specify a name, this command monitors all use-mode processes.

instance *instance-id*: Specifies a process instance ID in the range of 0 to 4294967295. The instance ID can be one that has not been created yet. If you do not specify an instance, EAA monitors all instances of the process.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command applies to the IRF fabric.

Usage guidelines

Use process event monitor policies to monitor process state changes. These changes can result from manual operations or automatic system operations.

You can configure only one event for a monitor policy. If the monitor policy already contains an event, the new event replaces the old event.

Examples

Configure a CLI-defined policy to monitor all instances of the process **snmpd** for restart events.

```
<Sysname>system-view
[Sysname] rtm cli-policy test
[Sysname-rtm-test] event process restart name snmpd
```

event snmp oid

Use **event snmp oid** to configure an SNMP event for a CLI-defined monitor policy.

Use **undo event** to delete the event in a CLI-defined monitor policy.

Syntax

event snmp oid *oid* **monitor-obj** { **get** | **next** } **start-op** *start-op* **start-val** *start-val* **restart-op** *restart-op* **restart-val** *restart-val* [**interval** *interval*]

undo event

Default

No SNMP event is configured.

Views

CLI-defined policy view

Predefined user roles

network-admin

context-admin

Parameters

oid *oid*: Specifies the OID of the monitored MIB variable, a string of 1 to 256 characters.

monitor-obj { **get** | **next** }: Specifies the SNMP operation used for sampling variable values. The **get** keyword represents the SNMP get operation, and the **next** keyword represents the SNMP getNext operation.

start-op *start-op*: Specifies the operator for comparing the sampled value with the start threshold. The start threshold is crossed if the comparison result meets the condition. For keywords available for the *start-op* argument, see Table 6.

start-val *start-val*: Specifies the start threshold to be compared with the sampled value. The *start-val* argument can be any data type supported by SNMP, including numerals and character strings. The value range for the *start-val* argument is a string of 1 to 512 characters. If the threshold value contains spaces, you must enclose the value in quotation marks (" ").

restart-op *op*: Specifies the operator for comparing the sampled value with the restart threshold. The restart threshold is crossed if the comparison result meets the condition. For keywords available for the *start-op* argument, see Table 6.

restart-op *restart-val*: Specifies the restart threshold to be compared with the sampled value. The *restart-val* argument can be any data type supported by SNMP, including numerals and character strings. The value range for the *restart-val* argument is a string of 1 to 512 characters. If the threshold value contains spaces, you must enclose the value in quotation marks (" ").

interval *interval*: Specifies the sampling interval in the range of 1 to 4294967295, in seconds. The default value is 300.

Usage guidelines

Use SNMP event monitor policy to monitor value changes of MIB variables.

You can configure only one event for a monitor policy. If the monitor policy already contains an event, the new event replaces the old event.

EAA executes an SNMP event policy when the monitored MIB variable's value crosses the start threshold in the following situations:

- The monitored variable's value crosses the start threshold for the first time.
- The monitored variable's value crosses the start threshold each time after it crosses the restart threshold.

The following is the SNMP event monitor process of EAA:

1. Compares the variable sample with the start threshold at sampling intervals until the start threshold is crossed.
2. Executes the policy.
3. Compares the variable sample with the restart threshold at sampling intervals until the restart threshold is crossed.
4. Compares the variable sample with the start threshold at sampling intervals until the start threshold is crossed.
5. Executes the policy again.

This process cycles for the monitor policy to be executed and re-executed.

For the command to take effect, enable SNMP before you execute this command. The device automatically deletes this command after you disable SNMP.

Examples

Configure a CLI-defined policy to get the value of the MIB variable **1.3.6.4.9.9.42.1.2.1.6.4** every five seconds. Set the start threshold to 1 and the restart threshold to 2. Enable EAA to execute the policy when the value changes to 1 for the first time. Enable EAA to re-execute the policy if the value changes to 1 each time after the value has changed to 2.

```
<Sysname> system-view
[Sysname] rtm cli-policy test
[Sysname-rtm-test] event snmp oid 1.3.6.4.9.9.42.1.2.1.6.4 monitor-obj get start-op eq
start-val 1 restart-op eq restart-val 2 interval 5
```

event snmp-notification

Use **event snmp-notification** to configure an SNMP-Notification event for a CLI-defined policy.

Use **undo event** to remove the event in a CLI-defined policy.

Syntax

event snmp-notification oid *oid* **oid-val** *oid-val* **op** *op* [**drop**]

undo event

Default

No SNMP-Notification event is configured.

Views

CLI-defined policy view

Predefined user roles

network-admin

context-admin

Parameters

oid *oid*: Specifies the OID of the monitored MIB variable, a string of 1 to 256 characters.

oid-val *oid-val*: Specifies the threshold to be compared with the sampled value. The *oid-val* argument can be any data type supported by SNMP, including numerals and character strings. The value range for the *oid-val* argument is a string of 1 to 512 characters. If the threshold value contains spaces, you must enclose the value in quotation marks (" ").

op *op*: Specifies the operator for comparing the sampled value with the threshold. The policy is executed if the comparison result meets the condition. For keywords available for the *start-op* argument, see Table 6.

drop: Drops the notification if the comparison result meets the condition. If you do not specify this keyword, the system sends the notification.

Usage guidelines

Use SNMP-Notification event monitor policies to monitor variables in SNMP notifications.

EAA executes an SNMP-Notification event monitor policy when the value of the monitored variable in an SNMP notification meets the specified condition.

You can configure only one event for a monitor policy. If the monitor policy already contains an event, the new event replaces the old event.

For the command to take effect, enable SNMP before you execute this command. The device automatically deletes this command after you disable SNMP.

Examples

Configure a CLI-defined policy to monitor SNMP notifications that contain the use name variable **1.3.6.1.4.1.25506.2.2.1.1.2.1.0**. Enable the system to execute the policy and drop the SNMP notification if the use name variable value is **admin**.

```
<Sysname> system-view
[Sysname] rtm cli-policy test
[Sysname-rtm-test] event snmp-notification oid 1.3.6.1.4.1.25506.2.2.1.1.2.1.0 oid-val
admin op eq drop
```

event syslog

Use **event syslog** to configure a Syslog event for a CLI-defined monitor policy.

Use **undo event** to delete the event in a CLI-defined monitor policy.

Syntax

event syslog priority { *priority* | **all** } **msg** *msg* **occurs** *times* **period** *period*

undo event

Default

No Syslog event is configured.

Views

CLI-defined policy view

Predefined user roles

network-admin

context-admin

Parameters

priority { *priority* | **all** }: Specifies the severity level for matching log messages.

- *priority*: Specifies the lowest severity level for matching log messages. It is an integer in the range of 0 to 7. A lower number represents higher severity level. For example, specify a severity level of 3 to match log messages from level 3 to level 0.
- **all:** Represents any severity level from 0 to 7.

msg *msg*: Specifies a regular expression to match the logs. The *msg* argument represents a regular expression, a string of 1 to 255 characters.

occurs *times* **period** *period*: Executes the policy if the number of log matches over an interval exceeds the limit. The *times* argument specifies the maximum number of log matches in the range of 1 to 32. The *period* argument specifies an interval in the range of 1 to 4294967295 seconds.

Usage guidelines

Use Syslog event monitor policies to monitor log messages.

EAA executes a Syslog event monitor policy when the number of matching logs over an interval reaches the limit.

NOTE:

EAA does not count log messages generated by the RTM module when it counts log matches.

You can configure only one event for a monitor policy. If the monitor policy already contains an event, the new event replaces the old event.

A regular expression can contain the special characters described in Table 7.

Table 7 Special characters supported in a regular expression

Characters	Meaning	Examples
^	Matches the beginning of a line.	"^u" matches all lines beginning with "u". A line beginning with "Au" is not matched.
$	Matches the end of a line.	"u$" matches all lines ending with "u". A line ending with "uA" is not matched.

Characters	Meaning	Examples
. (period)	Matches any single character.	".s" matches "as" and "bs".
*	Matches the preceding character or string zero, one, or multiple times.	"zo*" matches "z" and "zoo", and "(zo)*" matches "zo" and "zozo".
+	Matches the preceding character or string one or multiple times.	"zo+" matches "zo" and "zoo", but not "z".
|	Matches the preceding or succeeding string.	"def|int" matches a line containing "def" or "int".
( )	Matches the string in the parentheses, usually used together with the plus sign (+) or asterisk sign (*).	"(123A)" matches "123A". "408(12)+" matches "40812" and "408121212", but not "408".
\N	Matches the preceding strings in parentheses, with the *Nth* string repeated once.	"(string)\1" matches a string containing "stringstring". "(string1)(string2)\2" matches a string containing "string1string2string2". "(string1)(string2)\1\2" matches a string containing " string1string2string1string2".
[ ]	Matches a single character in the brackets.	"[16A]" matches a string containing 1, 6, or A; "[1-36A]" matches a string containing 1, 2, 3, 6, or A (- is a hyphen). To match the character "]", put it immediately after "[", for example, []abc]. There is no such limit on "[".
[^]	Matches a single character that is not in the brackets.	"[^16A]" matches a string that contains one or more characters except for 1, 6, or A, such as "abc". A match can also contain 1, 6, or A (such as "m16"), but it cannot contain these three characters only (such as 1, 16, or 16A).
{n}	Matches the preceding character *n* times. The number *n* must be a nonnegative integer.	"o{2}" matches "food", but not "Bob".
{n,}	Matches the preceding character *n* times or more. The number *n* must be a nonnegative integer.	"o{2,}" matches "foooood", but not "Bob".
{n,m}	Matches the preceding character *n* to *m* times or more. The numbers *n* and *m* must be nonnegative integers and *n* cannot be greater than *m*.	" o{1,3}" matches "fod", "food", and "foooood", but not "fd".
\<	Matches a string that starts with the pattern following \<. A string that contains the pattern is also a match if the characters preceding the pattern are not digits, letters, or underscores.	"\<do" matches "domain" and "doa".
\>	Matches a string that ends with the pattern preceding \>. A string that contains the pattern is also a match if the characters following the pattern are not digits, letters, or underscores.	"do\>" matches "undo" and "cdo".
\b	Matches a word that starts with the pattern following \b or ends with the pattern preceding \b.	"er\b" matches "never", but not "verb" or "erase". "\ber" matches "erase", but not "verb" or "never".

Characters	Meaning	Examples
\B	Matches a word that contains the pattern but does not start or end with the pattern.	"er\B" matches "verb", but not "never" or "erase".
\w	Same as [A-Za-z0-9_], matches a digit, letter, or underscore.	"v\w" matches "vlan" and "service".
\W	Same as [^A-Za-z0-9_], matches a character that is not a digit, letter, or underscore.	"\Wa" matches "-a", but not "2a" or "ba".
\	Escape character. If a special character listed in this table follows \, the specific meaning of the character is removed.	"\\" matches a string containing "\", "\^" matches a string containing "^", and "\\b" matches a string containing "\b".

Examples

Configure a CLI-defined policy to monitor Syslog messages for level 3 to level 0 messages that contain the **down** string. Enable the policy to execute when five log matches are found within 6 seconds.

```
<Sysname> system-view
[Sysname] rtm cli-policy test
[Sysname-rtm-test] event syslog priority 3 msg down occurs 5 period 6
```

event track

Use **event track** to configure a track event for a CLI-defined monitor policy.

Use **undo event** to delete the event in a CLI-defined monitor policy.

Syntax

event track *track-list* **state** { **negative** | **positive** } [**suppress-time** *suppress-time*]

undo event

Default

A CLI-defined policy does not contain a track event.

Views

CLI-defined policy view

Predefined user roles

network-admin

context-admin

Parameters

track-list: Specifies a space-separated list of up to 16 track items. Each item specifies a track entry number or a range of track entry numbers in the form of *track-entry-number* **to** *track-entry-number*. The value range for the *track-entry-number* argument is 1 to 1024.

state { **negative** | **positive** }: Monitors state change of the track entries.

- **negative**: Triggers the policy when the states of the track entries change from Positive to Negative.

- **positive**: Triggers the policy when the states of the track entries change from Negative to Positive.

suppress-time *suppress-time*: Sets a suppress time in the range of 1 to 4294967295, in seconds. The default value is 0.

Usage guidelines

Use track event monitor policies to monitor state change of track entries. If you specify one track entry for a policy, EAA triggers the policy when the state of the track entry changes from Positive to Negative or from Negative to Positive. If you specify multiple track entries for a policy, EAA triggers the policy only when the state of all the track entries changes from Positive to Negative or Negative to Positive.

If you set a suppress time for a track event monitor policy, the timer starts when the policy is triggered. The system does not process the messages that report the track entry positive-to-negative or negative-to-positive state change until the timer times out.

For example, to automatically disconnect the sessions between the local device and its down link BGP peers when the sessions between the local device and its uplink BGP peers are disconnected, you can configure a track event monitor policy as follows:

- Configure a track event for the policy and specify track entries to monitor the links between the local device and its uplink BGP peers.
- Add the CLI action **peer ignore** to the policy to disable BGP session establishment between the local device and its downlink BGP peers.

You can configure only one event entry for a monitor policy. If the monitor policy already contains an event entry, the new event entry replaces the old event entry.

Examples

Create CLI-defined monitor policy **test**. Configure a track event for the policy that occurs when the states of track entry 1 to track entry 8 change from Positive to Negative. Set the suppress time to 180 seconds for the policy.

```
<Sysname> system-view
[Sysname] rtm cli-policy test
[Sysname-rtm-test] event track 1 to 8 state negative suppress-time 180
```

rtm cli-policy

Use **rtm cli-policy** to create a CLI-defined EAA monitor policy and enter its view, or enter the view of an existing CLI-defined EAA monitor policy.

Use **undo rtm cli-policy** to delete a CLI-defined monitor policy.

Syntax

rtm cli-policy *policy-name*

undo rtm cli-policy *policy-name*

Default

No CLI-defined monitor policies exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies the name of a CLI-defined monitor policy, a case-sensitive string of 1 to 63 characters.

Usage guidelines

You must create a CLI-defined monitor policy before you can use the CLI to configure settings in the policy.

For a CLI-defined monitor policy to take effect, you must execute the **commit** command after you complete configuring the policy.

You can execute this command multiple times to create multiple CLI-defined monitor policies. Make sure the CLI-defined monitor policies that are executed at the same time do not have conflicting actions. If the actions conflict, the system executes the actions randomly.

You can assign the same name to a CLI-defined policy and a Tcl-defined policy.

Examples

Create a CLI-defined policy and enter its view.

```
<Sysname> system-view
[Sysname] rtm cli-policy test
```

Related commands

commit

rtm environment

Use **rtm environment** to configure an EAA environment variable.

Use **undo rtm environment** to delete a user-defined EAA environment variable.

Syntax

rtm environment *var-name var-value*

undo rtm environment *var-name*

Default

No user-defined EAA environment variables exist.

The system provides the variables in Table 8. You cannot create, delete, or modify these system-defined variables.

Table 8 System-defined EAA environment variables by event type

Event	Variable name and description
Any event	_event_id: Event ID. _event_type: Event type. _event_type_string: Event type description. _event_time: Time when the event occurs. _event_severity: Severity level of an event.
CLI	_cmd: Commands that are matched.
Syslog	_syslog_pattern: Log message content.
Hotplug	_slot: ID of the member device that joins or leaves the IRF fabric.
Interface	_ifname: Interface name.

Event	Variable name and description
SNMP	_oid: OID of the MIB variable where an SNMP operation is performed. _oid_value: Value of the MIB variable.
SNMP-Notification	_oid: OID that is included in the SNMP notification.
Process	_process_name: Process name.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

var-name: Specifies a user-defined EAA environment variable by its name, a case-sensitive string of 1 to 63 characters. The name can contain digits, letters, and the underscore sign (_), but its leading character cannot be the underscore sign.

var-value: Specifies the variable value.

Usage guidelines

When you define an action, you can enter a variable name with a leading dollar sign (**$***variable_name*) instead of entering a value for an argument. EAA will replace the variable name with the variable value when it performs the action.

For an action argument, you can specify a list of variable names in the form of **$***variable_name1***$***variable_name2...***$***variable_nameN.*

Examples

Create an environment variable: set its name to **if** and set its value to **interface**.

```
<Sysname> system-view
[Sysname] rtm environment if interface
```

rtm scheduler suspend

Use **rtm scheduler suspend** to suspend all monitor policies, including CLI monitor policies and Tcl monitor policies.

Use **undo rtm scheduler suspend** to resume monitor policies.

Syntax

rtm scheduler suspend

undo rtm scheduler suspend

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

You need to suspend the monitor policies under the following circumstances:

- The monitor policies are triggered frequently, affecting the system services and performance.
- The Tcl script of a policy needs to be revised.

After you execute this command, EAA will not execute the policies even if the trigger conditions are met.

This command does not suspend a running monitor policy until all its actions are executed.

Examples

Suspend monitor policies.

```
<Sysname> system-view
[Sysname] rtm scheduler suspend
```

rtm tcl-policy

Use **rtm tcl-policy** to create a Tcl-defined policy and bind it to a Tcl script file.

Use **undo rtm tcl-policy** to delete a Tcl policy.

Syntax

rtm tcl-policy *policy-name tcl-filename*

undo rtm tcl-policy *policy-name*

Default

No Tcl policies exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies a policy name, a case-sensitive string of 1 to 63 characters.

tcl-filename: Specifies a .tcl script file name. The file name is case sensitive. You must ensure that the file is available on a storage medium of the device.

Usage guidelines

When you use this command to create a Tcl-defined policy, follow these guidelines:

Make sure the script file is saved on all IRF member devices. This practice ensures that the policy can run correctly after a master/subordinate switchover occurs or the member device where the script file resides leaves the IRF.

This command both creates and enables the specified Tcl-defined monitor policy. To revise the Tcl script of a Tcl-defined policy, you must suspend all monitor policies first, and then resume the policies after you finish revising the script. The system cannot execute a Tcl-defined policy if you edit its Tcl script without suspending all monitor policies.

To bind a Tcl-defined policy to a different Tcl script file:

1. Execute the **undo rtm tcl-policy** command to delete the Tcl policy.
2. Create the Tcl policy again, and then bind it to the new Tcl script file.

You can assign the same policy name to a CLI-defined policy and a Tcl-defined policy. However, you cannot assign the same name to policies that are the same type.

Examples

Create a Tcl policy and bind it to a Tcl script file.

```
<Sysname> system-view
[Sysname] rtm tcl-policy test test.tcl
```

running-time

Use **running-time** to configure the action runtime of a CLI-defined policy.

Use **undo running-time** to restore the default.

Syntax

running-time *time*

undo running-time

Default

The action runtime of a CLI-defined policy is 20 seconds.

Views

CLI-defined policy view

Predefined user roles

network-admin

context-admin

Parameters

time: Specifies the action runtime in the range of 0 to 31536000 seconds. If you specify 0, the policy runs its actions forever once the policy is triggered.

Usage guidelines

The action runtime limits the amount of time that the monitor policy runs its actions from the time it is triggered. When the runtime is reached, the system stops executing the actions even if the execution is not finished.

This setting prevents an incorrectly defined policy from running its actions permanently to occupy resources.

Examples

Set the action runtime to **60** seconds for CLI-defined policy **test**.

```
<Sysname> system-view
[Sysname] rtm cli-policy test
[Sysname-rtm-test] running-time 60
```

user-role

Use **user-role** to assign a user role to a CLI-defined policy.

Use **undo user-role** to remove a user role from a CLI-defined policy.

Syntax

user-role *role-name*

undo user-role *role-name*

Default

A monitor policy contains user roles that its creator had at the time of policy creation.

Views

CLI-defined policy view

Predefined user roles

network-admin

context-admin

Parameters

role-name: Specifies a user role by its name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

For EAA to execute an action in a monitor policy, you must assign the policy the user role that has access to the action-specific commands and resources. If EAA lacks access to an action-specific command or resource, EAA does not perform the action and all the subsequent actions.

For example, a monitor policy has four actions numbered from 1 to 4. The policy has user roles that are required for performing actions 1, 3, and 4, but it does not have the user role required for performing action 2. When the policy is triggered, EAA executes only action 1.

A monitor policy supports a maximum of 64 valid user roles. User roles added after this limit is reached do not take effect.

An EAA policy cannot have both the **security-audit** user role and any other user roles. Any previously assigned user roles are automatically removed when you assign the **security-audit** user role to the policy. The previously assigned **security-audit** user role is automatically removed when you assign any other user roles to the policy.

Examples

Assign user roles to a CLI-defined policy.

```
<Sysname> system-view
[Sysname] rtm cli-policy test
[Sysname-rtm-test] user-role network-admin
[Sysname-rtm-test] user-role admin
```

Contents

Process monitoring and maintenance commands

The **display memory**, **display process**, **display process cpu**, **monitor process** and **monitor thread** commands display information about both user processes and kernel threads. In these commands, "process" refers to both user processes and kernel threads.

display exception context

Use **display exception context** to display context information of process exceptions.

Syntax

display exception context [**count** *value*] [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

context-admin

Parameters

count *value*: Specifies the number of context information entries, in the range of 1 to 20. The default value is 1.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays context information of process exceptions on the IRF master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

The system generates a context information entry for each process exception. A context information entry includes the process ID, the crash time, the core dump file directory, stack information, and register information.

Examples

Display the exception context information on the x86-based 32-bit terminal.

```
<Sysname> display exception context
Index 1 of 1
------------------------------
Crashed PID: 120 (routed)
Crash signal: SIGBUS
Crash time: Tue Apr  9 17:14:30 2013
Core file path:
flash:/core/node0_routed_120_7_20130409-171430_1365527670.core
#0  0xb7caba4a
#1  0x0804cb79
#2  0xb7cd77c4
#3  0x08049f45
```

```
Backtrace stopped.
                          Registers' content
  eax:0xfffffffc   ebx:0x00000003   ecx:0xbfe244ec   edx:0x0000000a
  esp:0xbfe244b8   ebp:0xbfe244c8   esi:0xffffffff   edi:0xbfe24674
  eip:0xb7caba4a eflag:0x00000292    cs:0x00000073    ss:0x0000007b
   ds:0x0000007b    es:0x0000007b    fs:0x00000000    gs:0x00000033
```

Display the exception context information on the x86-based 64-bit terminal.

```
<Sysname> display exception context
Index 1 of 1
------------------------------
Crashed PID: 121 (routed)
Crash signal: SIGBUS
Crash time: Sun Mar 31 11:12:21 2013
Core file path:
flash:/core/node0_routed_121_7_20130331-111221_1364728341.core
#0  0x00007fae7dbad20c
#1  0x00000000004059fa
#2  0x00007fae7dbd96c0
#3  0x0000000000402b29
Backtrace stopped.
                          Registers' content
       rax:0xfffffffffffffffc       rbx:0x00007fff88a5dd10
       rcx:0xffffffffffffffff       rdx:0x000000000000000a
       rsi:0x00007fff88a5dd10       rdi:0x0000000000000003
       rbp:0x00007fff88a5dcf0       rsp:0x00007fff88a5dcf0
        r8:0x00007fae7ea587e0        r9:0x0000000000000079
       r10:0xffffffffffffffff       r11:0x0000000000000246
       r12:0x0000000000405b18       r13:0x00007fff88a5ff7a
       r14:0x00007fff88a5de30       r15:0x0000000000000000
       rip:0x00007fae7dbad20c      flag:0x0000000000000246
        cs:0x0000000000000033        ss:0x000000000000002b
        ds:0x0000000000000000        es:0x0000000000000000
        fs:0x0000000000000000        gs:0x0000000000000000
   fs_base:0x00007fae80a5d6a0   gs_base:0x0000000000000000
   orig_ax:0x00000000000000e8
```

Display the exception context information on the PowerPC-based 32-bit terminal.

```
<Sysname> display exception context
Index 1 of 1
------------------------------
Crashed PID: 133 (routed)
Crash signal: SIGBUS
Crash time: Wed Apr 10 15:47:49 2013
Core file path:
flash:/core/node0_routed_133_7_20130410-154749_1365608869.core
#0  0x184720bc
#1  0x10006b4c
Backtrace stopped.
                          Registers' content
```

```
grp00: 0x000000ee 0x7ffd6ad0 0x1800f440 0x00000004
grp04: 0x7ffd6af8 0x0000000a 0xffffffff 0x184720bc
grp08: 0x0002d200 0x00000003 0x00000001 0x1847209c
grp12: 0x10006b4c 0x10020534 0xd6744100 0x00000000
grp16: 0x00000000 0xa0203ff0 0xa028b12c 0xa028b13c
grp20: 0xa028b148 0xa028b168 0xa028b178 0xa028b190
grp24: 0xa028b1a8 0xa028b1b8 0x00000000 0x7ffd6c08
grp28: 0x10006cac 0x7ffd6f92 0x184c1b84 0x7ffd6ae0

  nip:0x184720bc    lr:0x10006b4c    cr:0x38000022   ctr:0x1847209c
  msr:0x0002db00   xer:0x00000000   ret:0xfffffffc dsisr:0x08000000
  gr3:0x00000003    mq:0x00000000  trap:0x00000c00   dar:0x1833114c
```

Display the exception context information on the PowerPC-based 64-bit terminal.

```
<Sysname> display exception context
Index 1 of 1
------------------------------
Crashed PID: 172 (routed)
Crash signal: SIGBUS
Crash time: Sat Sep 15 16:53:16 2007
Core file path:
flash:/core/node1_routed_172_7_20070915-165316_1189875196.core
#0  0x00000fff803c66b4
#1  0x0000000010009b94
#2  0x00000fff80401814
Backtrace stopped.
                        Registers' content
     grp00: 0x00000000000000ee 0x00000fffffd04840
     grp02: 0x00000fff80425c28 0x0000000000000004
     grp04: 0x00000fffffd048c0 0x000000000000000a
     grp06: 0xffffffffffffffff 0x00000fff803c66b4
     grp08: 0x0000000008002d000 0x0000000000000000
     grp10: 0x0000000000000000 0x0000000000000000
     grp12: 0x0000000000000000 0x00000fff80a096b0
     grp14: 0x000000007b964c00 0x000000007b7d0000
     grp16: 0x0000000000000001 0x000000000000000b
     grp18: 0x0000000000000031 0x0000000000a205b8
     grp20: 0x0000000000a20677 0x0000000000000000
     grp22: 0x000000007bb91014 0x0000000000000000
     grp24: 0xc0000000005ae1c8 0x0000000000000000
     grp26: 0xc0000001f00bff20 0xc0000001f00b0000
     grp28: 0x00000fffffd04a30 0x0000000001001aed8
     grp30: 0x00000fffffd04fae 0x00000fffffd04840

       nip:0x00000fff803c66b4        lr:0x0000000010009b94
        cr:0x0000000058000482       ctr:0x00000fff803c66ac
       msr:0x0000000008002d000       xer:0x0000000000000000
       ret:0xfffffffffffffffc     dsisr:0x0000000000000000
       gr3:0x0000000000000003     softe:0x0000000000000001
```

```
      trap:0x0000000000000c00       dar:0x00000fff8059d14c
```

Display the exception context information on the MIPS-based 32-bit terminal.

```
<Sysname> display exception context
Index 1 of 1
------------------------------
Crashed PID: 182 (routed)
Crash signal: SIGBUS
Crash time: Sun Jan  2 08:11:38 2013
Core file path:
flash:/core/node4_routed_182_10_20130102-081138_1293955898.core
#0  0x2af2faf4
#1  0x00406d8c
Backtrace stopped.
                         Registers' content
 zero:0x00000000   at:0x1000dc00   v0:0x00000004   v1:0x00000003
   a0:0x00000003   a1:0x7fd267e8   a2:0x0000000a   a3:0x00000001
   t0:0x00000000   t1:0xcf08fa14   t2:0x80230510   t3:0xffffff8
   t4:0x69766520   t5:0x00000000   t6:0x63cc6000   t7:0x44617461
   s0:0x7fd26f81   s1:0x00401948   s2:0x7fd268f8   s3:0x803e1db0
   s4:0x803e1da0   s5:0x803e1d88   s6:0x803e1d70   s7:0x803e1d60
   t8:0x00000008   t9:0x2af2fae0   k0:0x00000000   k1:0x00000000
   gp:0x2af9a3a0   sp:0x7fd267c0   s8:0x7fd267c0   ra:0x00406d8c
   sr:0x0000dc13   lo:0xef9db265   hi:0x0000003f  bad:0x2add2010
cause:0x00800020   pc:0x2af2faf4
```

Display the exception context information on the MIPS-based 64-bit terminal.

```
<Sysname> display exception context
Index 1 of 1
------------------------------
Crashed PID: 270 (routed)
Crash signal: SIGBUS
Crash time: Wed Mar 27 12:39:12 2013
Core file path:
flash:/core/node16_routed_270_10_20130327-123912_1364387952.core
#0  0x0000005555a3bcb4
#1  0x0000000120006c1c
Backtrace stopped.
                         Registers' content
      zero:0x0000000000000000        at:0x0000000000000014
        v0:0x0000000000000004        v1:0x0000000000000003
        a0:0x0000000000000003        a1:0x000000ffff899d90
        a2:0x000000000000000a        a3:0x0000000000000001
        a4:0x0000005555a9b4e0        a5:0x0000000000000000
        a6:0xffffffff8021349c        a7:0x20696e206368616e
        t0:0x0000000000000000        t1:0xffffffff80105068
        t2:0xffffffff80213890        t3:0x0000000000000008
        s0:0x0000005555a99c40        s1:0x000000ffff89af5f
        s2:0x0000000120007320        s3:0x0000005555a5f470
        s4:0x000000ffff899f80        s5:0xffffffff803cc6c0
```

```
      s6:0xffffffff803cc6a8        s7:0xffffffff803cc690
      t8:0x0000000000000002        t9:0x0000005555a3bc98
      k0:0x0000000000000000        k1:0x0000000000000000
      gp:0x0000000120020460        sp:0x000000ffff899d70
      s8:0x000000ffff899d80        ra:0x0000000120006c1c
      sr:0x000000000400fff3        lo:0xdf3b645a1cac08c9
      hi:0x000000000000007f       bad:0x000000555589ba84
   cause:0x0000000000800020        pc:0x0000005555a3bcb4
```

Table 1 Command output

Filed	Description
Crashed PID	ID of the crashed process.
Crash signal	Signals that led to the crash: • **SIGABRT**—Abort. • **SIGBUS**—Bus error. • **SIGFPE**—Erroneous arithmetic operation. • **SIGILL**—Illegal hardware instructions. • **SIGQUIT**—Quit signal sent by the controlling terminal. • **SIGSEGV**—Invalid memory access. • **SIGSYS**—Invalid system call. • **SIGTRAP**—Trap message. • **SIGXCPU**—CPU usage limit exceeded. • **SIGXFSZ**—File size limit exceeded. • **SIGUNKNOW**—Unknown reason.
Crash time	Time when the crash occurred.
Core file path	Directory where the core dump file is saved.
Backtrace stopped	All stack information has been displayed.

Related commands

`reset exception context`

display exception filepath

Use **`display exception filepath`** to display the core dump file directory.

Syntax

`display exception filepath` [**`slot`** *`slot-number`* [**`cpu`** *`cpu-number`*]]

Views

Any view

Predefined user roles

network-admin

context-admin

Parameters

`slot` *`slot-number`*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the core dump file directory on the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Examples

Display the core dump file directory on the specified slot.

```
<Sysname> display exception filepath slot 1
The exception filepath on slot 1 is flash:.
```

display kernel deadloop

Use **display kernel deadloop** to display kernel thread deadloop information.

Syntax

display kernel deadloop *show-number* [*offset*] [**verbose**] [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

Parameters

show-number: Specifies the number of deadloops to display, in the range of 1 to 20.

offset: Specifies the offset between the starting deadloop and the most recent deadloop, in the range of 0 to 19. The default value is 0.

verbose: Displays detailed information. If you do not specify this keyword, the command displays brief information.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays kernel thread deadloop information on the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

This command is supported only on the default context.

Examples

Display brief information about the most recent kernel thread deadloop.

```
<Sysname> display kernel deadloop 1
----------------- Deadloop record 1 -----------------
Description          : BUG: soft lockup - CPU#0 stuck for 61! [comsh: 16306]
Recorded at          : 2013-05-01  11:16:00.823018
Occurred at          : 2013-05-01  11:16:00.823018
Instruction address  : 0x4004158c
Thread               : comsh (TID: 16306)
Context              : thread context
Slot                 : 1
Cpu                  : 0
VCPU ID              : 0
Kernel module info   : module name (mrpnc) module address (0xe332a000)
```

Display detailed information about the most recent kernel thread deadloop.

```
<Sysname> display kernel deadloop 1 verbose
----------------- Deadloop record 1 -----------------
```

```
Description          : BUG: soft lockup - CPU#0 stuck for 61! [comsh: 16306]
Recorded at          : 2013-05-01  11:16:00.823018
Occurred at          : 2013-05-01  11:16:00.823018
Instruction address  : 0x4004158c
Thread               : comsh (TID: 16306)
Context              : thread context
Slot                 : 1
Cpu                  : 0
VCPU ID              : 0
Kernel module info   : module name (mrpnc) module address (0xe332a000)

Last 5 thread switches : migration/0 (11:16:00.823018)-->
                         swapper (11:16:00.833018)-->
                         kthreadd (11:16:00.833518)-->
                         swapper (11:16:00.833550)-->
                         disk (11:16:00.833560)

Register content:
Reg:       r0, Val = 0x00000000 ; Reg:       r1, Val = 0xe2be5ea0 ;
Reg:       r2, Val = 0x00000000 ; Reg:       r3, Val = 0x77777777 ;
Reg:       r4, Val = 0x00000000 ; Reg:       r5, Val = 0x00001492 ;
Reg:       r6, Val = 0x00000000 ; Reg:       r7, Val = 0x0000ffff ;
Reg:       r8, Val = 0x77777777 ; Reg:       r9, Val = 0x00000000 ;
Reg:      r10, Val = 0x00000001 ; Reg:      r11, Val = 0x0000002c ;
Reg:      r12, Val = 0x057d9484 ; Reg:      r13, Val = 0x00000000 ;
Reg:      r14, Val = 0x00000000 ; Reg:      r15, Val = 0x02000000 ;
Reg:      r16, Val = 0xe2be5f00 ; Reg:      r17, Val = 0x00000000 ;
Reg:      r18, Val = 0x00000000 ; Reg:      r19, Val = 0x00000000 ;
Reg:      r20, Val = 0x024c10f8 ; Reg:      r21, Val = 0x057d9244 ;
Reg:      r22, Val = 0x00002000 ; Reg:      r23, Val = 0x0000002c ;
Reg:      r24, Val = 0x00000002 ; Reg:      r25, Val = 0x24000024 ;
Reg:      r26, Val = 0x00000000 ; Reg:      r27, Val = 0x057d9484 ;
Reg:      r28, Val = 0x0000002c ; Reg:      r29, Val = 0x00000000 ;
Reg:      r30, Val = 0x0000002c ; Reg:      r31, Val = 0x00000000 ;
Reg:       cr, Val = 0x84000028 ; Reg:      nip, Val = 0x057d9550 ;
Reg:      xer, Val = 0x00000000 ; Reg:       lr, Val = 0x0186eff0 ;
Reg:      ctr, Val = 0x682f7344 ; Reg:      msr, Val = 0x00784b5c ;
Reg:     trap, Val = 0x0000b030 ; Reg:      dar, Val = 0x77777777 ;
Reg:    dsisr, Val = 0x40000000 ; Reg:   result, Val = 0x00020300 ;

Dump stack (total 1024 bytes, 16 bytes/line):
0xe2be5ea0: 02 be 5e c0 24 00 00 24 00 00 00 00 05 7d 94 84
0xe2be5eb0: 00 00 00 04 00 00 00 00 00 00 00 28 05 8d 34 c4
0xe2be5ec0: 02 be 60 a0 01 86 ef f0 00 00 00 00 00 00 00 00
0xe2be5ed0: 02 04 05 b4 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5ee0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5ef0: 95 47 73 35 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5f00: a0 e1 64 21 00 00 00 00 00 00 00 00 00 00 00 00
```

```
0xe2be5f10: 00 00 00 00 00 00 00 00 00 00 00 00 01 e9 00 00
0xe2be5f20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5f30: 00 00 00 00 00 00 00 00 02 be 66 c0 02 be 66 d0
0xe2be5f40: 02 be 61 e0 00 00 00 02 00 00 00 00 02 44 b3 a4
0xe2be5f50: 02 be 5f 90 00 00 00 08 02 be 5f e0 00 00 00 08
0xe2be5f60: 02 be 5f 80 00 ac 1b 14 00 00 00 00 00 00 00 00
0xe2be5f70: 05 b4 5f 90 02 be 5f e0 00 00 00 30 02 be 5f e0
0xe2be5f80: 02 be 5f c0 00 ac 1b f4 00 00 00 00 02 45 00 00
0xe2be5f90: 00 03 00 00 00 00 00 00 02 be 5f e0 00 00 00 30
0xe2be5fa0: 02 be 5f c0 00 ac 1b 14 61 f1 2e ae 02 45 00 00
0xe2be5fb0: 02 44 b3 74 02 be 5f d0 00 00 00 30 02 be 5f e0
0xe2be5fc0: 02 be 60 60 01 74 ff f8 00 00 00 00 00 00 08 00
0xe2be5fd0: 02 be 5f f0 00 e8 93 7e 02 be 5f f8 02 be 5f fc
0xe2be5fe0: 00 00 00 00 00 00 00 00 00 00 00 00 02 be 60 18
0xe2be5ff0: 02 be 60 10 00 e9 65 98 00 00 00 58 00 00 2a 4f
0xe2be6000: 02 be 60 10 00 00 00 00 00 00 00 00 02 be 60 68
0xe2be6010: 02 be 60 40 00 e8 c6 a0 00 00 11 17 00 00 00 00
0xe2be6020: 02 be 60 40 00 00 00 00 00 00 00 00 02 be 60 98
0xe2be6030: 02 27 00 00 00 00 00 00 00 00 00 00 02 be 60 68
0xe2be6040: 02 be 60 60 00 00 00 01 00 00 b0 30 02 be 60 98
0xe2be6050: 00 00 00 04 02 21 00 00 00 00 00 00 01 e9 00 00
0xe2be6060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be6070: 00 00 00 00 00 00 00 00 02 be 66 c0 02 be 66 d0
0xe2be6080: 02 be 61 e0 00 00 00 02 00 00 00 00 02 be 61 70
0xe2be6090: 00 00 00 00 02 21 00 00 05 8d 34 c4 05 7d 92 44

Call trace:
Function Address = 0x8012a4b4
Function Address = 0x8017989c
Function Address = 0x80179b30
Function Address = 0x80127438
Function Address = 0x8012d734
Function Address = 0x80100a00
Function Address = 0xe0071004
Function Address = 0x8016ce0c
Function Address = 0x801223a0

Instruction dump:
41a2fe9c 812300ec 800200ec 7f890000 409efe8c 80010014 540b07b9 40a2fe80
4bfffe6c 80780290 7f64db78 4804ea35 <807f002c> 38800000 38a00080 3863000c
```

Table 2 Command output

Field	Description
Description	Description for the kernel thread deadloop, including the CPU number, thread running time, thread name, and thread number.
Recorded at	Time when the kernel thread deadloop was recorded, with microsecond precision.
Occurred at	Time when the kernel thread deadloop occurred, with microsecond

Field	Description
	precision.
Instruction address	Instruction address for the kernel thread deadloop.
Thread	Name and number of the kernel thread deadloop.
Context	Context for the kernel thread deadloop.
Cpu	Number of the CPU where the kernel thread ran.
VCPU ID	Number of the CPU core where the kernel thread ran.
Kernel module info	Information about kernel modules that had been loaded when the kernel thread deadloop was detected, including: • **Module name**—Kernel module name. • **Module address**—Memory address of the module.
Last 5 thread switches	Last five kernel thread switches on the CPU before the kernel thread deadloop was detected, including kernel thread name and kernel thread switching time with microsecond precision.
Register content	Register information: • **Reg**—Name of a register. • **Val**—Value saved in a register.
Dump stack	Stack information.
Call trace	Function call stack information, which shows the instruction address of a called function at each level.
Instruction dump	Instruction code when the kernel thread deadloop was detected. **ffffffff** indicates an illegitimate instruction code.
No information to display	No kernel thread deadloop information.

Related commands

`reset kernel deadloop`

display kernel deadloop configuration

Use **`display kernel deadloop configuration`** to display kernel thread deadloop detection configuration.

Syntax

`display kernel deadloop configuration` [**`slot`** *`slot-number`* [**`cpu`** *`cpu-number`*]]

Views

Any view

Predefined user roles

network-admin

Parameters

`slot` *`slot-number`*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the kernel thread deadloop detection configuration for the master device.

`cpu` *`cpu-number`*: Specifies a CPU by its number.

Usage guidelines

This command is supported only on the default context.

Examples

Display kernel thread deadloop detection configuration.

```
<Sysname> display kernel deadloop configuration
Thread dead loop detection: Enabled
Dead loop timer (in seconds): 20
Cores with dead loop detection enabled: 0-1
Dead loop action threshold: 2 consecutive dead loops
Threads excluded from monitoring: 1
  TID:     15   Name: co0
```

Table 3 Command output

Field	Description
Dead loop timer (in seconds): *n*	Time interval (in seconds) to identify a kernel thread deadloop. A kernel thread deadloop occurs if a kernel thread runs more than *n* seconds.
Threads excluded from monitoring	Kernel threads excluded from kernel thread deadloop detection. This field appears only if the **monitor kernel deadloop exclude-thread** command is configured.
Name	Kernel thread name.
TID	Kernel thread number.
No thread is excluded from monitoring	All kernel threads are monitored by kernel thread deadloop detection.

display kernel exception

Use **display kernel exception** to display kernel thread exception information.

Syntax

display kernel exception *show-number* [*offset*] [**verbose**] [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

Parameters

show-number: Specifies the number of kernel exceptions to display, in the range of 1 to 20.

offset: Specifies the offset between the starting exception and the most recent exception, in the range of 0 to 19. The default value is 0.

verbose: Displays detailed information. If you do not specify this keyword, the command displays brief information.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays kernel thread exception information of the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

This command is supported only on the default context.

If an exception occurs to a running kernel thread, the system automatically records the exception information.

Examples

Display brief information about the most recent kernel thread exception.

```
<Sysname> display kernel exception 1
----------------- Exception record 1 -----------------
Description          : Oops[#0]
Recorded at          : 2017-05-01  11:16:00.823018
Occurred at          : 2017-05-01  11:16:00.823018
Instruction address  : 0x4004158c
Thread               : comsh (TID: 16306)
Context              : thread context
Slot                 : 1
Cpu                  : 0
VCPU ID              : 0
Kernel module info   : module name (mrpnc) module address (0xe332a000)
                       module name (disk) module address (0xe00bd000)
```

Display detailed information about the most recent kernel thread exception.

```
<Sysname> display kernel exception 1 verbose
----------------- Exception record 1 -----------------
Description          : Oops[#0]
Recorded at          : 2017-05-01  11:16:00.823018
Occurred at          : 2017-05-01  11:16:00.823018
Instruction address  : 0x4004158c
Thread               : comsh (TID: 16306)
Context              : thread context
Slot                 : 1
Cpu                  : 0
VCPU ID              : 0
Kernel module info   : module name (mrpnc) module address (0xe332a000)
                       module name (12500) module address (0xe00bd000)

Last 5 thread switches : migration/0 (11:16:00.823018)-->
                         swapper (11:16:00.833018)-->
                         kthreadd (11:16:00.833518)-->
                         swapper (11:16:00.833550)-->
                         disk (11:16:00.833560)

Register content:
Reg:       r0, Val = 0x00000000 ; Reg:       r1, Val = 0xe2be5ea0 ;
Reg:       r2, Val = 0x00000000 ; Reg:       r3, Val = 0x77777777 ;
Reg:       r4, Val = 0x00000000 ; Reg:       r5, Val = 0x00001492 ;
Reg:       r6, Val = 0x00000000 ; Reg:       r7, Val = 0x0000ffff ;
Reg:       r8, Val = 0x77777777 ; Reg:       r9, Val = 0x00000000 ;
Reg:      r10, Val = 0x00000001 ; Reg:      r11, Val = 0x0000002c ;
```

```
Reg:      r12, Val = 0x057d9484 ; Reg:      r13, Val = 0x00000000 ;
Reg:      r14, Val = 0x00000000 ; Reg:      r15, Val = 0x02000000 ;
Reg:      r16, Val = 0xe2be5f00 ; Reg:      r17, Val = 0x00000000 ;
Reg:      r18, Val = 0x00000000 ; Reg:      r19, Val = 0x00000000 ;
Reg:      r20, Val = 0x024c10f8 ; Reg:      r21, Val = 0x057d9244 ;
Reg:      r22, Val = 0x00002000 ; Reg:      r23, Val = 0x0000002c ;
Reg:      r24, Val = 0x00000002 ; Reg:      r25, Val = 0x24000024 ;
Reg:      r26, Val = 0x00000000 ; Reg:      r27, Val = 0x057d9484 ;
Reg:      r28, Val = 0x0000002c ; Reg:      r29, Val = 0x00000000 ;
Reg:      r30, Val = 0x0000002c ; Reg:      r31, Val = 0x00000000 ;
Reg:       cr, Val = 0x84000028 ; Reg:      nip, Val = 0x057d9550 ;
Reg:      xer, Val = 0x00000000 ; Reg:       lr, Val = 0x0186eff0 ;
Reg:      ctr, Val = 0x682f7344 ; Reg:      msr, Val = 0x00784b5c ;
Reg:     trap, Val = 0x0000b030 ; Reg:      dar, Val = 0x77777777 ;
Reg:    dsisr, Val = 0x40000000 ; Reg:   result, Val = 0x00020300 ;

Dump stack (total 1024 bytes, 16 bytes/line):
0xe2be5ea0: 02 be 5e c0 24 00 00 24 00 00 00 00 05 7d 94 84
0xe2be5eb0: 00 00 00 04 00 00 00 00 00 00 00 28 05 8d 34 c4
0xe2be5ec0: 02 be 60 a0 01 86 ef f0 00 00 00 00 00 00 00 00
0xe2be5ed0: 02 04 05 b4 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5ee0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5ef0: 95 47 73 35 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5f00: a0 e1 64 21 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5f10: 00 00 00 00 00 00 00 00 00 00 00 00 01 e9 00 00
0xe2be5f20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5f30: 00 00 00 00 00 00 00 00 02 be 66 c0 02 be 66 d0
0xe2be5f40: 02 be 61 e0 00 00 00 02 00 00 00 00 02 44 b3 a4
0xe2be5f50: 02 be 5f 90 00 00 00 08 02 be 5f e0 00 00 00 08
0xe2be5f60: 02 be 5f 80 00 ac 1b 14 00 00 00 00 00 00 00 00
0xe2be5f70: 05 b4 5f 90 02 be 5f e0 00 00 00 30 02 be 5f e0
0xe2be5f80: 02 be 5f c0 00 ac 1b f4 00 00 00 00 02 45 00 00
0xe2be5f90: 00 03 00 00 00 00 00 00 02 be 5f e0 00 00 00 30
0xe2be5fa0: 02 be 5f c0 00 ac 1b 14 61 f1 2e ae 02 45 00 00
0xe2be5fb0: 02 44 b3 74 02 be 5f d0 00 00 00 30 02 be 5f e0
0xe2be5fc0: 02 be 60 60 01 74 ff f8 00 00 00 00 00 00 08 00
0xe2be5fd0: 02 be 5f f0 00 e8 93 7e 02 be 5f f8 02 be 5f fc
0xe2be5fe0: 00 00 00 00 00 00 00 00 00 00 00 00 02 be 60 18
0xe2be5ff0: 02 be 60 10 00 e9 65 98 00 00 00 58 00 00 2a 4f
0xe2be6000: 02 be 60 10 00 00 00 00 00 00 00 00 02 be 60 68
0xe2be6010: 02 be 60 40 00 e8 c6 a0 00 00 11 17 00 00 00 00
0xe2be6020: 02 be 60 40 00 00 00 00 00 00 00 00 02 be 60 98
0xe2be6030: 02 27 00 00 00 00 00 00 00 00 00 00 02 be 60 68
0xe2be6040: 02 be 60 60 00 00 00 01 00 00 b0 30 02 be 60 98
0xe2be6050: 00 00 00 04 02 21 00 00 00 00 00 00 01 e9 00 00
0xe2be6060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be6070: 00 00 00 00 00 00 00 00 02 be 66 c0 02 be 66 d0
0xe2be6080: 02 be 61 e0 00 00 00 02 00 00 00 00 02 be 61 70
```

```
0xe2be6090: 00 00 00 00 02 21 00 00 05 8d 34 c4 05 7d 92 44

Call trace:
Function Address = 0x8012a4b4
Function Address = 0x8017989c
Function Address = 0x80179b30
Function Address = 0x80127438
Function Address = 0x8012d734
Function Address = 0x80100a00
Function Address = 0xe0071004
Function Address = 0x8016ce0c
Function Address = 0x801223a0

Instruction dump:
41a2fe9c 812300ec 800200ec 7f890000 409efe8c 80010014 540b07b9 40a2fe80
4bfffe6c 80780290 7f64db78 4804ea35 <807f002c> 38800000 38a00080 3863000c
```

For more information about the command output, see Table 2.

Related commands

reset kernel exception

display kernel reboot

Use **display kernel reboot** to display reboot information of member devices.

Syntax

display kernel reboot *show-number* [*offset*] [**verbose**] [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

Parameters

show-number: Specifies the number of reboots to display, in the range of 1 to 20.

offset: Specifies the offset between the starting reboot and the most recent reboot, in the range of 0 to 19. The default value is 0.

verbose: Displays detailed information. If you do not specify this keyword, the command displays brief information.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays reboot information of the master device. Reboot information of member devices is recorded in the memory of the master device. If the master device is powered off, the reboot information is lost.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

This command is supported only on the default context.

Examples

Display brief information about the most recent reboot.

```
<Sysname> display kernel reboot 1
----------------- Reboot record 1 -----------------
Recorded at          : 2013-05-01  11:16:00.823018
Occurred at          : 2013-05-01  11:16:00.823018
Reason               : 0x31
Thread               : comsh (TID: 16306)
Context              : thread context
Slot                 : 1
Target Slot          : 0
Cpu                  : 0
Target CPU           : 0
VCPU ID              : 0
Kernel module info   : module name (mrpnc) module address (0xe332a000)
                       module name (12500) module address (0xe00bd000)
```

Display detailed information about the most recent reboot.

```
<Sysname> display kernel reboot 1 verbose
----------------- Reboot record 1 -----------------
Recorded at          : 2013-05-01  11:16:00.823018
Occurred at          : 2013-05-01  11:16:00.823018
Reason               : 0x31
Thread               : comsh (TID: 16306)
Context              : thread context
Slot                 : 1
Target Slot          : 0
Cpu                  : 0
Target CPU           : 0
VCPU ID              : 0
Kernel module info   : module name (mrpnc) module address (0xe332a000)
                       module name (12500) module address (0xe00bd000)

Last 5 thread switches : migration/0 (11:16:00.823018)-->
                         swapper (11:16:00.833018)-->
                         kthreadd (11:16:00.833518)-->
                         swapper (11:16:00.833550)-->
                         disk (11:16:00.833560)

Dump stack (total 1024 bytes, 16 bytes/line):
0xe2be5ea0: 02 be 5e c0 24 00 00 24 00 00 00 00 05 7d 94 84
0xe2be5eb0: 00 00 00 04 00 00 00 00 00 00 00 28 05 8d 34 c4
0xe2be5ec0: 02 be 60 a0 01 86 ef f0 00 00 00 00 00 00 00 00
0xe2be5ed0: 02 04 05 b4 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5ee0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5ef0: 95 47 73 35 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5f00: a0 e1 64 21 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5f10: 00 00 00 00 00 00 00 00 00 00 00 00 01 e9 00 00
0xe2be5f20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
0xe2be5f30: 00 00 00 00 00 00 00 00 02 be 66 c0 02 be 66 d0
0xe2be5f40: 02 be 61 e0 00 00 00 02 00 00 00 00 02 44 b3 a4
0xe2be5f50: 02 be 5f 90 00 00 00 08 02 be 5f e0 00 00 00 08
0xe2be5f60: 02 be 5f 80 00 ac 1b 14 00 00 00 00 00 00 00 00
0xe2be5f70: 05 b4 5f 90 02 be 5f e0 00 00 00 30 02 be 5f e0
0xe2be5f80: 02 be 5f c0 00 ac 1b f4 00 00 00 00 02 45 00 00
0xe2be5f90: 00 03 00 00 00 00 00 00 02 be 5f e0 00 00 00 30
0xe2be5fa0: 02 be 5f c0 00 ac 1b 14 61 f1 2e ae 02 45 00 00
0xe2be5fb0: 02 44 b3 74 02 be 5f d0 00 00 00 30 02 be 5f e0
0xe2be5fc0: 02 be 60 60 01 74 ff f8 00 00 00 00 00 00 08 00
0xe2be5fd0: 02 be 5f f0 00 e8 93 7e 02 be 5f f8 02 be 5f fc
0xe2be5fe0: 00 00 00 00 00 00 00 00 00 00 00 00 02 be 60 18
0xe2be5ff0: 02 be 60 10 00 e9 65 98 00 00 00 58 00 00 2a 4f
0xe2be6000: 02 be 60 10 00 00 00 00 00 00 00 00 02 be 60 68
0xe2be6010: 02 be 60 40 00 e8 c6 a0 00 00 11 17 00 00 00 00
0xe2be6020: 02 be 60 40 00 00 00 00 00 00 00 00 02 be 60 98
0xe2be6030: 02 27 00 00 00 00 00 00 00 00 00 00 02 be 60 68
0xe2be6040: 02 be 60 60 00 00 00 01 00 00 b0 30 02 be 60 98
0xe2be6050: 00 00 00 04 02 21 00 00 00 00 00 00 01 e9 00 00
0xe2be6060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be6070: 00 00 00 00 00 00 00 00 02 be 66 c0 02 be 66 d0
0xe2be6080: 02 be 61 e0 00 00 00 02 00 00 00 00 02 be 61 70
0xe2be6090: 00 00 00 00 02 21 00 00 05 8d 34 c4 05 7d 92 44

Call trace:
Function Address = 0x8012a4b4
Function Address = 0x8017989c
Function Address = 0x80179b30
Function Address = 0x80127438
Function Address = 0x8012d734
Function Address = 0x80100a00
Function Address = 0xe0071004
Function Address = 0x8016ce0c
Function Address = 0x801223a0
```

Table 4 Command output

Field	Description
Recorded at	Time when the reboot was recorded, with microsecond precision.
Occurred at	Time when the reboot occurred, with microsecond precision.
Reason	Reboot reason.
Thread	Name and number of the kernel thread that was running when the reboot occurred.
Context	Context where the reboot occurred.
Slot	Number of the slot that triggered the reboot.
Target Slot	Number of the rebooted slot.
Cpu	Number of the CPU that triggered the reboot.

Field	Description
Target CPU	Number of the CPU that rebooted.
VCPU ID	Number of the CPU core that triggered the reboot.
Kernel module info	Information about kernel modules that had been loaded when the reboot occurred, including the kernel module names and memory addresses.
Last 5 thread switches	Last five kernel thread switches that occurred on the CPU before the reboot, including the kernel thread names and kernel thread switching time points, with microsecond precision.
Dump stack	Stack information for the threads that were running when the reboot occurred.
Call trace	Function call stack information.
No information to display	No reboot information exists.

Related commands

reset kernel reboot

display kernel starvation

Use **display kernel starvation** to display kernel thread starvation information.

Syntax

display kernel starvation *show-number* [*offset*] [**verbose**] [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

Parameters

show-number: Specifies the number of thread starvations to display, in the range of 1 to 20.

offset: Specifies the offset between the starting starvation and the most recent starvation, in the range of 0 to 19. The default value is 0.

verbose: Displays detailed information. If you do not specify this keyword, the command displays brief information.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays kernel thread starvation information of the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

This command is supported only on the default context.

Examples

Display brief information about the most recent kernel thread starvation.

```
<Sysname> display kernel starvation 1
----------------- Starvation record 1 -----------------
Description          : INFO: task comsh: 16306 blocked for more than 10 seconds.
Recorded at          : 2013-05-01  11:16:00.823018
Occurred at          : 2013-05-01  11:16:00.823018
```

```
Instruction address  : 0x4004158c
Thread               : comsh (TID: 16306)
Context              : thread context
Slot                 : 1
Cpu                  : 0
VCPU ID              : 0
Kernel module info   : module name (mrpnc) module address (0xe332a000)
                       module name (12500) module address (0xe00bd000)
```

Display detailed information about the most recent kernel thread starvation.

```
<Sysname> display kernel starvation 1 verbose
----------------- Starvation record 1 -----------------
Description          : INFO: task comsh: 16306 blocked for more than 10 seconds.
Recorded at          : 2013-05-01  11:16:00.823018
Occurred at          : 2013-05-01  11:16:00.823018
Instruction address  : 0x4004158c
Thread               : comsh (TID: 16306)
Context              : thread context
Slot                 : 1
Cpu                  : 0
VCPU ID              : 0
Kernel module info   : module name (mrpnc) module address (0xe332a000)
                       module name (12500) module address (0xe00bd000)

Last 5 thread switches : migration/0 (11:16:00.823018)-->
                         swapper (11:16:00.833018)-->
                         kthreadd (11:16:00.833518)-->
                         swapper (11:16:00.833550)-->
                         disk (11:16:00.833560)

Register content:
Reg:       r0, Val = 0x00000000 ; Reg:       r1, Val = 0xe2be5ea0 ;
Reg:       r2, Val = 0x00000000 ; Reg:       r3, Val = 0x77777777 ;
Reg:       r4, Val = 0x00000000 ; Reg:       r5, Val = 0x00001492 ;
Reg:       r6, Val = 0x00000000 ; Reg:       r7, Val = 0x0000ffff ;
Reg:       r8, Val = 0x77777777 ; Reg:       r9, Val = 0x00000000 ;
Reg:      r10, Val = 0x00000001 ; Reg:      r11, Val = 0x0000002c ;
Reg:      r12, Val = 0x057d9484 ; Reg:      r13, Val = 0x00000000 ;
Reg:      r14, Val = 0x00000000 ; Reg:      r15, Val = 0x02000000 ;
Reg:      r16, Val = 0xe2be5f00 ; Reg:      r17, Val = 0x00000000 ;
Reg:      r18, Val = 0x00000000 ; Reg:      r19, Val = 0x00000000 ;
Reg:      r20, Val = 0x024c10f8 ; Reg:      r21, Val = 0x057d9244 ;
Reg:      r22, Val = 0x00002000 ; Reg:      r23, Val = 0x0000002c ;
Reg:      r24, Val = 0x00000002 ; Reg:      r25, Val = 0x24000024 ;
Reg:      r26, Val = 0x00000000 ; Reg:      r27, Val = 0x057d9484 ;
Reg:      r28, Val = 0x0000002c ; Reg:      r29, Val = 0x00000000 ;
Reg:      r30, Val = 0x0000002c ; Reg:      r31, Val = 0x00000000 ;
Reg:       cr, Val = 0x84000028 ; Reg:      nip, Val = 0x057d9550 ;
Reg:      xer, Val = 0x00000000 ; Reg:       lr, Val = 0x0186eff0 ;
```

```
Reg:      ctr, Val = 0x682f7344 ; Reg:      msr, Val = 0x00784b5c ;
Reg:     trap, Val = 0x0000b030 ; Reg:      dar, Val = 0x77777777 ;
Reg:    dsisr, Val = 0x40000000 ; Reg:   result, Val = 0x00020300 ;

Dump stack (total 1024 bytes, 16 bytes/line):
0xe2be5ea0: 02 be 5e c0 24 00 00 24 00 00 00 00 05 7d 94 84
0xe2be5eb0: 00 00 00 04 00 00 00 00 00 00 00 28 05 8d 34 c4
0xe2be5ec0: 02 be 60 a0 01 86 ef f0 00 00 00 00 00 00 00 00
0xe2be5ed0: 02 04 05 b4 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5ee0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5ef0: 95 47 73 35 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5f00: a0 e1 64 21 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5f10: 00 00 00 00 00 00 00 00 00 00 00 00 01 e9 00 00
0xe2be5f20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5f30: 00 00 00 00 00 00 00 00 02 be 66 c0 02 be 66 d0
0xe2be5f40: 02 be 61 e0 00 00 00 02 00 00 00 00 02 44 b3 a4
0xe2be5f50: 02 be 5f 90 00 00 00 08 02 be 5f e0 00 00 00 08
0xe2be5f60: 02 be 5f 80 00 ac 1b 14 00 00 00 00 00 00 00 00
0xe2be5f70: 05 b4 5f 90 02 be 5f e0 00 00 00 30 02 be 5f e0
0xe2be5f80: 02 be 5f c0 00 ac 1b f4 00 00 00 00 02 45 00 00
0xe2be5f90: 00 03 00 00 00 00 00 00 02 be 5f e0 00 00 00 30
0xe2be5fa0: 02 be 5f c0 00 ac 1b 14 61 f1 2e ae 02 45 00 00
0xe2be5fb0: 02 44 b3 74 02 be 5f d0 00 00 00 30 02 be 5f e0
0xe2be5fc0: 02 be 60 60 01 74 ff f8 00 00 00 00 00 00 08 00
0xe2be5fd0: 02 be 5f f0 00 e8 93 7e 02 be 5f f8 02 be 5f fc
0xe2be5fe0: 00 00 00 00 00 00 00 00 00 00 00 00 02 be 60 18
0xe2be5ff0: 02 be 60 10 00 e9 65 98 00 00 00 58 00 00 2a 4f
0xe2be6000: 02 be 60 10 00 00 00 00 00 00 00 00 02 be 60 68
0xe2be6010: 02 be 60 40 00 e8 c6 a0 00 00 11 17 00 00 00 00
0xe2be6020: 02 be 60 40 00 00 00 00 00 00 00 00 02 be 60 98
0xe2be6030: 02 27 00 00 00 00 00 00 00 00 00 00 02 be 60 68
0xe2be6040: 02 be 60 60 00 00 00 01 00 00 b0 30 02 be 60 98
0xe2be6050: 00 00 00 04 02 21 00 00 00 00 00 00 01 e9 00 00
0xe2be6060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be6070: 00 00 00 00 00 00 00 00 02 be 66 c0 02 be 66 d0
0xe2be6080: 02 be 61 e0 00 00 00 02 00 00 00 00 02 be 61 70
0xe2be6090: 00 00 00 00 02 21 00 00 05 8d 34 c4 05 7d 92 44

Call trace:
Function Address = 0x8012a4b4
Function Address = 0x8017989c
Function Address = 0x80179b30
Function Address = 0x80127438
Function Address = 0x8012d734
Function Address = 0x80100a00
Function Address = 0xe0071004
Function Address = 0x8016ce0c
Function Address = 0x801223a0
```

```
Instruction dump:
41a2fe9c 812300ec 800200ec 7f890000 409efe8c 80010014 540b07b9 40a2fe80
4bfffe6c 80780290 7f64db78 4804ea35 <807f002c> 38800000 38a00080 3863000c
```

For detailed information about the command output, see Table 2.

Related commands

reset kernel starvation

display kernel starvation configuration

Use **display kernel starvation configuration** to display kernel thread starvation detection configuration.

Syntax

display kernel starvation configuration [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays kernel thread starvation detection configuration on the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

This command is supported only on the default context.

Examples

Display kernel thread starvation detection configuration.

```
<Sysname> display kernel starvation configuration
Thread starvation detection: Disabled
Starvation timer (in seconds): 10
Threads excluded from monitoring: 1
  TID:    123   Name: co0
```

Table 5 Command output

Field	Description
Starvation timer (in seconds): *n*	Time interval (in seconds) to identify a kernel thread starvation. A kernel thread starvation occurs if a kernel thread does not run within *n* seconds.
Threads excluded from monitoring	Kernel threads excluded from kernel thread starvation detection.
Name	Kernel thread name.
TID	Kernel thread number.

Related commands

monitor kernel starvation enable

monitor kernel starvation exclude-thread

monitor kernel starvation time

display process

Use **display process** to display process state information.

Syntax

display process [**all** | **job** *job-id* | **name** *process-name*] [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

all: Specifies all processes. With the **all** keyword or without any parameters, the command displays state information for all processes.

job *job-id*: Specifies a process by its job ID, in the range of 1 to 2147483647. Each process has a fixed job ID.

name *process-name*: Specifies a process by its name, a case-insensitive string of 1 to 15 characters that must not contain question marks or spaces.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays process state information on the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Examples

Display state information for the process **scmd**.

```
<Sysname> display process name scmd
                              Job ID: 1
                                 PID: 1
                          Parent JID: 0
                          Parent PID: 0
                     Executable path: /sbin/scmd
                            Instance: 0
                             Respawn: OFF
                       Respawn count: 1
               Max. spawns per minute: 0
                         Last started: Wed Jun  1 14:45:46 2013
                       Process state: sleeping
                           Max. core: 0
                                ARGS: -
```

```
   TID  LAST_CPU    Stack      PRI    State   HH:MM:SS:MSEC  Name
     1      0          0K      120      S     0:0:5:220      scmd
```

Table 6 Command output

Field	Description
Job ID	Job ID of the process. The job ID never changes.
PID	Number of the process. The number identifies the process, and it might change as the process restarts.
Parent JID	Job ID of the parent process.
Parent PID	Number of the parent process.
Executable path	Executable path of the process. For a kernel thread, this field displays a hyphen (-).
Instance	Instance number of the process. Whether a process can run multiple instances depends on the software implementation.
Respawn	Indicates whether the process restarts when an error occurs: • **ON**—The process automatically restarts. • **OFF**—The process does not automatically restarts.
Respawn count	Times that the process has restarted. The starting value is 1.
Max. spawns per minute	Maximum number of times that the process can restart within one minute. If the threshold is reached, the system automatically shuts down the process.
Last started	Time when the most recent restart occurred.
Process state	State of the process: • **running**—Running or waiting in the queue. • **sleeping**—Interruptible sleep. • **traced** or **stopped**—Stopped. • **uninterruptible sleep**—Uninterruptible sleep. • **zombie**—The process has quit, but some resources are not released.
Max. core	Maximum number of core dump files that the process can create. 0 indicates that the process never creates a core dump file. A process creates a core dump file after it abnormally restarts. If the number of core dump files reaches the maximum value, no more core dump files are created. Core dump files are helpful for troubleshooting.
ARGS	Parameters carried by the process during startup. If the process carries no parameters, this field displays a hyphen (-).
TID	Thread ID.
LAST_CPU	Number of the CPU on which the process is last scheduled.
Stack	Stack size.
PRI	Thread priority.
State	Thread state: • **R**—Running. • **S**—Sleeping. • **T**—Traced or stopped. • **D**—Uninterruptible sleep. • **Z**—Zombie.
HH:MM:SS:MSEC	Running time since the most recent start.

Name	Process name.

Display state information for all processes.

```
<Sysname> display process all
    JID    PID %CPU %MEM STAT PRI TTY HH:MM:SS COMMAND
      1      1  0.0  0.0   S  120  -  00:00:04 scmd
      2      2  0.0  0.0   S  115  -  00:00:00 [kthreadd]
      3      3  0.0  0.0   S   99  -  00:00:00 [migration/0]
      4      4  0.0  0.0   S  115  -  00:00:05 [ksoftirqd/0]
      5      5  0.0  0.0   S   99  -  00:00:00 [watchdog/0]
      6      6  0.0  0.0   S  115  -  00:00:00 [events/0]
      7      7  0.0  0.0   S  115  -  00:00:00 [khelper]
      8      8  0.0  0.0   S  115  -  00:00:00 [kblockd/0]
      9      9  0.0  0.0   S  115  -  00:00:00 [ata/0]
     10     10  0.0  0.0   S  115  -  00:00:00 [ata_aux]
     11     11  0.0  0.0   S  115  -  00:00:00 [kseriod]
     12     12  0.0  0.0   S  120  -  00:00:00 [vzmond]
     13     13  0.0  0.0   S  120  -  00:00:00 [pdflush]
     14     14  0.0  0.0   S  120  -  00:00:00 [pdflush]
     15     15  0.0  0.0   S  115  -  00:00:00 [kswapd0]
     16     16  0.0  0.0   S  115  -  00:00:00 [aio/0]
     17     17  0.0  0.0   S  115  -  00:00:00 [scsi_eh_0]
     18     18  0.0  0.0   S  115  -  00:00:00 [scsi_eh_1]
     19     19  0.0  0.0   S  115  -  00:00:00 [scsi_eh_2]
     35     35  0.0  0.0   D  100  -  00:00:00 [lipc_topology]
---- More ----
```

Table 7 Command output

Field	Description
JID	Job ID of a process. It never changes.
PID	Number of a process.
%CPU	CPU usage in percentage (%).
%MEM	Memory usage in percentage (%).
STAT	State of a process: • **R**—Running. • **S**—Sleeping. • **T**—Traced or stopped. • **D**—Uninterruptible sleep. • **Z**—Zombie.
PRI	Priority of a process for scheduling.
TTY	TTY used by a process. It displays a hyphen (-) for non-default contexts.
HH:MM:SS	Running time since the most recent start. If the running time reaches or exceeds 100 hours, this field displays only the number of hours.
COMMAND	Name and parameters of a process. If square brackets ([ ]) exist in a process name, the process is a kernel thread.

display process cpu

Use **display process cpu** to display CPU usage of all processes.

Syntax

display process cpu [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays CPU usage of all processes on the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Examples

Display CPU usage for all processes.

```
<Sysname> display process cpu
CPU utilization in 5 secs: 16.8%; 1 min: 4.7%; 5 mins: 4.7%
    JID      5Sec      1Min      5Min    Name
      1      0.0%      0.0%      0.0%    scmd
      2      0.0%      0.0%      0.0%    [kthreadd]
      3      0.1%      0.0%      0.0%    [ksoftirqd/0]
```

...

Table 8 Command output

Field	Description
CPU utilization in 5 secs: 16.8%; 1 min: 4.7%; 5 mins: 4.7%	System CPU usage within the last 5 seconds, 1 minute, and 5 minutes.
JID	Job ID of a process. It never changes.
5Sec	CPU usage of the process within the last 5 seconds.
1Min	CPU usage of the process within the last minute.
5Min	CPU usage of the process within the last 5 minutes.
Name	Name of the process. If square brackets ([ ]) exist in a process name, the process is a kernel thread.

display process log

Use **display process log** to display log information for all user processes.

Syntax

display process log [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays log information for all user processes on the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Examples

Display log information for all user processes.

```
<Sysname> display process log
Process       JobID  PID    Abort Core Exit Kill StartTime      EndTime
knotify       92     92     N     N    0    36   12-17 07:10:27 12-17 07:10:27
knotify       93     93     N     N    0    --   12-17 07:10:27 12-17 07:10:27
automount     94     94     N     N    0    --   12-17 07:10:27 12-17 07:10:28
knotify       111    111    N     N    0    --   12-17 07:10:28 12-17 07:10:28
comsh         121    121    N     N    0    --   12-17 07:10:30 12-17 07:10:30
knotify       152    152    N     N    0    --   12-17 07:10:31 12-17 07:10:31
autocfgd      155    155    N     N    0    --   12-17 07:10:31 12-17 07:10:31
pkg_update    122    122    N     N    0    --   12-17 07:10:30 12-17 07:10:31
```

Table 9 Command output

Field	Description
Process	Name of a user process.
JobID	Job ID of a user process.
PID	ID of a user process.
Abort	Indicates whether the process exited abnormally: • **Y**—Yes. • **N**—No.
Core	Indicates whether the process can generate core dump files: • **Y**—Yes. • **N**—No.
Exit	Process exit code. This field displays two hyphens (--) if the process was killed by a signal.
Kill	Code of the signal that killed the process. This field displays two hyphens (--) if the process exited instead of being killed.
StartTime	Time when the user process started.
EndTime	Time when the user process ended.

display process memory

Use **display process memory** to display memory usage of all user processes.

Syntax

display process memory [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays memory usage of all user processes on the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

When a user process starts, it requests the following types of memory from the system:

- **Text memory**—Stores code for the user process.
- **Data memory**—Stores data for the user process.
- **Stack memory**—Stores temporary data.
- **Dynamic memory**—Heap memory dynamically assigned and released by the system according to the needs of the user process. To view dynamic memory information, execute the **display process memory heap** command.

Examples

Display memory usage for all user processes.

```
<Sysname> display process memory
   JID       Text      Data      Stack    Dynamic    Name
     1        384      1800         16         36    scmd
     2          0         0          0          0    [kthreadd]
     3          0         0          0          0    [ksoftirqd/0]
     4          0         0          0          0    [watchdog/0]
     5          0         0          0          0    [events/0]
     6          0         0          0          0    [khelper]
    29          0         0          0          0    [kblockd/0]
    49          0         0          0          0    [vzmond]
    52          0         0          0          0    [pdflush]
---- More ----
```

Table 10 Command output

Field	Description
JID	Job ID of a process. It never changes.
Text	Text memory used by the user process, in KB. The value for a kernel thread is 0.

Field	Description
Data	Data memory used by the user process, in KB. The value for a kernel thread is 0.
Stack	Stack memory used by the user process, in KB. The value for a kernel thread is 0.
Dynamic	Dynamic memory used by the user process, in KB. The value for a kernel thread is 0.
Name	Name of the user process. If square brackets ([ ]) exist in a process name, the process is a kernel thread.

Related commands

display process memory heap

display process memory heap address

display process memory heap size

display process memory heap

Use **display process memory heap** to display the heap memory usage of a user process.

Syntax

display process memory heap job *job-id* [**verbose**] [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

job *job-id*: Specifies a user process by its job ID, in the range of 1 to 2147483647.

verbose: Displays detailed information. If you do not specify this keyword, the command displays brief information.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the heap memory usage of the user process on the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

Heap memory comprises fixed-sized blocks such as 16-byte or 64-byte blocks. It stores data and variables used by the user process. When a user process starts, the system dynamically allocates heap memory to the process.

Each memory block has an address represented in hexadecimal format, which can be used to access the memory block. You can view memory block addresses by using the **display process memory heap size** command, and view memory block contents by using the **display process memory heap address** command.

Examples

Display brief information about heap memory usage for the process identified by job ID 1.

```
<Sysname> display process memory heap job 1
Total virtual memory heap space(in bytes) :  2228224
Total physical memory heap space(in bytes) :  262144
Total allocated memory(in bytes)          :  161576
```

Display detailed information about heap memory usage for the process identified by job ID 1.

```
<Sysname> display process memory heap job 1 verbose
Heap usage:
Size       Free      Used     Total     Free Ratio
16         8         52       60        13%
64         3         1262     1265      0.2%
128        2         207      209       1%
512        3         55       58        5.1%
4096       3         297      300       1%
8192       1         19       20        5%
81920      0         1        1         0%
Summary:
Total virtual memory heap space (in bytes)  :  2293760
Total physical memory heap space (in bytes) :  58368
Total allocated memory (in bytes)           :  42368
```

Table 11 Command output

Field	Description
Size	Size of each memory block, in bytes.
Free	Number of free memory blocks.
Used	Number of used memory blocks.
Total	Total number of memory blocks.
Free Ratio	Ratio of free memory to total memory. It helps identify fragment information.

Related commands

display process memory

display process memory heap address

display process memory heap size

display process memory heap address

Use **display process memory heap address** to display heap memory content starting from a specified memory block for a process.

Syntax

display process memory heap job *job-id* **address** *starting-address* **length** *memory-length* [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

job *job-id*: Specifies a user process by its job ID, in the range of 1 to 2147483647.

address *starting-address*: Specifies the starting memory block by its address.

length *memory-length*: Specifies the memory block length in the range of 1 to 1024 bytes.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays heap memory content information on the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

When a user process runs abnormally, the command helps locate the problem.

Examples

Display 128-byte memory block content starting from the memory block 0xb7e30580 for the process **job 1**.

```
<Sysname> display process memory heap job 1 address b7e30580 length 128
B7E30580:  14 00 EF FF 00 00 00 00 E4 39 E2 B7 7C 05 E3 B7  .........9..|...
B7E30590:  14 00 EF FF 2F 73 62 69 6E 2F 73 6C 62 67 64 00  ..../sbin/slbgd.
B7E305A0:  14 00 EF FF 00 00 00 00 44 3B E2 B7 8C 05 E3 B7  ........D;......
B7E305B0:  14 00 EF FF 2F 73 62 69 6E 2F 6F 73 70 66 64 00  ..../sbin/ospfd.
B7E305C0:  14 00 EF FF 00 00 00 00 A4 3C E2 B7 AC 05 E3 B7  .........<......
B7E305D0:  14 00 EF FF 2F 73 62 69 6E 2F 6D 73 74 70 64 00  ..../sbin/mstpd.
B7E305E0:  14 00 EF FF 00 00 00 00 04 3E E2 B7 CC 05 E3 B7  .........>......
B7E305F0:  14 00 EF FF 2F 73 62 69 6E 2F 6E 74 70 64 00 00  ..../sbin/ntpd..
```

Related commands

display process memory heap

display process memory heap size

display process memory heap size

Use **display process memory heap size** to display the addresses of heap memory blocks with a specified size used by a process.

Syntax

display process memory heap job *job-id* **size** *memory-size* [**offset** *offset-size*] [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

job *job-id*: Specifies a process by its job ID, in the range of 1 to 2147483647.

size *memory-size*: Specifies the memory block size in the range of 1 to 4294967295.

offset *offset-size*: Specifies an offset in the range of 0 to 4294967295. The default value is 128. For example, suppose the system allocates 100 16-byte memory blocks to process job 1, and the process has used 66 blocks. Then if you execute the **display process memory heap job** *1* **size** *16* **offset** *50* command, the output shows the addresses of the 51st through 66th 16-byte blocks used by the process.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays heap memory block address information on the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

The command displays memory block addresses in hexadecimal format. To view memory block content, execute the **display process memory heap address** command.

Examples

Display the addresses of 16-byte memory blocks used by process job 1.

```
<Sysname> display process memory heap job 1 size 16
0xb7e300c0  0xb7e300d0  0xb7e300e0  0xb7e300f0
0xb7e30100  0xb7e30110  0xb7e30120  0xb7e30130
0xb7e30140  0xb7e30150  0xb7e30160  0xb7e30170
0xb7e30180  0xb7e30190  0xb7e301a0  0xb7e301b0
0xb7e301c0  0xb7e301d0  0xb7e301e0  0xb7e301f0
0xb7e30200  0xb7e30210  0xb7e30220  0xb7e30230
```

Display the addresses of 16-byte memory blocks starting from the fifth block used by process job 1.

```
<Sysname> display process memory heap job 1 size 16 offset 4
0xb7e30100  0xb7e30110  0xb7e30120  0xb7e30130
0xb7e30140  0xb7e30150  0xb7e30160  0xb7e30170
0xb7e30180  0xb7e30190  0xb7e301a0  0xb7e301b0
0xb7e301c0  0xb7e301d0  0xb7e301e0  0xb7e301f0
0xb7e30200  0xb7e30210  0xb7e30220  0xb7e30230
```

Related commands

display process memory heap

display process memory heap address

exception filepath

Use **exception filepath** to specify the directory for saving core dump files.

Use **undo exception filepath** to remove the specified directory.

Syntax

exception filepath *directory*

undo exception filepath *directory*

Default

The directory for saving core dump files is the root directory of the default file system. For more information about the default file system, see file system management in *Fundamentals Configuration Guide*.

Views

User view

Predefined user roles

network-admin

Parameters

directory: Specifies the directory for saving core dump files. The directory must be the root directory of a file system.

Usage guidelines

This command is supported only on the default context.

The system will save core dump files to the **core** folder in the specified directory on the master. If the **core** folder does not exist in the specified directory, the system creates the **core** folder before saving core dump files.

You can use the command to change the directory if there are different types of storage media on the device.

If no directory is specified or the specified directory is not accessible, the system cannot save core dump files.

Examples

Set the directory for saving core dump files.

```
<Sysname> exception filepath flash:/
```

Related commands

display exception filepath

process core

monitor kernel deadloop action threshold

Use **monitor kernel deadloop action threshold** to set kernel thread deadloop protection thresholds.

Use **undo monitor kernel deadloop action threshold** to restore default settings.

Syntax

monitor kernel deadloop action threshold *threshold* [**slot** *slot-number* [**cpu** *cpu-number*]]

undo monitor kernel deadloop action threshold [**slot** *slot-number* [**cpu** *cpu-number*]]

Default

The kernel thread deadloop protection threshold is 1. The device takes protection actions immediately after detecting a kernel thread deadloop.

Views

System view

Predefined user roles

network-admin

Parameters

threshold: Specifies the number of kernel thread deadloops for triggering protection actions, in the range of 1 to 20.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command applies to the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

This command is supported only on the default context.

When the number of detected kernel thread deadloops reaches the kernel thread deadloop protection threshold, the device takes protection actions to remove the deadloops.

Examples

Set the kernel thread deadloop protection threshold to 5.

```
<Sysname> system-view
[Sysname] monitor kernel deadloop action threshold 5
```

Related commands

display kernel deadloop configuration

monitor kernel deadloop enable

monitor kernel deadloop enable

Use **monitor kernel deadloop enable** to enable kernel thread deadloop detection.

Use **undo monitor kernel deadloop enable** to disable kernel thread deadloop detection.

Syntax

monitor kernel deadloop enable [**slot** *slot-number* [**cpu** *cpu-number* [**core** *core-number*&<1-64>]]]

undo monitor kernel deadloop enable [**slot** *slot-number* [**cpu** *cpu-number*]]

Default

Kernel thread deadloop detection is enabled.

Views

System view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command applies to the master device.

cpu *cpu-number*: Specifies a CPU by its number.

core *core-number*&<1-64>: Specifies a maximum of 64 cores by their numbers. If you do not specify this option, all cores on the CPU are specified.

Usage guidelines

CAUTION:

Use this command only under the guidance of NSFOCUS Support. Inappropriate configuration can cause system breakdown. As a best practice, leave the default unchanged.

This command is supported only on the default context.

Kernel threads share resources in kernel space. If a kernel thread monopolizes the CPU for a long time, other threads cannot run, resulting in a deadloop.

This command enables the device to detect deadloops. If a thread occupies the CPU regularly, the device determines that a deadloop has occurred, logs the event, and reboots to resolve the issue.

Examples

Enable kernel thread deadloop detection.

```
<Sysname> system-view
[Sysname] monitor kernel deadloop enable
```

Related commands

display kernel deadloop

display kernel deadloop configuration

monitor kernel deadloop exclude-thread

monitor kernel deadloop time

monitor kernel deadloop exclude-thread

Use **monitor kernel deadloop exclude-thread** to exclude a kernel thread from kernel thread deadloop detection.

Use **undo monitor kernel deadloop exclude-thread** to include a kernel thread in kernel thread deadloop detection.

Syntax

monitor kernel deadloop exclude-thread *tid* [**slot** *slot-number* [**cpu** *cpu-number*]]

undo monitor kernel deadloop exclude-thread [*tid*] [**slot** *slot-number* [**cpu** *cpu-number*]]

Default

Kernel thread deadloop detection monitors all kernel threads.

Views

System view

Predefined user roles

network-admin

Parameters

tid: Specifies a kernel thread by its ID, in the range of 1 to 2147483647. If you do not specify a kernel thread, the **undo** command restores the default.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command applies to the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

This command is supported only on the default context.

Use this command only under the guidance of NSFOCUS Support. Inappropriate configuration can cause system breakdown. As a best practice, leave the default unchanged.

You can exclude up to 128 kernel threads from kernel thread deadloop detection.

Examples

Exclude kernel thread 15 from kernel thread deadloop detection.

```
<Sysname> system-view
[Sysname]monitor kernel deadloop exclude-thread 15
```

Related commands

display kernel deadloop configuration

display kernel deadloop

monitor kernel deadloop enable

monitor kernel deadloop time

Use **monitor kernel deadloop time** to set the interval for identifying a kernel thread deadloop.

Use **undo monitor kernel deadloop time** to restore the default.

Syntax

monitor kernel deadloop time *time* [**slot** *slot-number* [**cpu** *cpu-number*]]

undo monitor kernel deadloop time [**slot** *slot-number* [**cpu** *cpu-number*]]

Default

The interval for identifying a kernel thread deadloop is 28 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

time *time*: Specifies the interval for identifying a kernel thread deadloop, in the range of 1 to 65535 seconds.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command applies to the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

This command is supported only on the default context.

Use this command only under the guidance of NSFOCUS Support. Inappropriate configuration can cause system breakdown. As a best practice, leave the default unchanged.

If a kernel thread runs for the specified interval, kernel thread deadloop detection determines that a deadloop has occurred.

Examples

Set the interval for identifying a kernel thread deadloop to 8 seconds.

```
<Sysname> system-view
[Sysname] monitor kernel deadloop time 8
```

Related commands

display kernel deadloop configuration

display kernel deadloop

monitor kernel deadloop enable

monitor kernel starvation enable

Use **monitor kernel starvation enable** to enable kernel thread starvation detection.

Use **undo monitor kernel starvation enable** to disable kernel thread starvation detection.

Syntax

monitor kernel starvation enable [**slot** *slot-number* [**cpu** *cpu-number*]]

undo monitor kernel starvation enable [**slot** *slot-number* [**cpu** *cpu-number*]]

Default

Kernel thread starvation detection is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command applies to the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

CAUTION:

Use this command only under the guidance of NSFOCUS Support. Inappropriate configuration can cause system breakdown. As a best practice, leave the default unchanged.

This command is supported only on the default context.

Starvation occurs when a thread is unable to access shared resources.

The command enables the system to detect and report thread starvation. If a thread is not executed within an interval, the system considers that a starvation has occurred, and outputs a starvation message.

Thread starvation does not impact system operation. A starved thread can automatically run when certain conditions are met.

Examples

Enable kernel thread starvation detection.

```
<Sysname> system-view
```

```
[Sysname] monitor kernel starvation enable
```

Related commands

display kernel starvation configuration

display kernel starvation

monitor kernel starvation time

monitor kernel starvation exclude-thread

monitor kernel starvation exclude-thread

Use **monitor kernel starvation exclude-thread** to exclude a kernel thread from kernel thread starvation detection.

Use **undo monitor kernel starvation exclude-thread** to include a kernel thread in kernel thread starvation detection.

Syntax

monitor kernel starvation exclude-thread *tid* [**slot** *slot-number* [**cpu** *cpu-number*]]

undo monitor kernel starvation exclude-thread [*tid*] [**slot** *slot-number* [**cpu** *cpu-number*]]

Default

Kernel thread starvation detection, if enabled, monitors all kernel threads.

Views

System view

Predefined user roles

network-admin

Parameters

tid: Specifies a kernel thread by its ID, in the range of 1 to 2147483647. If you do not specify a kernel thread, the **undo** command restores the default.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command applies to the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

This command is supported only on the default context.

Use this command only under the guidance of NSFOCUS Support. Inappropriate configuration can cause system breakdown. As a best practice, leave the default unchanged.

You can exclude up to 128 kernel threads from kernel thread starvation detection.

Examples

Exclude kernel thread 15 from kernel thread starvation detection.

```
<Sysname> system-view
[Sysname] monitor kernel starvation exclude-thread 15
```

Related commands

display kernel starvation

display kernel starvation configuration

monitor kernel starvation enable

monitor kernel starvation time

Use **monitor kernel starvation time** to set the interval for identifying a kernel thread starvation.

Use **undo monitor kernel starvation time** to restore the default.

Syntax

monitor kernel starvation time *time* [**slot** *slot-number* [**cpu** *cpu-number*]]

undo monitor kernel starvation time [**slot** *slot-number* [**cpu** *cpu-number*]]

Default

The interval for identifying a kernel thread starvation is 120 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

time *time*: Specifies the interval for identifying a kernel thread starvation, in the range of 1 to 65535 seconds.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command applies to the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

This command is supported only on the default context.

Use this command only under the guidance of NSFOCUS Support. Inappropriate configuration can cause system breakdown. As a best practice, leave the default unchanged.

If a thread is not executed within the specified interval, the system considers that a starvation has occurred, and outputs a starvation message.

Examples

Set the interval for identifying a kernel thread starvation to 120 seconds.

```
<Sysname> system-view
[Sysname] monitor kernel starvation time 120
```

Related commands

display kernel starvation

display kernel starvation configuration

monitor kernel starvation enable

monitor process

Use **monitor process** to display process statistics.

Syntax

monitor process [**dumbtty**] [**iteration** *number*] [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

context-admin

Parameters

dumbtty: Specifies dumbtty mode. In this mode, the command displays process statistics in descending order of CPU usage without refreshing statistics. If you do not specify this keyword, the command displays statistics for the top 10 processes in descending order of CPU usage in an interactive mode, and refreshes statistics every 5 seconds by default.

iteration *number*: Specifies the number of display times, in the range of 1 to 4294967295. If you specify the **dumbtty** keyword, the *number* argument is 1 by default. If neither the **dumbtty** keyword nor the *number* argument is specified, there is no limit to the display times and process statistics are refreshed every 5 seconds.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays process statistics for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

If you do not specify the **dumbtty** keyword, the command displays process statistics in an interactive mode. In this mode, the system automatically determines the number of displayed processes according to the screen size, and does not display exceeding processes. You can also input interactive commands as shown in Table 12 to perform relevant operations.

Table 12 Interactive commands

Commands	Description
? or h	Displays help information that includes available interactive commands.
1	Displays state information for physical CPUs. For example, if you enter 1 for the first time, the state of each physical CPU is displayed in a separate row. If you enter 1 again, the average value of all CPU states is displayed. If you enter 1 for the third time, separate states are displayed. By default, the average value of all CPU states is displayed.
c	Sorts processes by CPU usage in descending order, which is the default setting.
d	Sets the interval for refreshing process statistics, in the range of 1 to 2147483647 seconds. The default value is 5 seconds.
f	Sorts processes by the number of open files in descending order. Files are identified by file descriptors (FDs).
k	Kills a process. Because the command can impact system operation, be cautious to use it.
l	Refreshes the screen.
m	Sorts processes by memory usage in descending order.
n	Changes the maximum number of processes displayed within a screen, in the range of 0 to 2147483647. The default value is 10. A value of 0 means no limit. Only processes not exceeding the screen size can be displayed.

Commands	Description
q	Quits the interactive mode.
t	Sorts processes by running time in descending order.
<	Moves sort field to the next left column.
>	Moves sort field to the next right column.

Examples

Display process statistics in dumbtty mode. In this mode, the system displays process statistics once, and then returns to command view.

```
<Sysname> monitor process dumbtty
428 processes; 561 threads; 2336 fds
Thread states: 18 running, 543 sleeping, 0 stopped, 0 zombie
CPU0: 89.53% idle, 0.00% user, 7.14% kernel, 3.33% interrupt, 0.00% steal
CPU1: 94.81% idle, 0.47% user, 2.36% kernel, 2.36% interrupt, 0.00% steal
Memory: 31775M total, 26159M available, page size 4K
        JID        PID  PRI  State  FDs     MEM  HH:MM:SS    CPU   Name
        404        404  120    S    16   16432K  03:22:57   0.68%  diagd
          1          1  120    S    18   11136K  00:08:21   0.27%  scmd
        348        348  115    R     0       0K  05:54:40   0.15%  [kdrvfwd20]
        349        349  115    R     0       0K  05:57:55   0.14%  [kdrvfwd21]
        350        350  115    R     0       0K  05:52:45   0.14%  [kdrvfwd22]
        352        352  115    R     0       0K  05:47:38   0.14%  [kdrvfwd24]
        354        354  115    R     0       0K  05:38:52   0.14%  [kdrvfwd26]
        344        344  115    R     0       0K  05:41:15   0.13%  [kdrvfwd16]
        345        345  115    R     0       0K  05:34:40   0.13%  [kdrvfwd17]
        346        346  115    R     0       0K  05:33:35   0.13%  [kdrvfwd18]
        347        347  115    R     0       0K  05:22:29   0.13%  [kdrvfwd19]
        351        351  115    R     0       0K  05:39:24   0.13%  [kdrvfwd23]
        353        353  115    R     0       0K  05:29:42   0.13%  [kdrvfwd25]
        355        355  115    R     0       0K  05:26:17   0.13%  [kdrvfwd27]
        356        356  115    R     0       0K  05:28:52   0.13%  [kdrvfwd28]
        357        357  115    R     0       0K  05:26:31   0.13%  [kdrvfwd29]
...
```

Display process statistics twice in dumbtty mode.

```
<Sysname> monitor process dumbtty iteration 2
428 processes; 561 threads; 2336 fds
Thread states: 18 running, 543 sleeping, 0 stopped, 0 zombie
CPU0: 89.53% idle, 0.00% user, 7.14% kernel, 3.33% interrupt, 0.00% steal
CPU1: 94.81% idle, 0.47% user, 2.36% kernel, 2.36% interrupt, 0.00% steal
Memory: 31775M total, 26159M available, page size 4K
        JID        PID  PRI  State  FDs     MEM  HH:MM:SS    CPU   Name
        404        404  120    S    16   16432K  03:22:57   0.68%  diagd
          1          1  120    S    18   11136K  00:08:21   0.27%  scmd
        348        348  115    R     0       0K  05:54:40   0.15%  [kdrvfwd20]
        349        349  115    R     0       0K  05:57:55   0.14%  [kdrvfwd21]
        350        350  115    R     0       0K  05:52:45   0.14%  [kdrvfwd22]
        352        352  115    R     0       0K  05:47:38   0.14%  [kdrvfwd24]
```

```
        354        354  115    R     0       0K  05:38:52   0.14%  [kdrvfwd26]
        344        344  115    R     0       0K  05:41:15   0.13%  [kdrvfwd16]
        345        345  115    R     0       0K  05:34:40   0.13%  [kdrvfwd17]
        346        346  115    R     0       0K  05:33:35   0.13%  [kdrvfwd18]
        347        347  115    R     0       0K  05:22:29   0.13%  [kdrvfwd19]
        351        351  115    R     0       0K  05:39:24   0.13%  [kdrvfwd23]
        353        353  115    R     0       0K  05:29:42   0.13%  [kdrvfwd25]
        355        355  115    R     0       0K  05:26:17   0.13%  [kdrvfwd27]
        356        356  115    R     0       0K  05:28:52   0.13%  [kdrvfwd28]
        357        357  115    R     0       0K  05:26:31   0.13%  [kdrvfwd29]
...
```

Five seconds later, the system refreshes process statistics as follows (which is the same as executing the **`monitor process dumbtty`** command twice at a 5-second interval):

```
428 processes; 561 threads; 2338 fds
Thread states: 19 running, 542 sleeping, 0 stopped, 0 zombie
CPU0: 86.26% idle, 1.05% user, 8.99% kernel, 3.70% interrupt, 0.00% steal
CPU1: 90.44% idle, 1.06% user, 4.78% kernel, 3.72% interrupt, 0.00% steal
Memory: 31775M total, 26158M available, page size 4K
        JID        PID  PRI  State  FDs     MEM  HH:MM:SS    CPU   Name
        404        404  120    R    18   16460K  03:23:03   0.50%  diagd
          1          1  120    S    18   11136K  00:08:21   0.24%  scmd
        344        344  115    R     0       0K  05:41:25   0.13%  [kdrvfwd16]
        348        348  115    R     0       0K  05:54:51   0.13%  [kdrvfwd20]
        349        349  115    R     0       0K  05:58:06   0.13%  [kdrvfwd21]
        350        350  115    R     0       0K  05:52:56   0.13%  [kdrvfwd22]
        352        352  115    R     0       0K  05:47:49   0.13%  [kdrvfwd24]
        345        345  115    R     0       0K  05:34:51   0.12%  [kdrvfwd17]
        346        346  115    R     0       0K  05:33:45   0.12%  [kdrvfwd18]
        347        347  115    R     0       0K  05:22:39   0.12%  [kdrvfwd19]
        351        351  115    R     0       0K  05:39:34   0.12%  [kdrvfwd23]
        353        353  115    R     0       0K  05:29:52   0.12%  [kdrvfwd25]
        354        354  115    R     0       0K  05:39:02   0.12%  [kdrvfwd26]
        356        356  115    R     0       0K  05:29:02   0.12%  [kdrvfwd28]
        357        357  115    R     0       0K  05:26:41   0.12%  [kdrvfwd29]
...
<Sysname>
```

Display process statistics in interactive mode.

```
<Sysname> monitor process
428 processes; 561 threads; 2336 fds
Thread states: 20 running, 541 sleeping, 0 stopped, 0 zombie
CPU: 98.21% idle, 0.17% user, 1.57% kernel, 0.05% interrupt, 0.00% steal
Memory: 31775M total, 26158M available, page size 4K
        JID        PID  PRI  State  FDs     MEM  HH:MM:SS    CPU   Name
        348        348  115    R     0       0K  05:55:08   0.09%  [kdrvfwd20]
        349        349  115    R     0       0K  05:58:22   0.09%  [kdrvfwd21]
        350        350  115    R     0       0K  05:53:12   0.09%  [kdrvfwd22]
        352        352  115    R     0       0K  05:48:05   0.09%  [kdrvfwd24]
        344        344  115    R     0       0K  05:41:41   0.09%  [kdrvfwd16]
```

```
351        351  115    R     0       0K  05:39:50   0.09%  [kdrvfwd23]
404        404  120    S    16   16468K  03:23:12   0.09%  diagd
353        353  115    R     0       0K  05:30:07   0.09%  [kdrvfwd25]
354        354  115    R     0       0K  05:39:18   0.09%  [kdrvfwd26]
345        345  115    R     0       0K  05:35:07   0.08%  [kdrvfwd17]
```

The system refreshes process statistics every 5 seconds. You can enter interactive commands to perform operation as follows:

- Enter **h** or a question mark (?) to display help information as follows:

```
Help for interactive commands:
      ?,h    Show the available interactive commands
        1    Toggle SMP view: '1' single/separate states
        c    Sort by the CPU field(default)
        d    Set the delay interval between screen updates
        f    Sort by number of open files
        k    Kill a job
        l    Refresh the screen
        m    Sort by memory used
        n    Set the maximum number of processes to display
        q    Quit the interactive display
        t    Sort by run time of processes since last restart
        <    Move sort field to the next left column
        >    Move sort field to the next right column
Press any key to continue
```

- Enter **d**, and then enter a number to modify the refresh interval. If you enter **3**, statistics are refreshed every 3 seconds.

```
Enter the delay interval between updates(1~2147483647): 3
```

- Enter **n**, and then enter a number to modify the maximum number of displayed processes. If you enter **5**, statistics for five processes are displayed.

```
Enter the max number of processes to display(0 means unlimited): 5
428 processes; 561 threads; 2336 fds
Thread states: 18 running, 543 sleeping, 0 stopped, 0 zombie
CPU: 97.24% idle, 0.28% user, 2.41% kernel, 0.07% interrupt, 0.00% steal
Memory: 31775M total, 26158M available, page size 4K
        JID        PID  PRI  State  FDs     MEM  HH:MM:SS    CPU   Name
        349        349  115    R     0       0K  05:59:31   0.14%  [kdrvfwd21]
        348        348  115    R     0       0K  05:56:16   0.14%  [kdrvfwd20]
        350        350  115    R     0       0K  05:54:20   0.14%  [kdrvfwd22]
        352        352  115    R     0       0K  05:49:12   0.14%  [kdrvfwd24]
        404        404  120    S    16   16480K  03:24:25   0.14%  diagd
```

- Enter **f** to sort processes by FDs in descending order. (You can also enter command **c**, **m**, or **t** to sort processes.)

```
428 processes; 561 threads; 2336 fds
Thread states: 18 running, 543 sleeping, 0 stopped, 0 zombie
CPU: 97.39% idle, 0.19% user, 2.04% kernel, 0.38% interrupt, 0.00% steal
Memory: 31775M total, 26158M available, page size 4K
        JID        PID  PRI  State  FDs     MEM  HH:MM:SS    CPU   Name
        526        526  120    S   360   64180K  00:25:14   0.01%  stamgrd
        426        426  120    S   329  167272K  04:50:26   0.11%  apmgrd
```

```
        398         398  100    S   181   52472K  00:00:59   0.00%  dbmd
        424         424  120    S   123  298916K  00:08:37   0.00%  ofcd
        601         601  125    S    87   25108K  00:00:12   0.00%  ipstackd
        620         620  120    S    84   54176K  00:01:42   0.00%  portald
        430         430  120    S    64   18340K  00:00:21   0.00%  aaad
        406         406  105    S    55    2192K  00:00:00   0.00%  had
        436         436  120    S    47   29212K  00:00:06   0.00%  aclmgrd
        600         600  125    S    41   30320K  00:01:54   0.00%  dhcpd
```

- Enter **k** and then enter a JID to kill a process. If you enter **406**, the process with the JID of 406 is killed.

```
Enter the JID to kill: 406
427 processes; 560 threads; 2280 fds
Thread states: 18 running, 542 sleeping, 0 stopped, 0 zombie
CPU: 97.11% idle, 0.34% user, 2.46% kernel, 0.09% interrupt, 0.00% steal
Memory: 31775M total, 26158M available, page size 4K
        JID         PID  PRI  State  FDs     MEM  HH:MM:SS    CPU   Name
        526         526  120    S   360   64180K  00:25:14   0.03%  stamgrd
        426         426  120    S   329  167272K  04:50:31   0.13%  apmgrd
        398         398  100    S   180   52472K  00:00:59   0.00%  dbmd
        424         424  120    S   123  298916K  00:08:37   0.00%  ofcd
        601         601  125    S    87   25108K  00:00:12   0.00%  ipstackd
        620         620  120    S    84   54176K  00:01:42   0.00%  portald
        430         430  120    S    64   18340K  00:00:21   0.00%  aaad
        436         436  120    S    47   29212K  00:00:06   0.00%  aclmgrd
        600         600  125    S    41   30320K  00:01:54   0.00%  dhcpd
        505         505  120    S    40   28196K  00:00:00   0.00%  qosd
```

- Enter **q** to quit interactive mode.

Table 13 Command output

Field	Description
84 processes; 107 threads; 683 fds	Numbers of processes, threads, and open files.
JID	Job ID of a process, which never changes.
PID	ID of a process.
PRI	Priority level of a process.
State	State of a process: • **R**—Running. • **S**—Sleeping. • **T**—Traced or stopped. • **D**—Uninterruptible sleep. • **Z**—Zombie.
FDs	Number of open files for a process.
MEM	Memory usage. It displays **0** for a kernel thread.
HH:MM:SS	Running time of a process since last restart.
CPU	CPU usage of a process.
Name	Name of a process. If square brackets ([ ]) exist in a process name, the process

	is a kernel thread.

monitor thread

Use **monitor thread** to display thread statistics.

Syntax

monitor thread [**dumbtty**] [**iteration** *number*] [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

context-admin

Parameters

dumbtty: Specifies dumbtty mode. In this mode, the command displays all thread statistics in descending order of CPU usage without refreshing statistics. If you do not specify the keyword, the command displays statistics for top 10 processes in descending order of CPU usage in an interactive mode, and refreshes statistics every 5 seconds by default.

iteration *number*: Specifies the number of display times, in the range of 1 to 4294967295. If you specify the **dumbtty** keyword, the *number* argument is 1 by default. If neither the **dumbtty** keyword nor the *number* argument is specified, there is no limit to the display times.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays thread statistics for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

If you do not specify the **dumbtty** keyword, the command displays thread statistics in an interactive mode. In this mode, the system automatically determines the number of displayed thread processes according to the screen size and does not display exceeding processes. You can also input interactive commands as shown in Table 14 to perform relevant operations.

Table 14 Interactive commands

Commands	Description
? or h	Displays help information that includes available interactive commands.
1	Displays one of the following items in turn when you press **1** again and again: • Values of parameters of physical CPUs. • Average values of parameters of all CPUs. By default, the command displays the average values of parameters of all CPUs.
c	Sorts statistics by CPU usage in descending order. By default, the command sorts statistics by CPU usage in descending order.
d	Sets the interval for refreshing statistics. The default interval is 5 seconds.
k	Kills a process. Because the command can impact system operation, be cautious when you use it.
l	Refreshes the screen.
n	Changes the maximum number of threads displayed within a screen, in the range of 0

	to 2147483647. The default value is 10. A value of 0 means no limit. Only threads not exceeding the screen size can be displayed.
q	Quits interactive mode.
t	Sorts statistics by the running time since the latest startup.
<	Moves sort field to the next left column.
>	Moves sort field to the next right column.

Examples

Display thread statistics in dumbtty mode.

```
<Sysname> monitor thread dumbtty
84 processes; 107 threads
Thread states: 1 running, 106 sleeping, 0 stopped, 0 zombie
CPU states: 83.19% idle, 1.68% user, 10.08% kernel, 5.04% interrupt
Memory: 755M total, 417M available, page size 4K
    JID    TID  LAST_CPU  PRI  State  HH:MM:SS   MAX    CPU    Name
   1175   1175      0     120    R    00:00:00     1  10.75%   top
      1      1      0     120    S    00:00:06     1   2.68%   scmd
    881    881      0     120    S    00:00:09     1   2.01%   diagd
    776    776      0     120    S    00:00:01     0   0.67%   [DEVD]
    866    866      0     120    S    00:00:11     1   0.67%   devd
      2      2      0     115    S    00:00:00     0   0.00%   [kthreadd]
      3      3      0     115    S    00:00:01     0   0.00%   [ksoftirqd/0]
      4      4      0      99    S    00:00:00     1   0.00%   [watchdog/0]
      5      5      0     115    S    00:00:00     0   0.00%   [events/0]
      6      6      0     115    S    00:00:00     0   0.00%   [khelper]
    796    796      0     115    S    00:00:00     0   0.00%   [kip6fs/1]

<Sysname>
```

Display thread statistics in interactive mode.

```
<Sysname> monitor thread
84 processes; 107 threads
Thread states: 1 running, 106 sleeping, 0 stopped, 0 zombie
CPU states: 94.43% idle, 0.76% user, 3.64% kernel, 1.15% interrupt
Memory: 755M total, 417M available, page size 4K
    JID    TID  LAST_CPU  PRI  State  HH:MM:SS   MAX    CPU    Name
   1176   1176      0     120    R    00:00:01     1   3.42%   top
    866    866      0     120    S    00:00:12     1   0.85%   devd
    881    881      0     120    S    00:00:09     1   0.64%   diagd
      1      1      0     120    S    00:00:06     1   0.42%   scmd
   1160   1160      0     120    S    00:00:01     1   0.21%   sshd
      2      2      0     115    S    00:00:00     0   0.00%   [kthreadd]
      3      3      0     115    S    00:00:01     0   0.00%   [ksoftirqd/0]
      4      4      0      99    S    00:00:00     1   0.00%   [watchdog/0]
      5      5      0     115    S    00:00:00     0   0.00%   [events/0]
      6      6      0     115    S    00:00:00     0   0.00%   [khelper]
```

- Enter **h** or a question mark (?) to display help information as follows:

  ```
  Help for interactive commands:
  ```

```
        ?,h      Show the available interactive commands
          1      Toggle SMP view: '1' single/separate states
          c      Sort by the CPU field(default)
          d      Set the delay interval between screen updates
          k      Kill a job
          l      Refresh the screen
          n      Set the maximum number of threads to display
          q      Quit the interactive display
          t      Sort by run time of threads since last restart
          <      Move sort field to the next left column
          >      Move sort field to the next right column
Press any key to continue
```

- Enter **d**, and then enter a number to modify the refresh interval. If you enter **3**, statistics are refreshed every 3 seconds.

  ```
  Enter the delay interval between screen updates (1~2147483647): 3
  ```

- Enter **n**, and then enter a number to modify the maximum number of displayed threads. If you enter **5**, statistics for five threads are displayed.

  ```
  Enter the max number of threads to display(0 means unlimited): 5
  84 processes; 107 threads
  Thread states: 1 running, 106 sleeping, 0 stopped, 0 zombie
  CPU states: 93.26% idle, 0.99% user, 4.23% kernel, 1.49% interrupt
  Memory: 755M total, 417M available, page size 4K
      JID    TID  LAST_CPU  PRI  State  HH:MM:SS   MAX    CPU    Name
     1176   1176      0     120    R    00:00:02     1   3.71%   top
        1      1      0     120    S    00:00:06     1   0.92%   scmd
      866    866      0     120    S    00:00:13     1   0.69%   devd
      881    881      0     120    S    00:00:10     1   0.69%   diagd
      720    720      0     115    D    00:00:01     0   0.23%   [TMTH]
  ```

- Enter **k** and then enter a JID to kill a thread. If you enter **881**, the thread with the JID of 881 is killed.

  ```
  Enter the JID to kill: 881
  83 processes; 106 threads
  Thread states: 1 running, 105 sleeping, 0 stopped, 0 zombie
  CPU states: 96.26% idle, 0.54% user, 2.63% kernel, 0.54% interrupt
  Memory: 755M total, 418M available, page size 4K
      JID    TID  LAST_CPU  PRI  State  HH:MM:SS   MAX    CPU    Name
     1176   1176      0     120    R    00:00:04     1   1.86%   top
      866    866      0     120    S    00:00:14     1   0.87%   devd
        1      1      0     120    S    00:00:07     1   0.49%   scmd
      730    730      0       0    S    00:00:04     1   0.12%   [DIBC]
      762    762      0     120    S    00:00:22     1   0.12%   [MNET]
  ```

- Enter **q** to quit interactive mode.

Table 15 Command output

Field	Description
84 processes; 107 threads	Numbers of processes and threads.
JID	Job ID of a thread, which never changes.

TID	ID of a thread.
LAST_CPU	Number of the CPU on which the most recent thread scheduling occurs.
PRI	Priority level of a thread.
State	State of a thread: • **R**—Running. • **S**—Sleeping. • **T**—Traced or stopped. • **D**—Uninterruptible sleep. • **Z**—Zombie.
HH:MM:SS	Running time of a thread since last restart.
MAX	Longest time that a single thread scheduling occupies the CPU, in milliseconds.
CPU	CPU usage of a thread.
Name	Name of a thread. If square brackets ([ ]) exist in a thread name, the thread is a kernel thread.

process core

Use **process core** to enable or disable a process to generate core dump files for exceptions and set the maximum number of core dump files.

Syntax

process core { **maxcore** *value* | **off** } { **job** *job-id* | **name** *process-name* } [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

User view

Default

A process generates a core dump file for the first exception and does not generate any core dump files for subsequent exceptions.

Predefined user roles

network-admin

context-admin

Parameters

off: Disables core dump file generation.

maxcore *value*: Enables core dump file generation and sets the maximum number of core dump files, in the range of 1 to 10.

name *process-name*: Specifies a process by its name, a case-insensitive string of 1 to 15 characters.

job *job-id*: Specifies a process by its job ID, in the range of 1 to 2147483647. The job ID does not change after the process restarts.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command applies to the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

The command applies to all instances of a process.

The command enables the system to generate a core dump file each time the specified process crashes until the maximum number of core dump files is reached. A core dump file records the exception information.

Because core dump files consume system storage resources, you can disable core dump file generation for processes for which you do not need to review exception information.

Examples

Disable core dump file generation for process **routed**.

```
<Sysname> process core off name routed
```

Enable core dump file generation for process **routed** and set the maximum number of core dump files to 5.

```
<Sysname> process core maxcore 5 name routed
```

Related commands

display exception context

exception filepath

reset exception context

Use **reset exception context** to clear context information for process exceptions.

Syntax

reset exception context [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears context information for process exceptions on the IRF master device.

cpu *cpu-number*: Specifies a CPU by its number.

Examples

Clear context information for exceptions.

```
<Sysname> reset exception context
```

Related commands

display exception context

reset kernel deadloop

Use **reset kernel deadloop** to clear kernel thread deadloop information.

Syntax

reset kernel deadloop [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears kernel thread deadloop information for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

This command is supported only on the default context.

Examples

Clear kernel thread deadloop information.

```
<Sysname> reset kernel deadloop
```

Related commands

display kernel deadloop

reset kernel exception

Use **reset kernel exception** to clear kernel thread exception information.

Syntax

reset kernel exception [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears kernel thread exception information for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

This command is supported only on the default context.

Examples

Clear kernel thread exception information.

```
<Sysname> reset kernel exception
```

Related commands

display kernel exception

reset kernel reboot

Use **reset kernel reboot** to clear kernel thread reboot information.

Syntax

reset kernel reboot [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears kernel thread reboot information for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

This command is supported only on the default context.

Examples

Clear kernel thread reboot information.

```
<Sysname> reset kernel reboot
```

Related commands

display kernel reboot

reset kernel starvation

Use **reset kernel starvation** to clear kernel thread starvation information.

Syntax

reset kernel starvation [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears kernel thread starvation information for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

This command is supported only on the default context.

Examples

Clear kernel thread starvation information.

```
<Sysname> reset kernel starvation
```

Related commands

`display kernel starvation`

Contents

NETCONF commands

display netconf service

Use **display netconf service** to display current NETCONF service status and global NETCONF service statistics.

Syntax

display netconf service

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display the current NETCONF service status and global NETCONF service statistics.

```
<Sysname> display netconf service
NETCONF over SOAP over HTTP: Enabled (port 80)
NETCONF over SOAP over HTTPS: Enabled (port 443)
NETCONF over SSH: Enabled (port 830)
NETCONF over Telnet: Enabled
NETCONF over Console: Enabled
SOAP timeout: 10 minutes    Agent timeout: 10 minutes
Active sessions: 1
Service statistics:
NETCONF start time: 2015-10-10T08:08:08
Output notifications: 50
Output RPC errors: 20
Dropped sessions: 0
Sessions: 100
Received bad hellos: 0
Received RPCs: 1000
Received bad RPCs: 20
```

Table 1 Command output

Field	Description
SOAP timeout	NETCONF session idle timeout time for NETCONF over SOAP over HTTP sessions and NETCONF over SOAP over HTTPS sessions.
Agent timeout	NETCONF session idle timeout time for NETCONF over SSH sessions, NETCONF over Telnet sessions, and NETCONF over console sessions.
Active sessions	Number of active NETCONF sessions.

NETCONF start time	Time when the NETCONF service was started.
Output notifications	Number of subscribed notifications output by the device.
Output RPC errors	Number of erroneous RPC requests output by the device.
Dropped sessions	Number of NETCONF sessions dropped due to timeout or abnormal network disconnection.
Sessions	Number of established NETCONF sessions.
Received bad hellos	Number of received erroneous hello messages.
Received RPCs	Total number of RPC requests received by the device.
Received bad RPCs	Number of received erroneous RPC requests.

display netconf session

Use **`display netconf session`** to display NETCONF session status and statistics.

Syntax

`display netconf session`

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display NETCONF session status and statistics.

```
<Sysname> display netconf session
Session ID: 1 Session type: Agent
Username: test
Login time: 2015-10-10T08:08:08
Client IP address: 192.168.1.1
Session statistics:
Received RPCs    : 10          Received bad RPCs   : 0
    Output RPC errors: 10          Output notifications: 0
Session ID: 2 Session type: SOAP
Username: test
Login time: 2015-10-10T08:08:08
Client IP address: 192.168.1.1
Session statistics:
    Received RPCs    : 10         Received bad RPCs   : 0
    Output RPC errors: 10         Output notifications: 0
```

Table 2 Command output

Field	Description
Session ID	ID of the NETCONF session.
Session type	NETCONF session type: • **soap**—NETCONF over SOAP over HTTP or NETCONF over SOAP over HTTPS. • **agent**—NETCONF over SSH, NETCONF over Telnet, or NETCONF over console.
Username	Username used by the NETCONF client to establish the session. If the session type is **agent** and login authentication was not performed, this field displays a hyphen (-).
Login time	Time when the NETCONF session was established.
Client IP address	IP address of the NETCONF client. This field displays a hyphen (-) for NETCONF over console sessions.
Received RPCs	Number of received RPC requests.
Received bad RPCs	Number of received erroneous RPC requests.
Output RPC errors	Number of erroneous RPC requests output by the device.
Output notifications	Number of subscribed notifications output by the device.

netconf capability specific-namespace

Use **netconf capability specific-namespace** to configure the device to use module-specific namespaces.

Use **undo netconf capability specific-namespace** to restore the default.

Syntax

netconf capability specific-namespace

undo netconf capability specific-namespace

Default

The device uses the common namespace.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

NETCONF supports both the common namespace and module-specific namespaces. The common namespace is incompatible with module-specific namespaces. To set up a NETCONF session, the device and the client must use the same type of namespaces. By default, the common namespace is used. If the client does not support the common namespace, use this command to configure the device to use module-specific namespaces.

For this command to take effect, you must reestablish the NETCONF session.

Examples

Configure the device to use module-specific namespaces.

```
<Sysname> system-view
[Sysname] netconf capability specific-namespace
```

netconf idle-timeout

Use **netconf idle-timeout** to set the NETCONF session idle timeout time.

Use **undo netconf idle-timeout** to restore the default.

Syntax

netconf { **soap** | **agent** } **idle-timeout** *minute*

undo netconf { **soap** | **agent** } **idle-timeout**

Default

The NETCONF session idle timeout time is 10 minutes for NETCONF over SOAP over HTTP sessions and NETCONF over SOAP over HTTPS sessions.

The NETCONF session idle timeout time is 0 minutes for NETCONF over SSH sessions, NETCONF over Telnet sessions, and NETCONF over console sessions. The sessions never time out.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

soap: Specifies the NETCONF over SOAP over HTTP sessions and NETCONF over SOAP over HTTPS sessions.

agent: Specifies the NETCONF over SSH sessions, NETCONF over Telnet sessions, and NETCONF over console sessions.

minute: Specifies the NETCONF session idle timeout time in minutes. The value range is as follows:

- 1 to 999 for NETCONF over SOAP over HTTP sessions and NETCONF over SOAP over HTTPS sessions.
- 0 to 999 for NETCONF over SSH sessions, NETCONF over Telnet sessions, and NETCONF over console sessions. To disable the timeout feature, set this argument to 0.

Usage guidelines

If no NETCONF packets are exchanged on a NETCONF session within the NETCONF session idle timeout time, the device tears down the session.

Examples

Set the NETCONF session idle timeout time to 20 minutes for NETCONF over SOAP over HTTP sessions and NETCONF over SOAP over HTTPS sessions.

```
<Sysname> system-view
[Sysname] netconf soap idle-timeout 20
```

netconf log

Use **netconf log** to enable NETCONF logging.

Use **undo netconf log** to remove the configuration for the specified NETCONF operation sources and NETCONF operations.

Syntax

netconf log source { **all** | { **agent** | **soap** | **web** } * } { **protocol-operation** { **all** | { **action** | **config** | **get** | **session** | **set** | **syntax** | **others** } * } | **row-operation** | **verbose** }

undo netconf log source { **all** | { **agent** | **soap** | **web** } * } { **protocol-operation** { **all** | { **action** | **config** | **get** | **session** | **set** | **syntax** | **others** } * } | **row-operation** | **verbose** }

Default

NETCONF logging is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

source: Specifies a NETCONF operation source that represents clients that use a protocol.

- **all**: Specifies NETCONF clients that use all protocols.
- **agent**: Specifies clients that use Telnet, SSH, NETCONF over console, or NETCONF over SSH.
- **soap**: Specifies clients that use SOAP over HTTP, or SOAP over HTTPS.
- **web**: Specifies clients that use Web.

protocol-operation: Logs requests and replies for specific types of NETCONF operations.

- **all**: Specifies all types of NETCONF operations.
- **action**: Specifies the <action> operation.
- **config**: Specifies the configuration-related NETCONF operations, including the <CLI>, <save>, <load>, <rollback>, <lock>, <unlock>, and <save-point> operations.
- **get**: Specifies the data retrieval-related NETCONF operations, including the <get>, <get-config>, <get-bulk>, <get-bulk-config>, and <get-sessions> operations.
- **session**: Specifies session-related NETCONF operations, including the <kill-session> and <close-session> operations, and capability exchanges by hello messages.
- **set**: Specifies all <edit-config> operations.
- **syntax**: Specifies the requests that include XML and schema errors.
- **others**: Specifies NETCONF operations except for those specified by keywords **action**, **config**, **get**, **set**, **session**, and **syntax**.

row-operation: Logs row operations for <action> and <edit-config> operations.

verbose: Logs detailed information about requests and replies for types of NETCONF operations, including packet contents of format-correct requests and error information about failed <edit-config> operations.

Usage guidelines

If you specify the **protocol-operation** keyword, the device logs each of the matching operation and the operation result.

For example, if you perform a NETCONF operation to create VLANs 3 through 5, the device outputs the following log messages:

```
%Mar 21 17:11:34:479 2017 Sysname XMLSOAP/6/XML_REQUEST: test from 192.168.100.198,
session id 2,message-id 100, receive edit-config request.
%Mar 21 17:11:34:483 2017 Sysname XMLSOAP/6/EDIT-CONFIG: test from 192.168.100.198,
session id 2,message-id 100, execute success.
```

If you specify the **row-operation** keyword, the device logs each row operation and the operation result for an <action> or <edit-config> operation. For example, if you perform a NETCONF operation to create VLANs 3 through 5, the device outputs the following log messages:

```
%Mar 31 17:50:02:608 2017 Sysname XMLSOAP/6/EDIT-CONFIG: User (test, 192.168.100.20,
session ID 1), message ID=100, operation=create VLAN/VLANs (ID=3), result=Succeeded. No
attributes.
%Mar 31 17:50:02:609 2017 Sysname XMLSOAP/6/EDIT-CONFIG: User (test, 192.168.100.20,
session ID 1), message ID=100, operation=create VLAN/VLANs (ID=4), result=Succeeded. No
attributes.
%Mar 31 17:50:02:611 2017 Sysname XMLSOAP/6/EDIT-CONFIG: User (test, 192.168.100.20,
session ID 1), message ID=100, operation=create VLAN/VLANs (ID=5), result=Succeeded. No
attributes.
```

For NETCONF to correctly send the generated logs to the information center, you must also configure the information center. For information about information center configuration, see *Network Management and Monitoring Configuration Guide*.

Examples

Configure the device to log NETCONF edit-config information sourced from agent clients.

```
<Sysname> system-view
[Sysname] netconf log source agent protocol-operation set
```

netconf soap acl

Use **netconf soap acl** to apply an ACL to control NETCONF over SOAP access.

Use **undo netconf soap acl** to restore the default.

Syntax

netconf soap { **http** | **https** } [**ipv6**] **acl** { *acl-number* | **name** *acl-name* }

undo netconf soap { **http** | **https** } [**ipv6**] **acl**

Default

No ACL is applied to control NETCONF over SOAP access.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

http: Applies an ACL to control NETCONF over SOAP over HTTP access.

https: Applies an ACL to control NETCONF over SOAP over HTTPS access.

ipv6: Specifies an IPv6 ACL. To specify an IPv4 ACL, do not specify this keyword. This keyword is supported only if you have specified the **http** keyword.

acl-number: Specifies an ACL by its number in the range of 2000 to 2999.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters. It must start with an English letter. To avoid confusion, it cannot be **all**.

Usage guidelines

To control NETCONF over SOAP access, specify an ACL that exists and has rules.

- If the specified ACL exists and has rules, only clients permitted by the ACL can establish NETCONF over SOAP sessions.
- If no ACL is applied or the applied ACL does not exist or does not have rules, all NETCONF clients can establish NETCONF over SOAP sessions.

If you execute the **netconf soap http acl** command multiple times, the most recent configuration takes effect. The same is true for the **netconf soap https acl** command.

Examples

Use IPv4 ACL 2001 to allow only NETCONF clients from subnet 10.10.0.0/16 to establish NETCONF over SOAP over HTTP sessions.

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 10.10.0.0 0.0.255.255
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] netconf soap http acl 2001
```

Use IPv6 ACL 2002 to allow only NETCONF clients from subnet 6::2/64 to establish NETCONF over SOAP over HTTP sessions.

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2002
[Sysname-acl-ipv6-basic-2002] rule deny source 6::2 64
[Sysname-acl-ipv6-basic-2002] quit
[Sysname] netconf soap http ipv6 acl 2002
```

netconf soap domain

Use **netconf soap domain** to specify a mandatory authentication domain for NETCONF users.

Use **undo netconf soap domain** to restore the default.

Syntax

netconf soap domain *domain-name*

undo netconf soap domain

Default

No mandatory authentication domain is specified for NETCONF users.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

domain-name: Specifies an ISP domain by its name, a case-insensitive string of 1 to 255 characters. For information about ISP domains, see AAA in *Security Configuration Guide*.

Usage guidelines

You can use either of the following methods to specify an authentication domain:

- Execute the **netconf soap domain** command to specify a mandatory authentication domain. After this command is executed, all NETCONF users are placed in the domain for authentication.
- Add an authentication domain to the <UserName> parameter of a SOAP request. The authentication domain takes effect only on the current request.

The authentication domain specified by using this command takes precedence over the authentication domain specified by the <UserName> parameter of a SOAP request.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify mandatory authentication domain **my-domain** for NETCONF users.

```
<Sysname> system-view
[Sysname] netconf soap domain my-domain
```

netconf soap enable

Use **netconf soap enable** to enable NETCONF over SOAP.

Use **undo netconf soap enable** to disable NETCONF over SOAP.

Syntax

netconf soap { **http** | **https** } **enable**

undo netconf soap { **http** | **https** } **enable**

Default

NETCONF over SOAP is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

http: Specifies NETCONF over SOAP over HTTP.

https: Specifies NETCONF over SOAP over HTTPS.

Usage guidelines

This command enables the device to resolve NETCONF messages that are encapsulated with SOAP in HTTP or HTTPS packets.

Examples

Enable NETCONF over SOAP over HTTP.

```
<Sysname> system-view
```

```
[Sysname] netconf soap http enable
```

netconf soap http port

Use **netconf soap http port** to specify a port to listen for NETCONF over SOAP over HTTP session requests.

Use **undo netconf soap http port** to restore the default.

Syntax

netconf soap http port *port-number*

undo netconf soap http port

Default

The device uses port 80 to listen for NETCONF over SOAP over HTTP session requests.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

*port-numbe*r: Specifies a port by its number in the range of 1 to 65535.

Usage guidelines

Executing this command causes existing NETCONF over SOAP sessions to become ineffective. You must re-establish the sessions again.

Examples

Use port 1000 to listen for NETCONF over SOAP over HTTP session requests.

```
<Sysname> system-view
[Sysname] netconf soap http port 1000
```

netconf soap https ssl-server-policy

Use **netconf soap https ssl-server-policy** to apply an SSL server policy to the NETCONF over SOAP over HTTPS service.

Use **undo netconf soap https ssl-server-policy** to restore the default.

Syntax

netconf soap https ssl-server-policy *policy-name*

undo netconf soap https ssl-server-policy

Default

No SSL server policy is applied to the NETCONF over SOAP over HTTPS service.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies an SSL server policy name, a string of 1 to 31 characters.

Usage guidelines

The NETCONF over SOAP over HTTPS service will use the SSL server policy to enhance service security. For more information about SSL server policies, see SSL configuration in *Security Configuration Guide*.

You can configure this command only when NETCONF over SOAP over HTTPS is disabled.

This command takes effect after you enable NETCONF over SOAP over HTTPS.

If you execute this command multiple times, the most recent configuration takes effect.

After NETCONF over SOAP over HTTPS is enabled, changes to the applied SSL server policy do not affect established NETCONF over SOAP over HTTPS sessions. The changes affect only NETCONF over SOAP over HTTPS sessions established after the changes are made.

Examples

Apply SSL server policy **myssl** to the NETCONF over SOAP over HTTPS service.

```
<Sysname> system-view
[Sysname] netconf soap https ssl-server-policy myssl
```

Related commands

netconf soap enable

ssl server-policy (*Security Command Reference*)

netconf ssh acl

Use **netconf ssh acl** to apply an IPv4 ACL to control NETCONF over SSH access.

Use **undo netconf ssh acl** to restore the default.

Syntax

netconf ssh acl { *ipv4-acl-number* | **name** *ipv4-acl-name* }

undo netconf ssh acl

Default

No IPv4 ACL is applied to control NETCONF over SSH access.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-acl-number: Specifies an IPv4 ACL by its number in the range of 2000 to 2999.

name *ipv4-acl-name*: Specifies an IPv4 ACL by its name. The *ipv4-acl-name* argument is a case-insensitive string of 1 to 63 characters. It must start with an English letter. To avoid confusion, it cannot be **all**.

Usage guidelines

To control NETCONF over SSH access, specify an ACL that exists and has rules.

- If the specified ACL exists and has rules, only clients permitted by the ACL can establish NETCONF over SSH sessions.
- If no ACL is applied, all NETCONF clients can establish NETCONF over SSH sessions.
- If the applied ACL does not exist or does not have rules, no NETCONF clients can establish NETCONF over SSH sessions.

For more information about ACL configuration, see *ACL and QoS Configuration Guide*.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Use IPv4 ACL 2001 to allow only NETCONF clients from subnet 10.10.0.0/16 to establish NETCONF over SSH sessions.

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 10.10.0.0 0.0.255.255
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] netconf ssh acl 2001
```

Related commands

netconf soap acl

netconf ssh server enable

Use **netconf ssh server enable** to enable NETCONF over SSH.

Use **undo netconf ssh server enable** to disable NETCONF over SSH.

Syntax

netconf ssh server enable

undo netconf ssh server enable

Default

NETCONF over SSH is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This feature allows you to use an SSH client to invoke NETCONF as an SSH subsystem. Then, you can directly use XML messages to perform NETCONF operations without using the **xml** command.

Before you execute this command, configure the authentication mode for users as **scheme** on the device. Then, the NETCONF-over-SSH-enabled user terminals can access the device through NETCONF over SSH.

Only capability set **urn:ietf:params:netconf:base:1.0** is available. It is supported by both the device and user terminals.

Examples

Enable NETCONF over SSH.

```
<Sysname> system-view
[Sysname] netconf ssh server enable
```

netconf ssh server port

Use **netconf ssh server port** to specify a port to listen for NETCONF over SSH session requests.

Use **undo netconf ssh server port** to restore the default.

Syntax

netconf ssh server port *port-number*

undo netconf ssh server port

Default

The device uses port 830 to listen for NETCONF over SSH session requests.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

*port-numbe*r: Specifies a port by its number in the range of 1 to 65535.

Usage guidelines

Make sure the specified port is not being used by other services.

Examples

Use port 800 to listen for NETCONF over SSH session requests.

```
<Sysname> system-view
[Sysname] netconf ssh server port 800
```

reset netconf service statistics

Use **reset netconf service statistics** to clear current global NETCONF service statistics.

Syntax

reset netconf service statistics

Views

User view

Predefined user roles

network-admin

context-admin

Examples

Clear current global NETCONF service statistics.

```
<Sysname> reset netconf service statistics
```

Related commands

`display netconf service`

reset netconf session statistics

Use **`reset netconf session statistics`** to clear current NETCONF session statistics.

Syntax

`reset netconf session statistics`

Views

User view

Predefined user roles

network-admin

context-admin

Examples

Clear current NETCONF session statistics.

```
<Sysname> reset netconf session statistics
```

Related commands

`display netconf session`

xml

Use **`xml`** to enter XML view.

Syntax

`xml`

Views

User view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Usage guidelines

In XML view, use NETCONF messages to configure the device or obtain data from the device. The NETCONF operations you can perform depend on the user roles you have, as shown in Table 3.

Table 3 NETCONF operations available for the predefined user roles

User role	NETCONF operations
network-admin context-admin	All NETCONF operations
network-operator	• Get

User role	NETCONF operations
Context-operator	• Get-bulk • Get-bulk-config • Get-config • Get-sessions • Close-session

To ensure the format correctness of NETCONF messages in XML view, do not enter NETCONF messages manually. Copy and paste the messages.

While the device is performing a NETCONF operation, do not perform any other operations, such as pasting a NETCONF message or pressing **Enter**.

For the device to identify NETCONF messages, you must add end mark **]]>]]>** at the end of each NETCONF message.

After you enter XML view, the device automatically advertises its NETCONF capabilities to the client. In response, you must configure the client to notify the device of its supported NETCONF capabilities. After the capability exchange, you can use the client to configure the device.

NETCONF messages must comply with the XML format requirements and semantic and syntactic requirements in the NETCONF XML API reference for the device. As a best practice, use third-party software to generate NETCONF messages to ensure successful configuration.

To quit XML view, use a NETCONF message instead of the **quit** command.

If you have configured a shortcut key (**Ctrl + C**, by default) by using the **escape-key** command in user line/user line class view, the NETCONF message should not contain the shortcut key string. If the NETCONF message contains the shortcut key string, relevant configurations in XML view might be affected. For example, in user line view, you configured "a" as the shortcut key by using the **escape-key a** command. When a NETCONF message includes the character "a," only the contents after the last "a" in the message can be processed.

Examples

Enter XML view.

```
<Sysname> xml
<?xml version="1.0" encoding="UTF-8"?><hello
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"><capabilities><capability>urn:ietf:pa
rams:netconf:base:1.1</capability><capability>urn:ietf:params:netconf:writable-runnin
g</capability><capability>urn:ietf:params:netconf:capability:notification:1.0</capabi
lity><capability>urn:ietf:params:netconf:capability:validate:1.1</capability><capabil
ity>urn:ietf:params:netconf:capability:interleave:1.0</capability><capability>urn:nsf
ocus:params:netconf:capability:nsfocus-netconf-ext:1.0</capability></capabilities><se
ssion-id>1</session-id></hello>]]>]]>
```

Notify the device of the NETCONF capabilities supported on the client.

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <capabilities>
    <capability>
           urn:ietf:params:netconf:base:1.0
    </capability>
  </capabilities>
</hello>]]>]]>
```

Quit XML view.

```
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <close-session/>
</rpc>]]>]]>
```

<Sysname>

Contents

SNMP commands

The SNMP agent sends notifications (traps and informs) to inform the NMS of significant events, such as link state changes and user logins or logouts. Unless otherwise stated, the **trap** keyword in the command line includes both traps and informs.

display snmp-agent community

Use **display snmp-agent community** to display information about SNMPv1 or SNMPv2c communities.

Syntax

display snmp-agent community [**read** | **write**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

read: Specifies SNMP read-only communities.

write: Specifies SNMP read and write communities.

Usage guidelines

If you do not specify the **read** or **write** keyword, this command displays information about all SNMPv1 and SNMPv2c communities.

SNMPv1 and SNMPv2c communities can be created in the following ways:

- Created by using the **snmp-agent community** command.
- Automatically created by the system for SNMPv1 and SNMPv2c users that have been assigned to an existing SNMP group.

This command displays information only about communities created and saved in plaintext form.

Examples

Display information about all SNMPv1 and SNMPv2c communities.

```
<Sysname> display snmp-agent community
   Community name: aa
       Group name: aa
       ACL:2001
       Storage-type: nonVolatile
       Context name: con1

   Community name: bb
       Role name: bb
       Storage-type: nonVolatile
```

```
   Community name: userv1
       Group name: testv1
       Storage-type: nonvolatile
Community name: cc
       Group name: cc
       ACL name: testacl
       Storage-type: nonVolatile
```

Table 1 Command output

Field	Description
Community name	Community name created by using the **snmp-agent community** command or username created by using the **snmp-agent usm-user { v1 | v2c }** command.
Group name	SNMP group name. • If the community is created by using the **snmp-agent community** command in VACM mode, the group name is the same as the community name. • If the community is created by using the **snmp-agent usm-user { v1 | v2c }** command, the name of the group that has the user is displayed.
Role name	User role name for the community. If the community is created by using the **snmp-agent community** command in RBAC mode, a user role can be bound to the community name.
ACL	Number of the IPv4 ACL. This field appears only when an IPv4 ACL number is specified for the SNMPv1 or SNMPv2c community.
ACL name	Name of the IPv4 ACL. This field appears only when an IPv4 ACL name is specified for the SNMPv1 or SNMPv2c community.
IPV6 ACL	Number of the IPv6 ACL. This field appears only when an IPv6 ACL number is specified for the SNMPv1 or SNMPv2c community.
IPV6 ACL name	Name of the IPv6 ACL. This field appears only when an IPv6 ACL name is specified for the SNMPv1 or SNMPv2c community.
Storage-type	Storage type: • **volatile**—Settings are lost when the system reboots. • **nonVolatile**—Settings remain after the system reboots. • **permanent**—Settings remain after the system reboots and can be modified but not deleted. • **readOnly**—Settings remain after the system reboots and cannot be modified or deleted. • **other**—Any other storage type.
Context name	SNMP context: • If a mapping between the SNMP community and an SNMP context is configured, the SNMP context is displayed. • If no mapping between the SNMP community and an SNMP context exists, this field is empty.

Related commands

snmp-agent community

snmp-agent usm-user { **v1** | **v2c** }

display snmp-agent context

Use **display snmp-agent context** to display SNMP contexts.

Syntax

display snmp-agent context [*context-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

context-name: Specifies an SNMP context by its name, a case-sensitive string of 1 to 32 characters. If you do not specify this argument, the command displays all SNMP contexts.

Examples

Display all SNMP contexts.

```
<Sysname> display snmp-agent context
   testcontext
```

Related commands

snmp-agent context

display snmp-agent group

Use **display snmp-agent group** to display information about SNMP groups.

Syntax

display snmp-agent group [*group-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

group-name: Specifies an SNMPv1, SNMPv2c, or SNMPv3 group name. It is a case-sensitive string of 1 to 32 characters. If you do not specify a group, this command displays information about all SNMP groups.

Examples

Display information about all SNMP groups.

```
<Sysname> display snmp-agent group
   Group name: groupv3
       Security model: v3 noAuthnoPriv
       Readview: ViewDefault
       Writeview: <no specified>
       Notifyview: <no specified>
       Storage-type: nonvolatile
        ACL name: testacl
```

Table 2 Command output

Field	Description
Group name	SNMP group name.
Security model	Security model of the SNMP group: • **authPriv**—Authentication with privacy. • **authNoPriv**—Authentication without privacy. • **noAuthNoPriv**—No authentication, no privacy. Security model of an SNMPv1 or SNMPv2c group can only be noAuthNoPriv.
Readview	Read-only MIB view accessible to the SNMP group.
Writeview	Write MIB view accessible to the SNMP group.
Notifyview	Notify MIB view for the SNMP group. The SNMP users in the group can send notifications only for the nodes in the notify MIB view.
Storage-type	Storage type, including **volatile**, **nonvolatile**, **permanent**, **readOnly**, and **other**. For more information, see Table 1.
ACL	Number of the IPv4 ACL. This field appears only when an IPv4 ACL number is specified for the SNMP group.
ACL name	Name of the IPv4 ACL. This field appears only when an ACL name is specified for the SNMP group.
IPv6 ACL	Number of the IPv6 ACL. This field appears only when an IPv6 ACL number is specified for the SNMP group.
IPV6 ACL name	Name of the IPv6 ACL. This field appears only when an IPv6 ACL name is specified for the SNMP group.

Related commands

snmp-agent group

display snmp-agent local-engineid

Use **display snmp-agent local-engineid** to display the local SNMP engine ID.

Syntax

display snmp-agent local-engineid

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Usage guidelines

Every SNMP entity has one SNMP engine to provide services for sending and receiving messages, authenticating and encrypting messages, and controlling access to managed objects.

An SNMP engine ID uniquely identifies an SNMP entity in an SNMP domain.

Examples

Display the local SNMP engine ID.

```
<Sysname> display snmp-agent local-engineid
   SNMP local engine ID: 800063A2800084E52BED7900000001
```

Related commands

snmp-agent local-engineid

display snmp-agent mib-node

Use **display snmp-agent mib-node** to display SNMP MIB node information.

Syntax

display snmp-agent mib-node [**details** | **index-node** | **trap-node** | **verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

details: Specifies detailed MIB node information, including node name, last octet of an OID string, and name of the next leaf node.

index-node: Specifies SNMP MIB tables, and node names and OIDs of MIB index nodes.

trap-node: Specifies node names and OIDs of MIB notification nodes, and node names and OIDs of notification objects.

verbose: Specifies detailed information about SNMP MIB nodes, including node names, OIDs, node types, permissions to MIB nodes, data types, MORs, and parent, child, and sibling nodes.

Usage guidelines

If you do not specify any keywords, this command displays information about all SNMP MIB nodes, including node name, OID, and permissions to MIB nodes.

The SNMP software package includes different MIB files. Support for MIBs varies by SNMP software versions.

Examples

Display SNMP MIB node information.

```
<Sysname> display snmp-agent mib-node

iso<1>(NA)
  |-std<1.0>(NA)
   |-iso8802<1.0.8802>(NA)
    |-ieee802dot1<1.0.8802.1>(NA)
     |-ieee802dot1mibs<1.0.8802.1.1>(NA)
      ...
```

Table 3 Command output

Field	Description
-std	MIB node name
<1.0>	MIB node OID
(NA)	Access right to the MIB node: • **NA**—Not accessible • **NF**—Notifications • **RO**—Read-only access • **RW**—Read and write access • **RC**—Read-write-create access • **WO**—Write-only access
*	Leaf node or MIB table node

Display detailed MIB node information.

```
<Sysname> display snmp-agent mib-node details

 iso(1)(dot1xPaeSystemAuthControl)
  |-std(0)(dot1xPaeSystemAuthControl)
   |-iso8802(8802)(dot1xPaeSystemAuthControl)
    |-ieee802dot1(1)(dot1xPaeSystemAuthControl)
     |-ieee802dot1mibs(1)(dot1xPaeSystemAuthControl)
      ...
```

Table 4 Command output

Field	Description
-std	MIB node name
(0)	Last bit of the MIB OID string
(lldpMessageTxInterval)	Name of the leaf node
*	Leaf node or MIB table node

Display MIB table names, and node names and OIDs of MIB index nodes.

```
<Sysname> display snmp-agent mib-node index-node

Table          |dot1xPaePortTable
Index          ||dot1xPaePortNumber
OID            |||  1.0.8802.1.1.1.1.1.2.1.1
...
```

Table 5 Command output

Field	Description
Table	MIB table name
Index	MIB index node name
OID	MIB index node OID

Display names and OIDs of MIB notification nodes, and names and OIDs of notification objects.

```
<Sysname> display snmp-agent mib-node trap-node


Name           |lldpRemTablesChange
OID            ||1.0.8802.1.1.2.0.0.1
Trap Object
Name           |||lldpStatsRemTablesInserts
OID            ||||1.0.8802.1.1.2.1.2.2
Name           |||lldpStatsRemTablesDeletes
OID            ||||1.0.8802.1.1.2.1.2.3
Name           |||lldpStatsRemTablesDrops
OID            ||||1.0.8802.1.1.2.1.2.4
Name           |||lldpStatsRemTablesAgeouts
OID            ||||1.0.8802.1.1.2.1.2.5
...
```

Table 6 Command output

Field	Description
Name	MIB notification node name
OID	MIB notification node OID
Trap Object	Name and OID of a notification object

Display detailed information about SNMP MIB nodes, including node names, OIDs, node types, permissions to MIB nodes, data types, MORs, and parent, child, and sibling nodes.

```
<Sysname> display snmp-agent mib-node verbose


Name           |iso
OID            ||1
Properties     ||NodeType:   Other
```

```
              ||AccessType: NA
              ||DataType:   NA
              ||MOR:        0x00000000
Parent        ||
First child   ||std
Next leaf     ||dot1xPaeSystemAuthControl
Next sibling  ||
...
```

Table 7 Command output

Field	Description
Name	MIB node name.
OID	MIB node OID.
Properties	MIB node properties.
NodeType	MIB node types: • **Table**—Table node. • **Row**—Row node in a MIB table. • **Column**—Column node in a MIB table. • **Leaf**—Leaf node. • **Group**—Group node (parent node of a leaf node). • **Trapnode**—Notification node. • **Other**—Other node types.
AccessType	Access right to the MIB node: • **NA**—Not accessible. • **NF**—Supports notifications. • **RO**—Supports read-only access. • **RW**—Supports read and write access. • **RC**—Supports read-write-create access. • **WO**—Supports write-only access.
DataType	Data type of the MIB node: • **Integer**—An integer. • **Integer32**—A 32-bit integer. • **Unsigned32**—A 32-bit integer with no mathematical sign. • **Gauge**—A non-negative integer that might increase or decrease. • **Gauge32**—A 32-bit non-negative integer that might increase or decrease. • **Counter**—A non-negative integer that might increase but not decrease. • **Counter32**—A 32-bit non-negative integer that might increase but not decrease. • **Counter64**—A 64-bit non-negative integer that might increase but not decrease. • **Timeticks**—A non-negative integer for time keeping. • **Octstring**—An octal string. • **OID**—Object identifier. • **IPaddress**—A 32-bit IP address. • **Networkaddress**—A network IP address. • **Opaque**—Any data. • **Userdefined**—User-defined data. • **BITS**—Bit enumeration. • **NA**—Other data type.
MOR	MOR for the MIB node.

Field	Description
Parent	Name of the parent node.
First child	Name of the first leaf node.
Next leaf	Name of the next leaf node.
Next sibling	Name of the next sibling node.
Allow	Operation types allowed: • **get/set/getnext**—All operations. • **get**—Get operation. • **set**—Set operation. • **getnext**—GetNext operation.
Value range	Value range of the MIB node.
Index	Table index. This field appears only for a table node.

display snmp-agent mib-view

Use **display snmp-agent mib-view** to display MIB views.

Syntax

display snmp-agent mib-view [**exclude** | **include** | **viewname** *view-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

exclude: Displays the subtrees excluded from any MIB view.

include: Displays the subtrees included in any MIB view.

viewname *view-name*: Displays information about the specified MIB view. The *view-name* argument is a case-sensitive string of 1 to 32 characters.

Usage guidelines

If you do not specify any parameters, this command displays all MIB views.

Examples

Display all MIB views.

```
<Sysname> display snmp-agent mib-view
   View name: ViewDefault
       MIB Subtree: iso
       Subtree mask:
```

```
    Storage-type: nonVolatile
    View Type: included
    View status: active

View name: ViewDefault
    MIB Subtree: snmpUsmMIB
    Subtree mask:
    Storage-type: nonVolatile
    View Type: excluded
    View status: active

View name: ViewDefault
    MIB Subtree: snmpVacmMIB
    Subtree mask:
    Storage-type: nonVolatile
    View Type: excluded
    View status: active

View name: ViewDefault
    MIB Subtree: snmpModules.18
    Subtree mask:
    Storage-type: nonVolatile
    View Type: excluded
    View status: active
```

ViewDefault is the default MIB view. The output shows that except for the MIB objects in the **snmpUsmMIB**, **snmpVacmMIB**, and **snmpModules.18** subtrees, all the MIB objects in the **iso** subtree are accessible.

Table 8 Command output

Field	Description
View name	MIB view name.
MIB Subtree	MIB subtree covered by the MIB view.
Subtree mask	MIB subtree mask.
Storage-type	Type of the medium (see Table 1) where the subtree view is stored.
View Type	Access privilege for the MIB subtree in the MIB view: • **Included**—All objects in the MIB subtree are accessible in the MIB view. • **Excluded**—None of the objects in the MIB subtree is accessible in the MIB view.
View status	Status of the MIB view: • **active**—MIB view is effective. • **inactive**—MIB view is ineffective. The objects in the MIB view are not accessible, but they can send notifications.

Related commands

snmp-agent mib-view

display snmp-agent remote

Use **display snmp-agent remote** to display engine IDs of the remote SNMP entities.

Syntax

display snmp-agent remote [{ *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

ipv4-address: Specifies a remote SNMP entity by its IPv4 address.

ipv6 *ipv6-address*: Specifies a remote SNMP entity by its IPv6 address.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the remote SNMP entity belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the remote SNMP entity belongs to the public network, do not specify this option.

Usage guidelines

Every SNMP entity has one SNMP engine to provide services for sending and receiving messages, authenticating and encrypting messages, and controlling access to managed objects.

An SNMP engine ID uniquely identifies an SNMP entity in an SNMP domain.

If you do not specify a remote SNMP entity, this command displays the engine IDs of all remote SNMP entities.

Examples

Display engine IDs of all remote SNMP entities.

```
<Sysname> display snmp-agent remote
   Remote engineID: 800063A28000A0FC00580400000001
       IPv4 address: 1.1.1.1
       VPN instance: vpn1
```

Table 9 Command output

Field	Description
Remote engineID	Remote SNMP engine ID you have configured using the **snmp-agent remote** command.
IPv4 address	IPv4 address of the remote SNMP entity.
IPv6 address	IPv6 address of the remote SNMP entity. This field is displayed if the remote SNMP entity is configured with an IPv6 address.
VPN instance	This field is available only if a VPN instance has been specified for the remote SNMP entity in the **snmp-agent remote** command.

Related commands

snmp-agent remote

display snmp-agent statistics

Use **display snmp-agent statistics** to display SNMP message statistics.

Syntax

display snmp-agent statistics

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display SNMP message statistics.

```
<Sysname> display snmp-agent statistics
  1684 messages delivered to the SNMP entity.
  5 messages were for an unsupported version.
  0 messages used an unknown SNMP community name.
  0 messages represented an illegal operation for the community supplied.
  0 ASN.1 or BER errors in the process of decoding.
  1679 messages passed from the SNMP entity.
  0 SNMP PDUs had badValue error-status.
  0 SNMP PDUs had genErr error-status.
  0 SNMP PDUs had noSuchName error-status.
  0 SNMP PDUs had tooBig error-status (Maximum packet size 1500).
  16544 MIB objects retrieved successfully.
  2 MIB objects altered successfully.
  7 GetRequest-PDU accepted and processed.
  7 GetNextRequest-PDU accepted and processed.
  1653 GetBulkRequest-PDU accepted and processed.
  1669 GetResponse-PDU accepted and processed.
  2 SetRequest-PDU accepted and processed.
  0 Trap PDUs accepted and processed.
  0 alternate Response Class PDUs dropped silently.
  0 forwarded Confirmed Class PDUs dropped silently.
```

Table 10 Command output

Field	Description
messages delivered to the SNMP entity	Number of messages that the SNMP agent has received.
messages were for an unsupported version	Number of messages that are not supported by the SNMP agent version.

Field	Description
messages used an unknown SNMP community name	Number of messages that used an unknown SNMP community name.
messages represented an illegal operation for the community supplied	Number of messages carrying an operation that the community has no right to perform.
ASN.1 or BER errors in the process of decoding	Number of messages that had ASN.1 or BER errors during decoding.
messages passed from the SNMP entity	Number of messages sent by the SNMP agent.
SNMP PDUs had badValue error-status	Number of PDUs with a BadValue error.
SNMP PDUs had genErr error-status	Number of PDUs with a genErr error.
SNMP PDUs had noSuchName error-status	Number of PDUs with a NoSuchName error.
SNMP PDUs had tooBig error-status	Number of PDUs with a TooBig error (the maximum packet size is 1500 bytes).
MIB objects retrieved successfully	Number of MIB objects that have been successfully retrieved.
MIB objects altered successfully	Number of MIB objects that have been successfully modified.
GetRequest-PDU accepted and processed	Number of GetRequest requests that have been received and processed.
GetNextRequest-PDU accepted and processed	Number of getNext requests that have been received and processed.
GetBulkRequest-PDU accepted and processed	Number of getBulk requests that have been received and processed.
GetResponse-PDU accepted and processed	Number of get responses that have been received and processed.
SetRequest-PDU accepted and processed	Number of set requests that have been received and processed.
Trap PDUs accepted and processed	Number of notifications that have been received and processed.
alternate Response Class PDUs dropped silently	Number of dropped response packets.
forwarded Confirmed Class PDUs dropped silently	Number of forwarded packets that have been dropped.

display snmp-agent sys-info

Use **display snmp-agent sys-info** to display SNMP agent system information.

Syntax

display snmp-agent sys-info [**contact** | **location** | **version**] *

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

contact: Displays the system contact.

location: Displays the physical location of the device.

version: Displays the SNMP agent version.

Usage guidelines

If you do not specify any keywords, this command displays all SNMP agent system information.

Examples

Display all SNMP agent system information.

```
<Sysname> display snmp-agent sys-info
   The contact information of the agent:
       NSFOCUS

   The location information of the agent:
       Beijing, China

   The SNMP version of the agent:
       SNMPv3
```

Related commands

snmp-agent sys-info

display snmp-agent trap queue

Use **display snmp-agent trap queue** to display basic information about the trap queue.

Syntax

display snmp-agent trap queue

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display the trap queue configuration and usage status.

```
<Sysname> display snmp-agent trap queue
   Queue size: 100
   Message number: 6
```

Related commands

snmp-agent trap life

snmp-agent trap queue-size

display snmp-agent trapbuffer drop

Use **display snmp-agent trapbuffer drop** to display SNMP notifications drop records.

Syntax

display snmp-agent trapbuffer drop

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Usage guidelines

When an SNMP notification is dropped from the SNMP trap queue, information about the notification is recorded in the SNMP trap buffer.

Examples

Display SNMP notifications drop records.

```
<Sysname> display snmp-agent trapbuffer drop
Current messages:1
Wed Dec 14 10:49:52:656 2019 Notification
nsfocusCfgManEventlog(1.3.6.1.4.1.25506.2.4.2.1) dropped.
```

Current messages in the command output indicates the total number of SNMP notifications drop records in the SNMP trap buffer.

Related commands

reset snmp-agent trapbuffer

display snmp-agent trapbuffer send

Use **display snmp-agent trapbuffer send** to display SNMP notifications sending records.

Syntax

display snmp-agent trapbuffer send

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Usage guidelines

After an SNMP notification is sent, information about the notification is recorded in the SNMP trap buffer. The information includes the content, destination IP address, and sending result of the notification.

Examples

Display SNMP notifications sending records.

```
<Sysname> display snmp-agent trapbuffer send
Current messages:2
Fri Jul 31 10:31:17 2020 Notification nsfocusLogOut(1.3.6.1.4.1.25506.2.2.1.1.3.0.2) failed to be sent to 19.16.11.89.
Fri Jul 31 10:31:17 2020 Notification nsfocusLogOut(1.3.6.1.4.1.25506.2.2.1.1.3.0.2) sent to 192.168.11.89 successfully.
```

Current messages in the command output indicates the total number of SNMP notifications sending records in the SNMP trap buffer.

Related commands

reset snmp-agent trapbuffer

display snmp-agent trap-list

Use **display snmp-agent trap-list** to display SNMP notifications enabling status for modules.

Syntax

display snmp-agent trap-list

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Usage guidelines

If a module has multiple sub-modules and SNMP notifications are enabled for one of its sub-modules, the command output shows that the module is SNMP notifications-enabled.

To determine whether a module supports SNMP notifications, execute the **snmp-agent trap enable ?** command.

The **display snmp-agent trap-list** command output varies by the **snmp-agent trap enable** command configuration and the module configuration.

Examples

Display SNMP notifications enabling status for modules.

```
<Sysname> display snmp-agent trap-list
   arp notification is disabled.
…
```

Related commands

snmp-agent trap enable

display snmp-agent usm-user

Use **display snmp-agent usm-user** to display SNMPv3 user information.

Syntax

display snmp-agent usm-user [**engineid** *engineid* | **group** *group-name* | **username** *user-name*] *

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

engineid *engineid*: Specifies an SNMP engine ID. The engine ID is case insensitive. When an SNMPv3 user is created, the system records the local SNMP entity engine ID. The user becomes invalid when the engine ID changes, and it becomes valid again when the recorded engine ID is restored.

group *group-name*: Specifies an SNMP group by its name. The group name is case sensitive.

username *user-name*: Specifies an SNMPv3 user by its name. The username is case sensitive.

Usage guidelines

This command displays only SNMPv3 users that you have created by using the **snmp-agent usm-user v3** command. To display SNMPv1 or SNMPv2c users created by using the **snmp-agent usm-user** { **v1** | **v2c** } command, use the **display snmp-agent community** command.

Examples

Display information about all SNMPv3 users.

```
<Sysname> display snmp-agent usm-user
   Username: userv3
   Group name: mygroupv3
       Engine ID: 800063A203000FE240A1A6
       Storage-type: nonVolatile
       UserStatus: active
       ACL: 2000

   Username: userv3
   Group name: mygroupv3
       Engine ID: 8000259503000BB3100A508
       Storage-type: nonVolatile
       UserStatus: active
       ACL name: testacl
```

```
Username: userv3code
Role name: groupv3code
           network-operator
    Engine ID: 800063A203000FE240A1A6
    Storage-type: nonVolatile
    UserStatus: active

Username: userv3code
Role name: snmprole
           network-operator
    Engine ID: 800063A280000002BB0001
    Storage-type: nonVolatile
    UserStatus: active
```

Table 11 Command output

Field	Description
Username	SNMP username.
Group name	SNMP group name.
Role name	SNMP user role name.
Engine ID	Engine ID that the SNMP agent used when the SNMP user was created.
Storage-type	Storage type: • **volatile**. • **nonvolatile**. • **permanent**. • **readOnly**. • **other**. For more information about these storage types, see Table 1.
UserStatus	SNMP user status: • **active**—The SNMP user is effective. • **notInService**—The SNMP user is correctly configured but not activated. • **notReady**—The SNMP user configuration is incomplete. • **other**—Any other status.
ACL	Number of the IPv4 ACL. This field appears only when an IPv4 ACL is specified for the SNMPv3 user.
ACL name	Name of the IPv4 ACL. This field appears only when an IPv4 ACL is specified for the SNMPv3 user.
IPv6 ACL	Number of the IPv6 ACL. This field appears only when an IPv6 ACL number is specified for the SNMPv3 user.
IPV6 ACL name	Name of the IPv6 ACL. This field appears only when an IPv6 ACL name is specified for the SNMPv3 user.

Related commands

snmp-agent usm-user v3

enable snmp trap updown

Use **enable snmp trap updown** to enable link state notifications on an interface.

Use **undo enable snmp trap updown** to disable link state notifications on an interface.

Syntax

enable snmp trap updown

undo enable snmp trap updown

Default

Link state notifications are enabled.

Views

Interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

For an interface to generate linkUp/linkDown notifications when its state changes, you must also enable the linkUp/linkDown notification function globally by using the **snmp-agent trap enable standard** [**linkdown** | **linkup**] * command.

Examples

Enable GigabitEthernet 1/0/1 to send linkUp/linkDown SNMP traps to 10.1.1.1 in the community **public**.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable
[Sysname] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname
public
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] enable snmp trap updown
```

Related commands

snmp-agent target-host

snmp-agent trap enable

reset snmp-agent trapbuffer

Use **reset snmp-agent trapbuffer** to clear all records from the SNMP trap buffer.

Syntax

reset snmp-agent trapbuffer

Views

User view

Predefined user roles

network-admin

context-admin

Examples

Clear all records from the SNMP trap buffer.

```
<Sysname> reset snmp-agent trapbuffer
```

Related commands

display snmp-agent trapbuffer drop

display snmp-agent trapbuffer send

snmp virtual-access visible

Use **snmp virtual-access visible** to enable virtual access (VA) interface query and configuration by using MIB objects.

Use **undo snmp virtual-access visible** to restore the default.

Syntax

snmp virtual-access visible

undo snmp virtual-access visible

Default

VA interfaces cannot be queried and configured by using MIB objects.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

By default, VA interfaces cannot be queried and configured by using MIB objects. The device ignores the query and configuration requests from the NMS for VA interfaces. This not only enhances the device efficiency to obtain other interface information and improves user experiences, but also reduces the device workload and avoids waster of CPU resources.

For more information about VA interfaces, see PPP configuration in *Layer 2—WAN Access Configuration Guide*.

To enable VA interface query and configuration by using MIB objects, execute this command.

Examples

Enable VA interface query and configuration by using MIB objects.

```
<Sysname> system-view
[Sysname] snmp virtual-access visible
```

snmp-agent

Use **snmp-agent** to enable the SNMP agent.

Use **undo snmp-agent** to disable the SNMP agent.

Syntax

snmp-agent

undo snmp-agent

Default

The SNMP agent is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

The SNMP agent is automatically enabled when you execute any command that begins with **snmp-agent** except for the **snmp-agent calculate-password** command.

The SNMP agent will fail to be enabled when the port that the agent will listen on is used by another service. You can use the **snmp-agent port** command to specify a listening port. To view the UDP port use information, execute the **display udp verbose** command.

If you disable the SNMP agent, the SNMP settings do not take effect. The **display current-configuration** command does not display the SNMP settings and the SNMP settings will not be saved in the configuration file. For the SNMP settings to take effect, enable the SNMP agent.

Examples

Enable the SNMP agent.

```
<Sysname> system-view
[Sysname] snmp-agent
```

Related commands

display udp verbose (see IP performance optimization commands in *Layer 3—IP Services Configuration Guide*)

snmp-agent port

snmp-agent { inform | trap } source

Use **snmp-agent** { **inform** | **trap** } **source** to specify a source IP address for the informs or traps sent by the SNMP agent.

Use **undo snmp-agent** { **inform** | **trap** } **source** to restore the default.

Syntax

snmp-agent { **inform** | **trap** } **source** *interface-type* { *interface-number* | *interface-number*.*subnumber* }

undo snmp-agent { **inform** | **trap** } **source**

Default

The SNMP agent uses the IP address of the outgoing interface as the source IP address of notifications.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

inform: Specifies informs.

trap: Specifies traps.

interface-type { *interface-number* | *interface-number.subnumber* }: Specifies an interface by its type and number. The *interface-number* argument specifies a main interface number. The *subnumber* argument specifies a subinterface number in the range of 1 to 4094.

Usage guidelines

The **snmp-agent source** command enables the SNMP agent to use the primary IP address of an interface or subinterface as the source IP address in all its SNMP informs or traps, regardless of their outgoing interfaces. An NMS can use this IP address to filter all the informs or traps sent by the SNMP agent.

The source IP address configured by using this command will be used for notifications sent to all NMSs. The source IP address configured by using the **snmp-agent target-host** command will be used for notifications sent to the specified NMS. For a notification sent to a particular NMS, the source IP address specified by using the **snmp-agent target-host** command overrides that specified by using this command.

Make sure the specified interface has been created and assigned a valid IP address. The configuration will fail if the interface has not been created and will take effect only after a valid IP address is assigned to the specified interface.

Examples

Configure the primary IP address of GigabitEthernet 1/0/1 as the source address of SNMP traps.

```
<Sysname> system-view
[Sysname] snmp-agent trap source gigabitethernet 1/0/1
```

Configure the primary IP address of GigabitEthernet 1/0/2 as the source address of SNMP informs.

```
<Sysname> system-view
[Sysname] snmp-agent inform source gigabitethernet 1/0/2
```

Related commands

snmp-agent target-host

snmp-agent trap enable

snmp-agent calculate-password

Use **snmp-agent calculate-password** to calculate the encrypted form for a key in plaintext form.

Syntax

snmp-agent calculate-password *plain-password* **mode** { **3desmd5** | **3dessha** | **md5** | **sha** } { **local-engineid** | **specified-engineid** *engineid* }

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

plain-password: Specifies a key in plaintext form. The *plain-password* argument is a case-sensitive string of 1 to 64 characters.

mode: Specifies an authentication algorithm and encryption algorithm. The device supports the HMAC-MD5 and HMAC-SHA1 authentication algorithms. The HMAC-MD5 algorithm is faster than the HMAC-SHA1 algorithm. The HMAC-SHA1 algorithm provides more security than the HMAC-MD5 algorithm. The AES, 3DES, and DES encryption algorithms (in descending order of security strength) are available for the device. A more secure algorithm calculates slower. DES is enough to meet general security requirements.

- **3desmd5**: Calculates the encrypted form for the encryption key by using the 3DES encryption algorithm and HMAC-MD5 authentication algorithm.
- **3dessha**: Calculates the encrypted form for the encryption key by using the 3DES encryption algorithm and HMAC-SHA1 authentication algorithm.
- **md5**: Calculates the encrypted form for the authentication key or encryption key by using the HMAC-MD5 authentication algorithm and AES or DES encryption algorithm. When the HMAC-MD5 authentication algorithm is used, you can get the same authentication key or encryption key in encrypted form regardless of whether the AES or DES encryption algorithm is used.
- **sha**: Calculates the encrypted form for the authentication key or encryption key by using HMAC-SHA1 authentication algorithm and AES or DES encryption algorithm. When the HMAC-SHA1 authentication algorithm is used, you can get the same authentication key or encryption key in encrypted form regardless of whether the AES or DES encryption algorithm is used.

local-engineid: Uses the local engine ID to calculate the encrypted form for the key. You can configure the local engine ID by using the **snmp-agent local-engineid** command.

specified-engineid *engineid*: Uses a user-defined engine ID to calculate the encrypted form for the key. The *engineid* argument is an even number of case-insensitive hexadecimal characters. All-zero and all-F strings are invalid. The even number is in the range of 10 to 64.

Usage guidelines

Make sure the SNMP agent is enabled before you execute the **snmp-agent calculate-password** command.

For security purposes, use the encrypted-form key generated by using this command when you create SNMPv3 users by specifying the **cipher** keyword in the **snmp-agent usm-user v3** command.

The encrypted form of the key is valid only under the engine ID specified for key conversion.

Examples

Use the local engine ID and the HMAC-SHA1 algorithm to calculate the encrypted form for key **authkey**.

```
<Sysname> system-view
[Sysname] snmp-agent calculate-password authkey mode sha local-engineid
The encrypted key is: 09659EC5A9AE91BA189E5845E1DDE0CC
```

Related commands

snmp-agent local-engineid

snmp-agent usm-user v3

snmp-agent community

Use **snmp-agent community** to configure an SNMPv1 or SNMPv2c community.

Use **undo snmp-agent community** to delete an SNMPv1 or SNMPv2c community.

Syntax

In VACM mode:

snmp-agent community { **read** | **write** } [**simple** | **cipher**] *community-name* [**mib-view** *view-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

undo snmp-agent community [**cipher**] *community-name*

In RBAC mode:

snmp-agent community [**simple** | **cipher**] *community-name* **user-role** *role-name* [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

undo snmp-agent community [**cipher**] *community-name*

Default

No SNMPv1 or SNMPv2c communities exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

read: Assigns the specified community read-only access to MIB objects. A read-only community can only inquire MIB information.

write: Assigns the specified community read and write access to MIB objects. A read and write community can configure MIB information.

simple: Specifies a community name in plaintext form. For security purposes, the community name specified in plaintext form will be stored in encrypted form.

cipher: Specifies a community name in encrypted form.

community-name: Specifies the community name. The plaintext form is a case-sensitive string of 1 to 32 characters. The encrypted form is a case-sensitive string of 33 to 73 characters. Input a string as escape characters after a backslash (\).

mib-view *view-name*: Specifies the MIB view available for the community. The *view-name* argument represents a MIB view name, a case-sensitive string of 1 to 32 characters. A MIB view represents a set of accessible MIB objects. If you do not specify a view, the specified community can access the MIB objects in the default MIB view **ViewDefault**.

user-role *role-name*: Specifies a user role name for the community, a case-sensitive string of 1 to 63 characters.

acl: Specifies a basic or advanced IPv4 ACL for the community.

ipv4-acl-number: Specifies a basic or advanced IPv4 ACL by its number. The basic IPv4 ACL number is in the range of 2000 to 2999. The advanced IPv4 ACL number is in the range of 3000 to 3999.

name *ipv4-acl-name*: Specifies a basic or advanced IPv4 ACL by its name, a case-insensitive string of 1 to 63 characters.

acl ipv6: Specifies a basic or advanced IPv6 ACL for the community.

ipv6-acl-number: Specifies a basic or advanced IPv6 ACL by its number. The basic IPv6 ACL number is in the range of 2000 to 2999. The advanced IPv6 ACL number is in the range of 3000 to 3999.

name *ipv6-acl-name*: Specifies a basic or advanced IPv6 ACL by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

Only users with the network-admin, context-admin, or level-15 user role can execute this command. Users with other user roles cannot execute this command even if these roles are granted access to commands of the SNMP feature or this command.

An SNMP community is identified by a community name. It contains a set of NMSs and SNMP agents. Devices in an SNMP community authenticate each other by using the community name. An NMS and an SNMP agent can communicate only when they use the same community name.

Typically, **public** is used as the read-only community name and **private** is used as the read and write community name. To enhance security, you can assign your SNMP communities a name other than **public** and **private**.

The **snmp-agent community** command allows you to use either of the following modes to control SNMP community access to MIB objects:

- **View-based access control model**—The VACM mode controls access to MIB objects by assigning MIB views to SNMP communities.
- **Role based access control**—The RBAC mode controls access to MIB objects by assigning user roles to SNMP communities.
  - The network-admin, context-admin, and level-15 user roles have the read and write access to all MIB objects.
  - The network-operator user role and context-operator user role have the read-only access to all MIB objects.

  For more information about user roles, see *Fundamentals Configuration Guide*.

RBAC mode controls access on a per MIB object basis, and VACM mode controls access on a MIB view basis. As a best practice to enhance MIB security, use RBAC mode.

You can create a maximum of 10 SNMP communities by using the **snmp-agent community** command.

If you execute the command multiple times to specify the same community name but different other settings each time, the most recent configuration takes effect.

To set and save a community name in plain text, do not specify the **simple** or **cipher** keyword.

The ACL is used to filter illegitimate NMSs.

- If the specified ACL does not exist, or the specified ACL does not contain any rule, all NMSs can access the device.
- If a VPN instance is specified in an ACL rule, the rule applies only to the packets of the VPN instance. If no VPN instance is specified in an ACL rule, the rule applies only to the packets on the public network.
- If you specify an ACL and the ACL has rules, only NMSs permitted by the ACL can access the device.

For more information about ACL, see *ACL and QoS Configuration Guide*.

You can also create an SNMP community by using the **snmp-agent usm-user** { **v1** | **v2c** } and **snmp-agent group** { **v1** | **v2c** } commands. These two commands create an SNMPv1 or

SNMPv2c user and the group to which the user is assigned. The system automatically creates an SNMP community by using the SNMPv1 or SNMPv2c username.

The **display snmp-agent community** command displays information only about communities created and saved in plaintext form.

Examples

Create the read-only community with the plaintext form name **readaccess** so an SNMPv1 or SNMPv2c NMS can use the community name **readaccess** to read the MIB objects in the default view **ViewDefault**.

```
<Sysname> system-view
[Sysname] snmp-agent sys-info version v1 v2c
[Sysname] snmp-agent community read simple readaccess
```

Create the read and write community with the plaintext form name **writeaccess** so only the SNMPv2c NMS at 1.1.1.1 can use the community name **writeaccess** to read or set the MIB objects in the default view **ViewDefault**.

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0.0.0.0
[Sysname-acl-ipv4-basic-2001] rule deny source any
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] snmp-agent sys-info version v2c
[Sysname] snmp-agent community write simple writeaccess acl 2001
```

Create the read and write community with the plaintext form name **writeaccess** so only the SNMPv2c NMS at 1.1.1.2 can use the community name **writeaccess** to read or set the MIB objects in the default view **ViewDefault**.

```
<Sysname> system-view
[Sysname] acl basic name testacl
[Sysname-acl-ipv4-basic-testacl] rule permit source 1.1.1.2 0.0.0.0
[Sysname-acl-ipv4-basic-testacl] rule deny source any
[Sysname-acl-ipv4-basic-testacl] quit
[Sysname] snmp-agent sys-info version v2c
[Sysname] snmp-agent community write simple writeaccess acl name testacl
```

Create the read and write community with the plaintext form name **wr-sys-acc** so an SNMPv1 or SNMPv2c NMS can use the community name **wr-sys-acc** to read or set the MIB objects in the system subtree (OID 1.3.6.1.2.1.1).

```
<Sysname> system-view
[Sysname] snmp-agent sys-info version v1 v2c
[Sysname] undo snmp-agent mib-view ViewDefault
[Sysname] snmp-agent mib-view included test system
[Sysname] snmp-agent community write simple wr-sys-acc mib-view test
```

Related commands

display snmp-agent community

snmp-agent mib-view

snmp-agent community-map

Use **snmp-agent community-map** to map an SNMP community to an SNMP context.

Use **undo snmp-agent community-map** to delete the mapping between an SNMP community and an SNMP context.

Syntax

snmp-agent community-map *community-name* **context** *context-name*

undo snmp-agent community-map *community-name* **context** *context-name*

Default

No mapping exists between an SNMP community and an SNMP context.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

community-name: Specifies an SNMP community, a case-sensitive string of 1 to 32 characters.

context-name: Specifies an SNMP context, a case-sensitive string of 1 to 32 characters.

Usage guidelines

This command enables a module on an agent to obtain the context mapped to a community name when an NMS accesses the agent by using SNMPv1 or SNMPv2c.

You can configure a maximum of 10 community-context mappings on the device.

Examples

Map SNMP community **private** to SNMP context **trillcontext**.

```
<Sysname> system-view
[Sysname] snmp-agent community-map private context testcontext
```

Related commands

display snmp-agent community

snmp-agent context

Use **snmp-agent context** to create an SNMP context.

Use **undo snmp-agent context** to delete an SNMP context.

Syntax

snmp-agent context *context-name*

undo snmp-agent context *context-name*

Default

No SNMP contexts exist.

Views

System view

Predefined use roles

network-admin

context-admin

Parameters

context-name: Specifies an SNMP context, a case-sensitive string of 1 to 32 characters.

Usage guidelines

For an NMS and an SNMP agent to communicate, configure the same SNMP context for them or do not configure a context for the NMS.

You can create a maximum of 20 SNMP contexts.

Examples

Create SNMP context **trillcontext**.

```
<Sysname> system-view
[Sysname] snmp-agent context testcontext
```

Related commands

display snmp-agent context

snmp-agent group

Use **snmp-agent group** to create an SNMP group.

Use **undo snmp-agent group** to delete an SNMP group.

Syntax

- SNMPv1 and SNMP v2c:

  snmp-agent group { **v1** | **v2c** } *group-name* [**notify-view** *view-name* | **read-view** *view-name* | **write-view** *view-name*] * [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

  undo snmp-agent group { **v1** | **v2c** } *group-name*

- SNMPv3:

  snmp-agent group v3 *group-name* [**authentication** | **privacy**] [**notify-view** *view-name* | **read-view** *view-name* | **write-view** *view-name*] * [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

  undo snmp-agent group v3 *group-name* [**authentication** | **privacy**]

Default

No SNMP groups exist.

Views

System view

Predefined use roles

network-admin

context-admin

Parameters

v1: Specifies SNMPv1.

v2c: Specifies SNMPv2c.

v3: Specifies SNMPv3.

group-name: Specifies an SNMP group name, a case-sensitive string of 1 to 32 characters.

authentication: Specifies the authentication without privacy security model for the SNMPv3 group.

privacy: Specifies the authentication with privacy security model for the SNMPv3 group.

notify-view *view-name*: Specifies a notify MIB view. The *view-name* represents a MIB view name, a case-sensitive string of 1 to 32 characters. The SNMP agent sends notifications to the users in the specified group only for the MIB objects included in the notify view. If you do not specify a notify view, the SNMP agent does not send any notification to the users in the specified group.

read-view *view-name*: Specifies a read-only MIB view. The *view-name* represents a MIB view name, a case-sensitive string of 1 to 32 characters. If you do not specify a read-only MIB view, the SNMP group has read access to the default view **ViewDefault**.

write-view *view-name:* Specifies a read and write MIB view. The *view-name* represents a MIB view name, a case-sensitive string of 1 to 32 characters. If you do not specify a read and write view, the SNMP group cannot set any MIB object on the SNMP agent.

acl: Specifies a basic or advanced IPv4 ACL for the group.

ipv4-acl-number: Specifies a basic or advanced IPv4 ACL by its number. The basic IPv4 ACL number is in the range of 2000 to 2999. The advanced IPv4 ACL number is in the range of 3000 to 3999.

name *ipv4-acl-name*: Specifies a basic or advanced IPv4 ACL by its name, a case-insensitive string of 1 to 63 characters.

acl ipv6: Specifies a basic or advanced IPv6 ACL for the group.

ipv6-acl-number: Specifies a basic or advanced IPv6 ACL by its number. The basic IPv6 ACL number is in the range of 2000 to 2999. The advanced IPv6 ACL number is in the range of 3000 to 3999.

name *ipv6-acl-name*: Specifies a basic or advanced IPv6 ACL by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

Only users with the network-admin, context-admin, or level-15 user role can execute this command. Users with other user roles cannot execute this command even if these roles are granted access to commands of the SNMP feature or this command.

All users in an SNMP group share the security model and access rights of the group.

You can create a maximum of 20 SNMP groups, including SNMPv1, SNMPv2c, and SNMPv3 groups.

All SNMPv3 users in a group share the same security model, but can use different authentication and encryption key settings. To implement a security model for a user and avoid SNMP communication failures, make sure the security model configuration for the group and the security key settings for the user are compliant with Table 12 and match the settings on the NMS.

Table 12 Basic security setting requirements for different security models

Security model	Security model keyword for the group	Security key settings for the user	Remarks
Authentication with privacy	**privacy**	Authentication key, encryption key	If the authentication key or the encryption key is not configured, SNMP communication will fail.
Authentication without privacy	**authentication**	Authentication key	If no authentication key is configured, SNMP communication will fail. The encryption key (if any) for the user does not take effect.

Security model	Security model keyword for the group	Security key settings for the user	Remarks
No authentication, no privacy	Neither **authentication** nor **privacy**	None	The authentication and encryption keys, if configured, do not take effect.

You can specify an ACL for the user and group, respectively, to filter illegitimate NMSs. Only the NMSs permitted by the ACLs for both the user and group can access the SNMP agent. The following rules apply to the ACLs for the user and group:

- If the specified ACL does not exist, or the specified ACL does not contain any rule, all NMSs can access the device.
- If a VPN instance is specified in an ACL rule, the rule applies only to the packets of the VPN instance. If no VPN instance is specified in an ACL rule, the rule applies only to the packets on the public network.
- If you specify an ACL and the ACL has rules, only NMSs permitted by the ACL can access the device.

For more information about ACL, see *ACL and QoS Configuration Guide*.

Examples

Create the SNMPv3 group **group1**.

```
<Sysname> system-view
[Sysname] snmp-agent group v3 group1
```

Related commands

display snmp-agent group

snmp-agent mib-view

snmp-agent usm-user

snmp-agent local-engineid

Use **snmp-agent local-engineid** to set an SNMP engine ID.

Use **undo snmp-agent local-engineid** to restore the default.

Syntax

snmp-agent local-engineid *engineid*

undo snmp-agent local-engineid

Default

The SNMP engine ID of the device is the company ID plus the device ID.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

engineid: Specifies an SNMP engine ID, a case-insensitive hexadecimal string. Its length is an even number in the range of 10 to 64. All-zero and all-F strings are invalid.

Usage guidelines

An SNMP engine ID uniquely identifies a device in an SNMP managed network. Make sure the local SNMP engine ID is unique within your SNMP managed network to avoid communication problems.

If you have configured SNMPv3 users, change the local SNMP engine ID only when necessary. The change can void the SNMPv3 usernames and encrypted keys you have configured.

You can use the default engine ID or configure an easy-to-remember engine ID based on the network plan. For example, you can set the engine ID for device 1 on the first floor of building A to 000Af0010001 and device 2 to 000Af0010002.

Examples

Set the local SNMP engine ID to **123456789A**.

```
<Sysname> system-view
[Sysname] snmp-agent local-engineid 123456789A
```

Related commands

display snmp-agent local-engineid

snmp-agent usm-user

snmp-agent log

Use **snmp-agent log** to enable SNMP logging.

Use **undo snmp-agent log** to disable SNMP logging.

Syntax

snmp-agent log { **all** | **authfail** | **get-operation** | **set-operation** }

undo snmp-agent log { **all** | **authfail** | **get-operation** | **set-operation** }

Default

SNMP logging operations are disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

all: Enables logging SNMP authentication failures, Get operations, and Set operations.

authfail: Enables logging SNMP authentication failures.

get-operation: Enables logging SNMP Get operations.

set-operation: Enables logging SNMP Set operations.

Usage guidelines

Use SNMP logging to record the SNMP operations performed on the SNMP agent or authentication failures from the NMS to the agent for auditing NMS behaviors. The SNMP agent sends log data to

the information center. You can configure the information center to output the data to a destination as needed.

Examples

Enable logging SNMP Get operations.

```
<Sysname> system-view
[Sysname] snmp-agent log get-operation
```

Enable logging SNMP Set operations.

```
<Sysname> system-view
[Sysname] snmp-agent log set-operation
```

Enable logging SNMP authentication failures.

```
<Sysname> system-view
[Sysname] snmp-agent log authfail
```

snmp-agent mib-view

Use **snmp-agent mib-view** to create or update a MIB view.

Use **undo snmp-agent mib-view** to delete a MIB view.

Syntax

snmp-agent mib-view { **excluded** | **included** } *view-name oid-tree* [**mask** *mask-value*]

undo snmp-agent mib-view *view-name*

Default

The system creates the **ViewDefault** view when the SNMP agent is enabled. In this default MIB view, all MIB objects in the **iso** subtree but the **snmpUsmMIB**, **snmpVacmMIB**, and **snmpModules.18** subtrees are accessible.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

excluded: Denies access to any node in the specified MIB subtree.

included: Permits access to all the nodes in the specified MIB subtree.

view-name: Specifies a view name, a case-sensitive string of 1 to 32 characters.

oid-tree: Specifies a MIB subtree by its root node's OID (for example, **1.3.6.1.2.1.1**) or object name (for example, **system**). The *oid-tree* argument is a case-sensitive string of 1 to 255 characters. An OID is a dotted numeric string that uniquely identifies an object in the MIB tree.

mask *mask-value*: Sets a MIB subtree mask, a case-insensitive hexadecimal string. Its length is an even number in the range of 1 to 32.

Usage guidelines

A MIB view represents a set of MIB objects (or MIB object hierarchies) with certain access privilege. The MIB objects included in the MIB view are accessible while those excluded from the MIB view are inaccessible.

Each *view-name oid-tree* pair represents a view record. If you specify the same record with different MIB subtree masks multiple times, the most recent configuration takes effect.

Be cautious with deleting the default MIB view. The operation blocks the access to any MIB object on the device from NMSs that use the default view.

Examples

Include the **mib-2** (OID 1.3.6.1.2.1) subtree in the **mibtest** view and exclude the **system** subtree from this view.

```
<Sysname> system-view
[Sysname] snmp-agent sys-info version v1
[Sysname] snmp-agent mib-view included mibtest 1.3.6.1.2.1
[Sysname] snmp-agent mib-view excluded mibtest system
[Sysname] snmp-agent community read public mib-view mibtest
```

An SNMPv1 NMS in the **public** community can query the objects in the **mib-2** subtree but not any object (for example, the **sysDescr or sysObjectID** node) in the **system** subtree.

Related commands

display snmp-agent mib-view

snmp-agent group

snmp-agent packet max-size

Use **snmp-agent packet max-size** to set the maximum size (in bytes) of SNMP packets that the SNMP agent can receive or send.

Use **undo snmp-agent packet max-size** to restore the default.

Syntax

snmp-agent packet max-size *byte-count*

undo snmp-agent packet max-size

Default

An SNMP agent can process SNMP packets with a maximum size of 1500 bytes.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

byte-count: Sets the maximum size (in bytes) of SNMP packets that the SNMP agent can receive or send. The value range is 484 to 17940.

Usage guidelines

If any device on the path to the NMS does not support packet fragmentation, limit the SNMP packet size to prevent large-sized packets from being discarded. For most networks, the default value is sufficient.

Examples

Set the maximum SNMP packet size to 1024 bytes.

```
<Sysname> system-view
```

```
[Sysname] snmp-agent packet max-size 1024
```

snmp-agent port

Use **snmp-agent port** to specify an SNMP listening port.

Use **undo snmp-agent port** to restore the default.

Syntax

snmp-agent port *port-number*

undo snmp-agent port

Default

The SNMP listening port is UDP port 161.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

port-number: Specifies an SNMP listening port by its number in the range of 1 to 65535.

Usage guidelines

The SNMP agent will fail to be enabled when the port that the agent will listen on is used by another service. You can use the **snmp-agent port** command to change the SNMP listening port. As a best practice, execute the **display udp verbose** command to view the UDP port use information before specifying a new SNMP listening port.

After changing the SNMP listening port, the NMS can perform SNMP set and get operations on the device only after reconnecting the device by using the new port number.

Examples

Specify **5555** as the SNMP listening port.

```
<Sysname> system-view
[Sysname] snmp-agent port 5555
```

Related commands

display udp verbose (see IP performance optimization commands in *Layer 3—IP Services Configuration Guide*)

snmp-agent remote

Use **snmp-agent remote** to set an SNMP engine ID for a remote SNMP entity.

Use **undo snmp-agent remote** to delete the SNMP engine ID of a remote SNMP entity.

Syntax

snmp-agent remote { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] **engineid** *engineid*

undo snmp-agent remote { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]

Default

No SNMP engine IDs are configured for remote SNMP entities.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-address: Specifies a remote SNMP entity by its IPv4 address.

ipv6 *ipv6-address*: Specifies a remote SNMP entity by its IPv6 address.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the remote SNMP entity belongs. The *vpn-instance-name* argument represents the VPN instance name. a case-sensitive string of 1 to 31 characters. If the SNMP entity belongs to the public network, do not specify this option.

engineid: Specifies the SNMP engine ID of the remote SNMP entity. This argument is a case-insensitive hexadecimal string. Its length is an even number in the range of 10 to 64. All-zero and all-F strings are invalid.

Usage guidelines

To send informs to an NMS, you must configure the SNMP engine ID of the NMS on the SNMP agent.

The NMS accepts the SNMPv3 informs from the SNMP agent only if the engine ID in the informs is the same as its local engine ID.

You can configure a maximum of 20 remote SNMP engine IDs.

Examples

Set the SNMP engine ID to **123456789A** for the remote entity **10.1.1.1**.

```
<Sysname> system-view
[Sysname] snmp-agent remote 10.1.1.1 engineid 123456789A
```

Related commands

display snmp-agent remote

snmp-agent sys-info contact

Use **snmp-agent sys-info contact** to configure the system contact.

Use **undo snmp-agent sys-info contact** to restore the default contact.

Syntax

snmp-agent sys-info contact *sys-contact*

undo snmp-agent sys-info contact

Default

The system contact is NSFOCUS.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

sys-contact: Specifies the system contact, a case-sensitive string of 1 to 255 characters.

Usage guidelines

Configure the system contact for system maintenance and management.

Examples

Configure the system contact as **Dial System Operator # 27345**.

```
<Sysname> system-view
[Sysname] snmp-agent sys-info contact Dial System Operator # 27345
```

Related commands

display snmp-agent sys-info

snmp-agent sys-info location

Use **snmp-agent sys-info location** to configure the system location.

Use **undo snmp-agent sys-info location** to restore the default location.

Syntax

snmp-agent sys-info location *sys-location*

undo snmp-agent sys-info location

Default

The system location is **Hangzhou, China**.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

sys-location: Specifies the system location, a case-sensitive string of 1 to 255 characters.

Usage guidelines

Configure the location of the device for system maintenance and management.

Examples

Configure the system location as **Room524-row1-3**.

```
<Sysname> system-view
[Sysname] snmp-agent sys-info location Room524-row1-3
```

Related commands

display snmp-agent sys-info

snmp-agent sys-info version

Use **snmp-agent sys-info version** to specify the SNMP version.

Use **undo snmp-agent sys-info version** to restore the default.

Syntax

snmp-agent sys-info contact version { **all** | { **v1** | **v2c** | **v3** } * }

undo snmp-agent sys-info version { **all** | { **v1** | **v2c** | **v3** } * }

Default

SNMPv3 is enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

all: Specifies SNMPv1, SNMPv2c, and SNMPv3.

v1: Specifies SNMPv1.

v2c: Specifies SNMPv2c.

v3: Specifies SNMPv3.

Usage guidelines

Configure the SNMP agent with the same SNMP version as the NMS for successful communications between them.

The community name and data carried in SNMPv1 and SNMPv2c messages are in plaintext form, putting the SNMP communication at risks. As a best practice, use SNMPv3.

SNMP notifications over IPv6 is supported only when you specify SNMPv2c or SNMPv3.

Examples

Enable SNMPv3.

```
<Sysname> system-view
[Sysname] snmp-agent sys-info version v3
```

Related commands

display snmp-agent sys-info

snmp-agent target-host

Use **snmp-agent target-host** to configure an SNMP notification target host.

Use **undo snmp-agent target-host** to remove an SNMP notification target host.

Syntax

snmp-agent target-host inform address udp-domain { *ipv4-target-host* | **ipv6** *ipv6-target-host* } [**source-ip** *source-ip-address* | **udp-port** *port-number* | **vpn-instance** *vpn-instance-name*] * **params securityname** *security-string* { **v2c** | **v3** [**authentication** | **privacy**] }

snmp-agent target-host trap address udp-domain { *ipv4-target-host* | **ipv6** *ipv6-target-host* } [**source-ip** *source-ip-address* | **udp-port** *port-number* | **vpn-instance** *vpn-instance-name*] * [**params securityname** *security-string* [**v1** | **v2c** | **v3** [**authentication** | **privacy**]]]

undo snmp-agent target-host { **trap** | **inform** } **address udp-domain** { *ipv4-target-host* | **ipv6** *ipv6-target-host* } **params securityname** *security-string* [**vpn-instance** *vpn-instance-name*]

Default

No SNMP notification target hosts exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

inform: Specifies a host that receives informs.

trap: Specifies a host that receives traps.

address: Specifies the destination address of SNMP notifications.

udp-domain: Specifies UDP as the transport protocol.

ipv4-target-host: Specifies a target host by its IPv4 address or host name. The host name is a case-insensitive string of 1 to 253 characters. The string can only contain letters, numbers, hyphens (-), underscores (_), and dots (.). If you specify a host name, the IPv4 address of the target host can be obtained.

ipv6 *ipv6-target-host*: Specifies a target host by its IPv6 address or host name. The host name is a case-insensitive string of 1 to 253 characters, which only contains letters, numbers, hyphens (-), underscores (_), and dots (.). If you specify a host name, the IPv6 address of the target host can be obtained. If you specify an IPv6 address, the address cannot be a link local address.

source-ip *source-ip-address*: Specifies the source IP address for SNMP notifications. If you do not specify this option, SNMP notifications uses the source IP address configured by using the **snmp-agent** { **inform** | **trap** } **source** command.

udp-port *port-number*: Specifies the UDP port for SNMP notifications. The default port number is 162.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the target host belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the target host belongs to the public network, do not specify this option.

params securityname *security-string*: Specifies the authentication parameter. The *security-string* argument specifies an SNMPv1 or SNMPv2c community name or an SNMPv3 username, a case-sensitive string of 1 to 32 characters.

v1: Specifies SNMPv1.

v2c: Specifies SNMPv2c.

v3: Specifies SNMPv3.

- **authentication**: Specifies the security model to be authentication without privacy. You must specify the authentication key when you create the SNMPv3 user.

- **privacy**: Specifies the security model to be authentication with privacy. You must specify the authentication key and encryption key when you create the SNMPv3 user.

Usage guidelines

You can specify multiple SNMP notification target hosts.

Make sure the SNMP agent uses the same UDP port for SNMP notifications as the target host. Typically, NMSs, for example, IMC and MIB Browser, use port 162 for SNMP notifications as defined in the SNMP protocols.

If none of the keywords **v1**, **v2c**, or **v3** is specified, SNMPv1 is used. Make sure the SNMP agent uses the same SNMP version as the target host so the host can receive the notification.

If neither **authentication** nor **privacy** is specified, the security model is no authentication, no privacy.

Examples

Configure the SNMP agent to send SNMPv3 traps to 10.1.1.1 by using the username **public**.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable standard
[Sysname] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname
public v3
```

Related commands

snmp-agent { **inform** | **trap** } **source**

snmp-agent trap enable

snmp-agent trap life

snmp-agent trap enable

Use **snmp-agent trap enable** to enable SNMP notifications.

Use **undo snmp-agent trap enable** to disable SNMP notifications.

Syntax

snmp-agent trap enable [**configuration** | *protocol* | **standard** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**] * | **system**]

undo snmp-agent trap enable [**configuration** | *protocol* | **standard** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**] * | **system**]

Default

SNMP configuration notifications, standard notifications, and system notifications are enabled. Whether other SNMP notifications are enabled varies by module.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

configuration: Specifies configuration notifications. If configuration notifications are enabled, the system checks the running configuration and the startup configuration every 10 minutes for any change and generates a notification for the most recent change.

protocol: Specifies protocol module notifications. You can use the **snmp-agent trap enable ?** command to obtain the value of this argument. For more information about this argument, see the command reference for each module.

standard: Specifies SNMP standard notifications.

Table 13 Standard SNMP notifications

Keyword	Definition
authentication	Authentication failure notification sent when an NMS fails to be authenticated by the SNMP agent.
coldstart	Notification sent when the device restarts.
linkdown	Notification sent when the link of a port goes down.
linkup	Notification sent when the link of a port comes up.
warmstart	Notification sent when the SNMP agent restarts.

system: Specifies system notifications sent when the system time is modified, the system reboots, or the main system software image is not available.

Usage guidelines

To enable the device to send SNMP notifications for a protocol, first enable the protocol and then enable SNMP notifications for the protocol. For SNMP notifications to be sent correctly, you must also configure the notification sending parameters as required.

If no optional parameters are specified, this command or its **undo** form enables or disables all SNMP notifications supported by the device.

SNMP notifications over IPv6 is supported only when you specify SNMPv2c or SNMPv3.

Examples

Enable the SNMP agent to send SNMP authentication failure notifications.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable standard authentication
```

Related commands

snmp-agent target-host

snmp-agent sys-info version

snmp-agent trap if-mib link extended

Use **snmp-agent trap if-mib link extended** to configure the SNMP agent to send extended linkUp/linkDown notifications.

Use **undo snmp-agent trap if-mib link extended** to restore the default.

Syntax

snmp-agent trap if-mib link extended

undo snmp-agent trap if-mib link extended

Default

The SNMP agent sends standard linkUp/linkDown notifications.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

Extended linkUp and linkDown notifications add interface name, interface type, and interface description to the standard linkUp/linkDown notifications for fast failure identification.

When you use this command, make sure the NMS supports the extended linkup and linkDown notifications.

Examples

Enable extended linkUp/linkDown notifications.

```
<Sysname> system-view
[Sysname] snmp-agent trap if-mib link extended
```

snmp-agent trap life

Use **snmp-agent trap life** to set the lifetime of notifications in the SNMP notification queue.

Use **undo snmp-agent trap life** to restore the default notification lifetime.

Syntax

snmp-agent trap life *seconds*

undo snmp-agent trap life

Default

The SNMP notification lifetime is 120 seconds.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Sets a lifetime in the range of 1 to 2592000, in seconds.

Usage guidelines

When congestion occurs, the SNMP agent buffers notifications in a queue. The notification lifetime sets how long a notification can stay in the queue. A notification is deleted when its lifetime expires.

Examples

Set the SNMP notification lifetime to 60 seconds.

```
<Sysname> system-view
[Sysname] snmp-agent trap life 60
```

Related commands

snmp-agent target-host

snmp-agent trap enable

snmp-agent trap queue-size

snmp-agent trap log

Use **snmp-agent trap log** to enable SNMP notification logging.

Use **undo snmp-agent trap log** to disable SNMP notification logging.

Syntax

snmp-agent trap log

undo snmp-agent trap log

Default

SNMP notification logging is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

Use SNMP notification logging to record SNMP notifications sent by the SNMP agent for notification tracking. The SNMP agent sends the logs to the information center. You can configure the information center to output the logs to a destination as needed.

Examples

Enable SNMP notification logging.

```
<Sysname> system-view
[Sysname] snmp-agent trap log
```

snmp-agent trap queue-size

Use **snmp-agent trap queue-size** to set the SNMP notification queue size.

Use **undo snmp-agent trap queue-size** to restore the default queue size.

Syntax

snmp-agent trap queue-size *size*

undo snmp-agent trap queue-size

Default

The SNMP notification queue can store a maximum of 100 notifications.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

size: Specifies the maximum number of notifications that the SNMP notification queue can hold. The value range is 1 to 1000.

Usage guidelines

When congestion occurs, the SNMP agent buffers notifications in a queue. SNMP notification queue size sets the maximum number of notifications that this queue can hold. When the queue size is reached, the oldest notifications are dropped for new notifications.

Examples

Set the SNMP notification queue size to 200.

```
<Sysname> system-view
[Sysname] snmp-agent trap queue-size 200
```

Related commands

snmp-agent target-host

snmp-agent trap enable

snmp-agent trap life

snmp-agent usm-user { v1 | v2c }

Use **snmp-agent usm-user** { **v1** | **v2c** } to create an SNMPv1 or SNMPv2c user.

Use **undo snmp-agent usm-user** { **v1** | **v2c** } to delete an SNMPv1 or SNMPv2c user.

Syntax

snmp-agent usm-user { **v1** | **v2c** } *user-name group-name* [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

undo snmp-agent usm-user { **v1** | **v2c** } *user-name*

Default

No SNMPv1 or SNMPv2c users exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

v1: Specifies SNMPv1.

v2c: Specifies SNMPv2c.

user-name: Specifies an SNMP username, a case-sensitive string of 1 to 32 characters.

group-name: Specifies an SNMPv1 or SNMPv2c group name, a case-sensitive string of 1 to 32 characters. The group can be one that has been created or not. The user takes effect only after you create the group.

acl: Specifies a basic or advanced IPv4 ACL for the user.

ipv4-acl-number: Specifies a basic or advanced IPv4 ACL by its number. The basic IPv4 ACL number is in the range of 2000 to 2999. The advanced IPv4 ACL number is in the range of 3000 to 3999.

name *ipv4-acl-name*: Specifies a basic or advanced IPv4 ACL by its name, a case-insensitive string of 1 to 63 characters.

acl ipv6: Specifies a basic or advanced IPv6 ACL for the user.

ipv6-acl-number: Specifies a basic or advanced IPv6 ACL by its number. The basic IPv6 ACL number is in the range of 2000 to 2999. The advanced IPv6 ACL number is in the range of 3000 to 3999.

name *ipv6-acl-name*: Specifies a basic or advanced IPv6 ACL by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

Only users with the network-admin, context-admin, or level-15 user role can execute this command. Users with other user roles cannot execute this command even if these roles are granted access to commands of the SNMP feature or this command.

On an SNMPv1 or SNMPv2c network, NMSs and agents authenticate each other by using the community name. On an SNMPv3 network, NMSs and agents authenticate each other by using the username.

You can create an SNMPv1 or SNMPv2c community by using either of the following ways:

- Execute the **snmp-agent community** command.
- Execute the **snmp-agent usm-user** { **v1** | **v2c** } and **snmp-agent group** { **v1** | **v2c** } commands to create an SNMPv1 or SNMPv2c user and the group that the user is assigned to. The system automatically creates an SNMP community by using the SNMPv1 or SNMPv2c username.

The **display snmp-agent community** command displays information only about communities created and saved in plaintext form.

You can specify an ACL for the user and group, respectively, to filter illegitimate NMSs. Only the NMSs permitted by the ACLs for both the user and group can access the SNMP agent. The following rules apply to the ACLs for the user and group:

- If the specified ACL does not exist, or the specified ACL does not contain any rule, all NMSs can access the device.
- If a VPN instance is specified in an ACL rule, the rule applies only to the packets of the VPN instance. If no VPN instance is specified in an ACL rule, the rule applies only to the packets on the public network.
- If you specify an ACL and the ACL has rules, only NMSs permitted by the ACL can access the device.

For more information about ACL, see *ACL and QoS Configuration Guide*.

Examples

Add the user **userv2c** to the SNMPv2c group **readCom** so an NMS can use the protocol SNMPv2c and the read-only community name **userv2c** to access the device.

```
<Sysname> system-view
[Sysname] snmp-agent sys-info version v2c
[Sysname] snmp-agent group v2c readCom
[Sysname] snmp-agent usm-user v2c userv2c readCom
```

Add the user **userv2c** in the SNMPv2c group **readCom** so only the NMS at 1.1.1.1 can use the protocol SNMPv2c and read-only community name **userv2c** to access the device.

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0.0.0.0
[Sysname-acl-ipv4-basic-2001] rule deny source any
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] snmp-agent sys-info version v2c
[Sysname] snmp-agent group v2c readCom
```

```
[Sysname] snmp-agent usm-user v2c userv2c readCom acl 2001
```

Add the user **userv2c** in the SNMPv2c group **readCom** so only the NMS at 1.1.1.2 can use the protocol SNMPv2c and read-only community name **userv2c** to access the device.

```
[Sysname] acl basic name testacl
[Sysname-acl-ipv4-basic-testacl] rule permit source 1.1.1.2 0.0.0.0
[Sysname-acl-ipv4-basic-testacl] rule deny source any
[Sysname-acl-ipv4-basic-testacl] quit
[Sysname] snmp-agent sys-info version v2c
[Sysname] snmp-agent group v2c readCom
[Sysname] snmp-agent usm-user v2c userv2c readCom acl name testacl
```

Related commands

display snmp-agent community

snmp-agent community

snmp-agent group

snmp-agent usm-user v3

Use **snmp-agent usm-user v3** to create an SNMPv3 user.

Use **undo snmp-agent usm-user v3** to delete an SNMPv3 user.

Syntax

- In VACM mode:

  snmp-agent usm-user v3 *user-name group-name* [**remote** { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]] [{ **cipher** | **simple** } **authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode** { **3des** | **aes128** | **des56** } *priv-password*]] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

  undo snmp-agent usm-user v3 *user-name* { **local** | **engineid** *engineid-string* | **remote** { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] }

- In RBAC mode:

  snmp-agent usm-user v3 *user-name* **user-role** *role-name* [**remote** { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]] [{ **cipher** | **simple** } **authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode** { **3des** | **aes128** | **des56** } *priv-password*]] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

  undo snmp-agent usm-user v3 *user-name* { **local** | **engineid** *engineid-string* | **remote** { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] }

Default

No SNMPv3 users exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

user-name: Specifies an SNMPv3 username, a case-sensitive string of 1 to 32 characters.

group-name: Specifies an SNMPv3 group name, a case-sensitive string of 1 to 32 characters. The group can be one that has been created or not. The user takes effect only after you create the group.

user-role *role-name*: Specifies a user role name, a case-sensitive string of 1 to 63 characters.

remote { *ipv4-address* | **ipv6** *ipv6-address* }: Specifies a target host by its IPv4 or IPv6 address, typically the NMS, to receive the informs. To send SNMPv3 informs to a target host, you must specify this option and use the **snmp-agent remote** command to bind the IPv4 or IPv6 address to the remote engine ID.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the target host belongs to. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the target host belongs to the public network, do not specify this option.

cipher: Specifies an authentication key and an encryption key in encrypted form. The keys will be converted to a digest in encrypted form and stored in the device.

simple: Specifies an authentication key and an encryption key in plaintext from. The keys will be converted to a digest in encrypted form and stored in the device.

authentication-mode: Specifies an authentication algorithm. If you do not specify the keyword, the system does not perform authentication.

- **md5**: Specifies the HMAC-MD5 authentication algorithm. For more information about this authentication algorithm, see IPSec configuration in *Security Configuration Guide*.
- **sha**: Specifies the HMAC-SHA1 authentication algorithm. For more information about this authentication algorithm, see IPSec configuration in *Security Configuration Guide*.

auth-password: Specifies an authentication key. This argument is case sensitive.

- The plaintext form of the key is a string of 1 to 64 characters.
- The encrypted form of the key can be calculated by using the **snmp-agent calculate-password** command.

privacy-mode: Specifies an encryption algorithm. If you do not specify this keyword, the system does not perform encryption.

- **3des**: Specifies the 3DES encryption algorithm that uses a 168-bit key.
- **aes128**: Specifies the AES encryption algorithm that uses a 128-bit key.
- **des56**: Specifies the DES encryption algorithm that uses a 56-bit key.

priv-password: Specifies an encryption key. This argument is case sensitive.

- The plaintext form of the key is a string of 1 to 64 characters.
- The encrypted form of the key can be calculated by using the **snmp-agent calculate-password** command.

acl: Specifies a basic or advanced IPv4 ACL for the user.

ipv4-acl-number: Specifies a basic or advanced IPv4 ACL by its number. The basic IPv4 ACL number is in the range of 2000 to 2999. The advanced IPv4 ACL number is in the range of 3000 to 3999.

name *ipv4-acl-name*: Specifies a basic or advanced IPv4 ACL by its name, a case-insensitive string of 1 to 63 characters.

acl ipv6: Specifies a basic or advanced IPv6 ACL for the user.

ipv6-acl-number: Specifies a basic or advanced IPv6 ACL by its number. The basic IPv6 ACL number is in the range of 2000 to 2999. The advanced IPv6 ACL number is in the range of 3000 to 3999.

name *ipv6-acl-name*: Specifies a basic or advanced IPv6 ACL by its name, a case-insensitive string of 1 to 63 characters.

local: Specifies the local SNMP engine. By default, an SNMPv3 user is associated with the local SNMP engine.

engineid *engineid-string*: Specifies an SNMP engine ID. The *engineid-string* argument is an even number of hexadecimal characters. All-zero and all-F strings are invalid. The even number is in the range of 10 to 64. If you change the local engine ID, the existing SNMPv3 users and keys become invalid. To delete an invalid username, specify the engine ID associated with the username in the **undo snmp-agent usm-user v3** command.

Usage guidelines

Only users with the network-admin, context-admin, or level-15 user role can execute this command. Users with other user roles cannot execute this command even if these roles are granted access to commands of the SNMP feature or this command.

You can use either of the following modes to control SNMPv3 user access to MIB objects.

- **VACM**—Controls user access to MIB objects by assigning the user to an SNMP group. To make sure the user takes effect, make sure the group has been created. An SNMP group contains one or multiple users and specifies the MIB views and security model for the users. The authentication and encryption algorithms for each user are specified when they are created.
- **RBAC**—Controls user access to MIB objects by assigning user roles to the user. A user role specifies the MIB objects accessible to the user and the operations that the user can perform on the objects. After you create a user in RBAC mode, you can use the **snmp-agent usm-user v3 user-role** command to assign more user roles to the user. You can assign a maximum of 64 user roles to a user.

RBAC mode controls access on a per MIB object basis, and VACM mode controls access on a MIB view basis. As a best practice to enhance MIB security, use RBAC mode.

You can execute the **snmp-agent usm-user v3** command multiple times to create different SNMPv3 users in VACM mode. If you do not change the username each time, the most recent configuration takes effect.

You can execute the **snmp-agent usm-user v3** command in RBAC mode multiple times to assign different user roles to an SNMPv3 user. The following restrictions and guidelines apply:

- If you specify only user roles but do not change any other settings each time, the **snmp-agent usm-user v3** command assigns different user roles to the user. Other settings remain unchanged.
- If you specify user roles and also change other settings each time, the **snmp-agent usm-user v3** command assigns different user roles to the user. The most recent configuration for other settings takes effect.

You can specify an ACL for the user and group, respectively, to filter illegitimate NMSs from accessing the agent. Only the NMSs permitted by the ACLs for both the user and group can access the SNMP agent. The following rules apply to the ACLs for the user and group:

- If the specified ACL does not exist, or the specified ACL does not contain any rule, all NMSs can access the device.
- If a VPN instance is specified in an ACL rule, the rule applies only to the packets of the VPN instance. If no VPN instance is specified in an ACL rule, the rule applies only to the packets on the public network.
- If you specify an ACL and the ACL has rules, only NMSs permitted by the ACL can access the device.

For more information about ACL, see *ACL and QoS Configuration Guide*.

Examples

In VACM mode:

Add user **testUser** to SNMPv3 group **testGroup**, and enable authentication for the group. Specify authentication algorithm **HMAC-SHA1** and plaintext-form authentication key **123456TESTplat&!** for the user.

```
<Sysname> system-view
[Sysname] snmp-agent group v3 testGroup authentication
[Sysname] snmp-agent usm-user v3 testUser testGroup simple authentication-mode sha
123456TESTplat&!
```

For an NMS to access the MIB objects in the default view **ViewDefault**, make sure the following configurations on the NMS are the same as the SNMP agent:

- SNMPv3 username.
- SNMP protocol version.
- Authentication algorithm and key.

Add user **testUser** to SNMPv3 group **testGroup**, and enable authentication and encryption for the group. Specify authentication algorithm **HMAC-SHA1**, encryption algorithm **AES**, plaintext-form authentication key **123456TESTauth&!**, and plaintext-form encryption key **123456TESTencr&!** for the user.

```
<Sysname> system-view
[Sysname] snmp-agent group v3 testGroup privacy
[Sysname] snmp-agent usm-user v3 testUser testGroup simple authentication-mode sha
123456TESTauth&! privacy-mode aes128 123456TESTencr&!
```

For an NMS to access the MIB objects in the default view **ViewDefault**, make sure the following configurations on the NMS are the same as the SNMP agent:

- SNMPv3 username.
- SNMP protocol version.
- Authentication algorithm.
- Privacy algorithm.
- Plaintext authentication and encryption keys.

Add user **remoteUser** for the SNMP remote engine at 10.1.1.1 to SNMPv3 group **testGroup**, and enable authentication and encryption for the group. Specify authentication algorithm **HMAC-SHA1**, encryption algorithm **AES**, plaintext-form authentication key **123456TESTauth&!**, and plaintext-form encryption key **123456TESTencr&!** for the user.

```
<Sysname> system-view
[Sysname] snmp-agent remote 10.1.1.1 engineid 123456789A
[Sysname] snmp-agent group v3 testGroup privacy
[Sysname] snmp-agent usm-user v3 remoteUser testGroup remote 10.1.1.1 simple
authentication-mode sha 123456TESTauth&! privacy-mode aes128 123456TESTencr&!
```

In RBAC mode:

Create SNMPv3 user **testUser** with user role **network-operator** and enable authentication for the user. Specify authentication algorithm **HMAC-SHA1** and plaintext-form authentication key **123456TESTplat&!** for the user.

```
<Sysname> system-view
[Sysname] snmp-agent usm-user v3 testUser user-role network-operator simple
authentication-mode sha 123456TESTplat&!
```

For an NMS to have read-only access to all MIB objects, make sure the following configurations on the NMS are the same as the SNMP agent:

- SNMPv3 username.
- SNMP protocol version.
- Authentication algorithm and key.

Related commands

display snmp-agent usm-user

snmp-agent calculate-password

snmp-agent group

snmp-agent remote

snmp-agent usm-user v3 user-role

snmp-agent usm-user v3 user-role

Use **snmp-agent usm-user v3 user-role** to assign a user role to an SNMPv3 user created in RBAC mode.

Use **undo snmp-agent usm-user user-role** to remove a user role.

Syntax

snmp-agent usm-user v3 *user-name* **user-role** *role-name*

undo snmp-agent usm-user v3 *user-name* **user-role** *role-name*

Default

An SNMPv3 user has the user role assigned to it at its creation.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

user-name: Specifies an SNMPv3 username, a case-sensitive string of 1 to 32 characters.

user-role *role-name*: Specifies a user role name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

You can assign a maximum of 64 user roles to an SNMPv3 user.

An SNMPv3 user must have a minimum of one user role.

Examples

Assign the user role **network-admin** to the SNMPv3 user **testUser**.

```
<Sysname> system-view
[Sysname] snmp-agent usm-user v3 testUser user-role network-admin
```

Related commands

snmp-agent usm-user v3

Contents

RMON commands

display rmon alarm

Use **`display rmon alarm`** to display information about RMON alarm entries.

Syntax

`display rmon alarm` [*`entry-number`*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

`entry-number`: Specifies an alarm entry by its index in the range of 1 to 65535. If you do not specify an entry, the command displays all RMON alarm entries.

Examples

Display information about all RMON alarm entries.

```
<Sysname> display rmon alarm
AlarmEntry 1 owned by user1 is VALID.
  Sample type                    : absolute
  Sampled variable               : 1.3.6.1.2.1.16.1.1.1.4.1<etherStatsOctets.1>
  Sampling interval (in seconds) : 10
  Rising threshold               : 50(associated with event 1)
  Falling threshold              : 5(associated with event 2)
  Alarm sent upon entry startup  : risingOrFallingAlarm
  Latest value                   : 0
```

Table 1 Command output

Field	Description

AlarmEntry *entry-number* owned by *owner* is *status*.	Alarm entry owner and status:
	• *entry-number*—Alarm entry index.
	• *owner*—Entry owner.
	• *status*—Entry status:
	  ○ **VALID**—The entry is valid.
	  ○ **UNDERCREATION**—The entry is invalid.
	The *status* field is not configurable at the CLI. All alarm entries created from the CLI are valid by default.
	The **`display rmon alarm`** command can display invalid entries, but the **`display current-configuration`** and **`display this`** commands do not display their settings.

Field	Description
Sample type	Sample type: • absolute. • delta.
Sampled variable	Monitored variable.
Sampling interval	Interval (in seconds) at which data is sampled.
Rising threshold	Alarm rising threshold.
associated with event	Event index associated with the alarm..
Falling threshold	Alarm falling threshold.
Alarm sent upon entry startup	Alarm that can be generated at the first sampling: • **risingAlarm**. • **fallingAlarm**. • **risingOrFallingAlarm**. The default is **risingOrFallingAlarm**.
Latest value	Most recent sampled value.

Related commands

`rmon alarm`

display rmon event

Use **`display rmon event`** to display information about RMON event entries.

Syntax

`display rmon event` [*`entry-number`*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

`entry-number`: Specifies an event entry by its index in the range of 1 to 65535. If you do not specify an entry, the command displays all event entries.

Usage guidelines

An event entry includes the following information:

- Event index.
- Event owner.
- Event description.
- Action triggered by the event (such as logging the event or sending an SNMP notification).
- Last time when the event occurred (seconds that elapsed since the system startup).

Examples

Display information about all RMON event entries.

```
<Sysname> display rmon event
EventEntry 1 owned by user1 is VALID.
  Description: N/A
  Community: Security
  Take the action log-trap when triggered, last triggered at 0days 00h:02m:27s uptime.
```

Table 2 Command output

Field	Description

EventEntry *entry-number* owned by *owner* is *status*.	Event entry owner and status:
	• *entry-number*—Event entry index.
	• *owner*—Entry owner.
	• *status*—Entry status:
	  ○ **VALID**—The entry is valid.
	  ○ **UNDERCREATION**—The entry is invalid.
	The *status* field is not configurable at the CLI. All alarm entries created from the CLI are valid by default.
	The **display rmon event** command can display invalid entries, but the **display current-configuration** and **display this** commands do not display their settings.

Description	Event description.
Community	SNMP community name for the RMON event.
Take the action *action* when triggered	Actions that the system takes when the event is triggered: • **none**—Takes no action. • **log**—Logs the event. • **trap**—Sends an SNMP notification. • **log-trap**—Logs the event and sends an SNMP notification.
last triggered at *time* uptime	Last time when the event occurred, which is represented as the amount of time that elapsed since the system startup.

Related commands

rmon event

display rmon eventlog

Use **display rmon eventlog** to display information about event log entries.

Syntax

display rmon eventlog [*entry-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

entry-number: Specifies an event entry by its index in the range of 1 to 65535. If you do not specify an entry, the command displays log entries for all event entries.

Usage guidelines

If the log action is specified for an event, the system adds a record in the event log table each time the event occurs. Each record contains the log entry index, time when the event was logged (the amount of time that elapsed since system startup), and event description.

The system can maintain a maximum of 10 records for an event. The most recent record replaces the oldest record if the number of records reaches 10.

Examples

Display the RMON log for event entry **99**.

```
<Sysname> display rmon eventlog 99
EventEntry 99 owned by ww is VALID.
  LogEntry 99.1 created at 50days 08h:54m:44s uptime.
  Description: The 1.3.6.1.2.1.16.1.1.1.4.5 defined in alarmEntry 77,
     uprise 16760000 with alarm value 16776314. Alarm sample type is absolute.
  LogEntry 99.2 created at 50days 09h:11m:13s uptime.
  Description: The 1.3.6.1.2.1.16.1.1.1.4.5 defined in alarmEntry 77,
     less than(or =) 20000000 with alarm value 16951648. Alarm sample type is absolute.
  LogEntry 99.3 created at 50days 09h:18m:43s uptime.
  Description: The alarm formula defined in prialarmEntry 777,
     less than(or =) 15000000 with alarm value 14026493. Alarm sample type is absolute.
  LogEntry 99.4 created at 50days 09h:23m:28s uptime.
  Description: The alarm formula defined in prialarmEntry 777,
     uprise 17000000 with alarm value 17077846. Alarm sample type is absolute.
```

This example shows that the event log table has four records for event 99:

- Two records were created when event 99 was triggered by alarm entry 77.
- Two records were created when event 99 was triggered by private alarm entry 777.

Table 3 Command output

Field	Description

EventEntry *entry-number* owned by *owner* is *status*.	Event log entry owner and status:
	• *entry-number*—Event log entry index, which is the same as the event entry index for which this log entry is generated.
	• *owner*—Entry owner.
	• *status*—Entry status:
	  ○ **VALID**—The entry is valid (default value).
	  ○ **UNDERCREATION**—The entry is invalid.
	The *status* field is not configurable at the CLI. All event log entries are valid by default.
	The **display rmon eventlog** command can display invalid entries, but the **display current-configuration** and **display this** commands do not display their settings.

Field	Description
LogEntry *entry-number* created at *created-time* uptime.	Time when an event record was created: • *entry-number*—Event record index, represented as logEventIndex.logIndex, where logEventIndex and logIndex are MIB objects. A record index uniquely identifies a record among all records for the event. • *created-time*—Time when the event entry was created.
Description	Record description.

Related commands

rmon event

display rmon history

Use **display rmon history** to display RMON history control entries and history samples of Ethernet statistics for Ethernet interfaces.

Syntax

display rmon history [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface-type i*nterface-number*: Specifies an interface by its type and number. If you do not specify an interface, the command displays history samples for all interfaces that have an RMON history control entry.

Usage guidelines

RMON uses the etherHistoryTable object to store the history samples of Ethernet statistics for Ethernet interfaces.

To collect history samples for an Ethernet interface, you must first create a history control entry on the interface.

To configure the number of history samples that can be displayed and the history sampling interval, use the **rmon history** command.

Examples

Display the RMON history control entry and history samples for GigabitEthernet 1/0/1.

```
<Sysname> display rmon history gigabitethernet 1/0/1
HistoryControlEntry 6 owned by user1 is VALID.
  Sampled interface     : GigabitEthernet1/0/1<ifIndex.117>
  Sampling interval     : 8(sec) with 3 buckets max
  Sampling record 1 :
    dropevents        : 0         , octets              : 5869
    packets           : 54        , broadcast packets   : 9
```

```
multicast packets : 23        , CRC alignment errors : 0
undersize packets : 0         , oversize packets     : 0
fragments         : 0         , jabbers              : 0
collisions        : 0         , utilization          : 0
```

Table 4 Command output

Field	Description

HistoryControlEntry *entry-number* owned by *owner* is *status*.	Status and owner of the history control entry:
	• *entry-number*—History control entry index.
	• *owner*—Entry owner.
	• *status*—Entry status:
	  ○ **VALID**—The entry is valid.
	  ○ **UNDERCREATION**—The entry is invalid.
	The *status* field is not configurable at the CLI. All history control entries created from the CLI are valid by default.
	The **`display rmon history`** command can display invalid entries, but the **`display current-configuration`** and **`display this`** commands do not display their settings.

Sampled Interface	Sampled interface.
Sampling interval	Sampling interval in seconds.
buckets max	Maximum number of samples that can be saved for the history control entry. If the expected bucket size specified with the **`rmon history`** command exceeds the available history table size, RMON sets the bucket size as closely to the expected bucket size as possible. If the bucket has been full, RMON overwrites the oldest sample with the new sample.
Sampling record	History sample index.
dropevents	Total number of events in which packets were dropped during the sampling interval. **NOTE:** This statistic is the number of times that a drop condition occurred. It is not necessarily the total number of dropped packets.
octets	Total number of octets received during the sampling interval.
packets	Total number of packets (including bad packets) received during the sampling interval.
broadcast packets	Number of broadcast packets received during the sampling interval.
multicast packets	Number of multicast packets received during the sampling interval.
CRC alignment errors	Number of packets received with CRC alignment errors during the sampling interval.
undersize packets	Number of undersize packets received during the sampling interval. Undersize packets are shorter than 64 octets (excluding framing bits but including FCS octets).
oversize packets	Number of oversize packets received during the sampling interval. Oversize packets are longer than 1518 octets (excluding framing bits but including FCS octets).
fragments	Number of undersize packets with CRC errors received during the sampling interval.

Field	Description
jabbers	Number of oversize packets with CRC errors received during the sampling interval.
collisions	Number of colliding packets received during the sampling interval.
utilization	Bandwidth utilization (in hundreds of a percent) during the sampling period.

Related commands

rmon history

display rmon prialarm

Use **display rmon prialarm** to display information about RMON private alarm entries.

Syntax

display rmon prialarm [*entry-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

entry-number: Specifies an alarm entry index in the range of 1 to 65535. If you do not specify an entry, the command displays all private alarm entries.

Examples

Display information about all RMON private alarm entries.

```
<Sysname> display rmon prialarm
PrialarmEntry 1 owned by user1 is VALID.
  Sample type                    : absolute
  Variable formula          : (.1.3.6.1.2.1.16.1.1.1.6.1*100/.1.3.6.1.2.1.16.1.1.1.5.1)
  Description                    : ifUtilization.GigabitEthernet1/0/1
  Sampling interval (in seconds) : 10
  Rising threshold               : 80(associated with event 1)
  Falling threshold              : 5(associated with event 2)
  Alarm sent upon entry startup  : risingOrFallingAlarm
  Entry lifetime                 : forever
  Latest value                   : 85
```

Table 5 Command output

Field	Description

PrialarmEntry *entry-number* owned by *owner* is *status*.	Alarm entry owner and status:
	• *entry-number*—Alarm entry index.
	• *owner*—Entry owner.
	• *status*—Entry status:
	  ○ **VALID**—The entry is valid.
	  ○ **UNDERCREATION**—The entry is invalid.
	The *status* field is not configurable at the CLI. All alarm entries created from the CLI are valid by default.
	The **display rmon prialarm** command can display invalid entries, but the **display current-configuration** and **display this** commands do not display their settings.

Sample type	Sample type: • absolute. • delta.
Variable formula	Variable formula.
Description	Description of the alarm.
Sampling interval	Interval (in seconds) at which data is sampled.
Rising threshold	Alarm rising threshold.
Falling threshold	Alarm falling threshold.
associated with event	Event index associated with the alarm..
Alarm sent upon entry startup	Alarm that can be generated at the first sampling: • **risingAlarm**. • **fallingAlarm**. • **risingOrFallingAlarm**. The default is **risingOrFallingAlarm**.
Entry lifetime	Lifetime of the entry. • If the lifetime is set to **forever**, the entry never expires. • If the lifetime is set to an amount of time, the entry is removed when the timer expires.
Latest value	Most recent sampled value.

Related commands

rmon prialarm

display rmon statistics

Use **display rmon statistics** to display RMON statistics.

Syntax

display rmon statistics [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, the command displays RMON statistics for all interfaces.

Usage guidelines

This command displays the cumulative interface statistics for the period from the time the statistics entry was created to the time the command was executed. The statistics are cleared when the device reboots.

Examples

Display RMON statistics for GigabitEthernet 1/0/1.

```
<Sysname> display rmon statistics gigabitethernet 1/0/1
EtherStatsEntry 1 owned by user1 is VALID.
  Interface : GigabitEthernet1/0/1<ifIndex.3>
  etherStatsOctets         : 43393306  , etherStatsPkts          : 619825
  etherStatsBroadcastPkts  : 503581    , etherStatsMulticastPkts : 44013
  etherStatsUndersizePkts  : 0         , etherStatsOversizePkts  : 0
  etherStatsFragments      : 0         , etherStatsJabbers       : 0
  etherStatsCRCAlignErrors : 0         , etherStatsCollisions    : 0
  etherStatsDropEvents (insufficient resources): 0
  Incoming packets by size:
  64     : 0         ,  65-127  : 0         ,  128-255  : 0
  256-511: 0         ,  512-1023: 0         ,  1024-1518: 0
```

Table 6 Command output

Field	Description

EtherStatsEntry *entry-number* owned by *owner* is *status*.	Statistics entry owner and status:
	• *entry-number*—Statistics entry index.
	• *owner*—Entry owner.
	• *status*—Entry status:
	  ○ **VALID**—The entry is valid.
	  ○ **UNDERCREATION**—The entry is invalid.
	The *status* field is not configurable at the CLI. All alarm entries created from the CLI are valid by default.
	The **display rmon statistics** command can display invalid entries, but the **display current-configuration** and **display this** commands do not display their settings.

Interface	Interface on which statistics are gathered.
etherStatsOctets	Total number of octets received on the interface.
etherStatsPkts	Total number of packets received on the interface.
etherStatsBroadcastPkts	Total number of broadcast packets received on the interface.
etherStatsMulticastPkts	Total number of multicast packets received on the interface.

Field	Description
etherStatsUndersizePkts	Total number of undersize packets received on the interface.
etherStatsOversizePkts	Total number of oversize packets received on the interface.
etherStatsFragments	Total number of undersize packets received with CRC errors on the interface.
etherStatsJabbers	Total number of oversize packets received with CRC errors on the interface.
etherStatsCRCAlignErrors	Total number of packets received with CRC errors on the interface.
etherStatsCollisions	Total number of colliding packets received on the interface.
etherStatsDropEvents	Total number of events in which packets were dropped. **NOTE:** This statistic is the number of times that a drop condition occurred. It is not necessarily the total number of dropped packets.
Incoming packets by size:	Incoming-packet statistics by packet length: • **64**—Number of packets with a length less than or equal to 64 bytes. • **65-127**—Number of 65- to 127-byte packets. • **128-255**—Number of 128- to 255-byte packets. • **256-511**—Number of 256- to 511-byte packets. • **512-1023**—Number of 512- to 1023-byte packets. • **1024-1518**—Number of 1024- to 1518-byte packets.

Related commands

rmon statistics

rmon alarm

Use **rmon alarm** to create an RMON alarm entry.

Use **undo rmon alarm** to remove an RMON alarm entry.

Syntax

rmon alarm *entry-number alarm-variable sampling-interval* { **absolute** | **delta** } [**startup-alarm** { **falling** | **rising** | **rising-falling** }] **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* [**owner** *text*]

undo rmon alarm *entry-number*

Default

No RMON alarm entries exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

entry-number: Specifies an alarm entry index in the range of 1 to 65535.

alarm-variable: Specifies an alarm variable, a string of 1 to 255 characters. You can only specify variables that can be parsed as an ASN.1 INTEGER value (INTEGER, INTEGER32, Unsigned32, Counter32, Counter64, Gauge, or TimeTicks) for the *alarm-variable* argument. The alarm variables must use one of the formats in Table 7.

Table 7 Alarm variable formats

Format	Examples
Dotted OID format: *entry.integer.instance*	1.3.6.1.2.1.2.1.10.1
Object name.instance	etherStatsOctets.1 etherStatsPkts.1 etherStatsBroadcastPkts.1 ifInOctets.1 ifInUcastPkts.1 ifInNUcastPkts.1

sampling-interval: Sets the sampling interval in the range of 5 to 65535 seconds.

absolute: Specifies absolute sampling. RMON compares the value of the variable with the rising and falling thresholds.

delta: Specifies delta sampling. RMON subtracts the value of the variable at the previous sample from the current sampled value, and then compares the difference with the rising and falling thresholds.

startup-alarm: Specifies alarms that can be generated at the first sampling when a rising or falling threshold is reached or exceeded. By default, a **rising-falling** alarm is generated.

rising: Generates a rising alarm.

falling: Generates a falling alarm.

rising-falling: Generates a rising or falling alarm.

rising-threshold *threshold-value1 event-entry1*: Sets the rising threshold. The *threshold-value1* argument represents the rising threshold in the range of –2147483648 to 2147483647. The *event-entry1* argument represents the index of the event that is triggered when the rising threshold is crossed. The value range for the *event-entry1* argument is 0 to 65535. If 0 is specified, the alarm does not trigger any event.

falling-threshold *threshold-value2 event-entry2*: Sets the falling threshold. The *threshold-value2* argument represents the falling threshold in the range of –2147483648 to 2147483647. The *event-entry2* argument represents the index of the event that is triggered when the falling threshold is crossed. The value range for the *event-entry2* argument is 0 to 65535. If 0 is specified, the alarm does not trigger any event.

owner *text*: Specifies the entry owner, a case-sensitive string of 1 to 127 characters.

Usage guidelines

You can create a maximum of 60 RMON alarm entries.

Each alarm entry must have a unique alarm variable, sampling interval, sample type, rising threshold, or falling threshold. You cannot create an alarm entry if all these parameters for the entry are the same as an existing entry.

To trigger the event associated with an alarm condition, you must create the event with the **rmon event** command.

RMON samples the monitored alarm variable at the specified sampling interval, compares the sampled value with the predefined thresholds, and performs one of the following operations:

- Triggers the event associated with the rising alarm if the sampled value is equal to or greater than the rising threshold.
- Triggers the event associated with the falling alarm if the sampled value is equal to or less than the falling threshold.

Examples

Create an alarm entry to perform absolute sampling on the number of octets received on GigabitEthernet 1/0/1 (object instance 1.3.6.1.2.1.16.1.1.1.4.1) at 10-seconds intervals. If the sampled value reaches or exceeds 5000, log the rising alarm event. If the sampled value is equal to or less than 5, take no actions.

```
<Sysname> system-view
[Sysname] rmon event 1 log
[Sysname] rmon event 2 none
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rmon statistics 1
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] rmon alarm 1 1.3.6.1.2.1.16.1.1.1.4.1 10 absolute rising-threshold 5000 1
falling-threshold 5 2 owner user1
```

In this example, you can replace 1.3.6.1.2.1.16.1.1.1.4.1 with etherStatsOctets.1, where 1 is the statistics entry index for the interface. If you execute the **rmon statistics 5** command, you can use etherStatsOctets.5 to replace 1.3.6.1.2.1.16.1.1.1.4.5.

Related commands

display rmon alarm

rmon event

rmon event

Use **rmon event** to create an RMON event entry.

Use **undo rmon event** to remove an RMON event entry.

Syntax

rmon event *entry-number* [**description** *string*] { **log** | **log-trap** *security-string* | **none** | **trap** *security-string* } [**owner** *text*]

undo rmon event *entry-number*

Default

No RMON event entries exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

entry-number: Specifies an event entry index in the range of 1 to 65535.

description *string*: Configures an event description, a case-sensitive string of 1 to 127 characters.

log: Logs the event .

log-trap: Logs the event and sends an SNMP notification.

security-string: Specifies the SNMP community name carried in the SNMP notifications. The *security-string* argument is a case-sensitive string of 1 to 127 characters and is determined by the SNMP configuration. This argument is supported but does not take effect in the current software version.

none: Performs no action.

trap: Sends an SNMP notification.

owner *text*: Specifies the entry owner, a case-sensitive string of 1 to 127 characters.

NOTE:

The SNMP community name setting for the *security-string* argument does not take effect even though you can configure it with the command. Instead, the system uses the settings you configure with SNMP when it sends RMON SNMP notifications. For more information about SNMP notifications, see *Network Management and Monitoring Configuration Guide*.

Usage guidelines

You can create a maximum of 60 event entries.

You can associate an event entry with a standard or private alarm entry to specify the action to take when an alarm condition occurs. Depending on your configuration, the system logs the event, sends an SNMP notification, does both, or does neither.

You can associate an event with multiple alarm entries.

Examples

Create an RMON log event entry. Specify its index as **10** and the entry owner as **user1**.

```
<Sysname> system-view
[Sysname] rmon event 10 log owner user1
```

Related commands

display rmon event

rmon alarm

rmon prialarm

rmon history

Use **rmon history** to create an RMON history control entry.

Use **undo rmon history** to remove an RMON history control entry.

Syntax

rmon history *entry-number* **buckets** *number* **interval** *interval* [**owner** *text*]

undo rmon history *entry-number*

Default

No RMON history control entries exist.

Views

Ethernet interface view

Predefined user roles

network-admin

context-admin

Parameters

entry-number: Specifies a history control entry index in the range of 1 to 65535.

buckets *number*: Specifies the expected maximum number of samples to be retained for the entry, in the range of 1 to 65535. RMON can retain a maximum of 50 samples for each history control entry. If the expected bucket size exceeds the available history table size, RMON sets the bucket size as closely to the expected bucket size as is possible. However, the granted bucket size will not exceed 50. For example, the bucket size for a history control entry will be 30 if the expected bucket size is set to 55, but the available bucket size is only 30.

interval *interval*: Specifies the sampling interval in the range of 5 to 3600 seconds.

owner *text*: Specifies the entry owner, a case-sensitive string of 1 to 127 characters.

Usage guidelines

The system supports a maximum of 100 history control entries.

If an Ethernet interface has a history control entry, RMON periodically samples packet statistics on the interface and stores the samples to the history table. When the bucket size for the history control entry is reached, RMON overwrites the oldest sample with the most recent sample.

You can create multiple RMON history control entries for an Ethernet interface.

Examples

Create RMON history control entry 1 for GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rmon history 1 buckets 10 interval 5 owner user1
```

Related commands

display rmon history

rmon prialarm

Use **rmon prialarm** to create an RMON private alarm entry.

Use **undo rmon prialarm** to remove an RMON private alarm entry.

Syntax

rmon prialarm *entry-number prialarm-formula prialarm-des sampling-interval* { **absolute** | **delta** } [**startup-alarm** { **falling** | **rising** | **rising-falling** }] **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* **entrytype** { **forever** | **cycle** *cycle-period* } [**owner** *text*]

undo rmon prialarm *entry-number*

Default

No RMON private alarm entries exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

entry-number: Specifies a private alarm entry index in the range of 1 to 65535.

prialarm-formula: Configures a private alarm variable formula, a string of 1 to 255 characters. The variables in the formula must be represented in OID format that starts with a dot (.), for example, (.1.3.6.1.2.1.2.1.10.1)*8. You can configure a formula to perform the basic math operations of addition, subtraction, multiplication, and division on these variables. To get a correct calculation result, make sure the following conditions are met:

- The values of the variables in the formula are positive integers.
- The result of each calculating step is in the value range for long integers.

prialarm-des: Configures an entry description, a case-sensitive string of 1 to 127 characters.

sampling-interval: Sets the sampling interval in the range of 10 to 65535 seconds.

absolute: Specifies absolute sampling. RMON compares the value of the variable with the rising and falling thresholds.

delta: Specifies delta sampling. RMON subtracts the value of the variable at the previous sample from the current sampled value, and then compares the difference with the rising and falling thresholds.

startup-alarm: Specifies alarms that can be generated at the first sampling when a rising or falling threshold is reached or exceeded. By default, a **rising-falling** alarm is generated.

rising: Generates a rising alarm.

falling: Generates a falling alarm.

rising-falling: Generates a rising or falling alarm.

rising-threshold *threshold-value1 event-entry1*: Sets the rising threshold. The *threshold-value1* argument represents the rising threshold in the range of –2147483648 to 2147483647. The *event-entry1* argument represents the index of the event that is triggered when the rising threshold is crossed. The value range for the *event-entry1* argument is 0 to 65535. If 0 is specified, the alarm does not trigger any event.

falling-threshold *threshold-value2 event-entry2*: Sets the falling threshold. The *threshold-value2* argument represents the falling threshold in the range of –2147483648 to 2147483647. The *event-entry2* argument represents the index of the event that is triggered when the falling threshold is crossed. The value range for the *event-entry2* argument is 0 to 65535. If 0 is specified, the alarm does not trigger any event.

forever: Configures the entry as a permanent entry. RMON retains a permanent private alarm entry until it is manually deleted.

cycle *cycle-period*: Sets the lifetime of the entry, in the range of 0 to 4294967 seconds. RMON deletes the entry when its lifetime expires.

owner *text*: Specifies the entry owner, a case-sensitive string of 1 to 127 characters.

Usage guidelines

You can create a maximum of 50 private alarm entries.

Each alarm entry must have a unique alarm variable, sampling interval, sample type, rising threshold, or falling threshold. You cannot create an alarm entry if all these parameters for the entry are the same as an existing entry.

To trigger the event associated with an alarm condition, you must create the event with the **rmon event** command.

The RMON agent samples variables and takes an alarm action based on a private alarm entry as follows:

1. Periodically samples the variables specified in the private alarm formula.
2. Processes the sampled values with the formula.
3. Compares the calculation result with the predefined thresholds, and then takes one of the following actions:
   - Triggers the event associated with the rising alarm event if the result is equal to or greater than the rising threshold.
   - Triggers the event associated with the falling alarm event if the result is equal to or less than the falling threshold.

Examples

Add a permanent private alarm entry to monitor the ratio of incoming broadcasts to the total number of incoming packets on GigabitEthernet 1/0/1. Log the rising alarm event when the ratio exceeds 80%, and take no actions when the ratio drops to 5%. The formula is (1.3.6.1.2.1.16.1.1.1.6.1*100/.1.3.6.1.2.1.16.1.1.1.5.1), where 1.3.6.1.2.1.16.1.1.1.6.1 is the OID of the object instance etherStatsBroadcastPkts.1, and 1.3.6.1.2.1.16.1.1.1.5.1 is the OID of the object instance etherStatsPkts.1.

```
<Sysname> system-view
[Sysname] rmon event 1 log
[Sysname] rmon event 2 none
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rmon statistics 1
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] rmon prialarm 1 (.1.3.6.1.2.1.16.1.1.1.6.1*100/.1.3.6.1.2.1.16.1.1.1.5.1)
BroadcastPktsRatioOfGE1/0/1 10 absolute rising-threshold 80 1 falling-threshold 5 2
entrytype forever owner user1
```

The last number in the OID forms of variables must be the same as the statistics entry index for the interface. For example, if you execute the **rmon statistics 5** command, you must replace 1.3.6.1.2.1.16.1.1.1.6.1 and 1.3.6.1.2.1.16.1.1.1.5.1 with 1.3.6.1.2.1.16.1.1.1.6.5 and 1.3.6.1.2.1.16.1.1.1.5.5, respectively.

Related commands

display rmon prialarm

rmon event

rmon statistics

Use **rmon statistics** to create an RMON statistics entry.

Use **undo rmon statistics** to remove an RMON statistics entry.

Syntax

rmon statistics *entry-number* [**owner** *text*]

undo rmon statistics *entry-number*

Default

No RMON statistics entries exist.

Views

Ethernet interface view

Predefined user roles

network-admin

context-admin

Parameters

entry-number: Specifies a statistics entry index in the range of 1 to 65535.

owner *text*: Specifies the entry owner, a case-sensitive string of 1 to 127 characters.

Usage guidelines

Each RMON statistics entry provides a set of cumulative traffic statistics collected up to the present time for an interface. Statistics include number of collisions, CRC alignment errors, number of undersize or oversize packets, number of broadcasts, number of multicasts, number of bytes received, and number of packets received. The statistics are cleared at a reboot.

The index of an RMON statistics entry must be globally unique. If the index has been used by another interface, the creation operation fails.

You can create only one RMON statistics entry for an Ethernet interface.

To display the RMON statistics table, use the **display rmon statistics** command.

Examples

Create an RMON statistics entry for GigabitEthernet 1/0/1. The index is 20 and the owner is **user1**.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rmon statistics 20 owner user1
```

Related commands

display rmon statistics

Contents

Event MIB commands

action

Use **action** to set an action for an event.

Use **undo action** to remove an action.

Syntax

action { **notification** | **set** }

undo action { **notification** | **set** }

Default

An event does not have an action.

Views

Event view

Predefined user roles

network-admin

context-admin

Parameters

notification: Specifies the notification action. The system sends a notification to the NMS when the event is triggered.

set: Specifies the set action. The system sets a value for the specified MIB object when the event is triggered.

Usage guidelines

You can set both set and notification actions for an event.

- When you specify the set action, the system automatically creates a set entry and enters action-set view. You can configure the set action in this view. For more information, see the configuration in action-set view.
- When you specify the notification action, the system automatically creates a notification entry and enters action-notification view. You can configure the notification action in this view. For more information, see the configuration in action-notification view.

Examples

Set the notification action for an event and specify notification OID **mteEventSetFailure** for the action. Set the set action for the event and set the value for the **ipForwarding.0** object to 2.

```
<Sysname> system-view
[Sysname] snmp mib event owner owner1 name EventA
[Sysname-event-owner1-EventA] action notification
[Sysname-event-owner1-EventA-notification] oid mteEventSetFailure
[Sysname-event-owner1-EventA-notification] quit
[Sysname-event-owner1-EventA] action set
[Sysname-event-owner1-EventA-set] oid ipForwarding.0
[Sysname-event-owner1-EventA-set] value 2
```

Related commands

event enable

snmp mib event

comparison

Use **comparison** to specify a Boolean comparison type for the sampled value and the reference value.

Use **undo comparison** to restore the default.

Syntax

comparison { **equal** | **greater** | **greaterorequal** | **less** | **lessorequal** | **unequal** }

undo comparison

Default

The Boolean comparison type is unequal.

Views

Trigger-Boolean view

Predefined user roles

network-admin

context-admin

Parameters

equal: Specifies the Boolean comparison type as equal. When the sampled value equals the reference value, the trigger condition is met.

greater: Specifies the Boolean comparison type as greater than. When the sampled value is greater than the reference value, the trigger condition is met.

greaterorequal: Specifies the Boolean comparison type as greater than or equal to. When the sampled value is greater than or equal to the reference value, the trigger condition is met.

less: Specifies the Boolean comparison type as smaller than. When the sampled value is smaller than the reference value, the trigger condition is met.

lessorequal: Specifies the Boolean comparison type as smaller than or equal to. When the sampled value is smaller than or equal to the reference value, the trigger condition is met.

unequal: Specifies the Boolean comparison type as unequal. When the sampled value is unequal to the reference value, the trigger condition is met.

Usage guidelines

If the sampled value meets the trigger condition at two or more samplings in succession, an event is triggered only at the first sampling.

For an event to be triggered at the first sampling, execute the **startup enable** command.

Examples

Specify the Boolean comparison type as **unequal**.

```
<Sysname> system-view
[Sysname] snmp mib event trigger owner owner1 name triggerA
[Sysname-trigger-owner1-triggerA] test boolean
[Sysname-trigger-owner1-triggerA-boolean] comparison unequal
```

Related commands

snmp mib event trigger

test

context (action-set view)

Use **context** to configure a context for the set-action object.

Use **undo context** to restore the default.

Syntax

context *context-name*

undo context

Default

A set-action object does not have a context.

Views

Action-set view

Predefined user roles

network-admin

context-admin

Parameters

context-name: Specifies a context, a case-sensitive string of 1 to 32 characters.

Usage guidelines

To uniquely identify a set-action object, configure a context for it.

Examples

Configure context **contextname1** for the set-action object.

```
<Sysname>system-view
[Sysname] snmp mib event owner owner1 name EventA
[Sysname-event-owner1-EventA] action set
[Sysname-event-owner1-EventA-set] context contextname1
```

Related commands

action

snmp mib event owner

wildcard context

context (trigger view)

Use **context** to configure a context for a monitored object.

Use **undo context** to restore the default.

Syntax

context *context-name*

undo context

Default

A monitored object does not have a context.

Views

Trigger view

Predefined user roles

network-admin

context-admin

Parameters

context-name: Specifies a context, a case-sensitive string of 1 to 32 characters.

Usage guidelines

To uniquely identify a monitored object, configure a context for it.

Examples

Configure context **contextname1** for a monitored object.

```
<Sysname> system-view
[Sysname] snmp mib event trigger owner owner1 name triggerA
[Sysname-trigger-owner1-triggerA] context contextname1
```

Related commands

snmp mib event trigger

wildcard context

delta falling

Use **delta falling** to set a delta falling threshold and specify a falling event.

Use **undo delta falling** to restore the default.

Syntax

delta falling { **event owner** *event-owner* **name** *event-name* | **value** *integer-value* }

undo delta falling { **event** | **value** }

Default

The delta falling threshold is 0, and no falling event is specified.

Views

Trigger-threshold view

Predefined user roles

network-admin

context-admin

Parameters

event owner *event-owner* **name** *event-name*: Specifies an event by its owner and its name. Use the trigger owner as the event owner. The *event-name* argument is a case-sensitive string of 1 to 32 characters.

value *integer-value*: Specifies a delta falling threshold in the range of –2147483648 to 2147483647. The value must be smaller than or equal to the delta rising threshold.

Usage guidelines

A falling event is triggered if the delta value (difference between the current sampled value and the previous sampled value) is smaller than or equal to the delta falling threshold.

If the delta value crosses the delta falling threshold multiple times in succession, a falling event is triggered only for the first crossing.

Examples

Set the delta falling threshold to 20.

```
<Sysname> system-view
[Sysname] snmp mib event trigger owner owner1 name triggerA
[Sysname-trigger-owner1-triggerA] test threshold
[Sysname-trigger-owner1-triggerA-threshold] delta falling value 20
```

Related commands

sample

snmp mib event trigger

test

delta rising

Use **delta rising** to set a delta rising threshold and specify a rising event.

Use **undo delta rising** to restore the default.

Syntax

delta rising { **event owner** *event-owner* **name** *event-name* | **value** *integer-value* }

undo delta rising { **event** | **value** }

Default

The delta rising threshold is 0, and no rising event is specified.

Views

Trigger-threshold view

Predefined user roles

network-admin

context-admin

Parameters

event owner *event-owner* **name** *event-name*: Specifies an event by its owner and its name. Use the trigger owner as the event owner. The *event-name* argument is a case-sensitive string of 1 to 32 characters.

value *integer-value*: Specifies a delta rising threshold in the range of –2147483648 to 2147483647. The value must be greater than or equal to the delta falling threshold.

Usage guidelines

A rising event is triggered if the delta value is greater than or equal to the delta rising threshold.

If the delta value of the monitored object crosses the delta rising threshold multiple times in succession, a rising event is triggered only for the first crossing.

Examples

Set the delta rising threshold to 50, and specify the event identified by owner **owner1** and name **event1** as the rising event.

```
<Sysname> system-view
[Sysname] snmp mib event trigger owner owner1 name triggerA
[Sysname-trigger-owner1-triggerA] test threshold
[Sysname-trigger-owner1-triggerA-threshold] delta rising value 50
[Sysname-trigger-owner1-triggerA-threshold] delta rising event owner owner1 name event1
```

Related commands

sample

snmp mib event trigger

test

description (event view)

Use **description** to configure a description for an event.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

An event does not have a description.

Views

Event view

Predefined user roles

network-admin

context-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 255 characters.

Examples

Configure a description of **EventA is an RMON event** for the event identified by owner **owner1** and name **eventA**.

```
<Sysname> system-view
[Sysname] snmp mib event owner owner1 name EventA
[Sysname-event-owner1-EventA] description EventA is an RMON event
```

Related commands

snmp mib event owner

description (trigger view)

Use **description** to configure a description for a trigger.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

A trigger does not have a description.

Views

Trigger view

Predefined user roles

network-admin

context-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 255 characters.

Examples

Configure a description of **triggerA is configured for configured for network management events** for the trigger identified by owner **owner1** and name **triggerA**.

```
<Sysname> system-view
[Sysname] snmp mib event trigger owner owner1 name triggerA
[Sysname-trigger-owner1-triggerA] description triggerA is configured for network
management events
```

Related commands

snmp mib event trigger

display snmp mib event

Use **display snmp mib event** to display Event MIB configuration and statistics.

Syntax

display snmp mib event

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display Event MIB configuration and statistics.

```
<Sysname> display snmp mib event
TriggerFailures              : 0
EventFailures                : 0
SampleMinimum                : 1
SampleInstanceMaximum        : 0
SampleInstance               : 0
```

```
SampleInstancesHigh           : 0
SampleInstanceLacks           : 0
Trigger entry triggerA owned by owner1:
  TriggerComment              : triggerA is to monitor the state of the interface
  TriggerTest                 : boolean
  TriggerSampleType           : absoluteValue
  TriggerValueID              : 1.3.6.1.2.1.2.2.1.7.3<ifAdminStatus.3>
  TriggerValueIDWildcard      : false
  TriggerTargetTag            : N/A
  TriggerContextName          : context1
  TriggerContextNameWildcard  : true
  TriggerFrequency(in seconds): 600
  TriggerEnabled              : true
  Boolean entry:
   BoolCmp                    : unequal
   BoolValue                  : 1
   BoolStartUp                : true
   BoolObjOwner               : owner1
   BoolObjName                : Objects1
   BoolEvtOwner               : N/A
   BoolEvtName                : N/A
Event entry eventA owned by owner2:
  EvtComment                  : event is to set ifAdminStatus
  EvtAction                   : notification | set
  EvtEnabled                  : true
  Notification entry:
   NotifyOID                  : 1.3.6.1.2.1.88.2.0.1<mteTriggerFired>
   NotifyObjOwner             : N/A
   NotifyObjName              : N/A
  Set entry:
   SetObj                     : 1.3.6.1.2.1.2.2.1.7<ifAdminStatus>
   SetObjWildcard             : true
   SetValue                   : 2
   SetTargetTag               : N/A
   SetContextName             : context1
   SetContextNameWildcard     : false
Object list objectA owned by owner3:
  ObjIndex                    : 1
  ObjID                       : 1.3.6.1.2.1.2.1.0<ifNumber.0>
  ObjIDWildcard               : false
Object list objectA owned by owner3:
  ObjIndex                    : 2
  ObjID                       : 1.3.6.1.2.1.2.2.1.2.0<ifDescr.0>
  ObjIDWildcard               : false
```

For more information about the command output, see Table 1 to Table 4.

Related commands

snmp mib event

snmp mib event object list

snmp mib event trigger

display snmp mib event event

Use **display snmp mib event event** to display information about an event and the event actions.

Syntax

display snmp mib event event [**owner** *event-owner* **name** *event-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

owner *event-owner* **name** *event-name*: Specifies an event by its owner and name. The *event-owner* argument must be an existing SNMPv3 user. The *event-name* argument is a case-sensitive string of 1 to 32 characters. If you do not specify an event, this command displays information about all events and event actions.

Examples

Display information about the event identified by owner **owner2** and name **eventA** and the event actions.

```
<Sysname>display snmp mib event event owner owner2 name eventA
Event entry eventA owned by owner2:
  EvtComment                  : event is to set ifAdminStatus
  EvtAction                   : notification | set
  EvtEnabled                  : true
  Notification entry:
   NotifyOID                  : 1.3.6.1.2.1.88.2.0.1<mteTriggerFired>
   NotifyObjOwner             : N/A
   NotifyObjName              : N/A
  Set entry:
   SetObj                     : 1.3.6.1.2.1.2.2.1.7<ifAdminStatus>
   SetObjWildcard             : true
   SetValue                   : 2
   SetTargetTag               : N/A
   SetContextName             : context1
   SetContextNameWildcard     : false
```

Table 1 Command output

Field	Description
Event entry	
EvtComment	Description for the event.

Field	Description
EvtAction	Event actions: • Set action. • Notification action.
EvtEnabled	Event status: • Enabled. • Disabled.
Notification entry	
NotifyOID	Notification OID.
NotifyObjOwner	Owner of the notification-action object.
NotifyObjName	Name of the object list to be added to the notification.
Set entry	
SetObj	OID of the set-action object.
SetObjWildcard	Wildcarding option for the OID: • **false**—Specifies an object by its OID. • **true**—Enables a wildcard search for OIDs.
SetValue	Value of the set-action object.
SetTargetTag	Remote tag for the set-action object.
SetContextName	Context for the set-action object.
SetContextNameWildcard	Wildcarding option for the context • **false**—Specifies a context. • **true**—Enables wildcard search for contexts.

Related commands

snmp mib event

display snmp mib event object list

Use **display snmp mib event event** to display information about object lists.

Syntax

display snmp mib event object list [**owner** *group-owner* **name** *group-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

owner *group-owner* **name** *group-name*: Specifies an object list by its owner and name. The *objects -owner* argument must be an existing SNMPv3 user. The *objects name* argument is

a case-sensitive string of 1 to 32 characters. If you do not specify an object list, this command displays information about all object lists.

Examples

Display information about the object list identified by owner **owner3** and name **objectA**.

```
<Sysname> display snmp mib event object list owner owner3 name objectA
Object list objectA owned by owner3:
ObjIndex                    : 1
ObjID                       : 1.3.6.1.2.1.2.1.0<ifNumber.0>
ObjIDWildcard               : false
Object list objectA owned by owner3:
ObjIndex                    : 2
ObjID                       : 1.3.6.1.2.1.2.2.1.2.0<ifDescr.0>
ObjIDWildcard               : false
```

Table 2 Command output

Field	Description
ObjIndex	Index of the object.
ObjID	OID of the object.
ObjIDWildcard	Wildcarding option for the OID: • **false**—Specifies the OID. • **true**—Enables wildcard search for OIDs.

Related commands

snmp mib event object list

display snmp mib event summary

Use **display snmp mib event summary** to display Event MIB brief information.

Syntax

display snmp mib event summary

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display Event MIB brief information.

```
<Sysname> display snmp mib event summary
TriggerFailures             : 0
EventFailures               : 0
SampleMinimum               : 1
SampleInstanceMaximum       : 0
```

```
SampleInstance                : 0
SampleInstancesHigh           : 0
SampleInstanceLacks           : 0
```

Table 3 Command output

Field	Description
TriggerFailures	Number of trigger test failures.
EventFailures	Number of notification or set action failures.
SampleMinimum	Minimum sampling interval.
SampleInstanceMaximum	Maximum number of sampled instances.
SampleInstance	Number of current sampled instances.
SampleInstancesHigh	Maximum number of sampled instances.
SampleInstanceLacks	Number of sampling failures after the maximum number of sampled instances is reached.

Related commands

display snmp mib event

display snmp mib event trigger

Use **display snmp mib event trigger** to display information about a trigger and the trigger tests.

Syntax

display snmp mib event trigger [**owner** *trigger-owner* **name** *trigger-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

owner *trigger-owner* **name** *trigger name*: Specifies a trigger by its owner and name. The *trigger-owner* argument must be an existing SNMPv3 user. The *trigger-name* argument is case-sensitive string of 1 to 32 characters. If you do not specify a trigger, this command displays information about all triggers and trigger tests.

Examples

Display information about the trigger identified by owner **owner1** and name **triggerA** and the trigger tests.

```
<Sysname> display snmp mib event trigger owner owner1 name triggerA
Trigger entry triggerA owned by owner1:
  TriggerComment              : triggerA is to monitor the state of the interface
  TriggerTest                 : existence | boolean | threshold
  TriggerSampleType           : absoluteValue
```

```
 TriggerValueID              : 1.3.6.1.2.1.2.2.1.7.3<ifAdminStatus.3>
 TriggerValueIDWildcard      : false
 TriggerTargetTag            : N/A
 TriggerContextName          : context1
 TriggerContextNameWildcard  : true
 TriggerFrequency(in seconds): 600
 TriggerObjOwner             : owner1
 TriggerObjName              : obj1
 TriggerEnabled              : true
 Existence entry:
  ExiTest                    : present | absent
  ExiStartUp                 : present | absent
  ExiObjOwner                : owner1
  ExiObjName                 : object1
  ExiEvtOwner                : owner1
  ExiEvtName                 : event1
 Boolean entry:
  BoolCmp                    : unequal
  BoolValue                  : 1
  BoolStartUp                : true
  BoolObjOwner               : owner1
  BoolObjName                : Objects1
  BoolEvtOwner               : N/A
  BoolEvtName                : N/A
 Threshold entry:
  ThresStartUp               : falling
  ThresRising                : 40
  ThresFalling               : 20
  ThresDeltaRising           : 40
  ThresDeltaFalling          : 20
  ThresObjOwner              : N/A
  ThresObjName               : N/A
  ThresRisEvtOwner           : owner1
  ThresRisEvtName            : event1
  ThresFalEvtOwner           : owner1
  ThresFalEvtName            : event1
  ThresDeltaRisEvtOwner      : owner1
  ThresDeltaRisEvtName       : event1
  ThresDeltaFalEvtOwner      : owner1
  ThresDeltaFalEvtName       : event1
```

Table 4 Command output

Field	Description
Trigger entry	
TriggerComment	Description for the trigger.

Field	Description
TriggerTest	Trigger test type: • Existence. • Boolean. • Threshold.
TriggerSampleType	Trigger sampling method: • **absoluteValue**—Absolute sampling. • **deltaValue**—Delta sampling.
TriggerValueID	OID of the monitored object.
TriggerValueIDWildcard	Wildcarding option for the object OIDs: • **false**—Object OIDs are fully specified • **true**—Object OIDs are wildcarded.
TriggerTargetTag	Remote tag for the monitored object.
TriggerContextName	Context for an object.
TriggerContextNameWildcard	Wildcarding option for the contexts • **false**—Contexts are fully specified. • **true**—Contexts are wildcarded.
TriggerFrequency	Trigger sampling interval.
TriggerObjOwner	Owner of the trigger object.
TriggerObjName	Name of the trigger object.
TriggerEnabled	Trigger status: • **true**—The trigger is enabled. • **false**—The trigger is disabled..
Existence entry	
ExiTest	Type of the existence trigger test: • present. • absent. • changed.
ExiStartUp	Type of the existence trigger test for the first sampling: • present. • absent. • changed.
ExiObjOwner	Owner of the existence trigger test object.
ExiObjName	Name of the existence trigger test object.
ExiEvtOwner	Owner of the existence trigger test event.
ExiEvtName	Name of the existence trigger test event.
Boolean entry	
BoolCmp	Boolean trigger test type: • unequal. • equal. • less. • lessOrEqual. • greater. • greaterOrEqual.

Field	Description
BoolValue	Reference value for the Boolean trigger test.
BoolStartUp	Whether the event is enabled for the first sampling: • **true**—The event is enabled for the first sampling. • **false**—The event is disabled for the first sampling.
BoolObjOwner	Owner of the Boolean trigger test object.
BoolObjName	Name of the Boolean trigger test object.
BoolEvtOwner	Owner of the Boolean event.
BoolEvtName	Name of the Boolean event.
Threshold entry	
ThresStartUp	Threshold trigger test for the first sampling: • rising. • falling. • risingOrFalling.
ThresRising	Rising threshold.
ThresFalling	Falling threshold.
ThresDeltaRising	Delta rising threshold.
ThresDeltaFalling	Delta falling threshold.
ThresObjOwner	Owner of the threshold test object.
ThresObjName	Name of the threshold test object.
ThresRisEvtOwner	Owner of the rising event.
ThresRisEvtName	Name of the rising event.
ThresFalEvtOwner	Owner of the falling event.
ThresFalEvtName	Name of the falling event.
ThresDeltaRisEvtOwner	Owner of the Delta rising event.
ThresDeltaRisEvtName	Name of the Delta rising event.
ThresDeltaFalEvtOwner	Owner of the Delta falling event.
ThresDeltaFalEvtName	Name of the Delta falling event.

Related commands

`snmp mib event trigger`

event (trigger-Boolean view)

Use **`event`** to specify an event for a Boolean trigger test.

Use **`undo event`** to restore the default.

Syntax

`event owner` *`event-owner`* **`name`** *`event-name`*

`undo event`

Default

No event is specified for a Boolean trigger test.

Views

Trigger-Boolean view

Predefined user roles

network-admin

context-admin

Parameters

owner *event-owner*: Specifies the owner of an event. Use the trigger owner as the event owner.

name *event-name*: Specifies the name of an event, a case-sensitive string of 1 to 32 characters.

Examples

Specify an event for a Boolean trigger test.

```
<Sysname> system-view
[Sysname] snmp mib event trigger owner owner1 name triggerA
[Sysname-trigger-owner1-triggerA] test boolean
[Sysname-trigger-owner1-triggerA-boolean] event owner owner1 name event1
```

Related commands

snmp mib event trigger

test

event (trigger-existence view)

Use **event** to specify an event for an existence trigger test.

Use **undo event** to restore the default.

Syntax

event owner *event-owner* **name** *event-name*

undo event

Default

No event is specified for an existence trigger test.

Views

Trigger-existence view

Predefined user roles

network-admin

context-admin

Parameters

owner *event-owner*: Specifies the owner of an event. Use the trigger owner as the event owner.

name *event-name*: Specifies the name of an event, a case-sensitive string of 1 to 32 characters.

Examples

Specify an event for an existence trigger test.

```
<Sysname> system-view
```

```
[Sysname] snmp mib event trigger owner owner1 name triggerA
[Sysname-trigger-owner1-triggerA] test existence
[Sysname-trigger-owner1-triggerA-existence] event owner owner1 name event1
```

Related commands

snmp mib event trigger

test

event enable

Use **event enable** to enable an event.

Use **undo event enable** to disable an event.

Syntax

event enable

undo event enable

Default

An event is disabled.

Views

Event view

Predefined user roles

network-admin

context-admin

Usage guidelines

For an event to be triggered when the trigger condition is met, execute the **event enable** command.

Examples

Enable the event identified by owner **owner1** and name **EventA**.

```
<Sysname> system-view
[Sysname] snmp mib event owner owner1 name EventA
[Sysname-event-owner1-EventA] event enable
```

Related commands

action

snmp mib event

falling

Use **falling** to set a falling threshold and specify a falling event.

Use **undo falling** to restore the default.

Syntax

falling { **event owner** *event-owner* **name** *event-name* | **value** *integer-value* }

undo falling { **event** | **value** }

Default

The falling threshold is 0, and no falling event is specified.

Views

Trigger-threshold view

Predefined user roles

network-admin

context-admin

Parameters

event owner *event-owner*: Specifies the owner of an event. Use the trigger owner as the event owner.

name *event-name*: Specifies the name of an event, a case-sensitive string of 1 to 32 characters.

value *integer-value*: Specifies a falling threshold in the range of –2147483648 to 2147483647. The value must be smaller than or equal to the rising threshold.

Usage guidelines

A falling event is triggered if the value of the monitored object is smaller than or equal to the falling threshold.

If the value of the monitored object crosses the falling threshold at two or more samplings in succession, the event is triggered only at the first sampling.

Examples

Set the falling threshold to 20.

```
<Sysname> system-view
[Sysname] snmp mib event trigger owner owner1 name triggerA
[Sysname-trigger-owner1-triggerA] test threshold
[Sysname-trigger-owner1-triggerA-threshold] falling value 20
```

Related commands

sample

snmp mib event trigger

test

frequency

Use **frequency** to set a sampling interval.

Use **undo event** to restore the default.

Syntax

frequency *interval*

undo frequency

Default

The sampling interval is 600 seconds.

Views

Trigger view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies a sampling interval in the range of 1 to 4294967295 seconds. The sampling interval must be greater than or equal to the minimum sampling interval.

Usage guidelines

To set the minimum sampling interval, execute the **snmp mib event sample minimum** command.

To avoid sampling failure, do not set the sampling interval too small when there are a large number of sampled objects.

Examples

Set the sampling interval for a trigger to 360 seconds.

```
<Sysname> system-view
[Sysname] snmp mib event trigger owner owner1 name triggerA
[Sysname-trigger-owner1-triggerA] frequency 360
```

Related commands

snmp mib event sample minimum

snmp mib event trigger

object list (action-notification view)

Use **object list** to specify an object list for a notification action. The objects in the list will be added to the notification when the notification action is triggered.

Use **undo object list** to restore the default.

Syntax

object list owner *group-owner* **name** *group-name*

undo object list

Default

No object list is specified for a notification action.

Views

Action-notification view

Predefined user roles

network-admin

context-admin

Parameters

owner *group-owner*: Specifies an object list owner. Use the event owner as the object list owner.

name *group-name*: Specifies an object list name, a case-sensitive string of 1 to 32 characters.

Usage guidelines

If you do not specify an object list for a notification action or the specified object list does not contain objects, no objects will be added to the triggered notification.

For more information, see "object list (trigger view)."

Examples

Specify the object list identified by owner **owner1** and name **listA** for the event identified by owner **owner1** and name **EventA**.

```
<Sysname> system-view
[Sysname] snmp mib event owner owner1 name EventA
[Sysname-event-owner1-EventA] action notification
[Sysname-event-owner1-EventA-notification] object list owner owner1 name listA
```

Related commands

action

snmp mib event owner

object list (trigger view)

Use **object list** to specify an object list for a trigger. The objects in the list will be added to the triggered notification.

Use **undo object list** to restore the default.

Syntax

object list owner *group-owner* **name** *group-name*

undo object list

Default

No object list is specified for a trigger.

Views

Trigger view

Predefined user roles

network-admin

context-admin

Parameters

owner *group-owner*: Specifies an object list owner. Use the trigger owner as the object list owner.

name *group-name*: Specifies an object list name, a case-sensitive string of 1 to 32 characters.

Usage guidelines

An object list is identified by its owner and name. After you specify a list of objects for a trigger, the objects in the list are added to the notification when the notification action is triggered.

You can configure the **object list** command in trigger view, trigger-test view (including trigger-Boolean view, trigger existence view, and trigger threshold view), and action-notification view. If the command is configured in any two of the views or all the three views, the object lists are added to the notification in the sequence: trigger view, trigger-test view, and action-notification view.

Examples

Specify the object list identified by owner **owner1** and name **objectA** for a trigger.

```
<Sysname> system-view
[Sysname] snmp mib event trigger owner owner1 name triggerA
[Sysname-trigger-owner1-triggerA] object list owner owner1 name objectA
```

Related commands

snmp mib event trigger

object list (trigger-Boolean view)

Use **object list** to specify an object list for a Boolean trigger test. The objects in the list will be added to the notification triggered by the test.

Use **undo object list** to restore the default.

Syntax

object list owner *group-owner* **name** *group-name*

undo object list

Default

No object list is specified for a Boolean trigger test.

Views

Trigger-Boolean view

Predefined user roles

network-admin

context-admin

Parameters

owner *group-owner*: Specifies an object list owner. Use the trigger owner as the object list owner.

name *group-name*: Specifies an object list name, a case-sensitive string of 1 to 32 characters.

Usage guidelines

For more information, see "object list (trigger view)."

Examples

Specify the object list identified by owner **owner1** and name **objectA** for the trigger-Boolean trigger test.

```
<Sysname> system-view
[Sysname] snmp mib event trigger owner owner1 name triggerA
[Sysname-trigger-owner1-triggerA] test boolean
[Sysname-trigger-owner1-triggerA-boolean] object list owner owner1 name objectA
```

Related commands

snmp mib event trigger

test

object list (trigger-existence view)

Use **object list** to specify an object list for an existence trigger test. The objects in the list will be added to the notification triggered by the test.

Use **undo object list** to restore the default.

Syntax

object list owner *group-owner* **name** *group-name*

undo object list

Default

No object list is specified for an existence trigger test.

Views

Trigger- existence view

Predefined user roles

network-admin

context-admin

Parameters

owner *group-owner*: Specifies an object list owner. Use the trigger owner as the object list owner

name *group-name*: Specifies an object list name, a case-sensitive string of 1 to 32 characters.

Usage guidelines

For more information, see "object list (trigger view)."

Examples

Specify the object list identified by owner **owner1** and name **objectA** for the existence trigger test.

```
<Sysname> system-view
[Sysname] snmp mib event trigger owner owner1 name triggerA
[Sysname-trigger-owner1-triggerA] test existence
[Sysname-trigger-owner1-triggerA-existence] object list owner owner1 name objectA
```

Related commands

snmp mib event trigger

test

object list (trigger-threshold view)

Use **object list** to specify an object list for a trigger-threshold test. The objects in the list will be added to the notification triggered by the test.

Use **undo object list** to restore the default.

Syntax

object list owner *group-owner* **name** *group-name*

undo object list

Default

No object list is specified for a trigger-threshold test.

Views

Trigger-threshold view

Predefined user roles

network-admin

context-admin

Parameters

owner *group-owner*: Specifies an object list owner. Use the trigger owner as the object list owner.

name *group-name*: Specifies an object list name, a case-sensitive string of 1 to 32 characters.

Usage guidelines

For more information, see "object list (trigger view)."

Examples

Specify the object list identified by owner **owner1** and name **objectA** for the trigger-threshold test.

```
<Sysname> system-view
[Sysname] snmp mib event trigger owner owner1 name triggerA
[Sysname-trigger-owner1-triggerA] test threshold
[Sysname-trigger-owner1-triggerA-threshold] object list owner owner1 name objectA
```

Related commands

snmp mib event trigger

test

oid (action-notification view)

Use **oid** to specify a notification to be sent when the notification action is triggered.

Use **undo oid** to restore the default.

Syntax

oid *object-identifier*

undo oid

Default

The OID is 0.0. No notification is specified for a notification action.

Views

Action-notification view

Predefined user roles

network-admin

context-admin

Parameters

object-identifier: Specifies a notification by its OID, a case-sensitive string of 1 to 255 characters. It must be a trap node.

Examples

Specify the notification identified by OID **1.3.6.1.2.1.14.16.2.1** for the event identified by owner **owner1** and name **EventA**.

```
<Sysname> system-view
[Sysname] snmp mib event owner owner1 name EventA
[Sysname-event-owner1-EventA] action notification
[Sysname-event-owner1-EventA-notification] oid 1.3.6.1.2.1.14.16.2.1
```

Related commands

action

snmp mib event owner

oid (action-set view)

Use **oid** to specify a set-action object.

Use **undo oid** to restore the default.

Syntax

oid *object-identifier*

undo oid

Default

The OID is 0.0. No object is specified for a set action.

Views

Action-set view

Predefined user roles

network-admin

context-admin

Parameters

object-identifier: Specifies an object by its OID or name, a case-sensitive string of 1 to 255 characters. The object can be a table node, conceptual row node, table column node, leaf node, or parent leaf node.

Examples

Specify the object identified by OID **1.3.6.1.2.1.2.2.1.7.3** for the set action of an event identified by owner **owner1** and name **EventA**.

```
<Sysname> system-view
[Sysname] snmp mib event owner owner1 name EventA
[Sysname-event-owner1-EventA] action set
[Sysname-event-owner1-EventA-set] oid 1.3.6.1.2.1.2.2.1.7.3
```

Related commands

action

snmp mib event owner

wildcard oid (**action-set view**)

oid (trigger view)

Use **oid** to specify a MIB object for trigger sampling.

Use **undo oid** to restore the default.

Syntax

oid *object-identifier*

undo oid

Default

The OID is 0.0. No MIB object is specified for trigger sampling.

Views

Trigger view

Predefined user roles

network-admin

context-admin

Parameters

object-identifier: Specifies an object by its OID or name, a case-sensitive string of 1 to 255 characters. The object can be a table node, conceptual row node, table column node, leaf node, or parent leaf node.

Examples

Specify the object identified by OID **1.3.6.1.2.1.2.2.1.1.3** for trigger sampling.

```
<Sysname> system-view
[Sysname] snmp mib event trigger owner owner1 name triggerA
[Sysname-trigger-owner1-triggerA] oid 1.3.6.1.2.1.2.2.1.1.3
```

Related commands

snmp mib event trigger

rising

Use **rising** to specify a rising threshold.

Use **undo rising** to restore the default.

Syntax

rising { **event owner** *event-owner* **name** *event-name* | **value** *integer-value* }

undo rising { **event** | **value** }

Default

The rising threshold is 0, and no rising event is specified.

Views

Trigger-threshold view

Predefined user roles

network-admin

context-admin

Parameters

event owner *event-owner*: Specifies an event owner. Use the trigger owner as the event owner.

name *event-name*: Specifies an event name, a case-sensitive string of 1 to 32 characters.

value *integer-value*: Specifies a rising threshold in the range of –2147483648 to 2147483647. The value must be greater than or equal to the falling threshold.

Usage guidelines

If the value of the monitored object crosses the rising threshold at two or more samplings in succession, an event is triggered only at the first sampling.

Examples

Set the rising threshold to 50 and specify the rising event identified by owner **owner1** and name **event1** for the threshold test.

```
<Sysname> system-view
```

```
[Sysname] snmp mib event trigger owner owner1 name triggerA
[Sysname-trigger-owner1-triggerA] test threshold
[Sysname-trigger-owner1-triggerA-threshold] rising value 50
[Sysname-trigger-owner1-triggerA-threshold] rising event owner owner1 name event1
```

Related commands

sample

snmp mib event trigger

test

sample

Use **sample** to specify a sampling method.

Use **undo sample** to restore the default.

Syntax

sample { **absolute** | **delta** }

undo sample

Default

The sampling method is **absolute**.

Views

Trigger view

Predefined user roles

network-admin

context-admin

Parameters

absolute: Specifies the absolute sampling method. Use the current sampled value.

delta: Specifies the delta sampling method. Use the difference between the current sampled value and previous sampled value.

Usage guidelines

For delta sampling, obtain the difference between the current sampled value and previous sampled value as follows:

- If the object value is UINT type, use the larger value to subtract the smaller value.
- If the object value is INT type, use the present sampled value to subtract the previous sampled value.

Examples

Specify the absolute sampling method.

```
<Sysname>system-view
[Sysname] snmp mib event trigger owner owner1 name triggerA
[Sysname-trigger-owner1-triggerA] sample absolute
```

Related commands

snmp mib event trigger

snmp mib event

Use **snmp mib event** to create an event and enter its view, or enter the view of an existing event.

Use **undo snmp mib event** to remove an event.

Syntax

snmp mib event owner *event-owner* **name** *event-name*

undo snmp mib event owner *event-owner* **name** *event-name*

Default

No event exists.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

event-owner: Specifies an event owner. The event owner must be an existing SNMPv3 user.

event-name: Specifies an event name, a case-sensitive string of 1 to 32 characters.

Usage guidelines

An event is identified by its owner and name.

Examples

Create an event identified by owner **owner1** and name **EventA** and enter its view.

```
<Sysname> system-view
[Sysname] snmp mib event owner owner1 name EventA
[Sysname-event-owner1-EventA]
```

Related commands

action

description

event enable

snmp mib event

snmp mib event object list

Use **snmp mib event object list** to configure an Event MIB object list.

Use **undo snmp mib event object list** to restore the default.

Syntax

snmp mib event object list owner *group-owner* **name** *group-name object-index* **oid** *object-identifier* [**wildcard**]

undo snmp mib event object list owner *group-owner* **name** *group-name object--index*

Default

No Event MIB object list is configured.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

owner *group-owner*: Specifies an object list owner. The object list owner must be an existing SNMPv3 user.

name *group-name*: Specifies an object list name, a case-sensitive string of 1 to 32 characters.

object-index argument: Specifies an object list index in the range of 1 to 4294967295.

oid *object-identifier*: Specifies an object by its OID or name, a case-sensitive string of 1 to 255 characters. The object can be a table node, a conceptual row node, a table column node, a leaf mode, or a parent leaf node.

wildcard: Enables wildcard search for objects. If you do not specify this keyword, the object is specified.

Usage guidelines

An object list is identified by its owner, name, and index. The specified objects in the object list will be carried in the triggered notification to the NMS.

Examples

Configure an object list identified by owner **owner1**, name **objectA**, and index **10**. Specify the object identified by OID **1.3.6.1.2.1.2.2.1.1.3** to be carried in the triggered notification.

```
<Sysname> system-view
[Sysname] snmp mib event object list owner owner1 name objectA 10 oid 1.3.6.1.2.1.2.2.1.1.3
```

Related commands

snmp mib event

snmp mib event trigger

snmp mib event sample instance maximum

Use **snmp mib event sample instance maximum** to specify the maximum number of object instances that can be concurrently sampled.

Use **undo snmp mib event sample instance maximum** to restore the default.

Syntax

snmp mib event sample instance maximum *max-number*

undo snmp mib event sample instance maximum

Default

The maximum number of object instances that can be concurrently sampled is limited by the available resources. The value is 0.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

max-number: Specifies the maximum number of object instances that can be concurrently sampled. The value is in the range of 0 to 4294967295.

Usage guidelines

If you use the wildcard option for an object, Event MIB also samples the wildcarded object instances. Include the wildcarded object instances when you calculate the number of the concurrently sampled instances.

Changing the maximum number of object instances that can be concurrently sampled does not affect the existing instances. If the maximum number of object instances that can be concurrently sampled is changed to a value smaller than the number of existing instances, the existing instances will continue to be sampled.

Examples

Set the maximum number to 10 for the object instances that can be concurrently sampled.

```
<Sysname> system-view
[Sysname] snmp mib event sample instance maximum 10
```

Related commands

snmp mib event sample minimum

snmp mib event sample minimum

Use **snmp mib event sample minimum** to specify the minimum sampling interval.

Use **undo snmp mib event sample minimum** to restore the default.

Syntax

snmp mib event sample minimum *min-number*

undo snmp mib event sample minimum

Default

The minimum sampling interval is 1 second.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

min-number: Specifies the minimum sampling interval in the range of 1 to 2147483647, in seconds.

Usage guidelines

After you configure the minimum sampling interval, make sure the trigger sampling interval is greater than or equal to the minimum sampling interval.

Changing the minimum sampling interval does not affect the existing instances. If the minimum sampling interval is changed to a value smaller than the sampling interval of a trigger, the existing instances of the trigger will continue to be sampled at its interval.

Examples

Set the minimum sampling interval to 50 seconds.

```
<Sysname> system-view
[Sysname] snmp mib event sample minimum 50
```

Related commands

frequency

snmp mib event trigger

snmp mib event trigger

Use **snmp mib event trigger** to create a trigger and enter its view, or enter the view of an existing trigger.

Use **undo snmp mib event trigger** to remove a trigger.

Syntax

snmp mib event trigger owner *trigger-owner* **name** *trigger-name*

undo snmp mib event trigger owner *trigger-owner* **name** *trigger-name*

Default

No trigger exists.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

trigger-owner: Specifies a trigger owner, which must be an existing SNMPv3 user.

trigger-name: Specifies a trigger name, a case-sensitive string of 1 to 32 characters.

Usage guidelines

A trigger is identified by its owner and name. In trigger view, you can specify a monitored object and set an interval for sampling the object. An event is triggered when the sampled object meets the trigger condition.

If the trigger owner has no read access to the monitored object configured in trigger view, sampling on the object cannot be performed. For more information about SNMPv3 user access rights, see *Network Management and Monitoring Configuration Guide*.

Examples

Create a trigger identified by owner **owner1** and name **triggerA**.

```
<Sysname> system-view
[Sysname] snmp mib event trigger owner owner1 name triggerA
[Sysname-trigger-owner1-triggerA]
```

snmp-agent trap enable event-mib

Use **snmp-agent trap enable event-mib** to enable the Event MIB trap feature.

Use **undo snmp-agent trap enable event-mib** to disable the Event MIB trap feature.

Syntax

snmp-agent trap enable event-mib

undo snmp-agent trap enable event-mib

Default

The Event MIB trap feature is enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

After you enable the Event MIB trap feature, traps are generated when object sampling fails or a trigger condition is met and sent to the SNMP module. Traps include trigger trap, rising threshold break trap, falling threshold break trap, trigger-condition detection failure trap, and set-action trigger failure trap.

For the traps to be sent correctly, you must also configure SNMP on the device. For more information about SNMP configuration, see *Network Management and Monitoring Configuration Guide*.

Examples

Enable the event MIB trap feature.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable event-mib
```

startup (trigger-existence view)

Use **startup** to specify existence trigger test types for the first sampling.

Use **undo startup** to remove the existence trigger test types for the first sampling.

Syntax

startup { **absent** | **present** }

undo startup { **absent** | **present** }

Default

The existence trigger test types for the first sampling are **present** and **absent**.

Views

Trigger-existence view

Predefined user roles

network-admin

context-admin

Parameters

absent: Monitors the absence of a MIB object.

present: Monitors the presence of a MIB object.

Usage guidelines

For the first sampling, an event is triggered when the following conditions are met:

- Both the **startup** and **type** commands specify the existence test type as present and the state of the monitored object changes to present at the first sampling. If the monitored objects are wildcarded, the event is triggered independently for each wildcarded object.
- Both the **startup** command and **type** commands specify the existence trigger test type as absent and the state of the monitored object changes to absent at the first sampling. If the monitored objects are wildcarded, no event is triggered.

Examples

Remove the present test configuration for the first sampling.

```
<Sysname> system-view
[Sysname] snmp mib event trigger owner owner1 name triggerA
[Sysname-trigger-owner1-triggerA] test existence
[Sysname-trigger-owner1-triggerA-existence] undo startup present
```

Related commands

type

startup (trigger-threshold view)

Use **startup** to specify a threshold trap type for the first sampling.

Use **undo startup** to restore the default.

Syntax

startup { **falling** | **rising** | **rising-or-falling** }

undo startup

Default

The threshold trap type for the first sampling is **rising-or-falling**.

Views

Trigger-threshold view

Predefined user roles

network-admin

context-admin

Parameters

falling: Specifies the falling trap.

rising: Specifies the rising trap.

rising-or-falling: Specifies the rising or falling trap.

Usage guidelines

If the trap type for the first sampling is **rising** or **rising-or-falling**, a rising trap is triggered when the first sample value is greater than or equal to the rising threshold.

If the trap type for the first sampling is **rising** or **rising-or-falling**, a falling trap is triggered when the first sample value is smaller than or equal to the rising threshold.

If the first sampling fails or the monitored object does not exist at the first sampling, the second sampling is considered the first sampling.

Examples

Specify the rising trap for the first sampling.

```
<Sysname> system-view
[Sysname] snmp mib event trigger owner owner1 name triggerA
[Sysname-trigger-owner1-triggerA] test threshold
[Sysname-trigger-owner1-triggerA-threshold] startup rising
```

Related commands

sample

snmp mib event trigger

test

startup enable

Use **startup enable** to enable an event to be triggered for the first Boolean sampling.

Use **undo startup enable** to disable an event to be triggered for the first Boolean sampling.

Syntax

startup enable

undo startup enable

Default

An event is triggered for the first Boolean sampling.

Views

Trigger-Boolean view

Predefined user roles

network-admin

context-admin

Usage guidelines

For an event to be triggered when a trigger condition is met at the first Boolean sampling, execute the **startup enable** command.

If the first sampling fails or the monitored object does not exist at the first sampling, the second sampling is considered the first sampling.

Examples

Trigger an event for the first Boolean sampling.

```
<Sysname> system-view
[Sysname] snmp mib event trigger owner owner1 name triggerA
[Sysname-trigger-owner1-triggerA] test boolean
[Sysname-trigger-owner1-triggerA-boolean] startup enable
```

Related commands

comparison

value

test

Use **test** to specify a trigger test type and enter its view.

Use **undo test** to remove a trigger test type.

Syntax

test { **boolean** | **existence** | **threshold** }

undo test { **boolean** | **existence** | **threshold** }

Default

No test type is specified for a trigger.

Views

Trigger view

Predefined user roles

network-admin

context-admin

Parameters

boolean: Specifies a Boolean trigger test. This test compares the value of the monitored object with the reference value.

existence: Specifies an existence trigger test. This test monitors the absence, presence, and change of the monitored object.

threshold: Specifies a threshold test. This test compares the value of the monitored object with the specified thresholds, such as rising threshold and falling threshold.

Usage guidelines

For more information about the trigger tests, see the commands in the trigger-Boolean view, trigger-existence view, and trigger-threshold view .

Examples

Specify the existence test for a trigger.

```
<Sysname> system-view
[Sysname] snmp mib event trigger owner owner1 name triggerA
[Sysname-trigger-owner1-triggerA] test existence
```

Related commands

snmp mib event trigger

trigger enable

Use **trigger enable** to enable a trigger.

Use **undo trigger enable** to disable a trigger.

Syntax

trigger enable

undo trigger enable

Default

A trigger is disabled.

Views

Trigger view

Predefined user roles

network-admin

context-admin

Usage guidelines

Before you enable a trigger, make sure the trigger meets the following conditions:

- A monitored object is specified for the trigger.
- The trigger sampling interval is greater than or equal to the minimum sampling interval.

Examples

Create and enable a trigger.

```
<Sysname>system-view
[Sysname] snmp mib event trigger owner owner1 name triggerA
[Sysname-trigger-owner1-triggerA] oid 1.3.6.1.2.1.2.2.1.1.3
[Sysname-trigger-owner1-triggerA] frequency 360
[Sysname-trigger-owner1-triggerA] trigger enable
```

Related commands

snmp mib event trigger

type

Use **type** to specify existence trigger test types.

Use **undo type** to remove the existence trigger test types.

Syntax

type { **absent** | **changed** | **present** }

undo type { **absent** | **changed** | **present** }

Default

The existence trigger test types are **present** and **absent**.

Views

Trigger-existence view

Predefined user roles

network-admin

context-admin

Parameters

absent: Monitors the absence of an object.

changed: Monitors the change of the value of an object. If the last sampling does not obtain a value, the event is not triggered.

present: Monitors the presence of an object.

Usage guidelines

For the first sampling, see "startup (trigger-existence view)".

The existence trigger tests also apply to the wildcarded instances of the monitor object.

Examples

Specify the existence trigger test type as **present**.

```
<Sysname> system-view
[Sysname] snmp mib event trigger owner owner1 name triggerA
[Sysname-trigger-owner1-triggerA] test existence
[Sysname-trigger-owner1-triggerA-existence] type present
```

Related commands

snmp mib event trigger

startup

test

value (action-set view)

Use **value** to set a value for a set-action object.

Use **undo value** to restore the default.

Syntax

value *integer-value*

undo value

Default

The value of a set-action object is 0.

Views

Action-set view

Predefined user roles

network-admin

context-admin

Parameters

integer-value: Specifies a value for a set-action object. The value is in the range of –2147483648 to +2147483647.

Examples

Set the value to 2 for the set-action object identified by OID **1.3.6.1.2.1.2.2.1.7.3**.

```
<Sysname> system-view
[Sysname] snmp mib event owner owner1 name EventA
[Sysname-event-owner1-EventA] action set
[Sysname-event-owner1-EventA-set] oid 1.3.6.1.2.1.2.2.1.7.3
[Sysname-event-owner1-EventA-set] value 2
```

Related commands

action

mib event owner

oid

value (trigger-Boolean view)

Use **value** to set a reference value for a Boolean trigger test.

Use **undo value** to restore the default.

Syntax

value *integer-value*

undo value

Default

The reference value is 0.

Views

Trigger-Boolean view

Predefined user roles

network-admin

context-admin

Parameters

integer-value: Specifies a reference value in the range of –2147483648 to +2147483647.

Usage guidelines

A Boolean trigger test compares the sampled value with the reference value.

Examples

Set the reference value to 5 for the Boolean trigger test.

```
<Sysname> system-view
[Sysname] snmp mib event trigger owner owner1 name triggerA
[Sysname-trigger-owner1-triggerA] test boolean
[Sysname-trigger-owner1-triggerA-boolean] value 5
```

Related commands

snmp mib event trigger

startup

test

wildcard context (action-set view)

Use **wildcard context** to enable wildcard search for the contexts of a set-action object.

Use **undo wildcard context** to restore the default.

Syntax

wildcard context

undo wildcard context

Default

The context of a set-action object is fully specified.

Views

Action-set view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command must be used with the **context** command. A wildcarded context has two parts: the context specified by the **context** command and the wildcarded part.

Examples

Specify the context for the set-action object as **contextname1** and enable wildcard search for the contexts.

```
<Sysname>system-view
[Sysname] snmp mib event owner owner1 name EventA
[Sysname-event-owner1-EventA] action set
[Sysname-event-owner1-EventA-set] context contextname1
[Sysname-event-owner1-EventA-set] wildcard context
```

Related commands

action set

context

snmp mib event owner

wildcard context (trigger view)

Use **wildcard context** to enable wildcard search for the contexts of a monitored object.

Use **undo wildcard context** to restore the default.

Syntax

wildcard context

undo wildcard context

Default

The context of a monitored object is fully specified.

Views

Trigger view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command must be used with the **context** command. A wildcarded context has two parts: the context specified by the **context** command and the wildcarded part.

Examples

Specify the contexts for the monitored object as **contextname** and enable wildcard search for the contexts.

```
<Sysname> system-view
[Sysname] snmp mib event trigger owner owner1 name triggerA
[Sysname-trigger-owner1-triggerA] context contextname
[Sysname-trigger-owner1-triggerA] wildcard context
```

Related commands

context

snmp mib event trigger

wildcard oid (action-set view)

Use **wildcard oid** to enable wildcard search for the set-action object OIDs.

Use **undo wildcard oid** to restore the default.

Syntax

wildcard oid

undo wildcard oid

Default

The set-action object OID is fully specified.

Views

Action-set view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command must be used in conjunction with the **oid** command. A wildcarded OID has two parts: the OID specified by the **oid** command and the wildcarded part.

Examples

Specify the set-action object by its OID **1.3.6.1.2.1.2.2.1.7** for the event identified by owner **owner1** and name **EventA**. Enable wildcard search for the sec-action object OIDs.

```
<Sysname> system-view
[Sysname] snmp mib event owner owner1 name EventA
[Sysname-event-owner1-EventA] action set
[Sysname-event-owner1-EventA-set] oid 1.3.6.1.2.1.2.2.1.7
[Sysname-event-owner1-EventA-set] wildcard oid
```

Related commands

action set

oid

snmp mib event owner

wildcard oid (trigger view)

Use **wildcard oid** to enable wildcard search for the monitored object OIDs.

Use **undo wildcard oid** to restore the default.

Syntax

wildcard oid

undo wildcard oid

Default

A monitored object OID is fully specified.

Views

Trigger view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command must be used in conjunction with the **oid** command.

A wildcarded OID has two parts: the OID specified by the **oid** command and the wildcarded part.

For example, to specify interface description nodes of all interfaces, execute the **oid ifDescr** and **wildcard oid** commands.

Examples

Specify the sampled object by its OID **1.3.6.1.2.1.1.6** for a trigger and enable wildcard search for the monitored object OIDs.

```
<Sysname>system-view
[Sysname] snmp mib event trigger owner owner1 name triggerA
[Sysname-trigger-owner1-triggerA] oid 1.3.6.1.2.1.1.6
[Sysname-trigger-owner1-triggerA] wildcard oid
```

Related commands

oid

snmp mib event trigger

Contents

CWMP commands

cwmp

Use **cwmp** to enter CWMP view.

Syntax

cwmp

Views

System view

Predefined user roles

network-admin

context-admin

Examples

Enter CWMP view.

```
<Sysname> system-view
[Sysname] cwmp
```

Related commands

cwmp enable

cwmp acs default password

Use **cwmp acs default password** to configure a password for authentication to the default ACS URL.

Use **undo cwmp acs default password** to restore the default.

Syntax

cwmp acs default password { **cipher** | **simple** } *string*

undo cwmp acs default password

Default

No password is configured for authentication to the default ACS URL.

Views

CWMP view

Predefined user roles

network-admin

context-admin

Parameters

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 255 characters. Its encrypted form is a case-sensitive string of 33 to 373 characters.

Usage guidelines

You can configure only one password for authentication to the default ACS URL. If you execute this command multiple times, the most recent configuration takes effect.

For a successful connection, make sure the CPE has the same username and password settings as the ACS.

Examples

Configure the password used for authentication to the default ACS URL.

```
<Sysname> system-view
[Sysname] cwmp
[Sysname-cwmp] cwmp acs default password simple newpsw
```

Related commands

cwmp acs default url

cwmp acs default username

cwmp acs default url

Use **cwmp acs default url** to specify a default ACS URL.

Use **undo cwmp acs default url** to restore the default.

Syntax

cwmp acs default url *url*

undo cwmp acs default url

Default

No default ACS URL is specified.

Views

CWMP view

Predefined user roles

network-admin

context-admin

Parameters

url: Specifies the default ACS URL, a string of 8 to 255 characters. The URL must use the **http://***host[:port]/path* or **https://***host[:port]/path* format.

Usage guidelines

The CPE attempts to connect to the default ACS URL if no ACS URL has been assigned to it through the **cwmp acs url** command or DHCP.

You can configure only one default ACS URL. If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the default ACS URL.

```
<Sysname> system-view
[Sysname] cwmp
[Sysname-cwmp] cwmp acs default url http://www.acs.com:9090
```

Related commands

cwmp acs default password

cwmp acs default username

cwmp acs default username

Use **cwmp acs default username** to configure the username for authentication to the default ACS URL.

Use **undo cwmp acs default username** to restore the default.

Syntax

cwmp acs default username *username*

undo cwmp acs default username

Default

No username is configured for authentication to the default ACS URL.

Views

CWMP view

Predefined user roles

network-admin

context-admin

Parameters

username: Specifies a username, a case-sensitive string of 1 to 255 characters.

Usage guidelines

You can configure only one username for authentication to the default ACS URL. If you execute this command multiple times, the most recent configuration takes effect.

For a successful connection, make sure the CPE has the same username and password settings as the ACS.

Examples

Configure the username for authentication to the default ACS URL.

```
<Sysname> system-view
[Sysname] cwmp
[Sysname-cwmp] cwmp acs default username newname
```

Related commands

cwmp acs default password

cwmp acs default url

cwmp acs password

Use **cwmp acs password** to configure the password for authentication to the preferred ACS URL.

Use **undo cwmp acs password** to restore the default.

Syntax

cwmp acs password { **cipher** | **simple** } *string*

undo cwmp acs password

Default

No password is configured for authentication to the preferred ACS URL.

Views

CWMP view

Predefined user roles

network-admin

context-admin

Parameters

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 255 characters. Its encrypted form is a case-sensitive string of 33 to 373 characters.

Usage guidelines

You can configure only one password for authentication to the preferred ACS URL. If you execute this command multiple times, the most recent configuration takes effect.

For a successful connection, make sure the CPE has the same username and password settings as the ACS.

Examples

Configure the password used for authentication to the preferred ACS URL.

```
<Sysname> system-view
[Sysname] cwmp
[Sysname-cwmp] cwmp acs password simple newpsw
```

Related commands

cwmp acs url

cwmp acs username

cwmp acs url

Use **cwmp acs url** to specify a preferred ACS URL.

Use **undo cwmp acs url** to restore the default.

Syntax

cwmp acs url *url*

undo cwmp acs url

Default

No preferred ACS URL is specified.

Views

CWMP view

Predefined user roles

network-admin

context-admin

Parameters

url: Specifies the preferred ACS URL, a string of 8 to 255 characters. The URL must use the **http://***host[:port]/path* or **https://***host[:port]/path* format.

Usage guidelines

The device supports only one preferred ACS URL. If you execute this command multiple times, the most recent configuration takes effect.

The preferred ACS URL is configurable from the CPE's CLI, the DHCP server, and the ACS. The CLI- and ACS-assigned URLs have higher priority than the DHCP-assigned URL. The CLI- and ACS-assigned URLs overwrite each other.

The CPE uses the default ACS attributes for connection establishment only when it is not assigned a preferred ACS URL from the CLI, ACS, or DHCP server.

Examples

Specify the ACS URL.

```
<Sysname> system-view
[Sysname] cwmp
[Sysname-cwmp] cwmp acs url http://www.acs.com:9090
```

cwmp acs username

Use **cwmp acs username** to configure the username for authentication to the preferred ACS URL.

Use **undo cwmp acs username** to restore the default.

Syntax

cwmp acs username *username*

undo cwmp acs username

Default

No username is configured for authentication to the preferred ACS URL.

Views

CWMP view

Predefined user roles

network-admin

context-admin

Parameters

username: Specifies a username, a case-sensitive string of 1 to 255 characters.

Usage guidelines

You can configure only one username for authentication to the preferred ACS URL. If you execute this command multiple times, the most recent configuration takes effect.

For a successful connection, make sure the CPE has the same username and password settings as the ACS.

Examples

Configure the username used for authentication to the preferred ACS URL.

```
<Sysname> system-view
[Sysname] cwmp
```

```
[Sysname-cwmp] cwmp acs username newname
```

Related commands

cwmp acs password

cwmp cpe connect interface

Use **cwmp cpe connect interface** to specify the CWMP connection interface.

Use **undo cwmp cpe connect interface** to restore the default.

Syntax

cwmp cpe connect interface *interface-type interface-number*

undo cwmp cpe connect interface

Default

No CWMP connection interface is specified.

Views

CWMP view

Predefined user roles

network-admin

context-admin

Parameters

interface-type interface-number: Specifies the type and number of the CWMP connection interface.

Usage guidelines

A CWMP connection interface is the interface that the CPE uses to communicate with the ACS. To establish a CWMP connection, the CPE sends the IP address of this interface in the Inform message, and the ACS replies to this IP address.

Typically, the CPE selects the CWMP connection interface automatically. If the CWMP connection interface is not the interface that connects the CPE to the ACS, the CPE fails to establish a CWMP connection with the ACS. For example, an incorrect CWMP connection interface selection occurs when the following conditions exist:

- The CPE has multiple Layer 3 interfaces.
- The IP addresses of the CWMP connection interface and the ACS are not in the same subnet.

In this case, you need to use this command to manually specify the CWMP connection interface.

Examples

Specify GigabitEthernet 1/0/1 as the CWMP connection interface.

```
<Sysname> system-view
[Sysname] cwmp
[Sysname-cwmp] cwmp cpe connect interface gigabitethernet 1/0/1
```

cwmp cpe connect retry

Use **cwmp cpe connect retry** to set the maximum number of attempts the CPE can make to retry a failed CWMP connection.

Use **undo cwmp cpe connect retry** to restore the default.

Syntax

cwmp cpe connect retry *retries*

undo cwmp cpe connect retry

Default

The CPE retries a failed connection until the connection is established with the ACS.

Views

CWMP view

Predefined user roles

network-admin

context-admin

Parameters

retries: Specifies the maximum number of CWMP connection retries. The value range is 0 to 100. To disable the CPE to retry a CWMP connection, set this argument to 0.

Usage guidelines

The CPE retries connecting to the ACS when its initial connection attempt fails or the CWMP session is ended before the CPE receives a session closed message from the ACS. The CPE does not stop its connection retry attempts until the connection is established or the number of connection retries reaches the upper limit.

Examples

Set the maximum number of CWMP connection retries to 5.

```
<Sysname> system-view
[Sysname] cwmp
[Sysname-cwmp] cwmp cpe connect retry 5
```

cwmp cpe inform interval

Use **cwmp cpe inform interval** to set the periodic Inform interval.

Use **undo cwmp cpe inform interval** to restore the default.

Syntax

cwmp cpe inform interval *interval*

undo cwmp cpe inform interval

Default

The periodic Inform interval is 600 seconds.

Views

CWMP view

Predefined user roles

network-admin

context-admin

Parameters

interval: Sets the periodic Inform interval in the range of 10 to 86400 seconds.

Usage guidelines

This command sets the interval for the CPE to send Inform messages automatically to the ACS. For the command to take effect, you must configure the **cwmp cpe inform interval enable** command.

Examples

Set the periodic Inform interval to 3600 seconds.

```
<Sysname> system-view
[Sysname] cwmp
[Sysname-cwmp] cwmp cpe inform interval enable
[Sysname-cwmp] cwmp cpe inform interval 3600
```

Related commands

cwmp cpe inform interval enable

cwmp cpe inform interval enable

Use **cwmp cpe inform interval enable** to enable the periodic Inform feature.

Use **undo cwmp cpe inform interval enable** to disable the periodic Inform feature.

Syntax

cwmp cpe inform interval enable

undo cwmp cpe inform interval enable

Default

The CPE does not send Inform messages periodically.

Views

CWMP view

Predefined user roles

network-admin

context-admin

Usage guidelines

If this command is configured, the CPE sends Inform messages regularly to establish a CWMP session with the ACS. To set the periodic Inform interval, use the **cwmp cpe inform interval** command.

Examples

Enable the periodic Inform feature.

```
<Sysname> system-view
[Sysname] cwmp
[Sysname-cwmp] cwmp cpe inform interval enable
```

Related commands

cwmp cpe inform interval

cwmp cpe inform time

Use **cwmp cpe inform time** to schedule a connection initiation for the CPE to connect to the ACS.

Use **undo cwmp cpe inform time** to restore the default.

Syntax

cwmp cpe inform time *time*

undo cwmp cpe inform time

Default

No connection initiation has been scheduled.

Views

CWMP view

Predefined user roles

network-admin

context-admin

Parameters

time: Specifies the time at which the CPE sends an Inform message. The time format is *yyyy-mm-dd*T*hh:mm:ss*, and the value range is 1970-01-01T00:00:00 to 2035-12-31T23:59:59. The specified time must be greater than the current system time.

Examples

Configure the CPE to send an Inform message at 2007-12-01T20:00:00.

```
<Sysname> system-view
[Sysname] cwmp
[Sysname-cwmp] cwmp cpe inform time 2012-12-01T20:00:00
```

cwmp cpe password

Use **cwmp cpe password** to configure the password for the CPE to authenticate the ACS.

Use **undo cwmp cpe password** to restore the default.

Syntax

cwmp cpe password { **cipher** | **simple** } *string*

undo cwmp cpe password

Default

No password is configured for authenticating the ACS.

Views

CWMP view

Predefined user roles

network-admin

context-admin

Parameters

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 255 characters. Its encrypted form is a case-sensitive string of 33 to 373 characters.

Usage guidelines

You can configure only one password for the ACS to authenticate to the CPE when it initiates a connection. If you execute this command multiple times, the most recent configuration takes effect.

For a successful connection, make sure the ACS has the same username and password settings as the CPE.

If a password is configured, the ACS must provide the correct password when it initiates a connection to the CPE. If the password is incorrect, the CPE denies the connection request from the ACS.

You do not need to configure this command if you want to authenticate the ACS only based on its username.

Examples

Configure the password used for authenticating the ACS.

```
<Sysname> system-view
[Sysname] cwmp
[Sysname-cwmp] cwmp cpe password simple newpsw
```

Related commands

cwmp cpe username

cwmp cpe provision-code

Use **cwmp cpe provision-code** to configure the provision code of the CPE.

Use **undo cwmp cpe provision-code** to restore the default.

Syntax

cwmp cpe provision-code *provision-code*

undo cwmp cpe provision-code

Default

The provision code is **PROVISIONINGCODE**.

Views

CWMP view

Predefined user roles

network-admin

context-admin

Parameters

provision-code: Specifies a provision code, a string of 1 to 64 characters. The string can contain uppercase letters, digits, and the full stop (.).

Usage guidelines

The ACS can use the provision code to identify services assigned to each CPE. For correct configuration deployment, make sure the same provision code is configured on the CPE and the ACS. For information about the support of your ACS for provision codes, see the ACS documentation.

The CPE can have only one provision code. If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the provision code to **ABC20150714**.

```
<Sysname> system
[Sysname] cwmp
[Sysname-cwmp] cwmp cpe provision-code ABC20150714
```

cwmp cpe stun enable

Use **cwmp cpe stun enable** to enable NAT traversal for the connection requests from the ACS to reach the CPE through a NAT gateway.

Use **undo cwmp cpe stun enable** to disable NAT traversal for the connection requests from the ACS to reach the CPE through a NAT gateway.

Syntax

cwmp cpe stun enable

undo cwmp cpe stun enable

Default

NAT traversal is disabled for CWMP.

Views

CWMP view

Predefined user roles

network-admin

context-admin

Usage guidelines

Connection requests initiated from the CPE can reach the ACS through a NAT gateway without NAT traversal. However, for the connection request initiated from the ACS to reach the CPE, you must enable NAT traversal on the CPE when a NAT gateway resides between the CPE and the ACS.

The NAT traversal feature complies with *Simple Traversal of UDP Through NATs (STUN)*, RFC 3489. The feature enables the CPE to do the following:

- Discovers the NAT gateway.
- Obtains an open NAT binding (a public IP address and port binding) through which the ACS can send unsolicited packets.

The CPE sends the binding to the ACS when it initiates a connection to the ACS. For the connection requests sent by the ACS at any time to reach the CPE, the CPE maintains the open NAT binding.

For more information about NAT, see *NAT Configuration Guide*.

Examples

Enable NAT traversal for the CPE.

```
<Sysname> system-view
[Sysname] cwmp
[Sysname-cwmp] cwmp cpe stun enable
```

cwmp cpe username

Use **cwmp cpe username** to configure the username for the CPE to authenticate the ACS.

Use **undo cwmp cpe username** to restore the default.

Syntax

cwmp cpe username *username*

undo cwmp cpe username

Default

No username is configured for authenticating the ACS.

Views

CWMP view

Predefined user roles

network-admin

context-admin

Parameters

username: Specifies a username, a case-sensitive string of 1 to 255 characters.

Usage guidelines

You can configure only one username for the ACS to authenticate to the CPE when it initiates a connection. If you execute this command multiple times, the most recent configuration takes effect.

For a successful connection, make sure the ACS has the same username setting as the CPE. If a password is required, you must also make sure the ACS has the same password setting as the CPE.

The ACS must provide the correct username when it initiates a connection to the CPE. If the username is incorrect, the CPE denies the connection request from the ACS.

Examples

Configure the username used for authenticating the ACS.

```
<Sysname> system-view
[Sysname] cwmp
[Sysname-cwmp] cwmp cpe username newname
```

Related commands

cwmp cpe password

cwmp cpe wait timeout

Use **cwmp cpe wait timeout** to set the close-wait timer for the CPE to close an idle connection.

Use **undo cwmp cpe wait timeout** to restore the default.

Syntax

cwmp cpe wait timeout *seconds*

undo cwmp cpe wait timeout

Default

The close-wait timer is 30 seconds.

Views

CWMP view

Predefined user roles

network-admin

context-admin

Parameters

seconds: Sets the close-wait timer, in the range of 30 to 1800 seconds.

Usage guidelines

The close-wait timer has the following functions:

- It specifies the amount of time the connection to the ACS can be idle before it is terminated. The CPE terminates the connection to the ACS if no traffic is transmitted before the timer expires.
- It also specifies the amount of time the CPE waits for the response to a session request. The CPE determines that its session attempt has failed when the timer expires. By default, the CPE retries a failed session until the session is established with the ACS. To limit the number of retries, use the **cwmp cpe connect retry** command.

Examples

Set the close-wait time to 60 seconds.

```
<Sysname> system-view
[Sysname] cwmp
[Sysname-cwmp] cwmp cpe wait timeout 60
```

Related commands

cwmp cpe connect retry

cwmp enable

Use **cwmp enable** to enable CWMP.

Use **undo cwmp enable** to disable CWMP.

Syntax

cwmp enable

undo cwmp enable

Default

CWMP is disabled.

Views

CWMP view

Predefined user roles

network-admin

context-admin

Usage guidelines

CWMP configuration takes effect only after CWMP is enabled.

Examples

Enable CWMP.

```
<Sysname> system-view
[Sysname] cwmp
[Sysname-cwmp] cwmp enable
```

Related commands

cwmp

display cwmp configuration

Use **display cwmp configuration** to display the CWMP configuration.

Syntax

display cwmp configuration

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display the CWMP configuration after CWMP is enabled.

```
<Sysname> display cwmp configuration
CWMP state                      : Enabled
ACS URL                         : http://www.acs.com:9090
ACS username                    : newname
ACS default URL                 : Null
ACS default username            : defname
Periodic inform                 : Disabled
Inform interval                 : 600s
Inform time                     : None
Wait timeout                    : 30s
Connection retries              : Unlimited
Source IP interface             : None
STUN state                      : Disabled
SSL policy name                 : Null
```

Table 1 Command output

Field	Description
CWMP state	Status of CWMP: **Enabled** or **Disabled**.
ACS URL	Preferred ACS URL. This field displays **Null** if no preferred ACS URL has been specified.
ACS username	Username for the CPE to authenticate to the ACS. This field displays **Null** if no username has been configured for authentication to the preferred ACS URL.
ACS default URL	Default ACS URL. This field displays **Null** if no default ACS URL has been configured.

Field	Description
ACS default username	Username for the CPE to authenticate to the default ACS URL. This field displays **Null** if no username has been configured for authentication to the default ACS URL.
Periodic inform	Status of the periodic Inform feature: **Enabled** or **Disabled**.
Inform interval	Periodic Inform interval. The default interval is 600 seconds.
Inform time	Date and time at which an Inform message is scheduled to be sent. If you do not schedule an Inform sending, this field displays **None**.
Wait timeout	Close-wait timer. This timer is configurable with the **cwmp cpe wait timeout** command.
Connection retries	Number of attempts the CPE can make to retry a failed CWMP connection. This field displays **Unlimited** if the default setting is used. The CPE retries a failed session until the session is established with the ACS.
Source IP interface	IP address of the specified CWMP connection interface. This field displays **None** if you have not specified a CWMP connection interface.
STUN state	Status of NAT traversal for CWMP: **Enabled** or **Disabled**.
SSL policy name	SSL client policy specified for the CPE to authenticate the ACS for establishing an HTTPS connection. You must specify an SSL client policy when HTTPS is used. This field displays **Null** if you have not specified an SSL client policy.

Related commands

display cwmp status

display cwmp status

Use **display cwmp status** to display CWMP state information.

Syntax

display cwmp status

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display CWMP state information.

```
<Sysname> display cwmp status
CWMP state                                : Enabled
ACS URL of most recent connection         : http://www.acs.com:9090
ACS information source                    : User
ACS username of most recent connection    : newname
Connection status                         : Disconnected
```

```
Data transfer status                          : None
Most recent successful connection attempt     : None
Length of time before next connection attempt : 1096832s
```

Table 2 Command output

Field	Description
CWMP state	Status of CWMP: **Enabled** or **Disabled**.
ACS URL of most recent connection	ACS URL used for the most recent connection attempt. This field displays **Null** if no ACS URL was available.
ACS information source	Source from which the CPE obtained the ACS URL: • **User**—ACS URL assigned by using the **cwmp acs url** command or by ACS. • **DHCP**—ACS URL assigned by the DHCP server. • **Default**—ACS URL assigned by using the **cwmp acs default url** command. This field displays **None** if no ACS URL was available.
ACS username of most recent connection	Username used for the most recent connection to the ACS. This field displays **Null** if no ACS username was available.
Connection status	Current CWMP session status: • **Connected**—A CWMP session has been established to the ACS. • **Disconnected**—No CWMP session has been established to the ACS. • **Waiting response**—The CPE is waiting for the connection response from the ACS.
Data transfer status	Data transfer status of the CPE: • **Uploading**—The CPE is uploading data. • **Downloading**—The CPE is downloading data. • **None**—No data is transferred.
Most recent successful connection attempt	Time of the most recent successful CWMP connection. This field displays **None** if no CWMP session was established.
Length of time before next connection attempt	Amount of time (in seconds) that the CPE must wait before it initiates the next connection. This field displays **None** if the CPE does not detect an event that will trigger a connection attempt.

Related commands

display cwmp configuration

ssl client-policy

Use **ssl client-policy** to specify an SSL client policy for CWMP.

Use **undo ssl client-policy** to restore the default.

Syntax

ssl client-policy *policy-name*

undo ssl client-policy

Default

No SSL client policy is specified for CWMP.

Views

CWMP view

Predefined user roles

network-admin

context-admin

Parameters

policy-name: Specifies the name of an SSL client policy, a string of 1 to 31 characters.

Usage guidelines

CWMP uses HTTP or HTTPS for data transmission. If the ACS uses HTTPS for secure access, its URL begins with **https://**. You must configure an SSL client policy for the CPE to authenticate the ACS for establishing an HTTPS connection. For more information about configuring SSL client policies, see *Security Configuration Guide*.

Examples

Specify the SSL client policy **test** for CWMP.

```
<Sysname> system
[Sysname] cwmp
[Sysname-cwmp] ssl client-policy test
```

Contents

Process placement commands

The following compatibility matrixes showsthe support of hardware platforms for process placement:

Models	Process placement compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	Yes
NFNX3-HDB680, NFNX3-HDB1080	No

affinity location-set

Use **affinity location-set** to set the affinity of a process to a set of CPUs.

Use **undo affinity location-set** to remove the affinity setting for the specified CPUs for a process.

Syntax

affinity location-set { **slot** *slot-number* }&<1-5> { **attract** *strength* | **default** | **none** | **repulse** *strength* }

undo affinity location-set { **slot** *slot-number* }&<1-5>

Default

No location affinity is set for any process.

Views

Placement process view

Predefined user roles

network-admin

context-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID.

&<1-5>: Indicates that you can specify a maximum of five CPUs.

attract *strength*: Sets a positive affinity in the range of 1 to 100000. The higher the value, the stronger the preference for the process to run on the specified CPUs.

default: Sets the affinity to the default, a positive affinity of 200.

none: Sets the affinity to 0, which means the active process has no preference for any location and the system determines its location.

repulse *strength*: Sets a negative affinity in the range of 1 to 100000. The higher the value, the weaker the preference for the process to run on the specified CPUs.

Examples

Set a positive affinity of 500 to the specified slot for the **staticroute** process.

```
<Sysname> system-view
[Sysname] placement program staticroute
```

```
[Sysname-program-staticroute] affinity location-set slot 1 attract 500
```

affinity location-type

Use **affinity location-type** to set the affinity of a process to a location type.

Use **undo affinity location-type** to remove the affinity setting for the specified location type for a process.

Syntax

affinity location-type { **current** | **paired** | **primary** } { **attract** *strength* | **default** | **none** | **repulse** *strength* }

undo affinity location-type { **current** | **paired** | **primary** }

Default

No location type affinity is set for any process.

Views

Placement process view

Predefined user roles

network-admin

context-admin

Parameters

current: Specifies the affinity to the current location of the active process. You can use the **display placement program** command to view the current location of an active process.

paired: Specifies the affinity to the locations of all standby processes.

primary: Specifies the affinity to the master device.

attract *strength*: Sets a positive affinity in the range of 1 to 100000. The higher the value, the stronger the preference of the process to run on the specified location type.

default: Sets the affinity to the default, a positive affinity of 200.

none: Sets the affinity to 0, which means the active process does not have any preference for any location type and the system determines its location.

repulse *strength*: Sets a negative affinity in the range of 1 to 100000. The higher the value, the weaker the preference for the process to run on the specified location type.

Examples

Set a positive affinity of 500 to the current location for the **staticroute** process.

```
<Sysname> system-view
[Sysname] placement program staticroute
[Sysname-program-staticroute] affinity location-type current attract 500
```

Related commands

affinity location-set

affinity program

affinity program

Use **affinity program** to set the affinity for one process to run on the same location as another process.

Use **undo affinity program** to remove the affinity setting for one process to run on the same location as the specified process.

Syntax

affinity program *program-name* { **attract** *strength* | **default** | **none** | **repulse** *strength* }

undo affinity program *program-name*

Default

No process affinity is set for any process.

Views

Placement process view

Predefined user roles

network-admin

context-admin

Parameters

program-name: Specifies the name of a process running on the device. The process name is a case-insensitive string of 1 to 15 characters. You can use the **display placement program all** command to view information about all processes running on the device.

attract *strength*: Sets a positive affinity in the range of 1 to 100000. The higher the value, the stronger the preference for the current process to run on the same location as the specified process.

default: Sets the affinity to the default, a positive affinity of 200.

none: Sets the affinity to 0, which means the active process has no preference for any other process and the system determines its location.

repulse *strength*: Sets a negative affinity in the range of 1 to 100000. The higher the value, the weaker the preference for the current process to run on the same location as the specified process.

Examples

Set a negative affinity of 200 for the **staticroute** process to run on the same location as the **syslog** process.

```
<Sysname> system-view
[Sysname] placement program staticroute
[Sysname-program-staticroute] affinity program syslog repulse 200
```

Related commands

affinity location-set

affinity location-type

affinity self

Use **affinity self** to set the affinity of all instances of a process to run on the same location.

Use **undo affinity self** to restore the default.

Syntax

affinity self { **attract** *strength* | **default** | **none** | **repulse** *strength* }

undo affinity self

Default

No self affinity is set for any process.

Views

Placement process view

Predefined user roles

network-admin

context-admin

Parameters

attract *strength*: Specifies a positive affinity in the range of 1 to 100000. The higher the value, the stronger the preference for all the instances of the current process to run on the same location.

default: Sets the affinity to the default, a positive affinity of 200.

none: Sets the affinity to 0, which means the instances of the process have no preference to run on the same location and the system determines their locations.

repulse *strength*: Sets a negative affinity in the range of 1 to 100000. The higher the value, the weaker the preference for all the instances of the current process to run on the same location.

Usage guidelines

This command sets the preference for a process to run all its instances on the same location or different locations. If the process has only one instance, the command does not take effect.

The self affinity set in the placement process view of a process or any of its instances takes effect on all the instances of the process. If you execute this command multiple times, the most recent configuration takes effect.

To view the instances of a process, use the **display placement program all** command.

Examples

Set a negative self affinity of 200 for the **staticroute** process.

```
<Sysname> system-view
[Sysname] placement program staticroute
[Sysname-program-staticroute] affinity self repulse 200
```

Related commands

affinity location-set

affinity location-type

display ha service-group

Use **display ha service-group** to display service group information.

Syntax

display ha service-group { *service-group-name* [**instance** *instance-name*] | **all** }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

service-group-name: Specifies a service group running on the device. The service group name is a case-insensitive string of 1 to 15 characters.

instance *instance-name*: Specifies a service group instance by its name, a case-insensitive string of 1 to 31 characters.

all: Specifies all service groups running on the device.

Usage guidelines

A service group is a collection of processes. Typically, a service group contains only one process. If a process has instances, the corresponding service group also has instances.

Examples

Display information about all service groups.

```
<Sysname> display ha service-group all
Service Group                     Current Location      State
-------------------------------------------------------------------------------
syslog                            1/0                   Realtime Backup
...
```

Display information about the **staticroute** service group.

```
<Sysname> display ha service-group staticroute
Service Group                     Current Location      State
-------------------------------------------------------------------------------
staticroute                       1/0 (Active)          Realtime Backup
  Detailed information about services of the program:
  Service           PID    Type      Location   State
  ------------------------------------------------------------
  ifm               200    Active    1/0        Realtime Backup
  staticroute       200    Active    1/0        Realtime Backup
```

Table 1 Command output

Field	Description
Service Group	Service group name.
Current Location	Current location of the active processes for a service group.
State	Backup state of the active and standby processes for a service group.
Detailed information about services of the program	Detailed information about all active and standby processes in a service group.
Service	Service name.
PID	Process ID.
Type	Process type: **Active** or **Standby**.

Field	Description
Location	Location of the active process of a service.
State	Process status: • **Realtime Backup**. • **Batch Backup**. • **Stopping**. • **Degrading**. • **Upgrading**.

display placement location

Use **display placement location** to display the processes running on the specified location.

Syntax

display placement location { **all** | **slot** *slot-number* }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

all: Displays all processes running on the device.

slot *slot-number*: Specifies an IRF member device by its member ID.

Examples

Display all processes running on the device.

```
<Sysname> display placement location all
Program(s) placed at location: 1/0
  syslog
...
```

display placement policy

Use **display placement policy** to display process placement policy information.

Syntax

display placement policy program { *program-name* | **all** | **default** }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

program-name: Specifies a process by its name, a case-insensitive string of 1 to 15 characters.

all: Displays all process placement policies.

default: Displays the default process placement policy. If no default process placement policy is configured by using the **placement program default** command, the **display placement policy program default** command does not display any information.

Usage guidelines

The information about a placement policy is displayed only when the placement policy is configured for the specified process.

Examples

Display the default process placement policy.

```
<Sysname> display placement policy program default
Program: [default]                                  : source
-------------------------------------------------------------
  affinity location-set slot 1 attract 500          : system [default]
```

Table 2 Command output

Field	Description
Program	Process name and the placement policy for the process. If you execute the **display placement policy program default** command, the process name is displayed as **[default]**.
source	Source of the setting. If a default placement setting is configured in the view you enter with the **placement program default** command, this field displays **system [default]**. If a placement setting for the **staticroute** process is configured in the view you enter with the **placement program** *program-name* command, this field displays **system staticroute**.

display placement program

Use **display placement program** to display the location of an active process.

Syntax

display placement program { *program-name* | **all** }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

program-name: Specifies a process by its name, a case-insensitive string of 1 to 15 characters.

all: Specifies all processes running on the device.

Examples

Display the location of the **staticroute** active process.

```
<Sysname> display placement program staticroute
Program                          Placed at location
--------------------------------------------------
staticroute                      1/0
```

Table 3 Command output

Field	Description
Program	Process name.
Placed at location	Location of the active process. If the active process is abnormal or is starting up, this field displays **NA**.

display placement reoptimize

Use **display placement reoptimize** to display the predicted location changes that will occur after you execute the **placement reoptimize** command.

Syntax

display placement reoptimize program { *program-name* [**instance** *instance-name*] | **all** }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

program-name: Specifies a process (that supports process optimization) by its name, a case-insensitive string of 1 to 15 characters.

instance *instance-name*: Specifies an instance of the specified process. The instance name is a case-insensitive string of 1 to 31 characters. Whether a process has multiple instances depends on the system software.

all: Specifies all processes that are running on the device and that support process optimization.

Examples

Display the predicted location changes for all processes.

```
<Sysname> display placement reoptimize program all
Predicted changes to the placement
Program                          Current location       New location
```

```
----------------------------------------------------------------------
staticroute                     1/0                 1/0
...
```

The output shows the process name, current location of the active process, and new location of the active process after optimization.

placement program

Use **placement program** to enter placement process view.

Use **undo placement program** to delete the placement policy for a process.

Syntax

placement program { *program-name* [**instance** *instance-name*] | **default** }

undo placement program { *program-name* [**instance** *instance-name*] | **default** }

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

program-name: Specifies a process name, a case-insensitive string of 1 to 15 characters.

instance *instance-name*: Specifies the name of an instance of the specified process. The instance name is a case-insensitive string of 1 to 31 characters. If you do not specify this option, this command enters process placement policy view and the settings in process placement policy view take effect on all instances. Whether a process has multiple instances depends on the system software.

default: Configures the default placement policy for all processes.

Usage guidelines

You configure a process placement policy to optimize the distribution of processes in your system for optimal distribution of CPU and memory resources.

For an instance of a process, the priorities of the settings in placement policy view of an instance, placement policy view of a process, and the default placement policy view are in descending order. For a process, the settings in placement policy view of the process take precedence over the settings in the default placement policy view.

A process placement policy contains the **affinity location-type**, **affinity location-set**, **affinity program**, and **affinity self** commands. The commands describe the preferences of the process for a specific location.

You can configure all the **affinity** commands in the placement policy for a process. Based on the placement policy and hardware resources, the system automatically determines the location for running the active process. Before you apply the policy, you can use the **display placement reoptimize** command to view the predicted location for the process. When a process switchover occurs, the process on the predicted location is selected as the active process.

Examples

Enter the placement process view of the **staticroute** process.

```
<Sysname> system-view
[Sysname] placement program staticroute
```

```
[Sysname-program-staticroute]
```

Enter the default placement process view.

```
<Sysname> system-view
[Sysname] placement program default
[Sysname-program-default]
```

placement reoptimize

Use **placement reoptimize** to apply configured process placement policies for optimizing process placement.

Syntax

placement reoptimize

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

CAUTION:

To avoid neighbor flapping of related protocols, make sure HA features such as NSR or GR are configured for the processes and are stable before optimizing process placement.

After you execute this command, the system bases its placement decisions on the new process placement policies, hardware resources, and locations and states of active processes. The process on the new location is selected as the active process. If the new location for an active process is different from its current location, a process switchover is triggered. The system changes the state of the original active process to standby and the state of the standby process on the new location to active. You can use the **display placement program** command to view the new location of the active process.

To keep the system stable, do not perform any tasks that require process restart when you execute this command.

Examples

Reoptimize process placement.

```
<Sysname> system-view
[Sysname] placement reoptimize
Predicted changes to the placement
Program                          Current location       New location
-------------------------------------------------------------------
staticroute                      1/0                    1/0
Continue? [y/n]:y
Re-optimization of the placement start. You will be notified on completion
Re-optimization of the placement complete. Use 'display placement' to view the new
placement
```

This example uses only the **staticroute** process.

NSFOCUS Firewall Series

NF VPN Instance Command Reference

NSFOCUS Technologies, Inc.

Document version: 6W600-20230221

Preface

This command reference describes the commands for configuring VPN instance features.

This preface includes the following topics about the documentation:

- Audience.
- Conventions.

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators.

Conventions

The following information describes the conventions used in the documentation.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select a minimum of one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
CAUTION:	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Contents

VPN instance commands

description (VPN instance view)

Use **description** to configure a description for a VPN instance.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

No description is configured for a VPN instance.

Views

VPN instance view

Predefined user roles

network-admin

context-admin

Parameters

text: Configures the description for the VPN instance, a case-sensitive string of 1 to 79 characters.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the description for VPN instance **vpn1** to **This is vpn1**.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] description This is vpn1
```

display ip vpn-instance

Use **display ip vpn-instance** to display VPN instance information.

Syntax

display ip vpn-instance [**instance-name** *vpn-instance-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

instance-name *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays brief information about all VPN instances.

Examples

Display brief information about all VPN instances.

```
<Sysname> display ip vpn-instance
  Total VPN-Instances configured : 1
  VPN-Instance Name               RD                    Create time
  management                      1000000000:1          2016/10/31
```

Table 1 Command output

Field	Description
VPN-Instance Name	Name of the VPN instance.
RD	Route distinguisher of the VPN instance.
Create time	Time when the VPN instance was created.

ip binding vpn-instance

Use **ip binding vpn-instance** to associate an interface with a VPN instance.

Use **undo ip binding vpn-instance** to restore the default.

Syntax

ip binding vpn-instance *vpn-instance-name*

undo ip binding vpn-instance

Default

An interface is not associated with a VPN instance and belongs to the public network.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance-name: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

This command or its **undo** form clears the IP address and routing protocol configuration on the interface. You must reconfigure the IP address and routing protocol for the interface after executing this command. To view the configuration of an interface, execute the **display this** command in interface view.

The specified VPN instance must have been created by using the **ip vpn-instance** command in system view.

To associate a new VPN instance with an interface, first execute the **undo ip binding vpn-instance** command to remove the existing association.

Examples

Associate interface GigabitEthernet 1/0/1 with VPN instance **vpn1**.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip binding vpn-instance vpn1
```

Related commands

ip vpn-instance (system view)

ip vpn-instance (system view)

Use **ip vpn-instance** to create a VPN instance and enter its view, or enter the view of an existing VPN instance.

Use **undo ip vpn-instance** to delete a VPN instance.

Syntax

ip vpn-instance *vpn-instance-name*

undo ip vpn-instance *vpn-instance-name*

Default

No VPN instances exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

vpn-instance-name: Specifies a name for the VPN instance, a case-sensitive string of 1 to 31 characters.

Examples

Create VPN instance **vpn1** and enter its view.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1]
```

NSFOCUS Firewall Series

NF VXLAN Command Reference

NSFOCUS Technologies, Inc.

Document version: 6W600-20230221

Preface

This command reference describes the commands for configuring VXLAN instance features.

This preface includes the following topics about the documentation:

- Audience.
- Conventions.

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators.

Conventions

The following information describes the conventions used in the documentation.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select a minimum of one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
CAUTION:	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Contents

VXLAN commands

Basic VXLAN commands

ac statistics enable

Use **ac statistics enable** to enable packet statistics for a Layer 3 interface that acts as an AC.

Use **undo ac statistics enable** to disable packet statistics for a Layer 3 interface that acts as an AC.

Syntax

ac statistics enable

undo ac statistics enable

The following compatibility matrix shows the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	Yes
NFNX3-HDB680, NFNX3-HDB1080	No

Default

The packet statistics feature is disabled for a Layer 3 interface that acts as an AC.

Views

Layer 3 aggregate interface view

Layer 3 Ethernet interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

For this command to take effect, you must map the Layer 3 interface to a VSI. If you modify the VSI mapping, packet statistics of the interface are cleared.

Examples

Map GigabitEthernet 1/0/1 to VSI **vsia** and enable packet statistics on the interface.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] xconnect vsi vsia
[Sysname-GigabitEthernet1/0/1] ac statistics enable
```

Related commands

display l2vpn interface verbose

reset l2vpn statistics ac

arp suppression enable

Use **arp suppression enable** to enable ARP flood suppression.

Use **undo arp suppression enable** to disable ARP flood suppression.

Syntax

arp suppression enable

undo arp suppression enable

The following compatibility matrix shows the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	Yes
NFNX3-HDB680, NFNX3-HDB1080	Yes

Default

ARP flood suppression is disabled.

Views

VSI view

Predefined user roles

network-admin

context-admin

Usage guidelines

ARP flood suppression reduces ARP request broadcasts by enabling the VTEP to reply to ARP requests on behalf of VMs.

This feature snoops ARP packets to populate the ARP flood suppression table with local and remote MAC addresses. If an ARP request has a matching entry, the VTEP replies to the request on behalf of the VM. If no match is found, the VTEP floods the request to both local and remote sites.

Examples

Enable ARP flood suppression for VSI **vsi1**.

```
<Sysname> system-view
[Sysname] vsi vsi1
[Sysname-vsi-vsi1] arp suppression enable
```

Related commands

display arp suppression vsi

reset arp suppression vsi

description

Use **description** to configure a description for a VSI.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

A VSI does not have a description.

Views

VSI view

Predefined user roles

network-admin

context-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 80 characters.

Examples

Configure a description for VSI **vpn1**.

```
<Sysname> system-view
[Sysname] vsi vpn1
[Sysname-vsi-vpn1] description vsi for vpn1
```

Related commands

display l2vpn vsi

display arp suppression vsi

Use **display arp suppression vsi** to display ARP flood suppression entries.

Syntax

display arp suppression vsi [**name** *vsi-name*] [**slot** *slot-number*] [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

name *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VSI, this command displays entries for all VSIs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays entries on the master device.

count: Displays the number of ARP flood suppression entries that match the command.

Examples

Display ARP flood suppression entries.

```
<Sysname> display arp suppression vsi
IP address      MAC address    Vsi Name                        Link ID    Aging
1.1.1.2         000f-e201-0101 vsi1                            0x70000    14
```

```
1.1.1.3         000f-e201-0202 vsi1                              0x80000    18
1.1.1.4         000f-e201-0203 vsi2                              0x90000    10
```

Display the number of ARP flood suppression entries.

```
<Sysname> display arp suppression vsi count
Total entries: 3
```

Table 1 Command output

Field	Description
Link ID	Link ID that uniquely identifies an AC or a VXLAN tunnel on a VSI.
Aging	Remaining lifetime (in minutes) of the ARP flood suppression entry. When the timer expires, the entry is deleted.

Related commands

arp suppression enable

reset arp suppression vsi

display l2vpn interface

Use **display l2vpn interface** to display L2VPN information for Layer 3 interfaces that are mapped to VSIs.

Syntax

display l2vpn interface [**vsi** *vsi-name* | *interface-type interface-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vsi *vsi-name*: Specifies a VSI name, a case-sensitive string of 1 to 31 characters.

interface-type interface-number: Specifies an interface by its type and number.

verbose: Displays detailed information about Layer 3 interfaces. If you do not specify this keyword, the command displays brief information about Layer 3 interfaces.

Usage guidelines

If you do not specify any parameters, this command displays brief L2VPN information for all Layer 3 interfaces that are mapped to VSIs.

Examples

Display brief L2VPN information for all Layer 3 interfaces that are mapped to VSIs.

```
<Sysname> display l2vpn interface
Total number of interfaces: 2, 1 up, 1 down
```

```
Interface                Owner                          Link ID   State    Type
GE1/0/1                  vxlan3                         1         Up       VSI
GE1/0/2                  vxlan4                         2         Down     VSI
```

Table 2 Command output

Field	Description
Interface	Layer 3 interface name.
Owner	VSI name.
Link ID	The interface's link ID on the VSI.
State	Physical state of the interface: • **Up**—The interface is physically up. • **Down**—The interface is physically down.
Type	L2VPN type of the interface. This field displays **VSI** for the VXLAN feature.

Display detailed L2VPN information for all Layer 3 interfaces that are mapped to VSIs.

```
<Sysname> display l2vpn interface verbose
Interface: GE1/0/1
    Owner         : vsi1
    Link ID       : 0
    State         : Up
    Type          : VSI
    Statistics    : Enabled
    Input Statistics:
      Octets   :994496
      Packets  :15539
    Output Statistics:
      Octets   :0
      Packets  :0

Interface: GE1/0/2
    Owner         : vsi2
    Link ID       : 0
    State         : Down
    Type          : VSI
    Statistics    : Enabled
    Input Statistics:
      Octets   :0
      Packets  :0
    Output Statistics:
      Octets   :0
      Packets  :0
```

Table 3 Command output

Field	Description
Interface	Layer 3 interface name.
Owner	VSI name.

Field	Description
Link ID	The interface's link ID on the VSI.
State	Physical state of the interface: • **Up**—The interface is physically up. • **Down**—The interface is physically down.
Type	L2VPN type of the interface. This field displays **VSI** for the VXLAN feature.
Statistics	Packet statistics state: • **Enabled**—The packet statistics feature is enabled for the interface. • **Disabled**—The packet statistics feature is disabled for the interface.
Input Statistics	Incoming traffic statistics: • **Octets**—Number of incoming bytes. • **Packets**—Number of incoming packets.
Output Statistics	Outgoing traffic statistics: • **Octets**—Number of outgoing bytes. • **Packets**—Number of outgoing packets.

display l2vpn mac-address

Use **display l2vpn mac-address** to display MAC address entries for VSIs.

Syntax

display l2vpn mac-address [**vsi** *vsi-name*] [**dynamic**] [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vsi *vsi-name*: Specifies a VSI name, a case-sensitive string of 1 to 31 characters. If you do not specify a VSI, this command displays MAC address entries for all VSIs.

dynamic: Specifies dynamic MAC address entries learned in the data plane. If you do not specify this keyword, the command displays all MAC address entries, including:

- Dynamic remote- and local-MAC entries.
- Manually added static remote-MAC entries.

VXLAN does not support static local-MAC entries.

count: Displays the number of MAC address entries. If you do not specify this keyword, the command displays detailed information about MAC address entries.

Examples

Display MAC address entries for all VSIs.

```
<Sysname> display l2vpn mac-address
MAC Address      State    VSI Name                       Link ID/Name  Aging
```

```
0000-0000-000b   Static   vpn1                            Tunnel10      NotAging
0000-0000-000c   Dynamic  vpn1                            Tunnel60      Aging
0000-0000-000d   Dynamic  vpn1                            Tunnel99      Aging
--- 3 mac address(es) found  ---
```

Display the total number of MAC address entries in all VSIs.

```
<Sysname> display l2vpn mac-address count
3 mac address(es) found
```

Table 4 Command output

Field	Description
State	Entry state: • **Dynamic**—Local- or remote-MAC entry dynamically learned in the data plane. • **Static**—Static remote-MAC entry.
Link ID/Name	For a local MAC address, this field displays the AC's link ID on the VSI. For a remote MAC address, this field displays the tunnel interface name.
Aging	Entry aging state: • **Aging**. • **NotAging**.

Related commands

reset l2vpn mac-address

display l2vpn service-instance

Use **display l2vpn service-instance** to display information about Ethernet service instances.

Syntax

display l2vpn service-instance [**interface** *interface-type interface-number* [**service-instance** *instance-id*]] [**verbose**]

The following compatibility matrix shows the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	Yes
NFNX3-HDB680, NFNX3-HDB1080	No

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

interface *interface-type interface-number*: Specifies a Layer 2 Ethernet interface or Layer 2 aggregate interface by its interface type and number. If you do not specify an interface, this command displays Ethernet service instance information for all Layer 2 Ethernet interfaces and Layer 2 aggregate interfaces.

service-instance *instance-id*: Specifies an Ethernet service instance by its ID in the range of 1 to 4096. If you do not specify an Ethernet service instance, this command displays information about all Ethernet service instances on the specified Layer 2 Ethernet interface or Layer 2 aggregate interface.

verbose: Displays detailed information about Ethernet service instances. If you do not specify this keyword, the command displays brief information about Ethernet service instances.

Examples

Display brief information about all Ethernet service instances.

```
<Sysname> display l2vpn service-instance
Total number of service-instances: 4, 4 up, 0 down
Total number of ACs: 2, 2 up, 0 down

Interface               SrvID Owner                          LinkID State Type
GE1/0/1                 3     vsi12                          1      Up    VSI
GE1/0/1                 4     vsi13                          1      Up    VSI
```

Table 5 Command output

Field	Description
Total number of ACs	Total number of attachment circuits (ACs) and the number of ACs in each state (up or down).
Interface	Name of a Layer 2 Ethernet interface or Layer 2 aggregate interface.
SrvID	Ethernet service instance ID.
Owner	VSI name. This field is empty if an Ethernet service instance is not mapped to any VSI.
LinkID	Ethernet service instance's link ID on the VSI.
State	Ethernet service instance state: • **Up**. • **Down**.
Type	L2VPN type of the Ethernet service instance: • **VSI**. • **VPWS**.

Display detailed information about all Ethernet service instances on GigabitEthernet 1/0/1.

```
<Sysname> display l2vpn service-instance interface gigabitethernet 1/0/1 verbose
Interface: GE1/0/1
  Service Instance: 1
    Encapsulation : s-vid 16
    VSI Name      : vsi10
    Link ID       : 1
    State         : Up
    Statistics    : Enabled
    Input Statistics:
```

```
    Octets   :0
    Packets  :0
  Output Statistics:
    Octets   :0
    Packets  :0
```

Table 6 Command output

Field	Description
Interface	Name of a Layer 2 Ethernet interface or Layer 2 aggregate interface.
Service Instance	Ethernet service instance ID.
Encapsulation	Frame match criterion of the Ethernet service instance. If the Ethernet service instance does not contain a match criterion, the command does not display this field.
Link ID	Ethernet service instance's link ID on the VSI.
State	Ethernet service instance state: • **Up**. • **Down**.
Statistics	Packet statistics state: • **Enabled**—The packet statistics feature is enabled for the Ethernet service instance. • **Disabled**—The packet statistics feature is disabled for the Ethernet service instance.
Input Statistics	Incoming traffic statistics: • **Octets**—Number of incoming bytes. • **Packets**—Number of incoming packets.
Output Statistics	Outgoing traffic statistics: • **Octets**—Number of outgoing bytes. • **Packets**—Number of outgoing packets.

Related commands

service-instance

display l2vpn vsi

Use **display l2vpn vsi** to display information about VSIs.

Syntax

display l2vpn vsi [**name** *vsi-name*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

name *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VSI, this command displays information about all VSIs.

verbose: Displays detailed information about VSIs. If you do not specify this keyword, the command displays brief information about VSIs.

Examples

Display brief information about all VSIs.

```
<Sysname> display l2vpn vsi
Total number of VSIs: 1, 1 up, 0 down, 0 admin down

VSI Name                        VSI Index       MTU    State
vpna                            0               1500   Up
```

Table 7 Command output

Field	Description
MTU	MTU on the VSI.
State	VSI state: • **Up**—The VSI is up. • **Down**—The VSI is down. • **Admin down**—The VSI has been manually shut down by using the **shutdown** command.

Display detailed information about all VSIs.

```
<Sysname> display l2vpn vsi verbose
VSI Name: vpna
  VSI Index               : 0
  VSI State               : Up
  MTU                     : 1500
  Bandwidth               : -
  Broadcast Restrain      : -
  Multicast Restrain      : -
  Unknown Unicast Restrain: -
  MAC Learning            : Enabled
  MAC Table Limit         : -
  MAC Learning rate       : -
  Drop Unknown            : Disabled
  PW Redundancy           : Slave
  Flooding                : Enabled
  Service Class           : -
  Gateway Interface       : VSI-interface 100
  VXLAN ID                : 10
  Tunnel Statistics       : Disabled
  Tunnels:
    Tunnel Name          Link ID    State  Type      Flood Proxy  Split horizon
    Tunnel1              0x5000001  Up     Manual    Disabled     Enabled
    Tunnel2              0x5000002  Up     Manual    Disabled     Enabled
  ACs:
    AC                              Link ID    State
```

```
GE1/0/1                         0           Up
```

Table 8 Command output

Field	Description
VSI Description	Description of the VSI. If the VSI does not have a description, the command does not display this field.
VSI State	VSI state: • **Up**—The VSI is up. • **Down**—The VSI is down. • **Administratively down**—The VSI has been manually shut down by using the **shutdown** command.
MTU	MTU on the VSI.
Bandwidth	Maximum bandwidth (in kbps) for known unicast traffic on the VSI. This field displays a hyphen (**-**) if it is not available in the current software version.
Broadcast Restrain	Broadcast restraint bandwidth (in kbps). This field displays a hyphen (**-**) if it is not available in the current software version.
Multicast Restrain	Multicast restraint bandwidth (in kbps). This field displays a hyphen (**-**) if it is not available in the current software version.
Unknown Unicast Restrain	Unknown unicast restraint bandwidth (in kbps). This field displays a hyphen (**-**) if it is not available in the current software version.
MAC Learning	State of the MAC learning feature.
MAC Table Limit	Maximum number of MAC address entries on the VSI. This field displays a hyphen (**-**) if it is not available in the current software version.
MAC Learning Rate	MAC address entry learning rate of the VSI.
Drop Unknown	Action on source MAC-unknown frames received after the maximum number of MAC entries is reached.
Service Class	Service class value of outgoing VXLAN packets.
Gateway Interface	VSI interface name.
Tunnel Statistics	Packet statistics state: • **Enabled**—The packet statistics feature is enabled for the VXLAN tunnels of the VSI. • **Disabled**—The packet statistics feature is disabled for the VXLAN tunnels of the VSI.
State	Tunnel state: • **Up**—The tunnel is operating correctly. • **Blocked**—The tunnel is a backup proxy tunnel. Its tunnel interface is up, but the tunnel is blocked because the primary proxy tunnel is operating correctly. • **Defect**—The tunnel interface is up, but BFD cannot detect the remote VTEP. This state is not supported in the current software version. • **Down**—The tunnel interface is down.
Type	Tunnel assignment method. **Manual** indicates that the tunnel was manually assigned to the VXLAN.
Flood Proxy	Flood proxy state: • **Enabled**—Flood proxy is enabled. The VTEP sends broadcast, multicast, and unknown unicast traffic to a flood proxy server through the tunnel. The flood proxy server replicates and forwards flood traffic to remote VTEPs. • **Disabled**—Flood proxy is disabled.

Field	Description
Split horizon	State of split horizon: • **Enabled**—Split horizon is enabled on the VXLAN tunnel. The VXLAN tunnel does not forward the traffic that is received on other VXLAN tunnels. • **Disabled**—Split horizon is disabled on the VXLAN tunnel. The VXLAN tunnel forwards the traffic that is received on other VXLAN tunnels.
ACs	ACs that are bound to the VSI.
Link ID	AC's link ID on the VSI.
State	AC state: • **Up**. • **Down**.

display vxlan tunnel

Use **display vxlan tunnel** to display VXLAN tunnel information for VXLANs.

Syntax

display vxlan tunnel [**vxlan-id** *vxlan-id* [**tunnel** *tunnel-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vxlan-id: Specifies a VXLAN ID in the range of 0 to 16777215. If you do not specify a VXLAN, this command displays VXLAN tunnel information for all VXLANs.

tunnel *tunnel-number*: Specifies a VXLAN tunnel. The *tunnel-number* argument represents the tunnel interface number. The value range for the *tunnel-number* argument is 0 to 1023. If you do not specify a VXLAN tunnel, this command displays information about all VXLAN tunnels associated with the specified VXLAN.

Examples

Display VXLAN tunnel information for all VXLANs.

```
<Sysname> display vxlan tunnel
Total number of VXLANs: 1

VXLAN ID: 10, VSI name: vpna, Total tunnels: 3 (3 up, 0 down, 0 defect, 0 blocked)
Tunnel name          Link ID    State  Type         Flood proxy  Split horizon
Tunnel1              0x5000001  Up     Manual       Disabled     Enabled
Tunnel2              0x5000002  Up     Manual       Disabled     Enabled
```

Display VXLAN tunnel information for VXLAN **10**.

```
<Sysname> display vxlan tunnel vxlan-id 10
VXLAN ID: 10, VSI name: vpna, Total tunnels: 3 (3 up, 0 down, 0 defect, 0 blocked)
Tunnel name          Link ID    State  Type         Flood proxy  Split horizon
```

```
Tunnel1              0x5000001  Up     Manual       Disabled     Enabled
Tunnel2              0x5000002  Up     Manual       Disabled     Enabled
```

Display information about VXLAN tunnel 0 for VXLAN **10**.

```
<Sysname> display vxlan tunnel vxlan-id 10 tunnel 0
Interface: Tunnel0
  Link ID    : 0x5000000
  State      : Up
  Type       : Auto
  Flood Proxy: Disabled
  Statistics : Enabled
    Input statistics:
      Octets : 994496
      Packets: 15539
    Output statistics:
      Octets : 0
      Packets: 0
```

Table 9 Command output

Field	Description
Link ID	Tunnel's link ID in the VXLAN.
State	Tunnel state: • **Up**—The tunnel is operating correctly. • **Blocked**—The tunnel is a backup proxy tunnel. Its tunnel interface is up, but the tunnel is blocked because the primary proxy tunnel is operating correctly. • **Defect**—The tunnel interface is up, but BFD cannot detect the remote VTEP. This state is not supported in the current software version. • **Down**—The tunnel interface is down.
Type	Tunnel assignment method. **Manual** indicates that tunnel was manually assigned to the VXLAN.
Flood proxy	Flood proxy state: • **Enabled**—Flood proxy is enabled. The VTEP sends broadcast, multicast, and unknown unicast traffic to a flood proxy server through the tunnel. The flood proxy server replicates and forwards flood traffic to remote VTEPs. • **Disabled**—Flood proxy is disabled.
Split horizon	State of split horizon: • **Enabled**—Split horizon is enabled on the VXLAN tunnel. The VXLAN tunnel does not forward the traffic that is received on other VXLAN tunnels. • **Disabled**—Split horizon is disabled on the VXLAN tunnel. The VXLAN tunnel forwards the traffic that is received on other VXLAN tunnels.
Statistics	Packet statistics state: • **Enabled**—The packet statistics feature is enabled for the VXLAN tunnel. • **Disabled**—The packet statistics feature is disabled for the VXLAN tunnel.
Input statistics	Incoming traffic statistics: • **Octets**—Number of incoming bytes. • **Packets**—Number of incoming packets.
Output statistics	Outgoing traffic statistics: • **Octets**—Number of outgoing bytes. • **Packets**—Number of outgoing packets.

Related commands

tunnel

vxlan

encapsulation

Use **encapsulation** to configure a frame match criterion for an Ethernet service instance.

Use **undo encapsulation** to restore the default.

Syntax

encapsulation s-vid *vlan-id-list* [**only-tagged**]

encapsulation s-vid *vlan-id* **c-vid** { *vlan-id-list* | **all** }

encapsulation c-vid *vlan-id-list*

encapsulation { **default** | **tagged** | **untagged** }

undo encapsulation

The following compatibility matrix shows the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	Yes
NFNX3-HDB680, NFNX3-HDB1080	No

Default

An Ethernet service instance does not contain a frame match criterion.

Views

Ethernet service instance view

Predefined user roles

network-admin

context-admin

Parameters

s-vid: Matches frames that are tagged with the specified outer 802.1Q VLAN IDs.

c-vid: Matches frames that are tagged with the specified inner 802.1Q VLAN IDs.

vlan-id: Specifies an 802.1Q VLAN ID in the range of 1 to 4094.

vlan-id-list: Specifies a space-separated list of up to eight VLAN items. Each item specifies a VLAN ID or a range of VLAN IDs in the format of *vlan-id1* **to** *vlan-id2*. The value range for VLAN IDs is 1 to 4094.

only-tagged: Matches tagged frames. If the outer 802.1Q VLAN is not the PVID, the matching result does not differ, whether or not you specify the **only-tagged** keyword. If the outer 802.1Q VLAN is the PVID, the matching result depends on whether or not the **only-tagged** keyword is specified.

- To match only PVID-tagged frames, specify the **only-tagged** keyword.
- To match both untagged frames and PVID-tagged frames, do not specify the **only-tagged** keyword.

all: Specifies all 802.1Q VLAN IDs.

default: Matches frames that do not match any other Ethernet service instance on the interface. On an interface, you can configure this criterion only in one Ethernet service instance. The Ethernet service instance matches any frames if it is the only instance on the interface.

tagged: Matches any frames that have an 802.1Q VLAN tag.

untagged: Matches any frames that do not have an 802.1Q VLAN tag.

Usage guidelines

An Ethernet service instance can contain only one match criterion. To change the match criterion, first execute the **undo encapsulation** command to remove the original criterion. When you remove the match criterion in an Ethernet service instance, the mapping between the service instance and the VSI is removed automatically.

Examples

Configure Ethernet service instance 1 on GigabitEthernet 1/0/1 to match frames that have an outer 802.1Q VLAN ID of 111.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] service-instance 1
[Sysname-GigabitEthernet1/0/1-srv1] encapsulation s-vid 111
```

Related commands

display l2vpn service-instance

flooding disable

Use **flooding disable** to disable flooding for a VSI.

Use **undo flooding disable** to enable flooding for a VSI.

Syntax

flooding disable

undo flooding disable

Default

Flooding is enabled for a VSI.

Views

VSI view

Predefined user roles

network-admin

context-admin

Usage guidelines

By default, the device floods unknown unicast frames received from the local site to the following interfaces in the frame's VXLAN:

- All site-facing interfaces except for the incoming interface.
- All VXLAN tunnel interfaces.

To confine unknown unicast traffic to the site-facing interfaces, use this command to disable flooding for the VSI bound to the VXLAN. The VSI will not flood unknown unicast frames to VXLAN tunnel interfaces.

Examples

Disable flooding for VSI **vsi1**.

```
<Sysname> system-view
[Sysname] vsi vsi1
[Sysname-vsi-vsi1] flooding disable
```

l2vpn enable

Use **l2vpn enable** to enable L2VPN.

Use **undo l2vpn enable** to disable L2VPN.

Syntax

l2vpn enable

undo l2vpn enable

Default

L2VPN is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

You must enable L2VPN before you can configure L2VPN settings.

Examples

Enable L2VPN.

```
<Sysname> system-view
[Sysname] l2vpn enable
```

l2vpn rewrite inbound tag

Use **l2vpn rewrite inbound tag** to configure the VLAN tag processing rule for incoming traffic.

Use **undo l2vpn rewrite inbound** to restore the default.

Syntax

l2vpn rewrite inbound tag { **nest** { **c-vid** *vlan-id* | **s-vid** *vlan-id* [**c-vid** *vlan-id*] } | **remark 1-to-2 s-vid** *vlan-id* **c-vid** *vlan-id* } [**symmetric**]

undo l2vpn rewrite inbound

The following compatibility matrix shows the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	Yes
NFNX3-HDB680, NFNX3-HDB1080	No

Default

VLAN tags of incoming traffic are not processed.

Views

Layer 3 aggregate interface view

Layer 3 Ethernet interface view

Predefined user roles

network-admin

context-admin

Parameters

nest: Adds VLAN tags.

c-vid: Specifies an inner VLAN tag.

s-vid: Specifies an outer VLAN tag.

vlan-id: Specifies a VLAN ID in the range of 1 to 4094.

remark: Maps VLAN tags.

1-to-2: Performs one-to-two mapping to replace the VLAN tag of single tagged packets with the specified outer and inner VLAN tags.

symmetric: Applies the reverse VLAN tag processing rule to outgoing traffic. If you do not specify this keyword, VLAN tags of outgoing traffic are not processed.

Usage guidelines

To modify the VLAN tag processing rule for incoming traffic, first execute the **undo l2vpn rewrite inbound** command to remove the existing rule, and then execute the **l2vpn rewrite inbound** command.

When you use this command, follow these restrictions:

- The **l2vpn rewrite inbound tag nest s-vid** *vlan-id* **c-vid** *vlan-id* command takes effect only on untagged packets.
- The **l2vpn rewrite inbound tag remark 1-to-2** command takes effect only on single tagged packets.

Examples

Configure Layer 3 Ethernet interface GigabitEthernet 1/0/1 to add outer VLAN tag 100 to incoming frames and remove outer VLAN tag 100 from outgoing frames.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] l2vpn rewrite inbound tag nest s-vid 100 symmetric
```

l2vpn statistics interval

Use **l2vpn statistics interval** to set the VXLAN statistics collection interval.

Use **undo l2vpn statistics interval** to restore the default.

Syntax

l2vpn statistics interval *interval*

undo l2vpn statistics interval

The following compatibility matrix shows the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	Yes
NFNX3-HDB680, NFNX3-HDB1080	No

Default

The VXLAN statistics collection interval is 15 minutes.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

interval: Specifies an interval value in the range of 30 to 65535 seconds.

Examples

Set the VXLAN statistics collection interval to 30 seconds.

```
<Sysname> system-view
[Sysname] l2vpn statistics interval 30
```

mac-address static vsi

Use **mac-address static vsi** to add a static remote-MAC address entry for a VXLAN VSI.

Use **undo mac-address static vsi** to remove static remote-MAC address entries for a VXLAN VSI.

Syntax

mac-address static *mac-address* **interface tunnel** *tunnel-number* **vsi** *vsi-name*

undo mac-address static [*mac-address*] [**interface tunnel** *tunnel-number*] **vsi** *vsi-name*

Default

VXLAN VSIs do not have static remote-MAC address entries.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

mac-address: Specifies a MAC address in H-H-H format. Do not specify a multicast MAC address or an all-zeros MAC address. You can omit the consecutive zeros at the beginning of each segment. For example, you can enter **f-e2-1** for **000f-00e2-0001**.

interface tunnel *tunnel-number*: Specifies a VXLAN tunnel interface by its tunnel interface number. The value range for the *tunnel-number* argument is 0 to 1023.

vsi *vsi-name*: Specifies a VSI name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

A remote MAC address is the MAC address of a VM in a remote site. Remote MAC entries can be manually added or dynamically learned.

When you add a remote MAC address entry, make sure the specified VSI's VXLAN has been assigned the specified VXLAN tunnel.

The **undo mac-address static vsi** *vsi-name* command removes all static MAC address entries for a VSI.

Examples

Add MAC address **000f-e201-0101** to VSI **vsi1**. Specify Tunnel-interface 1 as the outgoing interface.

```
<Sysname> system-view
[Sysname] mac-address static 000f-e201-0101 interface tunnel 1 vsi vsi1
```

Related commands

vxlan tunnel mac-learning disable

mtu

Use **mtu** to set the MTU for a VSI.

Use **undo mtu** to restore the default.

Syntax

mtu *size*

undo mtu

Default

The default MTU of a VSI is 1500 bytes.

Views

VSI view

Predefined user roles

network-admin

context-admin

Parameters

size: Specifies an MTU value. The value range for this argument is 300 to 65535.

Usage guidelines

The MTU set by using this command limits the maximum length of the packets that a VSI receives from ACs and forwards through VXLAN tunnels. The MTU does not limit the maximum length of other packets in the VXLAN VSI.

Fragmentation is disabled for a VSI that uses the default MTU. If you set a MTU for a VSI, the packets longer than the MTU are fragmented.

Examples

Set the MTU to 1400 bytes for VSI **vxlan1**.

```
<Sysname> system-view
[Sysname] vsi vxlan1
[Sysname-vsi-vxlan1] mtu 1400
```

Related commands

display l2vpn vsi

reserved vxlan

Use **reserved vxlan** to specify a reserved VXLAN.

Use **undo reserved vxlan** to restore the default.

Syntax

reserved vxlan *vxlan-id*

undo reserved vxlan

Default

No VXLAN has been reserved.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

vxlan-id: Specifies a VXLAN ID in the range of 0 to 16777215.

Usage guidelines

You can specify only one reserved VXLAN on the VTEP. The reserved VXLAN cannot be the VXLAN created on any VSI.

Examples

Specify VXLAN 10000 as the reserved VXLAN.

```
<Sysname> system-view
[Sysname] reserved vxlan 10000
```

reset arp suppression vsi

Use **reset arp suppression vsi** to clear ARP flood suppression entries on VSIs.

Syntax

reset arp suppression vsi [**name** *vsi-name*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

name *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VSI, this command clears ARP flood suppression entries on all VSIs.

Examples

Clear ARP flood suppression entries on all VSIs.

```
<Sysname> reset arp suppression vsi
This command will delete all entries. Continue? [Y/N]:y
```

Related commands

arp suppression enable

display arp suppression vsi

reset l2vpn mac-address

Use **reset l2vpn mac-address** to clear dynamic MAC address entries on VSIs.

Syntax

reset l2vpn mac-address [**vsi** *vsi-name*]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

vsi *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VSI, this command clears all dynamic MAC address entries on all VSIs.

Usage guidelines

Use this command when the number of dynamic MAC address entries reaches the limit or the device learns incorrect MAC addresses.

Examples

Clear the dynamic MAC address entries on VSI **vpn1**.

```
<Sysname> reset l2vpn mac-address vsi vpn1
```

Related commands

display l2vpn mac-address vsi

reset l2vpn statistics ac

Use **reset l2vpn statistics ac** to clear packet statistics on ACs.

Syntax

reset l2vpn statistics ac [**interface** *interface-type interface-number* [**service-instance** *instance-id*]]

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	Yes
NFNX3-HDB680, NFNX3-HDB1080	No

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number.

service-instance *instance-id*: Specifies an Ethernet service instance ID in the range of 1 to 4096. You must specify this option if the **interface** *interface-type interface-number* option specifies a Layer 2 interface. You cannot specify this option if the **interface** *interface-type interface-number* option specifies a Layer 3 interface.

Usage guidelines

If you do not specify any parameters, this command clears packet statistics on all ACs.

Examples

Clear packet statistics for Layer 3 interface GigabitEthernet 1/0/1.

```
<Sysname> reset l2vpn statistics ac interface gigabitethernet 1/0/1
```

Related commands

ac statistics enable

display l2vpn interface

display l2vpn service-instance verbose

statistics enable (Ethernet service instance view)

reset l2vpn statistics tunnel

Use **reset l2vpn statistics tunnel** to clear packet statistics on VXLAN tunnel interfaces.

Syntax

reset l2vpn statistics tunnel [**vsi** *vsi-name*]

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	Yes
NFNX3-HDB680, NFNX3-HDB1080	No

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

vsi *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VSI, this command clears packet statistics on VXLAN tunnel interfaces of all VSIs.

Examples

Clear packet statistics on VXLAN tunnel interfaces of all VSIs.

```
<Sysname> reset l2vpn statistics tunnel
```

Related commands

tunnel statistics enable

reset l2vpn statistics vsi

Use **reset l2vpn statistics vsi** to clear packet statistics on VSIs.

Syntax

reset l2vpn statistics vsi [**name** *vsi-name*]

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	Yes
NFNX3-HDB680, NFNX3-HDB1080	No

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

name *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VSI, this command clears packet statistics on all VSIs.

Examples

Clear packet statistics on all VSIs.

```
<Sysname> reset l2vpn statistics vsi
```

Related commands

statistics enable (VSI view)

selective-flooding mac-address

Use **selective-flooding mac-address** to enable selective flood for a MAC address.

Use **undo selective-flooding mac-address** to disable selective flood for a MAC address.

Syntax

selective-flooding mac-address *mac-address*

undo selective-flooding mac-address *mac-address*

Default

Selective flood is disabled for all MAC addresses.

Views

VSI view

Predefined user roles

network-admin

context-admin

Parameters

mac-address: Specifies a MAC address. The MAC address cannot be all Fs.

Usage guidelines

This command excludes a remote MAC address from the flood suppression done by using the **flooding disable** command. The VTEP will flood the frames destined for the specified MAC address to remote sites when unknown-unicast floods are confined to the local site.

Examples

Enable selective flood for **000f-e201-0101** on VSI **vsi1**.

```
<Sysname> system-view
[Sysname] vsi vsi1
[Sysname-vsi-vsi1] selective-flooding mac-address 000f-e201-0101
```

Related commands

flooding disable

service-class

Use **service-class** to set a service class value for outgoing VXLAN packets.

Use **undo service-class** to restore the default.

Syntax

service-class *service-class-value*

undo service-class

The following compatibility matrix shows the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	Yes

NFNX3-HDB680, NFNX3-HDB1080	No

Default

No service class value is set for outgoing VXLAN packets.

Views

VSI view

Predefined user roles

network-admin

context-admin

Parameters

service-class-value: Specifies a service class value. The value range for this argument is 0 to 15.

Usage guidelines

Class Based Tunnel Selection (CBTS) compares the service class value of VXLAN packets with the service class values of MPLS TE tunnels. CBTS uses the following rules to select a tunnel to forward the traffic:

- If the packets match only one MPLS TE tunnel, CBTS uses this tunnel.
- If the packets match multiple MPLS TE tunnels, CBTS randomly selects one tunnel from them.
- If the packets do not match any MPLS TE tunnel, CBTS selects the MPLS TE tunnel that meets the following requirements:
  - Its service class value is smaller than the service class value of the traffic.
  - Its service class value is the nearest to the service class value of the traffic.

  If multiple qualified tunnels exist, CBTS randomly selects one of them to forward the packets. If an MPLS TE tunnel is not configured with a service class value, this tunnel has the smallest service class value.

The service class value is used only when MPLS TE tunnels are used to forward the VXLAN packets. This value is meaningless if any other tunnel is used to forward the VXLAN packets.

To set the service class value for an MPLS TE tunnel, use the **mpls te service-class** command. For more information about this command, see MPLS TE commands in *MPLS Command Reference*.

If you execute the **service-class** command multiple times for a VSI, the most recent configuration takes effect.

Examples

Set the service class value to 2 for outgoing VXLAN packets.

```
<Sysname> system-view
[Sysname] vsi vpna
[Sysname-vsi-vpna] service-class 2
```

Related commands

display l2vpn vsi

service-instance

Use **service-instance** to create an Ethernet service instance and enter its view, or enter the view of an existing Ethernet service instance.

Use **undo service-instance** to delete an Ethernet service instance.

Syntax

service-instance *instance-id*

undo service-instance *instance-id*

The following compatibility matrix shows the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	Yes
NFNX3-HDB680, NFNX3-HDB1080	No

Default

No Ethernet service instances exist.

Views

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

context-admin

Parameters

instance-id: Specifies an Ethernet service instance ID in the range of 1 to 4096.

Examples

On Layer 2 Ethernet interface GigabitEthernet 1/0/1, create Ethernet service instance 1 and enter Ethernet service instance view.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] service-instance 1
[Sysname-GigabitEthernet1/0/1-srv1]
```

Related commands

display l2vpn service-instance

shutdown

Use **shutdown** to shut down a VSI.

Use **undo shutdown** to bring up a VSI.

Syntax

shutdown

undo shutdown

Default

VSIs are not manually shut down.

Views

VSI view

Predefined user roles

network-admin

context-admin

Usage guidelines

Use this command to temporarily disable a VSI to provide Layer 2 switching services. The shutdown action does not change settings on the VSI. You can continue to configure the VSI. After you bring up the VSI again, the VSI provides services based on the latest settings.

Examples

Shut down VSI **vpn1**.

```
<Sysname> system-view
[Sysname] vsi vpn1
[Sysname-vsi-vpn1] shutdown
```

Related commands

`display l2vpn vsi`

statistics enable (Ethernet service instance view)

Use **`statistics enable`** to enable packet statistics for an Ethernet service instance.

Use **`undo statistics enable`** to disable packet statistics for an Ethernet service instance.

Syntax

`statistics enable`

`undo statistics enable`

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	Yes
NFNX3-HDB680, NFNX3-HDB1080	No

Default

The packet statistics feature is disabled for an Ethernet service instance.

Views

Ethernet service instance view

Predefined user roles

network-admin

context-admin

Usage guidelines

For this command to take effect, you must configure a frame match criterion for the Ethernet service instance and map it to a VSI. If you modify the frame match criterion or VSI mapping, packet statistics of the instance is cleared.

Examples

Enable packet statistics for Ethernet service instance 200 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] service-instance 200
[Sysname-GigabitEthernet1/0/1-srv200] statistics enable
```

Related command

display l2vpn service-instance verbose

reset l2vpn statistics ac

statistics enable (VSI view)

Use **statistics enable** to enable packet statistics for a VSI.

Use **undo statistics enable** to disable packet statistics for a VSI.

Syntax

statistics enable

undo statistics enable

The following compatibility matrix shows the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	Yes
NFNX3-HDB680, NFNX3-HDB1080	No

Default

The packet statistics feature is disabled for a VSI.

Views

VSI view

Predefined user roles

network-admin

context-admin

Examples

Enable packet statistics for VSI **vsi1**.

```
<Sysname> system-view
[Sysname] vsi vsi1
[Sysname-vsi-vsi1] statistics enable
```

Related commands

display l2vpn vsi verbose

reset l2vpn statistics vsi

tunnel

Use **tunnel** to assign a VXLAN tunnel to a VXLAN.

Use **undo tunnel** to remove a VXLAN tunnel from a VXLAN.

Syntax

tunnel *tunnel-number*

undo tunnel *tunnel-number*

Default

A VXLAN does not contain VXLAN tunnels.

Views

VXLAN view

Predefined user roles

network-admin

context-admin

Parameters

*tunnel-numbe*r: Specifies a tunnel interface number. The value range for this argument is 0 to 1023. The tunnel must be a VXLAN tunnel.

remote-vni *vxlan-id*: Specifies a remote VXLAN ID. The value range for the *vxlan-id* argument varies by device model. You can specify this option only for a VXLAN-DCI tunnel.

Usage guidelines

This command assigns a VXLAN tunnel to a VXLAN to provide Layer 2 connectivity for the VXLAN between two sites. In unicast mode, the system floods unknown unicast, multicast, and broadcast traffic to each tunnel in the VXLAN.

You can assign multiple VXLAN tunnels to a VXLAN, and configure a VXLAN tunnel to trunk multiple VXLANs.

Examples

Assign VXLAN tunnels 1 and 2 to VXLAN 10000.

```
<Sysname> system-view
[Sysname] vsi vpna
[Sysname-vsi-vpna] vxlan 10000
[Sysname-vsi-vpna-vxlan-10000] tunnel 1
[Sysname-vsi-vpna-vxlan-10000] tunnel 2
```

Related commands

display vxlan tunnel

tunnel bfd enable

Use **tunnel bfd enable** to enable BFD on a VXLAN tunnel interface.

Use **undo tunnel bfd enable** to disable BFD on a VXLAN tunnel interface.

Syntax

tunnel bfd enable destination-mac *mac-address*

undo tunnel bfd enable

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	Yes
NFNX3-HDB680, NFNX3-HDB1080	No

Default

BFD is disabled on a VXLAN tunnel interface.

Views

VXLAN tunnel interface view

Predefined user roles

network-admin

context-admin

Parameters

destination-mac *mac-address*: Specifies a destination MAC address in H-H-H format for BFD control packets. The MAC address can be a remote VTEP address or a multicast address. You can omit the consecutive zeros at the beginning of each segment. For example, you can enter **f-e2-1** for **000f-00e2-0001**.

Usage guidelines

Enable BFD on both ends of a VXLAN tunnel for quick link connectivity detection. The VTEPs periodically send BFD single-hop control packets to each other through the VXLAN tunnel. A VTEP sets the tunnel state to Defect if it has not received control packets from the remote end for 5 seconds. In this situation, the tunnel interface state is still Up. The tunnel state will change from Defect to Up if the VTEP can receive BFD control packets again.

Examples

Enable BFD on VXLAN tunnel interface Tunnel 9, and specify 1-1-1 as the destination MAC address for BFD control packets.

```
<Sysname> system-view
[Sysname] interface tunnel 9 mode vxlan
[Sysname-Tunnel9] tunnel bfd enable destination-mac 1-1-1
```

tunnel statistics enable

Use **tunnel statistics enable** to enable packet statistics for all VXLAN tunnels associated with a VSI.

Use **undo tunnel statistics enable** to disable packet statistics for all VXLAN tunnels associated with a VSI.

Syntax

tunnel statistics enable

undo tunnel statistics enable

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	Yes
NFNX3-HDB680, NFNX3-HDB1080	No

Default

The packet statistics feature is disabled for the VXLAN tunnels associated with a VSI.

Views

VSI view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command enables packet statistics only for VXLAN tunnels. It does not take effect on VXLAN-DCI tunnels.

Examples

Enable packet statistics for all VXLAN tunnels associated with VSI **vpna**.

```
<Sysname> system-view
[Sysname] vsi vpna
[Sysname-vsi-vpna] tunnel statistics enable
```

Related commands

display vxlan tunnel

VSİ

Use **vsi** to create a VSI and enter its view, or enter the view of an existing VSI.

Use **undo vsi** to delete a VSI.

Syntax

vsi *vsi-name*

undo vsi *vsi-name*

Default

No VSIs exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

vsi-name: Specifies a VSI name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

A VSI acts as a virtual switch to provide Layer 2 switching services for a VXLAN on a VTEP. A VSI has all functions of a physical Ethernet switch, including source MAC address learning, MAC address aging, and flooding.

A VSI can provide services only for one VXLAN.

Examples

Create VSI **vxlan10** and enter VSI view.

```
<Sysname> system-view
[Sysname] vsi vxlan10
[Sysname-vsi-vxlan10]
```

Related commands

display l2vpn vsi

vxlan

Use **vxlan** to create a VXLAN and enter its view, or enter the view of an existing VXLAN.

Use **undo vxlan** to restore the default.

Syntax

vxlan *vxlan-id*

undo vxlan

Default

No VXLANs exist.

Views

VSI view

Predefined user roles

network-admin

context-admin

Parameters

vxlan-id: Specifies a VXLAN ID in the range of 0 to 16777215.

Usage guidelines

You can create only one VXLAN for a VSI. The VXLAN ID for each VSI must be unique.

Examples

Create VXLAN 10000 for VSI **vpna** and enter VXLAN view.

```
<Sysname> system-view
[Sysname] vsi vpna
[Sysname-vsi-vpna] vxlan 10000
[Sysname-vsi-vpna-vxlan-10000]
```

Related commands

vsi

vxlan fast-forwarding enable

Use **vxlan fast-forwarding enable** to enable VXLAN fast forwarding.

Use **undo vxlan fast-forwarding enable** to disable VXLAN fast forwarding.

Syntax

vxlan fast-forwarding enable

undo vxlan fast-forwarding enable

Default

VXLAN fast forwarding is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

VXLAN fast forwarding enables the device to bypass QoS and security services when the device forwards data traffic over VXLAN tunnels based on the software. As a best practice, enable this feature to improve forwarding speed only when QoS and security services are not configured on the following interfaces:

- VSI interfaces.
- Traffic outgoing interfaces for VXLAN tunnels.

When VXLAN fast forwarding is enabled, a VXLAN tunnel cannot use ECMP routes to load share traffic. Instead, it selects one route from the ECMP routes to forward VXLAN packets.

Examples

Enable VXLAN fast forwarding.

```
<Sysname> system
[Sysname] vxlan fast-forwarding enable
```

vxlan invalid-udp-checksum discard

Use **vxlan invalid-udp-checksum discard** to enable the device to drop the VXLAN packets that fail UDP checksum check.

Use **undo vxlan invalid-udp-checksum discard** to restore the default.

Syntax

vxlan invalid-udp-checksum discard

undo vxlan invalid-udp-checksum discard

Default

The device does not check the UDP checksum of VXLAN packets.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command enables the device to check the UDP checksum of VXLAN packets.

The device always sets the UDP checksum of VXLAN packets to 0. For compatibility with third-party devices, a VXLAN packet can pass the check if its UDP checksum is 0 or correct. If its UDP checksum is incorrect, the VXLAN packet fails the check and is dropped.

Examples

Enable the device to drop the VXLAN packets that fail UDP checksum check.

```
<Sysname> system-view
[Sysname] vxlan invalid-udp-checksum discard
```

vxlan ip-forwarding

Use **vxlan ip-forwarding** to enable Layer 3 forwarding for all VXLANs.

Use **undo vxlan ip-forwarding** to enable Layer 2 forwarding for all VXLANs.

Syntax

vxlan ip-forwarding

undo vxlan ip-forwarding

The following compatibility matrixes show the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	Yes
NFNX3-HDB680, NFNX3-HDB1080	No

Default

Layer 3 forwarding is enabled for all VXLANs.

Views.

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

If the device is a VTEP, enable Layer 2 forwarding for VXLANs. If the device is a VXLAN IP gateway, enable Layer 3 forwarding for VXLANs.

In Layer 3 forwarding mode, the VTEP uses the ARP table (IPv4 network) or ND table (IPv6 network) to forward traffic for VXLANs. In Layer 2 forwarding mode, the VTEP uses the MAC address table to forward traffic for VXLANs.

You must delete all VSIs, VSI interfaces, and VXLAN tunnel interfaces before you can change the forwarding mode.

Examples

Enable Layer 3 forwarding for all VXLANs.

```
<Sysname>system-view
[Sysname] vxlan ip-forwarding
```

vxlan local-mac report

Use **vxlan local-mac report** to enable local-MAC logging.

Use **undo vxlan local-mac report** to disable local-MAC logging.

Syntax

vxlan local-mac report

undo vxlan local-mac report

Default

Local-MAC logging is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

When the local-MAC logging feature is enabled, the VXLAN module immediately sends a log message with its local MAC addresses to the information center. When a local MAC address is added or removed, a log message is also sent to the information center to notify the local-MAC change.

With the information center, you can set log message filtering and output rules, including output destinations. For more information about configuring the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Enable local-MAC logging.

```
<Sysname> system-view
[Sysname] vxlan local-mac report
```

vxlan source udp-port acl

Use **vxlan source udp-port acl** to configure an ACL match criterion and specify the source UDP port number in the VXLAN encapsulation for matching frames.

Use **undo vxlan source udp-port** to restore the default.

Syntax

vxlan source udp-port *port-number* **acl** *acl-number*

undo vxlan source udp-port

The following compatibility matrix shows the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	Yes
NFNX3-HDB680, NFNX3-HDB1080	No

Default

The source UDP port number in the VXLAN encapsulation is generated based on the source and destination MAC addresses of the inner Ethernet frame.

Views

VXLAN tunnel interface view

Predefined user roles

network-admin

context-admin

Parameters

port-number: Specifies a UDP port number in the range of 1024 to 65535. As a best practice, specify a port number in the range of 1024 to 49151.

acl-number: Specifies an ACL by its number in the range of 3000 to 3999. The ACL must be an advanced ACL.

Usage guidelines

This command takes effect only on IPv4-based VXLAN. Only manually created VXLAN tunnel interfaces support this command.

This command enables a VXLAN tunnel interface to filter frames by using an ACL and encapsulate a specific source UDP port number for matching frames. This allows IPsec to identify the VXLAN packets to encrypt by the source UDP port number in the VXLAN encapsulation.

If the ACL specified by using this command does not exist or does not contain an IP address-related rule, frames are encapsulated based on the default setting.

This command has a higher priority than the **vxlan source udp-port five-tuple** command.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure VXLAN tunnel interface **Tunnel 1** to encapsulate source UDP port number 50001 for the frames that match ACL 3001.

```
<Sysname> system-view
[Sysname] interface tunnel 1 mode vxlan
[Sysname-Tunnel1] vxlan source udp-port 50001 acl 3001
```

Related commands

acl (*ACL and QoS Command Reference*)

vxlan source udp-port five-tuple

vxlan source udp-port five-tuple

Use **vxlan source udp-port five-tuple** to configure a VXLAN tunnel interface to generate the source UDP port number in the VXLAN encapsulation based on the IP five-tuple of the inner Ethernet frame.

Use **undo vxlan source udp-port five-tuple** to restore the default.

Syntax

vxlan source udp-port five-tuple

undo vxlan source udp-port five-tuple

The following compatibility matrix shows the support of hardware platforms for this command:

Models	Command compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	Yes
NFNX3-HDB680, NFNX3-HDB1080	No

Default

The source UDP port number in the VXLAN encapsulation is generated based on the source and destination MAC addresses of the inner Ethernet frame.

Views

VXLAN tunnel interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

This command takes effect only on IPv4-based VXLAN. Only manually created VXLAN tunnel interfaces support this command.

This command has a lower priority than the **vxlan source udp-port acl** command. If you use both commands on a VXLAN tunnel interface, the **vxlan source udp-port five-tuple** command takes effect only on the frames that fail to match the ACL specified by using the **vxlan source udp-port acl** command.

Examples

Configure VXLAN tunnel interface **Tunnel 1** to generate the source UDP port number in the VXLAN encapsulation based on the IP five-tuple of the inner Ethernet frame.

```
<Sysname> system-view
[Sysname] interface tunnel 1 mode vxlan
[Sysname-Tunnel1] vxlan source udp-port five-tuple
```

Related commands

vxlan source udp-port acl

vxlan tunnel mac-learning disable

Use **vxlan tunnel mac-learning disable** to disable remote-MAC address learning.

Use **undo vxlan tunnel mac-learning disable** to enable remote-MAC address learning.

Syntax

vxlan tunnel mac-learning disable

undo vxlan tunnel mac-learning disable

Default

Remote-MAC address learning is enabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

When network attacks occur, use this command to prevent the device from learning incorrect remote MAC addresses in the data plane.

Examples

Disable remote-MAC address learning.

```
<Sysname> system-view
[Sysname] vxlan tunnel mac-learning disable
```

vxlan udp-port

Use **vxlan udp-port** to set the destination UDP port number for VXLAN packets.

Use **undo vxlan udp-port** to restore the default.

Syntax

vxlan udp-port *port-number*

undo vxlan udp-port

Default

The destination UDP port number is 4789 for VXLAN packets.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

port-number: Specifies a UDP port number in the range of 1 to 65535. As a best practice, specify a port number in the range of 1024 to 65535 to avoid conflict with well-known ports.

Usage guidelines

You must configure the same destination UDP port number on all VTEPs in a VXLAN.

Examples

Set the destination UDP port number to 6666 for VXLAN packets.

```
<Sysname> system-view
[Sysname] vxlan udp-port 6666
```

xconnect vsi

Use **xconnect vsi** to map an AC to a VSI.

Use **undo xconnect vsi** to restore the default.

Syntax

xconnect vsi *vsi-name* [**track** *track-entry-number*&<1-3>]

undo xconnect vsi

Default

An AC is not mapped to any VSI.

Views

Interface view

Predefined user roles

network-admin

context-admin

Parameters

vsi-name: Specifies the VSI name, a case-sensitive string of 1 to 31 characters.

track *track-entry-number*&<1-3>: Specifies a space-separated list of up to three track entry numbers in the range of 1 to 1024. The AC is up only if a minimum of one associated track entry is in positive state.

Usage guidelines

For traffic that matches a Layer 3 interface, the system uses the VSI's MAC address table to make a forwarding decision.

Examples

Map GigabitEthernet 1/0/1 to VSI **vpn1**.

```
<Sysname> system-view
[Sysname] vsi vpn1
[Sysname-vsi-vpn1] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] xconnect vsi vpn1
```

Related commands

display l2vpn interface

vsi

VXLAN IP gateway commands

arp distributed-gateway dynamic-entry synchronize

Use **arp distributed-gateway dynamic-entry synchronize** to enable dynamic ARP entry synchronization for distributed VXLAN IP gateways.

Use **undo arp distributed-gateway dynamic-entry synchronize** to disable dynamic ARP entry synchronization for distributed VXLAN IP gateways.

Syntax

arp distributed-gateway dynamic-entry synchronize

undo arp distributed-gateway dynamic-entry synchronize

Default

Dynamic ARP entry synchronization is disabled for distributed VXLAN IP gateways.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

When local proxy ARP is enabled on distributed VXLAN IP gateways, each gateway learns ARP information independently. A gateway does not forward ARP packets destined for its local VSI interfaces to other gateways. For distributed VXLAN IP gateways to have the same ARP entries, you must enable dynamic ARP entry synchronization.

A controller can also synchronize ARP entries among distributed VXLAN IP gateways. When you use a controller, do not enable dynamic ARP entry synchronization.

Examples

Enable dynamic ARP entry synchronization for distributed VXLAN IP gateways.

```
<Sysname> system-view
[Sysname] arp distributed-gateway dynamic-entry synchronize
```

Related commands

distributed-gateway local

local-proxy-arp enable (*Layer 3—IP Services Command Reference*)

bandwidth

Use **bandwidth** to set the expected bandwidth for a VSI interface.

Use **undo bandwidth** to restore the default.

Syntax

bandwidth *bandwidth-value*

undo bandwidth

Default

The expected bandwidth (in kbps) equals the interface baudrate divided by 1000.

Views

VSI interface view

Predefined user roles

network-admin

context-admin

Parameters

bandwidth-value: Specifies the expected bandwidth, in the range of 1 to 400000000 kbps.

Usage guidelines

The expected bandwidth is an informational parameter used only by higher-layer protocols for calculation. You cannot adjust the actual bandwidth of an interface by using this command.

Examples

Set the expected bandwidth to 10000 kbps for VSI-interface 100.

```
<Sysname> system-view
[Sysname] interface vsi-interface 100
[Sysname-Vsi-interface100] bandwidth 10000
```

default

Use **default** to restore the default settings for a VSI interface.

Syntax

default

Views

VSI interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

CAUTION:

The **default** command might interrupt ongoing network services. Make sure you are fully aware of the impact of this command when you use it on a live network.

This command might fail to restore the default settings for some commands for reasons such as command dependencies and system restrictions.

To resolve this problem:

1. Use the **display this** command in interface view to identify these commands.
2. Use their **undo** forms or follow the command reference to restore their default settings.
3. If the restoration attempt still fails, follow the error message instructions to resolve the problem.

Examples

Restore the default settings for VSI-interface 100.

```
<Sysname> system-view
[Sysname] interface vsi-interface 100
[Sysname-Vsi-interface100] default
This command will restore the default settings. Continue? [Y/N]:y
```

description

Use **description** to configure the description of a VSI interface.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

The description of a VSI interface is *interface-name* plus **Interface** (for example, **Vsi-interface100 Interface**).

Views

VSI interface view

Predefined user roles

network-admin

context-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 255 characters.

Examples

Configure the description as **gateway for VXLAN 10** for VSI-interface 100.

```
<Sysname> system-view
[Sysname] interface vsi-interface 100
[Sysname-Vsi-interface100] description gateway for VXLAN 10
```

display interface vsi-interface

Use **display interface vsi-interface** to display information about VSI interfaces.

Syntax

display interface [**vsi-interface** [*vsi-interface-id*]] [**brief** [**description** | **down**]]

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

vsi-interface [*vsi-interface-id*]: Specifies a VSI interface by its number. Make sure the specified VSI interface has been created on the device. If you do not specify the **vsi-interface** [*vsi-interface-id*] option, this command displays information about all interfaces. If you specify only the **vsi-interface** keyword, this command displays information about all VSI interfaces. If you specify a VSI interface, this command displays information about the specified interface.

brief: Display brief interface information. If you do not specify this keyword, the command displays detailed interface information.

description: Displays complete interface descriptions. If you do not specify this keyword, the command displays only the first 27 characters of interface descriptions.

down: Displays interfaces that are physically down as well as the down reason. If you do not specify this keyword, the command does not filter output by physical interface state.

Examples

Display information about VSI-interface 100.

```
<Sysname> display interface vsi-interface 100
Vsi-interface100
Current state: UP
Line protocol state: UP
Description: Vsi-interface100 Interface
Bandwidth: 1000000 kbps
Maximum transmission unit: 1500
Internet address: 10.1.1.1/24 (primary)
IP packet frame type: Ethernet II, hardware address: 0011-2200-0102
IPv6 packet frame type: Ethernet II, hardware address: 0011-2200-0102
Physical: Unknown, baudrate: 1000000 kbps
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

Table 10 Command output

Field	Description
Current state	Physical link state of the interface: • **Administratively DOWN**—The interface has been shut down by using the **shutdown** command. • **DOWN**—The interface is administratively up, but its physical state is down. • **UP**—The interface is both administratively and physically up.
Line protocol state	Data link layer state of the interface: • **UP**—The data link layer protocol is up. • **UP(spoofing)**—The data link layer protocol is up, but the link is an on-demand link or does not exist. • **DOWN**—The data link layer protocol is down.
Description	Description of the interface.
Bandwidth	Expected bandwidth of the interface.
Maximum transmission unit	MTU of the interface.
Internet protocol processing: Disabled	The interface is not assigned an IP address and cannot process IP packets.
Internet address: *ip-address*/*mask-length* (*Type*)	IP address of the interface and type of the address in parentheses. Possible IP address types include: • **Primary**—Manually configured primary IP address. • **Sub**—Manually configured secondary IP address. If the interface has both primary and secondary IP addresses, the primary IP address is displayed. If the interface has only secondary IP addresses, the lowest secondary IP address is displayed. • **DHCP-allocated**—DHCP allocated IP address. For more information, see DHCP client configuration in *Layer 3—IP Services Configuration Guide*. • **BOOTP-allocated**—BOOTP allocated IP address. For more information, see BOOTP client configuration in *Layer 3—IP*

Field	Description
	Services Configuration Guide. • **PPP-negotiated**—IP address assigned by a PPP server during PPP negotiation. For more information, see PPP configuration in *PPP and PPPoE Configuration Guide*. • **Unnumbered**—IP address borrowed from another interface. • **MAD**—IP address assigned to an IRF member device for MAD on the interface. For more information, see IRF configuration in *Virtual Technologies Configuration Guide*.
IP packet frame type	IPv4 packet framing format.
hardware address	MAC address.
IPv6 packet frame type	IPv6 packet framing format.
Physical	Physical type of the interface, which is fixed at **Unknown**.
baudrate	Interface baudrate in kbps.
Last clearing of counters	Last time when the **reset counters interface vsi-interface** command was used to clear interface statistics. This field displays **Never** if the **reset counters interface vsi-interface** command has never been used on the interface since the device startup.
Last 300 seconds input rate	Average input rate for the last 300 seconds.
Last 300 seconds output rate	Average output rate for the last 300 seconds.
Input: 0 packets, 0 bytes, 0 drops	Incoming traffic statistics on the interface: • Number of incoming packets. • Number of incoming bytes. • Number of dropped incoming packets.
Output: 0 packets, 0 bytes, 0 drops	Outgoing traffic statistics on the interface: • Number of outgoing packets. • Number of outgoing bytes. • Number of dropped outgoing packets.

Display brief information about all VSI interfaces.

```
<Sysname> display interface vsi-interface brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP      Description
Vsi100               DOWN DOWN     --
```

Display brief information and complete description for VSI-interface 100.

```
<Sysname> display interface vsi-interface 100 brief description
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP      Description
Vsi100               UP   UP       1.1.1.1         VSI-interface100
```

Displays interfaces that are physically down and the down reason.

```
<Sysname> display interface brief down
```

```
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Interface            Link   Cause
Vsi100               DOWN   Administratively
Vsi200               DOWN   Administratively
```

Table 11 Command output

Field	Description
Interface	Abbreviated interface name.
Link	Physical link state of the interface: • **UP**—The interface is physically up. • **DOWN**—The interface is physically down. • **ADM**—The interface has been shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command. • **Stby**—The interface is a backup interface in standby state. To see the primary interface, use the **display interface-backup state** command.
Protocol	Data link layer protocol state of the interface: • **UP**—The data link layer protocol of the interface is up. • **UP (s)**—The data link layer protocol of the interface is up, but the link is an on-demand link or does not exist. The **(s)** attribute represents the spoofing flag. • **DOWN**—The data link layer protocol of the interface is down.
Primary IP	Primary IP address of the interface. This field displays two hyphens (**--**) if the interface does not have an IP address.
Description	Description of the interface.
Cause	Cause for the physical link state of an interface to be **DOWN**: • **Administratively**—The interface has been manually shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command. • **Not connected**—The interface is not mapped to any VSI, or the mapped VSI does not have any AC or VXLAN tunnel.

Related commands

reset counters interface vsi-interface

distributed-gateway local

Use **distributed-gateway local** to specify a VSI interface as a distributed gateway to provide services for the local site.

Use **undo distributed-gateway local** to restore the default.

Syntax

distributed-gateway local

undo distributed-gateway local

Default

A VSI interface is not a distributed gateway.

Views

VSI interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

If a VXLAN uses distributed gateway services, you must assign the same IP address to the VXLAN's VSI interfaces on different VTEPs. To avoid IP address conflicts, you must specify the VSI interface on each VTEP as a distributed gateway.

Examples

Specify VSI-interface 100 as a distributed gateway.

```
<Sysname> system-view
[Sysname] interface vsi-interface 100
[Sysname-Vsi-interface100] distributed-gateway local
```

gateway subnet

Use **gateway subnet** to assign a subnet to a VSI.

Use **undo gateway subnet** to remove a subnet from a VSI.

Syntax

gateway subnet { *ipv4-address wildcard-mask* | *ipv6-address prefix-length* }

undo gateway subnet { *ipv4-address wildcard-mask* | *ipv6-address prefix-length* }

Default

No subnet is assigned to a VSI.

Views

VSI view

Predefined user roles

network-admin

context-admin

Parameters

ipv4-address: Specifies an IPv4 subnet address in dotted-decimal notation.

wildcard-mask: Specifies a wildcard mask in dotted decimal notation. In contrast to a network mask, the 0 bits in a wildcard mask represent "do care" bits, and the 1 bits represent "don't care" bits. If the "do care" bits in a packet's IP address are identical to the "do care" bits in the specified subnet address, the packet is assigned to the VSI. All "don't care" bits are ignored. The 0s and 1s in a wildcard mask can be noncontiguous. For example, 0.255.0.255 is a valid wildcard mask.

ipv6-address prefix-length: Specifies an IPv6 subnet address and the address prefix length in the range of 1 to 128.

Usage guidelines

You must configure this command on VSIs that share a gateway interface. This command enables the VSI interface to identify the VSI of a packet.

You can assign a maximum of eight IPv4 and IPv6 subnets to a VSI.

You must specify a gateway interface for a VSI before you can assign subnets to the VSI. If you remove the gateway interface from the VSI, the VSI's subnet settings are automatically deleted.

For VSIs that share a gateway interface, the subnets must be unique.

Examples

Assign subnet 100.0.10.0/24 to VSI **vxlan**.

```
<Sysname> system-view
[Sysname] vsi vxlan
[Sysname-vsi-vxlan] gateway subnet 100.0.10.0 0.0.0.255
```

gateway vsi-interface

Use **gateway vsi-interface** to specify a gateway interface for a VSI.

Use **undo gateway vsi-interface** to restore the default.

Syntax

gateway vsi-interface *vsi-interface-id*

undo gateway vsi-interface

Default

No gateway interface is specified for a VSI.

Views

VSI view

Predefined user roles

network-admin

context-admin

Parameters

vsi-interface-id: Specifies a VSI interface by its number. The value range for this argument is 0 to 8191.

Usage guidelines

A VSI can have only one gateway interface. Multiple VSIs can share a gateway interface.

Examples

Specify VSI-interface 100 as the gateway interface for VSI **vpna**.

```
<Sysname> system-view
[Sysname] vsi vpna
[Sysname-vsi-vpna] gateway vsi-interface 100
```

Related commands

interface vsi-interface

interface vsi-interface

Use **interface vsi-interface** to create a VSI interface and enter its view, or enter the view of an existing VSI interface.

Use **undo interface vsi-interface** to delete a VSI interface.

Syntax

interface vsi-interface *vsi-interface-id*

undo interface vsi-interface *vsi-interface-id*

Default

No VSI interfaces exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

vsi-interface-id: Specifies a VSI interface number. The value range for this argument is 0 to 8191.

Examples

Create VSI-interface 100 and enter VSI interface view.

```
<Sysname> system-view
[Sysname] interface vsi-interface 100
[Sysname-Vsi-interface100]
```

Related commands

gateway vsi-interface

mac-address

Use **mac-address** to assign a MAC address to a VSI interface.

Use **undo mac-address** to restore the default.

Syntax

mac-address *mac-address*

undo mac-address

Default

A VSI interface does not have a MAC address.

Views

VSI interface view

Predefined user roles

network-admin

context-admin

Parameters

mac-address: Specifies a MAC address in H-H-H format.

Examples

Assign MAC address 0001-0001-0001 to VSI-interface 100.

```
<Sysname> system-view
```

```
[Sysname] interface vsi-interface 100
[Sysname-Vsi-interface100] mac-address 1-1-1
```

mtu

Use **mtu** to set the MTU for a VSI interface.

Use **undo mtu** to restore the default.

Syntax

mtu *size*

undo mtu

Default

The MTU is 1500 bytes.

Views

VSI interface view

Predefined user roles

network-admin

context-admin

Parameters

size: Specifies an MTU value in the range of 46 to 1500 bytes.

Examples

Set the MTU to 1430 bytes for VSI-interface 100.

```
<Sysname> system-view
[Sysname] interface vsi-interface 100
[Sysname-Vsi-interface100] mtu 1430
```

reset counters interface vsi-interface

Use **reset counters interface vsi-interface** to clear packet statistics on VSI interfaces.

Syntax

reset counters interface [**vsi-interface** [*vsi-interface-id*]]

Views

User view

Predefined user roles

network-admin

context-admin

Parameters

vsi-interface [*vsi-interface-id*]: Specifies a VSI interface by its number. Make sure the specified VSI interface has been created on the device. If you do not specify the **vsi-interface** [*vsi-interface-id*] option, this command clears packet statistics on all interfaces. If you specify only the **vsi-interface** keyword, this command clears packet statistics on all VSI interfaces. If you specify a VSI interface, this command clears packet statistics on the specified interface.

Usage guidelines

Use this command to clear history statistics before you collect traffic statistics for a time period.

Examples

Clear packet statistics on VSI-interface 100.

```
<Sysname> reset counters interface vsi-interface 100
```

Related commands

display interface vsi-interface

shutdown

Use **shutdown** to shut down a VSI interface.

Use **undo shutdown** to bring up a VSI interface.

Syntax

shutdown

undo shutdown

Default

A VSI interface is not manually shut down.

Views

VSI interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

CAUTION:

If you shut down a VSI interface, the VXLAN network using this VSI interface as the gateway will be unable to communicate with other networks at Layer 3. Make sure you are fully aware of the impact of this command when you use it on a live network.

Examples

Shut down VSI-interface 100.

```
<Sysname> system-view
[Sysname] interface vsi-interface 100
[Sysname-Vsi-interface100] shutdown
```

vtep group member local

Use **vtep group member local** to assign the local VTEP to a VTEP group.

Use **undo vtep group member local** to remove the local VTEP from a VTEP group.

Syntax

vtep group *group-ip* **member local** *member-ip*

undo vtep group *group-ip* **member local**

Default

A VTEP is not assigned to any VTEP group.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

group-ip: Specifies a VTEP group by its group IP address. The IP address must already exist on the local VTEP.

member-ip: Specifies the member VTEP IP address for the local VTEP. The IP address must already exist on the local VTEP.

Usage guidelines

Member VTEPs in a VTEP group cannot use the group IP address or share an IP address.

Examples

Assign the local VTEP to VTEP group 1.1.1.1, and specify 2.2.2.2 as the member VTEP IP address of the local VTEP.

```
<Sysname> system-view
[Sysname] vtep group 1.1.1.1 member local 2.2.2.2
```

Related commands

vtep group member remote

vtep group member remote

Use **vtep group member remote** to specify a VTEP group and its member VTEPs.

Use **undo vtep group member remote** to remove a VTEP group and its member VTEPs.

Syntax

vtep group *group-ip* **member remote** *member-ip*&<1-8>

undo vtep group *group-ip* **member remote**

Default

No VTEP group is specified.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

group-ip: Specifies a VTEP group by its group IP address.

member-ip&<1-8>: Specifies a space-separated list of up to eight member VTEP IP addresses.

Examples

Specify VTEP group 1.1.1.1 and its member VTEPs at 2.2.2.2, 3.3.3.3, and 4.4.4.4.

```
<Sysname> system-view
[Sysname] vtep group 1.1.1.1 member remote 2.2.2.2 3.3.3.3 4.4.4.4
```

Related commands

vtep group member local

vxlan tunnel arp-learning disable

Use **vxlan tunnel arp-learning disable** to disable remote ARP learning for VXLANs.

Use **undo vxlan tunnel arp-learning disable** to enable remote ARP learning for VXLANs.

Syntax

vxlan tunnel arp-learning disable

undo vxlan tunnel arp-learning disable

Default

Remote ARP learning is enabled for VXLANs.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

By default, the device learns ARP information of remote VMs from packets received on VXLAN tunnel interfaces. To save resources on VTEPs in an SDN transport network, you can temporarily disable remote ARP learning when the controller and VTEPs are synchronizing entries. After the entry synchronization is completed, use the **undo vxlan tunnel arp-learning disable** command to enable remote ARP learning.

As a best practice, disable remote ARP learning for VXLANs only when the controller and VTEPs are synchronizing entries.

Examples

Disable remote ARP learning for VXLANs.

```
<Sysname> system
[Sysname] vxlan tunnel arp-learning disable
```

OVSDB commands

The following compatibility matrixes show the support of hardware platforms for OVSDB commands:

Models	OVSDB compatibility
NFNX5-HD6480, NFNX3-HDB3280, NFNX5-T6280, NFNX5-HD5280, NFNX3-HDB1780, NFNX3-HDB3080, NFNX3-HDB1180, NFNX3-HDB1480	Yes

Models	OVSDB compatibility
NFNX3-HDB680, NFNX3-HDB1080	No

ovsdb server bootstrap ca-certificate

Use **ovsdb server bootstrap ca-certificate** to specify a CA certificate file for establishing OVSDB SSL connections.

Use **undo ovsdb server bootstrap ca-certificate** to restore the default.

Syntax

ovsdb server bootstrap ca-certificate *ca-filename*

undo ovsdb server bootstrap ca-certificate

Default

SSL uses the CA certificate file in the PKI domain.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ca-filename: Specifies the CA certificate file name, a case-insensitive string. The file name cannot contain the **slot** string, and the file must be stored on the active MPU.

Usage guidelines

For the specified certificate to take effect, you must execute the **ovsdb server enable** command to enable the OVSDB server. You must disable and then re-enable the OVSDB server if it has been enabled.

If the specified CA certificate file does not exist, the device obtains a self-signed certificate from the controller. The obtained file uses the name specified for the *ca-filename* argument.

Examples

Specify CA certificate file **ca-new** for establishing OVSDB SSL connections.

```
<Sysname> system-view
[Sysname] ovsdb server bootstrap ca-certificate ca-new
```

Related commands

ovsdb server enable

ovsdb server pki domain

ovsdb server pssl

ovsdb server ssl

ovsdb server enable

Use **ovsdb server enable** to enable the OVSDB server.

Use **undo ovsdb server enable** to disable the OVSDB server.

Syntax

ovsdb server enable

undo ovsdb server enable

Default

The OVSDB server is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

To obtain configuration data from controllers, you must enable the OVSDB server.

Before you enable the OVSDB server, you must establish an OVSDB SSL or TCP connection with a minimum of one controller.

Examples

Enable the OVSDB server.

```
<Sysname> system-view
[Sysname] ovsdb server enable
```

ovsdb server pki domain

Use **ovsdb server pki domain** to specify a PKI domain for establishing OVSDB SSL connections.

Use **undo ovsdb bootstrap server pki domain** to restore the default.

Syntax

ovsdb server pki domain *domain-name*

undo ovsdb server pki domain

Default

No PKI domain is specified for establishing OVSDB SSL connections.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

domain-name: Specifies a PKI domain name, a case-sensitive string of 1 to 31 characters. The PKI domain must already exist and contain a complete certificate and key.

Usage guidelines

To communicate with controllers through SSL, you must specify a PKI domain.

For the specified PKI domain to take effect, you must execute the **ovsdb server enable** command to enable the OVSDB server. You must disable and then re-enable the OVSDB server if it has been enabled.

For more information about PKI domains, see PKI in *Security Configuration Guide*.

Examples

Specify PKI domain **ovsdb_test** for establishing OVSDB SSL connections.

```
<Sysname> system-view
[Sysname] ovsdb server pki domain ovsdb_test
```

Related commands

ovsdb server bootstrap ca-certificate

ovsdb server enable

ovsdb server pssl

ovsdb server ssl

ovsdb server pssl

Use **ovsdb server pssl** to enable the device to listen for OVSDB SSL connection requests.

Use **undo ovsdb server pssl** to restore the default.

Syntax

ovsdb server pssl [**port** *port-number*]

undo ovsdb server pssl

Default

The device does not listen for OVSDB SSL connection requests.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

port *port-number*: Specifies a port to listen for OVSDB SSL connection requests. The value range for the *port-number* argument is 1 to 65535. If you do not specify a port, the device uses the port number 6640.

Usage guidelines

Before you use this command, you must specify a PKI domain for SSL.

You can specify only one port to listen for OVSDB SSL connection requests. If you execute this command multiple times, the most recent configuration takes effect.

For the specified port setting to take effect, you must execute the **ovsdb server enable** command to enable the OVSDB server. You must disable and then re-enable the OVSDB server if it has been enabled.

Examples

Enable the device to listen for OVSDB SSL connection requests on port 6640.

```
<Sysname> system-view
```

```
[Sysname] ovsdb server pssl
```

Related commands

ovsdb server bootstrap ca-certificate

ovsdb server enable

ovsdb server pki domain

ovsdb server ssl

ovsdb server ptcp

Use **ovsdb server ptcp** to enable the device to listen for OVSDB TCP connection requests.

Use **undo ovsdb server ptcp** to restore the default.

Syntax

ovsdb server ptcp [**port** *port-number*]

undo ovsdb server ptcp

Default

The device does not listen for OVSDB TCP connection requests.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

port-number: Specifies a port to listen for OVSDB TCP connection requests. The value range for the *port-number* argument is 1 to 65535. If you do not specify a port, the device uses the port number 6640.

Usage guidelines

You can specify only one port to listen for OVSDB TCP connection requests. If you execute this command multiple times, the most recent configuration takes effect.

For the specified port setting to take effect, you must execute the **ovsdb server enable** command to enable the OVSDB server. You must disable and then re-enable the OVSDB server if it has been enabled.

Examples

Enable the device to listen for OVSDB TCP connection requests on port 6640.

```
<Sysname> system-view
[Sysname] ovsdb server ptcp
```

Related commands

ovsdb server enable

ovsdb server tcp

ovsdb server ssl

Use **ovsdb server ssl** to set up an active OVSDB SSL connection to a controller.

Use **undo ovsdb server ssl** to remove an OVSDB SSL connection from a controller.

Syntax

ovsdb server ssl ip *ip-address* **port** *port-number*

undo ovsdb server ssl ip *ip-address* **port** *port-number*

Default

The device does not have active OVSDB SSL connections to a controller.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ip *ip-address*: Specifies the destination IP address for the SSL connection.

port *port-number*: Specifies the destination port for the SSL connection. The value range for the *port-number* argument is 1 to 65535.

Usage guidelines

Before you use this command, you must specify a PKI domain for SSL.

The device can have a maximum of eight active SSL connections.

To establish the connection, you must execute the **ovsdb server enable** command. You must disable and then re-enable the OVSDB server if it has been enabled.

Examples

Set up an active SSL connection to port 6632 at 192.168.12.2.

```
<Sysname> system-view
[Sysname] ovsdb server ssl ip 192.168.12.2 port 6632
```

Related commands

ovsdb server bootstrap ca-certificate

ovsdb server enable

ovsdb server pki domain

ovsdb server pssl

ovsdb server tcp

Use **ovsdb server tcp** to set up an active OVSDB TCP connection to a controller.

Use **undo ovsdb server tcp** to remove an OVSDB TCP connection.

Syntax

ovsdb server tcp ip *ip-address* **port** *port-number*

undo ovsdb server tcp ip *ip-address* **port** *port-number*

Default

The device does not have active OVSDB TCP connections.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

ip *ip-address*: Specifies the destination IP address for the TCP connection.

port *port-number*: Specifies the destination port for the TCP connection. The value range for the *port-number* argument is 1 to 65535.

Usage guidelines

The device can have a maximum of eight active OVSDB TCP connections.

To establish the connection, you must execute the **ovsdb server enable** command. You must disable and then re-enable the OVSDB server if it has been enabled.

Examples

Set up an active OVSDB TCP connection to port 6632 at 192.168.12.2.

```
<Sysname> system-view
[Sysname] ovsdb server tcp ip 192.168.12.2 port 6632
```

Related commands

ovsdb server enable

ovsdb server ptcp

vtep access port

Use **vtep access port** to specify a site-facing interface as a VTEP access port.

Use **undo vtep access port** to restore the default.

Syntax

vtep access port

undo vtep access port

Default

An interface is not a VTEP access port.

Views

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

Layer 3 interface view

Predefined user roles

network-admin

context-admin

Usage guidelines

For controllers to manage a site-facing interface, you must specify the interface as a VTEP access port.

Examples

Specify GigabitEthernet 1/0/1 as a VTEP access port.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] vtep access port
```

vtep enable

Use **vtep enable** to enable the OVSDB VTEP service.

Use **undo vtep enable** to disable the OVSDB VTEP service.

Syntax

vtep enable

undo vtep enable

Default

The OVSDB VTEP service is disabled.

Views

System view

Predefined user roles

network-admin

context-admin

Examples

Enable the OVSDB VTEP service.

```
<Sysname> system-view
[Sysname] vtep enable
```

vxlan tunnel flooding-proxy

Use **vxlan tunnel flooding-proxy** to enable flood proxy on multicast VXLAN tunnels.

Use **undo vxlan tunnel flooding-proxy** to disable flood proxy on multicast VXLAN tunnels.

Syntax

vxlan tunnel flooding-proxy

undo vxlan tunnel flooding-proxy

Default

Flood proxy is disabled on multicast VXLAN tunnels.

Views

System view

Predefined user roles

network-admin

context-admin

Usage guidelines

If you use a flood proxy server, you must enable flood proxy globally on multicast tunnels. Then the multicast tunnels are converted into flood proxy tunnels. The VTEP sends broadcast, multicast, and unknown unicast traffic for a VXLAN to the flood proxy server through the tunnels. The flood proxy server then replicates and forwards flood traffic to remote VTEPs.

The **vxlan tunnel flooding-proxy** command and its **undo** form affect only VXLAN tunnels that are issued after the **vxlan tunnel flooding-proxy** command.

Examples

Enable flood proxy on all multicast VXLAN tunnels.

```
<Sysname> system
[Sysname] vxlan tunnel flooding-proxy
```

NSFOCUS Firewall Series

NF Service Chain Instance

Command Reference

NSFOCUS Technologies, Inc.

Document version: 6W600-20230221

Preface

This command reference describes the commands for configuring Service Chain instance features.

This preface includes the following topics about the documentation:

- Audience.
- Conventions.

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators.

Conventions

The following information describes the conventions used in the documentation.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select a minimum of one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
CAUTION:	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Contents

Service chain commands

display service-chain path

Use **display service-chain path** to display service chain information.

Syntax

display service-chain path { *path-id* | **all** }

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Parameters

path-id: Specifies a service chain by its path ID in the range of 1 to 8388606.

all: Displays information for all service chains.

Examples

Display information for all service chains.

```
<Sysname> display service-chain path all
PathID: 22
  Next service node: 4.4.4.4
  Previous service node: 5.5.5.5
  Function: 1
    Service-list: fw
```

Table 1 Command output

Field	Description
PathID	Path ID of the service chain.
Next service node	IP address of the next service node.
Previous service node	IP address of the previous service node.
Function	ID of the service node.
Service-list	Services in the service list.

display service-chain statistics

Use **display service-chain statistics** to display service chain statistics.

Syntax

display service-chain statistics

Views

Any view

Predefined user roles

network-admin

network-operator

context-admin

context-operator

Examples

Display all service chain statistics.

```
<Sysname> display service-chain statistics
 Service-chain statistics
 Board : all
  Total receive : 0          Total send : 0
  Service drop  : 0          Error drop : 0
```

Table 2 Command output

Field	Description
Board	ID of a card. This field displays **all** in the current software version.
Total receive	Number of received packets.
Total send	Number of sent packets.
Service drop	Number of dropped packets.
Error drop	Number of dropped error packets.

next-service-node

Use **next-service-node** to specify the IP address of the next service node in an inter-device service chain.

Use **undo next-service-node** to restore the default.

Syntax

next-service-node *ip-address*

undo next-service-node

Default

The IP address of the next service node in an inter-device service chain is not specified.

Views

Service chain view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the IP address of the next service node.

Usage guidelines

If the service node is the end node, you do not need to specify the IP address of the next service node.

Examples

Specify the IP address of the next service node as 2.2.2.2 for service chain 1.

```
<Sysname> system-view
[Sysname] service-chain path 1
[Sysname-spath1] next-service-node 2.2.2.2
```

Related commands

display service-chain path

previous-service-node

Use **previous-service-node** to specify the IP address of the previous service node in an inter-device service chain.

Use **undo previous-service-node** to restore the default.

Syntax

previous-service-node *ip-address*

undo previous-service-node

Default

The IP address of the previous service node in an inter-device service chain is not specified.

Views

Service chain view

Predefined user roles

network-admin

context-admin

Parameters

ip-address: Specifies the IP address of the previous service node.

Usage guidelines

If the service node is the head node, you do not need to specify the IP address of the previous service node.

Examples

Specify the IP address of the previous service node as 3.3.3.3 for service chain 1.

```
<Sysname> system-view
[Sysname] service-chain path 1
[Sysname-spath1] previous-service-node 3.3.3.3
```

Related commands

display service-chain path

service-chain path

Use **service-chain path** to create a service chain and enter its view, or enter the view of an existing service chain.

Use **undo service-chain path** to delete a service chain or all service chains on a device.

Syntax

service-chain path *path-id*

undo service-chain path { *path-id* | **all** }

Default

No service chains exist.

Views

System view

Predefined user roles

network-admin

context-admin

Parameters

path-id: Specifies the path ID of a service chain, in the range of 1 to 8388606. A path ID uniquely identifies a service chain.

all: Deletes all service chains on the device.

Examples

Create service chain 1 and enter its view.

```
<Sysname> system-view
[Sysname] service-chain path 1
[Sysname-spath1]
```

Related commands

display service-chain path

service function

Use **service function** to create a service node and enter its view, or enter the view of an existing service node.

Use **undo service function** to delete a service node or all service nodes on the service chain.

Syntax

service function *function-number*

undo service function { *function-number* | **all** }

Default

No service nodes exist.

Views

Service chain view

Predefined user roles

network-admin

context-admin

Parameters

function-number: Assigns an ID to the service node. The value for the *function-number* argument is fixed at 1.

all: Deletes all service nodes on the service chain.

Usage guidelines

You can configure only one service node for a service chain.

Examples

Create service node 1 and enter its view.

```
<Sysname> system-view
[Sysname] service-chain path 1
[Sysname-spath1] service function 1
[Sysname-spath1-func1]
```

Related commands

display service-chain path

service list

Use **service list** to create a service list.

Use **undo service list** to restore the default.

Syntax

service list { **acg** | **atk** | **connect-limit** | **dpi** | **fw** | **ips** | **ipsec** | **lb** | **nat** }*

undo service list

Default

No service list exists.

Views

Service node view

Predefined user roles

network-admin

context-admin

Parameters

acg: Specifies the application control gateway (ACG) service.

atk: Specifies the attack detection and prevention service.

connect-limit: Specifies the connection limit service.

dpi: Specifies the deep packet inspection (DPI) service.

fw: Specifies the firewall (FW) service.

ips: Specifies the intelligent protection switching (IPS) service.

ipsec: Specifies the IP security (IPsec) service.

lb: Specifies the load balancing (LB) service.

nat: Specifies the network address translation (NAT) service.

Usage guidelines

You can configure only one service list for each service node. All services in a service chain must be different from each other.

The services in a service list are applied to the traffic in the order they are specified in a service list.

Examples

Create a service list that contains the FW and LB services for service node 1.

```
<Sysname> system-view
[Sysname] service-chain path 1
[Sysname-spath1] service function 1
[Sysname-spath1-func1] service list fw lb
```

Related commands

display service-chain path